

ETSI TS 131 127 V18.5.0 (2026-07)



**5G;  
UICC-terminal interaction;  
non-removable Universal Subscriber Identity Module (nrUSIM)  
application behavioural test specification  
(3GPP TS 31.127 version 18.5.0 Release 18)**



---

**Reference**

RTS/TSGC-0631127vi50

---

**Keywords**

5G

**ETSI**

---

650 Route des Lucioles  
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B  
Association à but non lucratif enregistrée à la  
Sous-Préfecture de Grasse (06) N° w061004871

---

**Important notice**

The present document can be downloaded from the  
[ETSI Search & Browse Standards](#) application.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on [ETSI deliver](#) repository.

Users should be aware that the present document may be revised or have its status changed,  
this information is available in the [Milestones listing](#).

If you find errors in the present document, please send your comments to  
the relevant service listed under [Committee Support Staff](#).

If you find a security vulnerability in the present document, please report it through our  
[Coordinated Vulnerability Disclosure \(CVD\)](#) program.

---

**Notice of disclaimer & limitation of liability**

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

---

**Copyright Notification**

No part of this document may be reproduced in any form, by any means and in any media, without the prior written authorization of ETSI and except as expressly permitted below.

By way of exception and when the document is a normative deliverable (European Standard (EN), Technical Specification (TS), Group Specification (GS) or ETSI Standard (ES)), ETSI authorizes to reproduce and incorporate into products, services and technical documentation only those extracts (e.g. templates) that are strictly necessary for the technical implementation of the normative deliverable, to ensure compliance with the latter. Nothing in this notice shall be construed as limiting any mandatory exceptions to copyright provided by applicable law.

© ETSI 2026.  
All rights reserved.

---

# Intellectual Property Rights

## Essential patents

IPRs essential or potentially essential to normative deliverables (European Standard (EN), Technical Specification (TS), Group Specification (GS) or ETSI Standard (ES)) may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: "*Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards*", which is available from the ETSI Secretariat. Latest updates are available on the [ETSI IPR online database](#).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

## Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

**DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

---

# Legal Notice

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities. These shall be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between 3GPP and ETSI identities can be found at [3GPP to ETSI numbering cross-referencing](#).

---

# Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

# Contents

Intellectual Property Rights .....	2
Legal Notice .....	2
Modal verbs terminology.....	2
Foreword.....	24
Introduction .....	25
1 Scope .....	26
2 References .....	26
3 Definitions of terms, symbols and abbreviations .....	29
3.1 Terms.....	29
3.2 Symbols.....	29
3.3 Abbreviations .....	29
3.4 Coding Conventions.....	29
3.5 Generic procedures for 5G-NR, E-UTRAN, IMS and NB-IoT.....	29
3.6 Table of optional features.....	30
3.7 Applicability.....	31
3.7.1 Applicability to user equipment.....	31
3.7.2 Supported additional explicit verification methods .....	32
3.7.3 Applicability of the individual tests .....	32
3.8 Applicability table .....	33
3.9 Rules for the representation of number systems and strings .....	39
4 Test environment.....	40
4.1.1 General test environment .....	40
4.1.2 Example - test environment for implicit testing.....	41
4.1.3 Example - test environment for contents verification .....	41
4.1.4 Example - test environment for seamless testing.....	42
4.1.5 Example – test environment for test toolkit events based testing .....	42
4.1.6 Example – test environment for UEs with ETSI eSSP/iSSP .....	43
4.2 Requirements to the EUT and the test environment.....	44
4.2.1 General Requirements.....	44
4.2.2 Requirements to the UE (EUT) – supported interfaces.....	44
4.2.3 Supported RATs .....	44
4.2.4 Initial and final procedure steps.....	45
4.3 Random value generation.....	45
4.4 Suitability assessment.....	45
4.4.1 Suitability assessment in present test procedures.....	45
4.4.2 Suitability assessment in test descriptions .....	46
4.4.3 Suitability assessment in the test protocol .....	46
4.4.4 Justification of additional measures .....	46
4.5 Definition of default values .....	46
4.5.1 Introduction.....	46
4.5.1.1 Installation, provisioning or modification methods for EFs and DFs .....	46
4.5.1.2 TS.48 Version and usage.....	46
4.5.2 Definition of the Default UICC .....	46
4.5.3 Definition of FDN UICC .....	47
4.5.4 Definition of E-UTRAN/EPC UICC .....	48
4.5.5 Definition of E-UTRAN/EPC ISIM-UICC.....	49
4.5.6 Definition of ACSGL/OCSGL E-UTRAN/EPC UICC .....	49
4.5.7 Definition of Non-Access Stratum Configuration UICC.....	54
4.5.8 Definition of Non-Access Stratum Configuration of E-UTRAN/EPC UICC.....	54
4.5.9 Definition of 5G-NR UICC .....	54
4.5.10 Definition of 5G-NR UICC – non-IMSI SUPI Type .....	57
4.5.11 Definition of 5G-NR UICC – support of Rel-16 features.....	59
4.5.12 Definition of 5G-NR UICC – support of Rel-17 features .....	61

4.5.13	Definition 5G-NR UICC – CAG support .....	62
4.5.14	Definition of 5G-NR ISIM-UICC.....	62
4.5.15	Definition of 5G-NR UICC – support of Rel-18 features .....	62
4.5.16	Definition of 5G-NR SSIM-UICC.....	63
4.6	Definition of default values for EFs commonly used with random value generation .....	63
4.6.1	EF <sub>IMSI</sub> with 3-digit MNC and random value .....	63
4.6.2	EF <sub>IMSI</sub> "short", with 3-digit MNC and random value.....	64
4.6.3	EF <sub>IMSI</sub> "short", with 2-digit MNC and random value.....	64
4.6.4	EF <sub>IMSI</sub> "long", with 3-digit MNC and random value.....	64
4.6.5	EF <sub>IMSI</sub> for SUCI calculation tests .....	64
4.6.6	EF <sub>IMSI</sub> for "change IMSI" tests.....	65
4.6.7	EF <sub>Routing_Indicator</sub> with 2-digit MNC and random value.....	65
4.6.8	EF <sub>LOCI</sub> with "short" random TMSI value .....	65
4.6.9	EF <sub>LOCI</sub> with "long" random TMSI value .....	66
4.6.10	EF <sub>EPSLOCI</sub> .....	66
4.6.11	EF <sub>FDN</sub> .....	66
4.6.12	EF <sub>ECC</sub> .....	67
4.7	Default values for NG-SS and UE configurations.....	68
4.7.1	Default NG-SS and UE configuration for different usage settings .....	68
4.7.2	Default NG-SS configuration for 3GPP access with IMS service .....	68
4.7.2.1	Default NG-SS configuration for IMS Registration support.....	68
4.7.2.2	Default NG-SS configuration for PS voice support .....	68
4.7.3	Default NG-SS procedure for 5G Registration on 3GPP access with IMS service .....	68
4.7.4	Default UE configuration for IMS service.....	69
5	Subscription related tests.....	69
5.1	IMSI/TMSI handling.....	69
5.1.1	UE identification by short IMSI .....	69
5.1.2	UE identification by short IMSI using a 2-digit MNC .....	69
5.1.3	UE identification by "short" TMSI.....	69
5.1.4	UE identification by "long" TMSI.....	69
5.1.5	UE identification by long IMSI, TMSI updating and key set identifier assignment.....	69
5.1.6	UE identification by short IMSI when accessing E-UTRAN/EPC.....	69
5.1.6.1	Definition and applicability.....	69
5.1.6.2	Conformance requirement.....	69
5.1.6.3	Test purpose .....	70
5.1.6.4	Method of test .....	70
5.1.6.4.1	Initial conditions .....	70
5.1.6.4.2	Procedure.....	70
5.1.6.4.2.1	Test procedure A.....	70
5.1.6.4.2.2	Test procedure B.....	71
5.1.6.5	Acceptance criteria.....	71
5.1.6.5.1	Acceptance criteria for Test Procedure A.....	71
5.1.6.5.2	Acceptance criteria for Test Procedure B.....	71
5.1.6.4.3	Common acceptance criteria .....	71
5.1.7	UE identification by short IMSI using a 2-digit MNC when accessing E-UTRAN/EPC.....	71
5.1.7.1	Definition and applicability.....	71
5.1.7.2	Conformance requirement.....	71
5.1.7.3	Test purpose .....	72
5.1.7.4	Method of test .....	72
5.1.7.4.1	Initial conditions .....	72
5.1.7.4.2	Procedure.....	72
5.1.7.4.2.1	Test procedure A.....	72
5.1.7.4.2.2	Test procedure B.....	73
5.1.7.4	Acceptance criteria.....	73
5.1.8	UE identification after changed IMSI with service "EMM Information" not available .....	73
5.1.8.1	Definition and applicability.....	73
5.1.8.2	Conformance requirement.....	73
5.1.8.3	Test purpose .....	74
5.1.8.4	Method of test .....	74
5.1.8.4.1	Initial conditions .....	74
5.1.8.4.2	Procedure.....	74

5.1.8.4.2.1	Test procedure A.....	74
5.1.8.4.2.2	Test procedure B.....	75
5.1.8.5	Acceptance criteria.....	75
5.1.9	UE identification by GUTI when using USIM with service "EMM Information" not available.....	76
5.1.10	UE identification by GUTI when using USIM with service "EMM Information" available.....	78
5.1.10.2	Conformance requirement.....	78
5.1.10.3	Test purpose.....	78
5.1.10.4	Method of test.....	78
5.1.10.4.1	Initial conditions.....	78
5.1.10.4.2	Procedure.....	79
5.1.10.4.2.1	Test procedure A.....	79
5.1.10.4.2.2	Test procedure B.....	79
5.1.10.4.2.3	Common final Test Procedure.....	79
5.1.10.5	Acceptance criteria.....	80
5.2	Access Control handling.....	80
5.2.1	Access Control information handling.....	80
5.2.2	Access Control information handling for E-UTRAN/EPC.....	80
5.2.2.1	Definition and applicability.....	80
5.2.2.2	Conformance requirement.....	80
5.2.2.3	Test purpose.....	81
5.2.2.4	Method of test.....	81
5.2.2.4.1	Initial conditions.....	81
5.2.2.4.2	Coding details.....	81
5.2.2.4.3	Procedure.....	82
5.2.2.5	Acceptance criteria.....	82
5.2.3	Access Control information handling for NB-IoT.....	82
5.2.3.1	Definition and applicability.....	82
5.2.3.2	Conformance requirement.....	82
5.2.3.3	Test purpose.....	82
5.2.3.4	Method of test.....	83
5.2.3.4.1	Initial conditions.....	83
5.2.3.4.2	Coding details.....	83
5.2.3.4.3	Procedure.....	83
5.2.3.5	Acceptance criteria.....	83
5.3	Handling subscription identifier privacy for 5G.....	83
5.3.1	SUCI calculation by ME using null scheme.....	83
5.3.1.1	Definition and applicability.....	83
5.3.1.2	Conformance requirement.....	84
5.3.1.3	Test purpose.....	84
5.3.1.4	Method of test.....	84
5.3.1.4.1	Initial conditions.....	84
5.3.1.4.2	Procedure.....	86
5.3.1.5	Acceptance criteria.....	86
5.3.2	SUCI calculation by ME using Profile B.....	86
5.3.2.1	Definition and applicability.....	86
5.3.2.2	Conformance requirement.....	86
5.3.2.3	Test purpose.....	87
5.3.2.4	Method of test.....	87
5.3.2.4.1	Initial conditions.....	87
5.3.2.4.2	Procedure.....	88
5.3.2.5	Acceptance criteria.....	88
5.3.3	UE identification by SUCI during initial registration – SUCI calculation by USIM using profile B.....	88
5.3.3.1	Definition and applicability.....	88
5.3.3.2	Conformance requirement.....	88
5.3.3.3	Test purpose.....	89
5.3.3.4	Method of test.....	89
5.3.3.4.1	Initial conditions.....	89
5.3.3.4.2	Procedure.....	90
5.3.3.5	Acceptance criteria.....	91
5.3.4	UE identification by SUCI in response to IDENTITY REQUEST message.....	91
5.3.4.1	Definition and applicability.....	91
5.3.4.2	Conformance requirement.....	91

5.3.4.3	Test purpose .....	92
5.3.4.4	Method of test .....	92
5.3.4.4.1	Initial conditions .....	92
5.3.4.4.2	Procedure.....	93
5.3.4.5	Acceptance criteria.....	93
5.3.5	UE identification by SUCI in response to IDENTITY REQUEST message with T3519 timer expiry .....	94
5.3.5.1	Definition and applicability.....	94
5.3.5.2	Conformance requirement.....	94
5.3.5.3	Test purpose .....	95
5.3.5.4	Method of test .....	95
5.3.5.4.1	Initial conditions .....	95
5.3.5.4.2	Procedure.....	96
5.3.5.5	Acceptance criteria.....	96
5.3.6	UE identification by SUCI in response to IDENTITY REQUEST message and AUTHENTICATION REJECT .....	97
5.3.6.1	Definition and applicability.....	97
5.3.6.2	Conformance requirement.....	97
5.3.6.3	Test purpose .....	98
5.3.6.4	Method of test .....	98
5.3.6.4.1	Initial conditions .....	98
5.3.6.4.2	Procedure.....	99
5.3.6.5	Acceptance criteria.....	99
5.3.7	SUCI calculation by the ME using null scheme – missing parameters for subscription identifier privacy support by the USIM.....	99
5.3.7.1	Definition and applicability.....	99
5.3.7.2	Conformance requirement.....	100
5.3.7.3	Test purpose .....	100
5.3.7.4	Method of test .....	100
5.3.7.4.1	Initial conditions .....	100
5.3.7.4.2	Procedure.....	101
5.3.7.5	Acceptance criteria.....	101
5.3.8	UE identification by 5G-GUTI – Last Registered TAI stored on USIM .....	101
5.3.8.1	Definition and applicability.....	101
5.3.8.2	Conformance requirement.....	101
5.3.8.3	Test purpose .....	102
5.3.8.4	Method of test .....	102
5.3.8.4.1	Initial conditions .....	102
5.3.8.4.2	Procedure.....	102
5.3.8.5	Acceptance criteria.....	103
5.3.9	UE identification by 5G-GUTI – Last Registered TAI stored by ME .....	103
5.3.9.1	Definition and applicability.....	103
5.3.9.2	Conformance requirement.....	103
5.3.9.3	Test purpose .....	103
5.3.9.4	Method of test .....	104
5.3.9.4.1	Initial conditions .....	104
5.3.9.4.2	Procedure.....	104
5.3.9.5	Acceptance criteria.....	105
5.3.10	UE identification after SUPI is changed .....	105
5.3.10.1	Definition and applicability.....	105
5.3.10.2	Conformance requirement.....	105
5.3.10.3	Test purpose .....	106
5.3.10.4	Method of test .....	106
5.3.10.4.1	Initial conditions .....	106
5.3.10.4.2	Procedure.....	106
5.3.10.5	Acceptance criteria.....	106
5.3.11	SUCI calculation by ME using Profile A.....	107
5.3.11.1	Definition and applicability.....	107
5.3.11.2	Conformance requirement.....	107
5.3.11.3	Test purpose .....	107
5.3.11.4	Method of test .....	107
5.3.11.4.1	Initial conditions .....	107
5.3.11.4.2	Procedure.....	108

5.3.11.5	Acceptance criteria.....	108
5.3.12	UE identification by SUCI during initial registration – SUCI calculation by USIM using profile A.....	109
5.3.12.1	Definition and applicability.....	109
5.3.12.2	Conformance requirement.....	109
5.3.12.3	Test purpose .....	109
5.3.12.4	Method of test .....	109
5.3.12.4.1	Initial conditions.....	109
5.3.12.4.2	Procedure.....	110
5.3.12.5	Acceptance criteria.....	111
5.3.13	SUCI calculation by ME using null scheme– no Protection Scheme Identifier provisioned in the USIM .....	111
5.3.13.1	Definition and applicability.....	111
5.3.13.2	Conformance requirement.....	111
5.3.13.3	Test purpose .....	111
5.3.13.4	Method of test .....	112
5.3.13.4.1	Initial conditions.....	112
5.3.13.4.2	Procedure.....	112
5.3.13.5	Acceptance criteria.....	112
5.3.14	SUCI calculation by ME using null scheme – no Home Network Public Key for supported protection scheme provisioned in the USIM.....	113
5.3.14.1	Definition and applicability.....	113
5.3.14.2	Conformance requirement.....	113
5.3.14.3	Test purpose .....	113
5.3.14.4	Method of test .....	113
5.3.14.4.1	Initial conditions.....	113
5.3.14.4.2	Procedure.....	114
5.3.14.5	Acceptance criteria.....	114
5.3.15	SUCI calculation by ME using null scheme with the E-UTRAN/EPC UICC.....	114
5.3.15.1	Definition and applicability.....	114
5.3.15.2	Conformance requirement.....	114
5.3.15.3	Test purpose .....	115
5.3.15.4	Method of test .....	115
5.3.15.4.1	Initial conditions.....	115
5.3.15.4.2	Procedure.....	115
5.3.15.5	Acceptance criteria.....	115
5.3.16	SUCI calculation by ME using the lower priority protection scheme when the higher priority protection scheme is not supported by the ME .....	116
5.3.16.1	Definition and applicability.....	116
5.3.16.2	Conformance requirement.....	116
5.3.16.3	Test purpose .....	116
5.3.16.4	Method of test .....	117
5.3.16.4.1	Initial conditions.....	117
5.3.16.4.2	Procedure.....	118
5.3.16.5	Acceptance criteria.....	118
5.3.17	SUCI calculation by ME using Profile B with compressed Home Network Public Key.....	119
5.3.17.1	Definition and applicability.....	119
5.3.17.2	Conformance requirement.....	119
5.3.17.3	Test purpose .....	119
5.3.17.4	Method of test .....	119
5.3.17.4.1	Initial conditions.....	119
5.3.17.4.2	Procedure.....	121
5.3.17.5	Acceptance criteria.....	121
5.4	Unified Access Control information handling for 5G-NR .....	121
5.4.1	Unified Access Control – Access identity 0, no access identities indicated by USIM .....	121
5.4.1.1	Definition and applicability.....	121
5.4.1.2	Conformance requirement.....	122
5.4.1.3	Test purpose .....	122
5.4.1.4	Method of test .....	122
5.4.1.4.1	Initial conditions.....	122
5.4.1.4.2	Test sequence settings .....	123
5.4.1.4.3	Procedure.....	123
5.4.1.5	Acceptance criteria.....	124

5.4.1A	Unified Access Control – Access identity 0, no access identities indicated by USIM, Access Category 8.....	124
5.4.1A.1	Definition and applicability.....	124
5.4.1A.2	Conformance requirement.....	124
5.4.1A.3	Test purpose .....	125
5.4.1A.4	Method of test .....	125
5.4.1A.4.1	Initial conditions.....	125
5.4.1A.4.2	Test sequence settings .....	126
5.4.1A.4.3	Procedure.....	126
5.4.1A.5	Acceptance criteria.....	127
5.4.2	Unified Access Control – Access Identity 1 – MPS indicated by USIM.....	127
5.4.2.1	Definition and applicability.....	127
5.4.2.2	Conformance requirement.....	127
5.4.2.3	Test purpose .....	128
5.4.2.4	Method of test .....	128
5.4.2.4.1	Initial conditions.....	128
5.4.2.4.2	Test sequence settings .....	129
5.4.2.4.3	Procedure.....	129
5.4.2.5	Acceptance criteria.....	130
5.4.2A	Unified Access Control – Access Identity 1 – MPS indicated by USIM, Access Category 8 .....	130
5.4.2A.1	Definition and applicability.....	130
5.4.2A.2	Conformance requirement.....	130
5.4.2A.3	Test purpose .....	131
5.4.2A.4	Method of test .....	131
5.4.2A.4.1	Initial conditions.....	131
5.4.2A.4.2	Test sequence settings .....	132
5.4.2A.4.3	Procedure.....	132
5.4.2A.5	Acceptance criteria.....	133
5.4.3	Unified Access Control – Access Identity 1 – no MPS indication by USIM and SUPI not changed.....	133
5.4.3.1	Definition and applicability.....	133
5.4.3.2	Conformance requirement.....	134
5.4.3.3	Test purpose .....	134
5.4.3.4	Method of test .....	135
5.4.3.4.1	Initial conditions.....	135
5.4.3.4.2	Test sequence settings .....	136
5.4.3.4.3	Procedure.....	136
5.4.3.5	Acceptance criteria.....	137
5.4.4	Unified Access Control – Access Identity 1 – no MPS indication by USIM and SUPI is changed .....	137
5.4.4.1	Definition and applicability.....	137
5.4.4.2	Conformance requirement.....	138
5.4.4.3	Test purpose .....	138
5.4.4.4	Method of test .....	139
5.4.4.4.1	Initial conditions.....	139
5.4.4.4.2	Test sequence settings .....	139
5.4.4.4.3	Procedure.....	140
5.4.4.5	Acceptance criteria.....	141
5.4.5	Unified Access Control – Access Identity 2 – MCS indicated by USIM .....	141
5.4.5.1	Definition and applicability.....	141
5.4.5.2	Conformance requirement.....	141
5.4.5.3	Test purpose .....	142
5.4.5.4	Method of test .....	142
5.4.5.4.1	Initial conditions.....	142
5.4.5.4.2	Test sequence settings .....	143
5.4.5.4.3	Procedure.....	143
5.4.5.5	Acceptance criteria.....	144
5.4.5A	Unified Access Control – Access Identity 2 – MCS indicated by USIM .....	144
5.4.5A.1	Definition and applicability.....	144
5.4.5A.2	Conformance requirement.....	145
5.4.5A.3	Test purpose .....	145
5.4.5A.4	Method of test .....	146
5.4.5A.4.1	Initial conditions.....	146
5.4.5A.4.2	Test sequence settings .....	146

5.4.5A.4.2	Procedure.....	147
5.4.5A.5	Acceptance criteria.....	147
5.4.6	Unified Access Control – Access Identity 2 – no MCS indication by USIM and SUPI is not changed ...	148
5.4.6.1	Definition and applicability.....	148
5.4.6.2	Conformance requirement.....	148
5.4.6.3	Test purpose .....	149
5.4.6.4	Method of test .....	149
5.4.6.4.1	Initial conditions.....	149
5.4.6.4.2	Test sequence settings .....	150
5.4.6.4.3	Procedure.....	150
5.4.6.4.3	Acceptance criteria.....	151
5.4.7	Unified Access Control – Access Identity 2 – no MCS indication by USIM and SUPI is changed.....	152
5.4.7.1	Definition and applicability.....	152
5.4.7.2	Conformance requirement.....	152
5.4.7.3	Test purpose .....	153
5.4.7.4	Method of test .....	153
5.4.7.4.1	Initial conditions.....	153
5.4.7.4.2	Test sequence settings .....	154
5.4.7.4.3	Procedure.....	154
5.4.7.5	Acceptance criteria.....	155
5.4.8	Unified Access Control – Access Identities 11 and 15 indicated by USIM.....	155
5.4.8.1	Definition and applicability.....	155
5.4.8.2	Conformance requirement.....	156
5.4.8.3	Test purpose .....	156
5.4.8.4	Method of test .....	156
5.4.8.4.1	Initial conditions.....	156
5.4.8.4.2	Test sequence settings .....	157
5.4.8.4.3	Procedure.....	158
5.4.8.5	Acceptance criteria.....	158
5.4.8A	Unified Access Control – Access Identities 11 and 15 indicated by USIM, Access Category 8.....	159
5.4.8A.1	Definition and applicability.....	159
5.4.8A.2	Conformance requirement.....	159
5.4.8A.3	Test purpose .....	160
5.4.8A.4	Method of test .....	160
5.4.8A.4.1	Initial conditions.....	160
5.4.8A.4.2	Test sequence settings .....	161
5.4.8A.4.3	Procedure.....	161
5.4.8A.5	Acceptance criteria.....	162
5.4.9	Unified Access Control – Access Identities 12, 13 and 14 indicated by USIM.....	162
5.4.9.1	Definition and applicability.....	162
5.4.9.2	Conformance requirement.....	162
5.4.9.3	Test purpose .....	163
5.4.9.4	Method of test .....	163
5.4.9.4.1	Initial conditions.....	163
5.4.9.4.2	Tables related to the test case .....	164
5.4.9.4.3	Procedure.....	165
5.4.9.5	Acceptance criteria.....	165
5.4.9A	Unified Access Control – Access Identities 12, 13 and 14 indicated by USIM, Access Category 8.....	166
5.4.9A.1	Definition and applicability.....	166
5.4.9A.2	Conformance requirement.....	166
5.4.9A.3	Test purpose .....	167
5.4.9A.4	Method of test .....	167
5.4.9A.4.1	Initial conditions.....	167
5.4.9A.4.2	Tables related to the test case .....	168
5.4.9A.4.3	Procedure.....	168
5.4.9A.5	Acceptance criteria.....	169
5.4.10	Unified Access Control – Operator-Defined Access Category.....	169
5.4.10.1	Definition and applicability.....	169
5.4.10.2	Conformance requirement.....	169
5.4.10.3	Test purpose .....	171
5.4.10.4	Method of test .....	171
5.4.10.4.1	Initial conditions.....	171

5.4.10.4.2	Tables related to the test case .....	172
5.4.10.4.3	Procedure.....	173
5.4.10.5	Acceptance criteria.....	174
5.4.11	Unified Access Control – Operator-Defined Access Categories, no change in SUPI .....	174
5.4.11.1	Definition and applicability.....	174
5.4.11.2	Conformance requirement.....	175
5.4.11.3	Test purpose .....	176
5.4.11.4	Method of test .....	176
5.4.11.4.1	Initial conditions.....	176
5.4.11.4.2	Tables related to the test case .....	178
5.4.11.4.3	Procedure.....	178
5.4.11.5	Acceptance criteria.....	179
5.4.12	Unified Access Control – Operator-Defined Access Categories, SUPI change .....	179
5.4.12.1	Definition and applicability.....	179
5.4.12.2	Conformance requirement.....	180
5.4.12.3	Test purpose .....	181
5.4.12.4	Method of test .....	182
5.4.12.4.1	Initial conditions.....	182
5.4.12.4.2	Tables related to the test case .....	183
5.4.12.4.3	Procedure.....	184
5.4.12.5	Acceptance criteria.....	185
5.5	Handling of operator controlled features.....	185
5.5.1	Display of registered 5G PLMN name from USIM.....	185
5.5.1.1	Definition and applicability.....	185
5.5.1.2	Conformance requirement.....	185
5.5.1.3	Test purpose .....	185
5.5.1.4	Method of tests.....	185
5.5.1.4.1	Initial conditions.....	185
5.5.1.4.2	Procedure.....	188
5.5.1.4.3	Acceptance criteria .....	188
5.5.2	Display of registered 5G PLMN name from ME.....	189
5.5.2.1	Definition and applicability.....	189
5.5.2.2	Conformance requirement.....	189
5.5.2.3	Test purpose .....	189
5.5.2.4	Method of tests.....	189
5.5.2.4.1	Initial conditions.....	189
5.5.2.4.2	Procedure.....	191
5.5.1.4.3	Acceptance criteria .....	192
5.6.1.1	Definition and applicability.....	192
5.6.1.2	Conformance requirement.....	192
5.6.1.3	Test purpose .....	193
5.6.1.4	Method of test .....	193
5.6.1.4.1	Initial conditions.....	193
5.6.1.4.2	Procedure.....	194
5.6.1.5	Acceptance criteria.....	195
5.6.2.1	Definition and applicability.....	195
5.6.2.2	Conformance requirement.....	195
5.6.2.3	Test purpose .....	196
5.6.2.4	Method of test .....	196
5.6.2.4.1	Initial conditions.....	196
5.6.2.4.2	Procedure.....	198
5.6.2.5	Acceptance criteria.....	198
5.6.3.1	Definition and applicability.....	198
5.6.3.2	Conformance requirement.....	199
5.6.3.3	Test purpose .....	199
5.6.3.4	Method of test .....	200
5.6.3.4.1	Initial conditions.....	200
5.6.3.4.2	Procedure.....	201
5.6.3.5	Acceptance criteria.....	201
5.6.4	UE identification after SUPI is changed .....	202
5.6.4.1	Definition and applicability.....	202
5.6.4.2	Conformance requirement.....	202

5.6.4.3	Test purpose .....	202
5.6.4.4	Method of test .....	203
5.6.4.4.1	Initial conditions .....	203
5.6.4.4.2	Procedure.....	203
5.6.4.5	Acceptance criteria.....	204
5.6.5	UE identification by SUCI during initial registration – SUCI calculation by ME using profile A.....	204
5.6.5.1	Definition and applicability.....	204
5.6.5.2	Conformance requirement.....	204
5.6.5.3	Test purpose .....	205
5.6.5.4	Method of test .....	205
5.6.5.4.1	Initial conditions .....	205
5.6.5.4.2	Procedure.....	206
5.6.5.5	Acceptance criteria.....	207
5.6.6	UE identification by SUCI during initial registration – SUCI calculation by ME using profile B .....	207
5.6.6.1	Definition and applicability.....	207
5.6.6.2	Conformance requirement.....	207
5.6.6.3	Test purpose .....	208
5.6.6.4	Method of test .....	208
5.6.6.4.1	Initial conditions .....	208
5.6.6.4.2	Procedure.....	209
5.6.6.5	Acceptance criteria.....	209
6	Security related Tests .....	210
6.1	PIN handling .....	210
6.1.1	Entry of PIN.....	210
6.1.1.1	Definition and applicability.....	210
6.1.1.2	Conformance requirement.....	210
6.1.1.3	Test purpose .....	210
6.1.1.4	Method of test .....	210
6.1.1.4.1	Initial conditions .....	210
6.1.1.4.2	Procedure.....	210
6.1.1.5	Acceptance criteria.....	211
6.1.2	Change of PIN .....	211
6.1.2.1	Definition and applicability.....	211
6.1.2.2	Conformance requirement.....	211
6.1.2.3	Test purpose .....	211
6.1.2.4	Method of test .....	211
6.1.2.4.1	Initial conditions .....	211
6.1.2.4.2	Procedure.....	211
6.1.2.5	Acceptance criteria.....	212
6.1.3	Unblock PIN .....	212
6.1.3.1	Definition and applicability.....	212
6.1.3.2	Conformance requirement.....	212
6.1.3.3	Test purpose .....	213
6.1.3.4	Method of test .....	213
6.1.3.4.1	Initial conditions .....	213
6.1.3.4.2	Procedure.....	213
6.1.3.4.2	Procedure.....	213
6.1.3.5	Acceptance criteria.....	214
6.1.4	Entry of PIN2.....	215
6.1.4.1	Definition and applicability.....	215
6.1.4.2	Conformance requirement.....	215
6.1.4.3	Test purpose .....	215
6.1.4.4	Method of test .....	215
6.1.4.4.1	Initial conditions .....	215
6.1.4.4.2	Procedure.....	215
6.1.4.5	Acceptance criteria.....	216
6.1.5	Change of PIN2 .....	216
6.1.5.1	Definition and applicability.....	216
6.1.5.2	Conformance requirement.....	216
6.1.5.3	Test purpose .....	216
6.1.5.4	Method of test .....	216

6.1.5.4.1	Initial conditions .....	216
6.1.5.4.2	Procedure .....	216
6.1.5.5	Acceptance criteria .....	217
6.1.6	Unblock PIN2 .....	217
6.1.6.1	Definition and applicability .....	217
6.1.6.2	Conformance requirement .....	217
6.1.6.3	Test purpose .....	218
6.1.6.4	Method of test .....	218
6.1.6.4.1	Initial conditions .....	218
6.1.6.4.2	Procedure .....	218
6.1.6.5	Acceptance criteria .....	219
6.1.7	Replacement of PIN .....	220
6.1.7.1	Definition and applicability .....	220
6.1.7.2	Conformance requirement .....	220
6.1.7.3	Test purpose .....	220
6.1.7.4	Method of test .....	220
6.1.7.4.1	Initial conditions .....	220
6.1.7.4.2	Procedure .....	220
6.1.7.5	Acceptance criteria .....	221
6.1.8	Change of Universal PIN .....	221
6.1.8.1	Definition and applicability .....	221
6.1.8.2	Conformance requirement .....	222
6.1.8.3	Test purpose .....	222
6.1.8.4	Method of test .....	222
6.1.8.4.1	Initial conditions .....	222
6.1.8.4.2	Procedure .....	222
6.1.8.5	Acceptance criteria .....	223
6.1.9	Unblock Universal PIN .....	223
6.1.9.1	Definition and applicability .....	223
6.1.9.2	Conformance requirement .....	223
6.1.9.3	Test purpose .....	223
6.1.9.4	Method of test .....	223
6.1.9.4.1	Initial conditions .....	223
6.1.9.4.2	Procedure .....	223
6.1.9.5	Acceptance criteria .....	224
6.1.10	Entry of PIN on multi-verification capable UICCs .....	224
6.1.10.1	Definition and applicability .....	224
6.1.10.2	Conformance requirement .....	224
6.1.10.4	Method of test .....	225
6.1.10.4.1	Initial conditions .....	225
6.1.10.4.2	Procedure .....	226
6.1.10.5	Acceptance criteria .....	226
6.1.11	Change of PIN on multi-verification capable UICCs .....	226
6.1.11.1	Definition and applicability .....	226
6.1.11.2	Conformance requirement .....	226
6.1.11.3	Test purpose .....	226
6.1.11.4	Method of test .....	227
6.1.11.4.1	Initial conditions .....	227
6.1.11.4.2	Procedure .....	228
6.1.11.5	Acceptance criteria .....	228
6.1.12	Unblock PIN on multi-verification capable UICCs .....	228
6.1.12.1	Definition and applicability .....	228
6.1.12.2	Conformance requirement .....	228
6.1.12.3	Test purpose .....	229
6.1.12.4	Method of test .....	229
6.1.12.4.1	Initial conditions .....	229
6.1.12.4.2	Procedure .....	230
6.1.12.5	Acceptance criteria .....	231
6.1.13	Entry of PIN2 on multi-verification capable UICCs .....	231
6.1.13.1	Definition and applicability .....	231
6.1.13.2	Conformance requirement .....	231
6.1.13.3	Test purpose .....	231

6.1.13.4	Method of test .....	232
6.1.13.4.1	Initial conditions .....	232
6.1.13.4.2	Procedure.....	233
6.1.13.5	Acceptance criteria.....	233
6.1.14	Change of PIN2 on multi-verification capable UICCs .....	233
6.1.14.1	Definition and applicability.....	233
6.1.14.2	Conformance requirement.....	233
6.1.14.3	Test purpose .....	234
6.1.14.4	Method of test .....	234
6.1.14.4.1	Initial conditions .....	234
6.1.14.4.2	Procedure.....	235
6.1.14.5	Acceptance criteria.....	235
6.1.15	Unblock PIN2 on multi-verification capable UICCs .....	235
6.1.15.1	Definition and applicability.....	235
6.1.15.2	Conformance requirement.....	236
6.1.15.3	Test purpose .....	236
6.1.15.4	Method of test .....	236
6.1.15.4.1	Initial conditions .....	236
6.1.15.4.2	Procedure.....	237
6.1.15.5	Acceptance criteria.....	238
6.1.16	Replacement of PIN with key reference "07" .....	239
6.1.16.1	Definition and applicability.....	239
6.1.16.2	Conformance requirement.....	239
6.1.16.3	Test purpose .....	239
6.1.16.4	Method of test .....	239
6.1.16.4.1	Initial conditions .....	239
6.1.16.4.2	Procedure.....	240
6.1.16.5	Acceptance criteria.....	241
6.2	Fixed Dialling Numbers (FDN) handling.....	241
6.2.1	ME and USIM with FDN enabled, EF <sub>ADN</sub> readable and updateable.....	241
6.2.2	ME and USIM with FDN disabled .....	242
6.2.3	Enabling, disabling and updating of FDN .....	242
6.2.4	ME and USIM with FDN enabled, EF <sub>ADN</sub> readable and updateable (Rel-4 and onwards) .....	242
6.3	Void.....	242
6.4	Advice of charge (AoC) handling .....	242
6.4.1	AoC not supported by USIM .....	242
6.4.2	Maximum frequency of ACM updating.....	242
6.4.3	Call terminated when ACM greater than ACM <sub>max</sub> .....	242
6.4.4	Response codes of increase command of ACM.....	242
7	PLMN related tests.....	242
7.1	FPLMN handling.....	242
7.1.1	Adding FPLMN to the Forbidden PLMN list .....	242
7.1.2	UE updating forbidden PLMNs .....	242
7.1.3	UE deleting forbidden PLMNs .....	242
7.1.4	Adding FPLMN to the forbidden PLMN list when accessing E-UTRAN.....	243
7.1.4.1	Definition and applicability.....	243
7.1.4.2	Conformance requirement.....	243
7.1.4.3	Test purpose .....	243
7.1.4.4	Method of test .....	244
7.1.4.4.1	Initial conditions .....	244
7.1.4.4.2	Procedure.....	244
7.1.4.4	Acceptance criteria.....	245
7.1.5	UE updating forbidden PLMNs when accessing E-UTRAN.....	246
7.1.5.1	Definition and applicability.....	246
7.1.5.2	Conformance requirement.....	246
7.1.5.3	Test purpose .....	246
7.1.5.4	Method of test .....	246
7.1.5.4.1	Initial conditions .....	246
7.1.5.4.2	Procedure.....	247
7.1.5.5	Acceptance criteria.....	247
7.1.6	UE deleting forbidden PLMNs when accessing E-UTRAN .....	248

7.1.6.1	Definition and applicability.....	248
7.1.6.2	Conformance requirement.....	248
7.1.6.3	Test purpose .....	248
7.1.6.4	Method of test .....	248
7.1.6.4.1	Initial conditions.....	248
7.1.6.4.2	Procedure.....	248
7.1.6.5	Acceptance criteria.....	249
7.1.7	Updating the Forbidden PLMN list after receiving non-integrity protected reject message – UTRAN ...	249
7.1.8	Updating the Forbidden PLMN list after receiving non-integrity protected reject message – E-UTRAN.....	250
7.1.8.1	Definition and applicability.....	250
7.1.8.2	Conformance requirement.....	250
7.1.8.3	Test purpose .....	250
7.1.8.4	Method of test .....	250
7.1.8.4.1	Initial conditions.....	250
7.1.8.4.2	Procedure.....	251
7.1.8.5	Acceptance criteria.....	251
7.2	User controlled PLMN selector handling .....	252
7.2.1	UE updating the User controlled PLMN selector list .....	252
7.2.1.1	Definition and applicability.....	252
7.2.1.2	Conformance requirement.....	252
7.2.1.3	Test purpose .....	252
7.2.1.4	Method of test .....	252
7.2.1.4.1	Initial conditions.....	252
7.2.1.4.2	Procedure.....	252
7.2.1.5	Acceptance criteria.....	253
7.2.2	UE recognizing the priority order of the User controlled PLMN selector list with the same access Technology .....	253
7.2.3	UE recognizing the priority order of the User controlled PLMN selector list using an ACT Preference .....	253
7.2.4	Void.....	254
7.2.5	UE updating the User controlled PLMN selector list for E-UTRAN .....	254
7.2.5.1	Definition and applicability.....	254
7.2.5.2	Conformance requirement.....	254
7.2.5.3	Test purpose .....	254
7.2.5.4	Method of test .....	254
7.2.5.4.1	Initial conditions.....	254
7.2.5.4.2	Procedure.....	254
7.2.5.5	Acceptance criteria.....	254
7.2.6	UE recognizing the priority order of the User controlled PLMN selector list using an ACT preference - UTRAN/E-UTRAN .....	255
7.2.7	UE recognizing the priority order of the User controlled PLMN selector list using an ACT preference - GSM/E-UTRAN .....	255
7.2.8	UE recognising the priority order of the User controlled PLMN selector list with the same access technology – E-UTRAN in NB-S1 mode .....	255
7.2.8.1	Definition and applicability.....	255
7.2.8.2	Conformance requirement.....	255
7.2.8.3	Test purpose .....	256
7.2.8.4	Method of test .....	256
7.2.8.4.1	Initial conditions.....	256
7.2.8.4.2	Procedure.....	257
7.2.8.5	Acceptance criteria.....	257
7.2.9	UE recognising the priority order of the User controlled PLMN selector list using the ACT preference – E-UTRAN in WB-S1/E-UTRAN in NB-S1 .....	258
7.2.9.1	Definition and applicability.....	258
7.2.9.2	Conformance requirement.....	258
7.2.9.3	Test purpose .....	258
7.2.9.4	Method of test .....	258
7.2.9.4.1	Initial conditions.....	258
7.2.9.4.2	Procedure.....	259
7.2.9.5	Acceptance criteria.....	259
7.3	Operator controlled PLMN selector handling .....	260

7.3.1	UE recognizing the priority order of the Operator controlled PLMN selector list.....	260
7.3.2	UE recognizing the priority order of the User controlled PLMN selector over the Operator controlled PLMN selector list .....	260
7.3.3	UE recognizing the priority order of the Operator controlled PLMN selector list when accessing E-UTRAN.....	260
7.3.3.1	Definition and applicability.....	260
7.3.3.2	Conformance requirement.....	260
7.3.3.3	Test purpose .....	261
7.3.3.4	Method of test .....	261
7.3.3.4.1	Initial conditions .....	261
7.3.3.4.2	Procedure.....	262
7.3.3.5	Acceptance criteria.....	262
7.3.4	UE recognizing the priority order of the User controlled PLMN selector over the Operator controlled PLMN selector list – E-UTRAN.....	263
7.3.4.1	Definition and applicability.....	263
7.3.4.2	Conformance requirement.....	263
7.3.4.3	Test purpose .....	263
7.3.4.4	Method of test .....	263
7.3.4.4.1	Initial conditions .....	263
7.3.4.4.2	Procedure.....	264
7.3.4.5	Acceptance criteria.....	264
7.3.5	UE recognising the priority order of the Operator controlled PLMN selector list when accessing E-UTRAN in NB-S1 mode.....	265
7.3.5.1	Definition and applicability.....	265
7.3.5.2	Conformance requirement.....	265
7.3.5.3	Test purpose .....	265
7.3.5.4	Method of test .....	265
7.3.5.4.1	Initial conditions.....	265
7.3.5.4.2	Procedure.....	266
7.3.5.5	Acceptance criteria.....	267
7.3.6	UE recognising the priority order of the User controlled PLMN selector over the Operator controlled PLMN selector list – E-UTRAN in NB-S1 mode.....	267
7.3.6.1	Definition and applicability.....	267
7.3.6.2	Conformance requirement.....	268
7.3.6.3	Test purpose .....	268
7.3.6.4	Method of test .....	268
7.3.6.4.1	Initial conditions .....	268
7.3.6.4.2	Procedure.....	270
7.3.6.5	Acceptance criteria.....	270
7.3.7	UE recognising the priority order of the Operator controlled PLMN selector list using the ACT preference – E-UTRAN in NB-S1/ E-UTRAN in WB-S1 mode.....	271
7.3.7.1	Definition and applicability.....	271
7.3.7.2	Conformance requirement.....	271
7.3.7.3	Test purpose .....	271
7.3.7.4	Method of test .....	271
7.3.7.4.1	Initial conditions .....	271
7.3.7.4.2	Procedure.....	272
7.3.7.5	Acceptance criteria.....	272
7.3.8	UE recognising the priority order of the Operator controlled PLMN selector list using the ACT preference – E-UTRAN in NB-S1 mode/ GSM .....	273
7.3.9	UE recognising the priority order of the Operator controlled PLMN selector list using the ACT preference – E-UTRAN in WB-S1 mode/GSM.....	273
7.4	Higher priority PLMN search handling.....	273
7.4.1	UE recognizing the search period of the Higher priority PLMN .....	273
7.4.2	GSM/UMTS dual mode UEs recognizing the search period of the Higher priority PLMN .....	273
7.4.3	UE recognizing the search period of the Higher priority PLMN – E-UTRAN.....	273
7.4.3.1	Definition and applicability.....	273
7.4.3.2	Conformance requirement.....	274
7.4.3.3	Test purpose .....	274
7.4.3.4	Method of test .....	274
7.4.3.4.1	Initial conditions .....	274
7.4.3.4.2	Procedure.....	275

7.4.3.5	Acceptance criteria.....	275
7.4.4	E-UTRAN/EPC capable UEs recognizing the search period of the Higher priority PLMN – GSM/E-UTRAN .....	276
7.4.5	E-UTRAN/EPC capable UEs recognizing the search period of the Higher priority PLMN – UTRAN/E-UTRAN.....	276
7.4.6	UE recognising the search period of the higher priority PLMN – Satellite NG-RAN.....	276
7.4.7	UE recognising the search period of the higher priority PLMN – NG-RAN.....	276
7.4.7.1	Definition and applicability.....	276
7.4.7.2	Conformance requirement.....	276
7.4.7.3	Test purpose .....	277
7.4.7.4	Method of test .....	277
7.4.7.4.1	Initial conditions.....	277
7.4.7.4.2	Procedure.....	278
7.4.7.5	Acceptance criteria.....	279
7.5	Void.....	280
8	Subscription independent tests .....	280
8.1	Phone book procedures .....	280
8.1.1	Recognition of a previously changed phonebook .....	280
8.1.2	Update of the Phonebook Synchronization Counter (PSC) .....	280
8.1.2.1	Definition and applicability.....	280
8.1.2.2	Conformance requirement.....	280
8.1.2.3	Test purpose .....	280
8.1.2.4	Method of test .....	280
8.1.2.4.1	Initial conditions.....	280
8.1.2.4.2	Procedure.....	281
8.1.2.5	Acceptance criteria.....	282
8.1.3	Handling of BCD number/ SSC content extension.....	282
8.1.3.1	Definition and applicability.....	282
8.1.3.2	Conformance requirement.....	282
8.1.3.3	Test purpose .....	282
8.1.3.4	Method of test .....	283
8.1.3.4.1	Initial conditions.....	283
8.1.3.4.2	Procedure.....	285
8.1.3.5	Acceptance criteria.....	287
8.1.4	Phonebook selection .....	287
8.1.4.1	Definition and applicability.....	287
8.1.4.2	Conformance requirement.....	287
8.1.4.3	Test purpose .....	288
8.1.4.4	Method of test .....	288
8.1.4.4.1	Initial conditions.....	288
8.1.4.4.2	Procedure.....	291
8.1.4.5	Acceptance criteria.....	292
8.1.5	Local Phonebook handling .....	293
8.1.5.1	Definition and applicability.....	293
8.1.5.2	Conformance requirement.....	293
8.1.5.3	Test purpose .....	293
8.1.5.4	Method of test .....	293
8.1.5.4.1	Initial conditions.....	293
8.1.5.4.2	Procedure.....	294
8.1.5.5	Acceptance criteria.....	295
8.2	Short message handling report .....	296
8.2.1	Correct storage of a SM on the USIM .....	296
8.2.2	Correct reading of a SM on the USIM.....	296
8.2.3	SM memory capacity exceeded handling .....	296
8.2.4A	Correct storage of an SM on the UICC.....	296
8.2.4B	Correct storage of an SM on the UICC.....	296
8.2.5	Correct reading of a SM on the USIM if USIM and ISIM are present .....	296
8.2.6	Correct reading of a SM on the ISIM if USIM and ISIM are present.....	296
8.2.7	Correct storage of an SM on the UICC.....	296
8.3	MMS related tests.....	297
8.3.0	General condition.....	297

8.3.1	UE recognizing the priority order of MMS Issuer Connectivity Parameters .....	297
8.3.2	UE recognizing the priority order of MMS User Connectivity Parameters .....	297
8.3.3	UE recognizing the priority order of MMS Issuer Connectivity Parameters over the MMS User Connectivity Parameters .....	297
8.3.4	Usage of MMS notification .....	297
8.4	UICC presence detection.....	297
8.5	UICC presence detection when connected to E-UTRAN/EPC .....	297
9	USIM service handling.....	297
9.1	Access Point Name Control List handling .....	297
9.1.1	Access Point Name Control List handling for UEs supporting ACL.....	297
9.1.2	Network provided APN handling for UEs supporting ACL .....	297
9.1.3	Access Point Name Control List handling for UEs not supporting ACL .....	298
9.1.4	Access Point Name Control List handling for UEs supporting ACL connected to E-UTRAN/EPC.....	298
9.1.4.1	Definition and applicability.....	298
9.1.4.2	Conformance requirement.....	298
9.1.4.3	Test purpose .....	298
9.1.4.4	Method of test .....	298
9.1.4.4.1	Initial conditions .....	298
9.1.4.4.2	Procedure.....	299
9.1.4.5	Acceptance criteria.....	300
9.2	Service Dialling Numbers handling .....	300
9.2.1	Service Dialling Numbers handling.....	300
10	CSG list handling .....	300
10.1	CSG list handling for E-UTRA .....	300
10.1.1	Automatic CSG selection in E-UTRA with CSG list on USIM, success.....	300
10.1.1.1	Definition and applicability.....	300
10.1.1.2	Conformance requirement.....	300
10.1.1.3	Test purpose .....	301
10.1.1.4	Method of test .....	301
10.1.1.4.1	Initial conditions .....	301
10.1.1.4.2	Procedure.....	301
10.1.1.5	Acceptance criteria.....	302
10.1.2.1	Definition and applicability.....	302
10.1.2.2	Conformance requirement.....	302
10.1.2.3	Test purpose .....	303
10.1.2.4	Method of test .....	303
10.1.2.4.1	Initial conditions .....	303
10.1.2.4.2	Procedure.....	303
10.1.2.5	Acceptance criteria.....	303
10.1.3	Manual CSG selection in E-UTRA with CSG list on USIM, success .....	304
10.1.3.1	Definition and applicability.....	304
10.1.3.2	Conformance requirement.....	304
10.1.3.3	Test purpose .....	305
10.1.3.4	Method of test .....	305
10.1.3.4.1	Initial conditions .....	305
10.1.3.4.2	Procedure.....	305
10.1.3.5	Acceptance criteria.....	306
10.1.4	Manual CSG selection in E-UTRA with CSG list on USIM, rejected.....	307
10.1.4.1	Definition and applicability.....	307
10.1.4.2	Conformance requirement.....	307
10.1.4.3	Test purpose .....	307
10.1.4.4	Method of test .....	308
10.1.4.4.1	Initial conditions .....	308
10.1.4.4.2	Procedure.....	308
10.1.4.5	Acceptance criteria.....	308
10.1.5	CSG selection in E-UTRA with no CSG list on USIM, no IMSI change.....	309
10.1.5.1	Definition and applicability.....	309
10.1.5.2	Conformance requirement.....	309
10.1.5.3	Test purpose .....	310
10.1.5.4	Method of test .....	310

10.1.5.4.1	Initial conditions .....	310
10.1.5.4.2	Procedure .....	310
10.1.5.5	Acceptance criteria .....	311
10.1.6	CSG selection in E-UTRA with no CSG list on USIM, with IMSI change .....	312
10.1.6.1	Definition and applicability .....	312
10.1.6.2	Conformance requirement .....	312
10.1.6.3	Test purpose .....	312
10.1.6.4	Method of test .....	312
10.1.6.4.1	Initial conditions .....	312
10.1.6.4.2	Procedure .....	313
10.1.6.5	Acceptance criteria .....	314
10.1.7	Manual CSG selection without display restrictions in E-UTRA with ACSG list and OCSG list on USIM .....	314
10.1.7.1	Definition and applicability .....	314
10.1.7.2	Conformance requirement .....	314
10.1.7.3	Test purpose .....	315
10.1.7.4	Method of test .....	315
10.1.7.4.1	Initial conditions .....	315
10.1.7.4.2	Procedure .....	315
10.1.7.5	Acceptance criteria .....	316
10.1.8	Manual CSG selection with display restrictions in E-UTRA with ACSG list and OCSG list on USIM ..	317
10.1.8.1	Definition and applicability .....	317
10.1.8.2	Conformance requirement .....	317
10.1.8.3	Test purpose .....	318
10.1.8.4	Method of test .....	318
10.1.8.4.1	Initial conditions .....	318
10.1.8.4.2	Procedure .....	318
10.1.8.5	Acceptance criteria .....	319
10.2	CSG list handling for UTRA .....	320
10.2.1	Manual CSG selection without display restrictions in UTRA with ACSG list and OCSG list on USIM .....	320
10.2.2	Manual CSG selection with display restrictions in UTRA with ACSG list and OCSG list on USIM .....	321
10.2.3	Manual CSG selection in UTRA with CSG list on USIM, success .....	321
11	NAS security context parameter handling .....	321
11.1	NAS security context parameter handling when service "EMM Information" is available .....	321
11.1.1	Definition and applicability .....	321
11.1.2	Conformance requirement .....	321
11.1.3	Test purpose .....	321
11.1.4	Method of test .....	321
11.1.4.1	Initial conditions .....	321
11.1.4.2	Procedure .....	322
11.1.4.5	Acceptance criteria .....	322
11.2	NAS security context parameter handling when service "EMM Information" is not available, no IMSI change .....	323
11.2.1	Definition and applicability .....	323
11.2.2	Conformance requirement .....	323
11.2.3	Test purpose .....	324
11.2.4	Method of test .....	324
11.2.4.1	Initial conditions .....	324
11.2.4.2	Procedure .....	324
11.2.5	Acceptance criteria .....	325
11.3	NAS security context parameter handling when service "EMM Information" is not available, IMSI Changed .....	325
11.3.1	Definition and applicability .....	325
11.3.2	Conformance requirement .....	325
11.3.3	Test purpose .....	326
11.3.4	Method of test .....	326
11.3.4.1	Initial conditions .....	326
11.3.4.2	Procedure .....	326
11.3.5	Acceptance criteria .....	327
11.4	EPS NAS Security Context Storage .....	327

11.4.1	Definition and applicability .....	327
11.4.2	Conformance requirement .....	327
11.4.3	Test purpose.....	328
11.4.4	Method of test .....	328
11.4.4.1	Initial conditions .....	328
11.4.4.2	Procedure .....	328
11.4.5	Acceptance criteria .....	329
12	Non Access Stratum (NAS) Configuration parameter handling .....	329
12.1	EF <sub>NASCONFIG</sub> - NAS signalling priority handling.....	329
12.2	EF <sub>NASCONFIG</sub> - NMO I Network Mode of Operation I handling .....	329
12.3	EF <sub>NASCONFIG</sub> - Attach with IMSI handling .....	329
12.4	EF <sub>NASCONFIG</sub> - Verifying Minimum Periodic Search Timer .....	329
12.5	EF <sub>NASCONFIG</sub> - Extended access barring handling.....	330
12.6	EF <sub>NASCONFIG</sub> - Verifying Timer T3245 Behaviour .....	330
12.7	EF <sub>NASCONFIG</sub> - Override NAS signalling low priority .....	330
12.8	EF <sub>NASCONFIG</sub> - Override Extended access barring .....	330
12.9	EF <sub>NASCONFIG</sub> - Fast First Higher Priority PLMN Search .....	330
12.10	EF <sub>NASCONFIG</sub> - E-UTRA Disabling Allowed for EMM cause #15.....	330
12.11	EF <sub>NASCONFIG</sub> - SM_RetryWaitTime .....	330
12.12	EF <sub>NASCONFIG</sub> - SM_RetryAtRATChange .....	330
13	UICC interface during PSM .....	330
13.1	UICC interface in PSM handling for E-UTRAN – No UICC deactivation in PSM.....	330
13.1.1	Definition and applicability .....	330
13.1.2	Conformance requirement .....	331
13.1.3	Test purpose.....	331
13.1.4	Method of test .....	331
13.1.4.1	Initial conditions .....	331
13.1.4.2	Procedure .....	331
13.1.5	Acceptance criteria .....	332
13.2	UICC interface in PSM handling for E-UTRAN – PSM not accepted by E-USS/NB-SS .....	332
13.2.1	Definition and applicability .....	332
13.2.2	Conformance requirement .....	332
13.2.3	Test purpose.....	332
13.2.4	Method of test .....	332
13.2.4.1	Initial conditions .....	332
13.2.4.2	Procedure .....	333
13.2.5	Acceptance criteria .....	333
13.3	UICC interface in PSM handling for E-UTRAN – UICC deactivation in PSM.....	333
13.4	UICC interface in PSM for E-UTRAN – SUSPEND UICC .....	334
13.4.1	Definition and applicability .....	334
13.4.2	Conformance requirement .....	334
13.4.3	Test purpose.....	334
13.4.4	Method of test .....	334
13.4.4.1	Initial conditions .....	334
13.4.4.2	Procedure .....	335
13.4.5	Acceptance criteria .....	335
14	UICC interface during eDRX.....	335
14.1	UICC interface during eDRX for E-UTRAN – eDRX is not supported by the UICC .....	335
14.1.1	Definition and applicability .....	335
14.1.2	Conformance requirement .....	336
14.1.3	Test purpose.....	336
14.1.4	Method of test .....	336
14.1.4.1	Initial conditions .....	336
14.1.4.2	Procedure .....	336
14.1.5	Acceptance criteria .....	337
14.2	UICC interface during eDRX for E-UTRAN – eDRX is not accepted by E-USS/NB-SS.....	337
14.2.1	Definition and applicability .....	337
14.2.2	Conformance requirement .....	337
14.2.3	Test purpose.....	338
14.2.4	Method of test .....	338

14.2.4.1	Initial conditions .....	338
14.2.4.2	Procedure .....	338
14.2.5	Acceptance criteria .....	339
14.3	UICC interface during eDRX for E-UTRAN – UICC deactivation during eDRX.....	339
14.4	UICC interface during eDRX for E-UTRAN– SUSPEND UICC.....	339
15	Authentication procedure and NAS security context handling for 5G.....	339
15.1	Authentication procedure for EAP-AKA'.....	339
15.1.1	Authentication procedure for EAP-AKA' - Authentication is successful .....	339
15.1.1.1	Definition and applicability.....	339
15.1.1.2	Conformance requirement.....	340
15.1.1.3	Test purpose .....	340
15.1.1.4	Method of test .....	341
15.1.1.4.1	Initial conditions.....	341
15.1.1.4.2	Procedure.....	341
15.1.1.5	Acceptance criteria.....	342
15.1.1.5	Acceptance criteria.....	343
15.1A.1	Authentication procedure for EAP-AKA' - Authentication is successful .....	343
15.1A.1.1	Definition and applicability.....	343
15.1A.1.2	Conformance requirement.....	343
15.1A.1.3	Test purpose .....	344
15.1A.1.4	Method of test .....	344
15.1A.1.4.1	Initial conditions.....	344
15.1A.1.4.2	Procedure.....	344
15.1A.1.5	Acceptance criteria.....	345
15.1.2	Authentication procedure for EAP-AKA' – Authentication is successful - GSM UICC .....	346
15.1.2.1	Definition and applicability.....	346
15.1.2.2	Conformance requirement.....	346
15.1.2.3	Test purpose .....	347
15.1.2.4	Method of test .....	347
15.1.2.4.1	Initial conditions.....	347
15.1.2.4.2	Procedure.....	347
15.1.2.5	Acceptance criteria.....	348
15.1.3	Authentication procedure for EAP-AKA' – AUTN fails on the USIM .....	348
15.1.3.1	Definition and applicability.....	348
15.1.3.2	Conformance requirement.....	349
15.1.3.3	Test purpose .....	349
15.1.3.4	Method of test .....	349
15.1.3.4.1	Initial conditions.....	349
15.1.3.4.2	Procedure.....	349
15.1.3.5	Acceptance criteria.....	350
15.1.4	Authentication procedure for EAP-AKA' - after SUPI is changed .....	350
15.1.4.1	Definition and applicability.....	350
15.1.4.2	Conformance requirement.....	350
15.1.4.3	Test purpose .....	351
15.1.4.4	Method of test .....	351
15.1.4.4.2	Procedure.....	351
15.1.4.5	Acceptance criteria.....	353
15.2	Authentication procedure for 5G AKA .....	353
15.2.1	Authentication procedure for 5G AKA - Authentication is successful.....	353
15.2.1.4	Method of test .....	354
15.2.1.4.1	Initial conditions.....	354
15.2.1.5	Acceptance criteria.....	355
15.2A.1	Authentication procedure for 5G AKA - Authentication is successful.....	356
15.2A.1.4	Method of test .....	357
15.2A.1.4.1	Initial conditions.....	357
15.2A.1.5	Acceptance criteria.....	358
15.2.2	Authentication procedure for 5G AKA – Authentication is successful - GSM UICC.....	359
15.2.2.1	Definition and applicability.....	359
15.2.2.2	Conformance requirement.....	359
15.2.2.3	Test purpose .....	359
15.2.2.4	Method of test .....	360

15.2.2.4.1	Initial conditions .....	360
15.2.2.4.2	Procedure .....	360
15.2.2.5	Acceptance criteria .....	361
15.2A.2	Authentication procedure for 5G AKA - Authentication is successful .....	361
15.2A.2.1	Definition and applicability .....	361
15.2A.2.2	Conformance requirement .....	361
15.2A.2.3	Test purpose .....	362
15.2A.2.4	Method of test .....	362
15.2A.2.4.1	Initial conditions .....	362
15.2A.2.4.2	Procedure .....	362
15.2A.2.5	Acceptance criteria .....	363
15.2.3	Authentication procedure 5G AKA – AUTN fails on the USIM .....	363
15.2.3.1	Definition and applicability .....	363
15.2.3.2	Conformance requirement .....	363
15.2.3.3	Test purpose .....	364
15.2.3.4	Method of test .....	364
15.2.3.4.1	Initial conditions .....	364
15.2.3.4.2	Procedure .....	364
15.2.3.5	Acceptance criteria .....	365
15.2.4	Authentication procedure for 5G AKA - after SUPI is changed .....	365
15.2.4.1	Definition and applicability .....	365
15.2.4.2	Conformance requirement .....	365
15.2.4.3	Test purpose .....	366
15.2.4.4	Method of test .....	366
15.2.4.4.1	Initial conditions .....	366
15.2.4.4.2	Procedure .....	366
15.2.4.5	Acceptance criteria .....	368
15.2.5.2	Conformance requirement .....	368
15.2.5.4	Method of test .....	369
15.2.5.4.1	Initial conditions .....	369
15.2.5.4.2	Procedure .....	370
15.2.5.5	Acceptance criteria .....	371
16	UE Route Selection Policy (URSP) procedure .....	373
16.1	Pre-configured URSP rules .....	373
16.1.1	Support for URSP by USIM .....	373
16.1.1.1	Definition and applicability .....	373
16.1.1.2	Conformance requirement .....	374
16.1.1.3	Test purpose .....	374
16.1.1.4	Method of test .....	374
16.1.1.4.1	Initial conditions .....	374
16.1.1.4.2	Procedure .....	376
16.1.1.5	Acceptance criteria .....	376
16.1.2	Support for URSP by ME .....	376
16.1.2.1	Definition and applicability .....	376
16.1.2.2	Conformance requirement .....	376
16.1.2.3	Test purpose .....	377
16.1.2.4	Method of test .....	377
16.1.2.4.1	Initial conditions .....	377
16.1.2.4.2	Procedure .....	378
16.1.2.5	Acceptance criteria .....	378
16.1.3	Support of Signalled URSP .....	378
16.1.3.1	Definition and applicability .....	378
16.1.3.2	Conformance requirement .....	378
16.1.3.3	Test purpose .....	379
16.1.3.4	Method of test .....	379
16.1.3.4.1	Initial conditions .....	379
16.1.3.4.2	Procedure .....	380
16.1.3.5	Acceptance criteria .....	380
17	CAG list handling .....	381
17.1	CAG list handling for 5G .....	381

17.1.1	Automatic CAG selection with preconfigured CAG list on USIM.....	381
17.1.1.1	Definition and applicability.....	381
17.1.1.2	Conformance requirement.....	381
17.1.1.3	Test purpose.....	381
17.1.1.4	Method of tests.....	381
17.1.1.4.1	Initial conditions.....	381
17.1.1.4.2	Procedure.....	382
17.1.1.5	Acceptance criteria.....	382
18	NSSAA procedure with SSIM.....	383
18.1	SSIM management procedures.....	383
18.1.1	SSIM identification, S-NSSAI list request.....	383
18.1.1.1	Definition and applicability.....	383
18.1.1.2	Conformance requirement.....	383
18.1.1.3	Test purpose.....	383
18.1.1.4	Method of tests.....	384
18.1.1.4.1	Initial conditions.....	384
18.1.1.4.2	Procedure.....	385
18.1.1.4.2	Acceptance criteria.....	386
18.2	SSIM commands.....	386
18.2.1	AUTHENTICATE command, Identity EAP-Request/EAP-Response messages.....	386
18.2.1.1	Definition and applicability.....	386
18.2.1.2	Conformance requirement.....	386
18.2.1.3	Test purpose.....	387
18.2.1.4	Method of tests.....	387
18.2.1.4.1	Initial conditions.....	387
18.2.1.4.2	Procedure.....	387
18.2.1.4.3	Acceptance criteria.....	388
18.2.2	AUTHENTICATE command, other EAP-Request/EAP-Response messages.....	388
18.2.2.1	Definition and applicability.....	388
18.2.2.2	Conformance requirement.....	388
18.2.2.3	Test purpose.....	389
18.2.2.4	Method of tests.....	389
18.2.2.4.1	Initial conditions.....	389
18.2.2.4.2	Procedure.....	389
18.2.2.4.3	Acceptance criteria.....	389
18.2.3	AUTHENTICATE command, EAP-Success/EAP-Failure messages.....	389
18.2.3.1	Definition and applicability.....	389
18.2.3.2	Conformance requirement.....	389
18.2.3.3	Test purpose.....	390
18.2.3.4	Method of tests.....	390
18.2.3.4.1	Initial conditions.....	390
18.2.3.4.2	Procedure.....	390
18.2.3.4.3	Acceptance criteria.....	391
<b>Annex A (informative): Suggested requirements lists for Test Applet functionality.....</b>		<b>392</b>
A.1	General requirements.....	392
A.2	Test instruction or input data requirements.....	392
A.2.1	Test instruction or input data requirements list-1.....	392
A.2.2	Test instruction or input data requirements list-2.....	393
A.3	APDU content verification requirements.....	393
A.3.1	APDU content verification requirements list-1.....	393
A.3.2	APDU content verification requirements list-2.....	393
<b>Annex B (informative): Examples of Test EFs in the Test-nrUICC configuration.....</b>		<b>394</b>
B.1	Test EF structure - 1.....	394
B.1.1	EF <sub>STK</sub> (SIMToolkit data).....	394
B.1.2	EF <sub>SETSTK</sub> (Set SIM Toolkit).....	395
B.1.3	EF <sub>CC</sub> (CALL CONTROL).....	395
B.1.4	EF <sub>EVENTLIST</sub> (EVENT LIST).....	396

B.2	Test EF structure - 2 .....	396
B.2.1	EF <sub>TC_IN</sub> (Test Case Input) .....	396
B.2.2	EF <sub>TC_OUT</sub> (Test Case Output) .....	397
B.2.3	EF <sub>EF_RESET</sub> (EF_RESET) .....	398
<b>Annex C (informative): 5G-NR generic procedure for 5G Registration on 3GPP access with IMS service.....</b>		<b>400</b>
C.1	5G-NR generic procedure for 5G Registration on 3GPP access with IMS service.....	400
C.1.1	'voice centric' Procedure .....	400
<b>Annex D (informative): APDU logging in seamless testing.....</b>		<b>401</b>
D.1	Example of SIM APDU logging via AT interface .....	401
<b>Annex E (informative): Change history .....</b>		<b>402</b>
History .....		403

---

# Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

- shall** indicates a mandatory requirement to do something
- shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

- should** indicates a recommendation to do something
- should not** indicates a recommendation not to do something
- may** indicates permission to do something
- need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

- can** indicates that something is possible
- cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

- will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document
- will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document
- might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

---

## Introduction

The present document defines application behavioural tests for a UE with a non-removable UICC/USIM where no access to the physical UICC-Terminal interface can be granted when interacting with a 3GPP network.

The aim of the present document is to ensure the correct behaviour of a UE interfacing with a 3GPP network whilst it is proved that card specific data and functionality is used wherever indicated, similar to application tests defined in TS 31.121 [2] but without direct access to the UICC-Terminal interface.

The present document does not define any aspects related to the administrative management phase of the UICC. Any internal technical realisation of either the UICC or the ME is only specified where these are important for the verification of specific behaviour. Application specific details for applications residing on an UICC are specified in the respective application specific documents.

---

# 1 Scope

The present document provides application behavioural tests for a UE to interoperability with dedicated 3GPP network operations. Where there shall be a description for each compliant implementation including the:

- the test case specific setting of the USIM;
- the applicability of each test case;
- the test configurations;
- the conformance requirement(s) and reference(s) to the related core specifications;
- the test purposes; and
- a brief description of the test procedure and the specific acceptance criteria.

The present document is applicable for MEs supporting a non-removable UICC only. MEs that allow access to the physical card interface as defined in ETSI TS 102 221 [8] or ETSI TS 102 671 [29] shall be tested in accordance to TS 31.121 [2].

This document shall provide alternative verification and testing approaches for test cases initially defined in TS 31.121 [2]. If no ETSI or 3GPP defined alternative method to verify an existing requirement is available or if the result generated by the proposed verification method is less reliable, this has to be clearly stated in the test description.

Due to possible limitations in profile handling and updating it is not intended to use the test case defined within this document with 2G only MEs or MEs implemented in accordance to Rel-12 or earlier.

A 3GPP ME may support functionality that is not required by 3GPP, but the requirements to do so are outside of the scope of 3GPP. The present document does not contain tests for features that are out of scope of 3GPP.

In the present document, unless explicitly stated otherwise, for Rel-13 onwards the term E-UTRAN implicitly refers to E-UTRAN in WB-S1 mode. E-UTRAN in NB-S1 mode is always explicitly referred to as NB-IoT.

---

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

- [1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".
- [2] 3GPP TS 31.121: "UICC-terminal interface; Universal Subscriber Identity Module (USIM) application test specification".
- [3] 3GPP TS 38.508-1: "5GS; User Equipment (UE) conformance specification; Part 1: Common test environment".
- [4] 3GPP TS 36.508: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Packet Core (EPC); Common test environments for User Equipment (UE) conformance testing".
- [5] 3GPP TS 34.108: "Common test environments for User Equipment (UE) conformance testing".

- [6] 3GPP TS 34.229-1: "Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); User Equipment (UE) conformance specification; Part 1: Protocol conformance specification".
- [7] ISO/IEC 9646-7: "Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 7: Implementation Conformance Statements".
- [8] ETSI TS 102 221: "UICC-Terminal interface; Physical and logical characteristics".
- [9] GSMA TS.48: "Generic eUICC Test Profile for Device Testing".
- [10] ETSI TS 103 666-1: "Smart Secure Platform (SSP); Part 1: General characteristics".
- [11] ETSI TS 103 666-2: "Smart Secure Platform (SSP); Part 2: Integrated SSP (iSSP) characteristics".
- [12] ETSI TS 103 666-3: "Smart Secure Platform (SSP); Part 3: Embedded SSP (eSSP) Type 1 characteristics".
- [13] 802.11-2016: "IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".
- [14] ETSI TS 102 225: "Secured packet structure for UICC based applications".
- [15] ETSI TS 102 226: "Remote APDU structure for UICC based applications".
- [16] 3GPP TS 27.007: "AT command set for User Equipment (UE) ".
- [17] 3GPP TS 31.130: "(U)SIM Application Programming Interface (API); (U)SIM API for Java™Card".
- [18] 3GPP TS 22.011: "Service accessibility".
- [19] 3GPP TS 31.102: "Characteristics of the Universal Subscriber Identity Module (USIM) application".
- [20] 3GPP TS 21.111: "USIM and IC card requirements".
- [21] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".
- [22] Trusted Connectivity Alliance: "eUICC Profile Package: Interoperable Format Technical Specification".
- [23] ETSI TS 102 241: "UICC Application Programming Interface (UICC API) for Java Card™".
- [24] 3GPP TS 33.501: "Security architecture and procedures for 5G system".
- [25] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".
- [26] 3GPP TS 31.111: "Universal Subscriber Identity Module (USIM) Application Toolkit (USAT)".
- [27] Void
- [28] Void
- [29] ETSI TS 102 671: "Machine to Machine UICC; Physical and logical characteristics".
- [30] GSMA SGP.22: "RSP Technical specification".
- [31] 3GPP TS 24.008: "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3".
- [32] Void
- [33] 3GPP TS 31.101: "UICC-terminal interface; Physical and logical characteristics".
- [34] 3GPP TS 23.003: "Numbering, addressing and identification".

- [35] 3GPP TS 31.117: "Universal Subscriber Identity Module Application Toolkit (USAT) application behavioural test specification".
- [36] 3GPP TS 22.261: "Service requirements for the 5G system; Stage 1".
- [37] 3GPP TS 38.331: "NR Radio Resource Control (RRC) protocol specification".
- [38] 3GPP TS 24.526: "User Equipment (UE) policies for 5G System (5GS); Stage 3".
- [39] 3GPP TS 23.501: "System architecture for the 5G System (5GS); Stage 2".
- [40] 3GPP TS 23.503: "Policy and charging control framework for the 5G System (5GS); Stage 2".
- [41] 3GPP TS 23.122: "Non-Access-Stratum functions related to Mobile Station (MS) in idle mode".
- [42] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN)".
- [43] 3GPP TS 34.123-1: "User Equipment (UE) conformance specification; Part 1: Protocol conformance specification".
- [44] 3GPP TS 22.030: "Man-Machine Interface (MMI) of the User Equipment (UE)".
- [45] 3GPP TS 22.101: "Smart cards; ETSI numbering system for telecommunication application providers".
- [46] 3GPP TS 23.086: "Advice of Charge (AoC) supplementary services; Stage 2".
- [47] 3GPP TS 24.086: "Advice of Charge (AoC) supplementary services; Stage 3".
- [48] 3GPP TS 22.024: "Description of Charge Advice Information (CAI)".
- [49] 3GPP TS 24.080: "Mobile radio interface layer 3 supplementary services specification; Formats and coding".
- [50] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".
- [51] RFC 5480: "Elliptic Curve Cryptography Subject Public Key Information".
- [52] 3GPP TS 22.220: "Universal Mobile Telecommunications System (UMTS); Service requirements for Home Node B (HNB) and Home eNode B (HeNB)".
- [53] 3GPP TS 33.102: "3G security; Security architecture".
- [54] RFC 4187: "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)".
- [55] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".
- [56] 3GPP TS 23.316: "Wireless and wireline convergence access support for the 5G System (5GS)".
- [57] 3GPP TS 33.203: "Technical Specification Group Services and System Aspects; 3G security; Access security for IP-based services".
- [58] 3GPP TS 34.229-5: "Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Part 5: Protocol conformance specification using 5G System (5GS)".
- [59] 3GPP TS 31.105: "Characteristics of the Slice Subscriber Identity Module application".
- [60] ETSI TS 101 220 v18.2.0: "ETSI numbering system for telecommunication application providers".
- [61] 3GPP TS 23.502: "Procedures for the 5G System (5GS); Stage 2".

## 3 Definitions of terms, symbols and abbreviations

### 3.1 Terms

For the purposes of the present document, the terms given in TR 21.905 [1], TS 31.121 [2] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

**nrUSIM:** non-removable Universal Subscriber Identity Module, i.e. a USIM application or equivalent functionality embedded or integrated into a ME.

**nrSSIM:** non-removable Slice Subscriber Identity Module, i.e. a SSIM application as defined in TS 31.105 [59] or equivalent functionality embedded or integrated into a ME.

**TT:** Test Tool: collective term for requirements fulfilling but not clearly specified test environment

### 3.2 Symbols

For the purposes of the present document, the following symbols apply:

bx	Bit x of byte (leftmost bit is MSB)
Bn	Byte No. n

### 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1], TS 31.121 [2] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

CR	Conformance Requirement
EUT	Equipment Under Test
SA	Suitability Assessment
TT	Test Tool

### 3.4 Coding Conventions

For the purposes of the present document, the following coding conventions apply:

All lengths are presented in bytes, unless otherwise stated. Each byte B is represented by eight bits b8 to b1, where b8 is the most significant bit (MSB) and b1 is the least significant bit (LSB). In each representation, the leftmost bit is the MSB.

In the UICC, all bytes specified as RFU shall be set to '00' and all bits specified as RFU shall be set to '0'. If the GSM and/or USIM application exists on a UICC or is built on a generic telecommunications card, then other values may apply for the non-GSM or non-USIM applications. The values will be defined in the appropriate specifications for such cards and applications. These bytes and bits shall not be interpreted by a Terminal in 3GPP session.

The coding of all data objects in the present document is according to ETSI TS 102 221 [8]. All data objects are BER-TLV except if otherwise defined.

### 3.5 Generic procedures for 5G-NR, E-UTRAN, IMS and NB-IoT

If a test case contains the statement "This test applies to UEs accessing 5G-NR", the procedures defined in TS 38.508-1 [3] shall be the basis for all performed procedures during the test. The procedures in TS 38.508-1 [3] clause 4.5 describe the default behaviour of a conformant UE regarding the specified protocols to be used for 5G-NR and the required procedures from the NAS. TT (NG-SS) and UE shall use the default configuration defined in clause 4.7 appropriate to the supported options (e.g. 'voice centric').

5G-NR generic procedure for 5G Registration on 3GPP access with IMS service is defined in Annex C.1.

If a test case contains the statement "This test applies to UEs accessing NB", the procedures defined in TS 36.508 [4] shall be the basis for all performed procedures during the test. The procedures in TS 36.508 [4] clause 8.1.5 describe the default behaviour of a conformant UE regarding the specified protocols to be used for NB-IoT and the required procedures from the NAS.

If a test case contains the statement "This test applies to UEs accessing E-UTRAN", the procedures defined in TS 36.508 [4] shall be the basis for all performed procedures during the test. The procedures in TS 36.508 [4], clause 4.5 describe the default behaviour of a conformant UE regarding the specified protocols to be used for E-UTRAN and the required procedures from the NAS.

TS 34.229-1 [6], Annex C describes the generic test procedures for IMS.

## 3.6 Table of optional features

Support of several features is optional or release dependent for the user equipment. However, if a UE states conformance with a specific 3GPP release, it is mandatory for the UE to support all mandatory functions of that release, as stated in table A.1.

The supplier of the implementation shall state the support of possible options in table A.1.

**Table A.1: Options**

Item	Option	Status	Support	Mnemonic
1	Support of CS	O		O_CS
2	Support of a feature requiring PIN2 entry (such as e.g. AoC or FDN)	O		O_PIN2_ENTRY_FEAT
3	Support of UTRAN access	N/A		O_UTRAN
4	Support of GERAN access	N/A		O_GERAN
5	Support of Fixed Dialling Numbers	O		O_FDN
6	Support of Advice of Charge Charging	O		O_AoCC
7	Support of Higher Priority PLMN selector with Access Technology service	O		O_HPLMNwACT
8	Support of local phonebook	O		O_LOCAL_PB
9	Support of global phonebook	C001		O_GLOBAL_PB
10	Support of storing received Class 2 Short Messages in the USIM	O		O_STORE_CLASS2_SMS
11	Support of MMS	O		O_MMS
12	Support of usage of MMS related data stored on the USIM	C002		O_MMS_USIM_DATA
13	Supported of unselected user MMS connectivity parameters	O		O_NO_USER_MMS_CONF_SELEC
14	Support of MMS notification storage on the USIM	O		O_MMS_NOTIF_STORAGE
15	Support of ACL	O		O_ACL
16	Support of SDN	O		O_SDN
17	Support of numerical entry of PLMN codes in EF PLMNwACT	O		O_EFPLMNwACT_NUM_ENTRY
18	ME does support speech call	O		O_SPEECH_CALL
19	ME support PIN MMI strings	O		O_PIN_MMI_STRING
20	ME does support eFDD	O		O_eFDD
21	ME does support eTDD	O		O_eTDD
22	ME does support CSG list handling (for E-UTRA)	O		O_CSG_LIST
23	ME supports SM-over-IP-receiver	O		O_SM-OVER-IP_RECEIVER
24	ME supports reading SMS' stored in EF <sub>SMS</sub> on the USIM if USIM and ISIM are present	O		O_READ_USIM-EF_SMS_IF_USIM+ISIM
25	ME supports reading SMS' stored in EF SMS on the ISIM if USIM and ISIM are present	O		O_READ_ISIM-EF_SMS_IF_USIM+ISIM
26	ME can store more than 1000 text messages	O		O_LARGE_SMS_STORAGE

Item	Option	Status	Support	Mnemonic
27	Support for multiple PDN connections	O		O_MULTIPLE_PDN
28	ME does support CSG (for UTRA)	O		O_CSG
29	Support of manual CSG selection	O		O_MANUAL_CSG_SELECTION
30	Support of PS	O		O_PS
31	ME does support display	O		O_DISPLAY
32	ME does support keypad	O		O_KEYPAD
33	ME supports E-UTRA Disabling Allowed for EMM cause #15	O		O_DISABLE_EUTRA_EMM_CAUSE#15
34	ME supports Override NAS Signalling Low Priority	O		O_OVERRIDE_NAS_SLP
35	ME supports T3245 timer	O		O_T3245
36	ME supports Override Extended Access Barring	O		O_OVERRIDE_EAB
37	ME does support NB-IoT	O		O_NB-IoT
38	ME maintains a list of PLMN-specific attempt counters	O		O_PLMN_ATTEMPT_COUNTER
39	ME does support deactivation of the UICC in PSM.	O		O_PSM_DEAC_UICC
40	ME does support deactivation of the UICC during extended DRX	O		O_eDRX_DEAC_UICC
41	ME does support the UICC suspension mechanism in PSM.	O		O_PSM_SUSPEND_UICC
42	ME does support the UICC suspension mechanism during extended DRX	O		O_eDRX_SUSPEND_UICC
43	Support of 5G Core Network	O		O_5G_CN
44	Support of 5G New Radio access	O		O_5G_NR
45	Support of URSP by USIM	O		O_URSP_BY_USIM
46	ME supports SUPI as Network Access Identifier (NSI, GLI or GCI)	O		O_SUPI_NAI
47	Support of RRC_INACTIVE state	O		O_INACTIVE
48	Support of RSP(SGP.22)	O		O_RSP22
49	Support of AT+CSIM	O		O_AT+CSIM
50	ME supports non-removable UICC only (see NOTE 1)	M		O_NON-REMOVABLE_UICC_ONLY
51	Support of UICC and USIM API for Java Card (see NOTE 2)	O		O_JAVA_CARD_API
52	Support of USAT functionality (see NOTE 3)	O		O_USAT
53	Support of CAG	O		pc_CAG
54	Support of multiple registrations by USIM	O		O_multregs_by_USIM
55	ME does support voice centric mode	O		pc_VOICE_CENTRIC
56	ME does support SSIM during NSSAA procedure	O		O_SSIM

C001	If ((A.1/18 is supported) AND (A.1/31 is supported) AND (A.1/32 is supported)) THEN M, ELSE O
C002	If (A.1/11 is NOT supported) THEN N/A, ELSE M
NOTE 1:	'ME supports non-removable UICC only' means that access to the physical card interface as defined in ETSI TS 102 221 is not available
NOTE 2:	The UE shall claim to support the Java Card API if test relevant functions as defined in Annex A, clause A.2 are supported.
NOTE 3:	The support of the USAT functionalities as expected here requires the support of the UICC API defined in ETSI TS 102 241 [23] and the USIM API defined in TS 31.130 [17]

## 3.7 Applicability

### 3.7.1 Applicability to user equipment

The applicability to user equipment supporting the non-removable USIM is specified in table B.1.

Test cases where no verification of APDUs or transferred data, timing, or checks on file (DF/EF) content is required, may refer to tests defined in TS 31.121 [2]. Regardless of references to complete tests, test purposes, conformance requirements or test methods from TS 31.121 [2] the applicability of the individual test cases is defined within the present document.

Tests where the implicit verification of conformance requirements is not considered sufficient on its own require additional (explicit) verification methods. The support of additional verification methods by the EUT has to be declared in accordance to table A.2 (see clause 3.7.2). Test sequence specific declarations of methods required to be supported are listed in the Applicability table – Table B.1.

### 3.7.2 Supported additional explicit verification methods

The support of additional verification methods is optional for an nrUICC operated device (EUT). As the implicit verification of test results is not sufficient in some test cases the support of an explicit testing option and the provisioning of an interface for file contents verification improves test coverage. The UE manufacturer shall declare the support of possible testable options listed in Table A.2. This declaration is used for the suitability assessment of the conformance requirement (CR) per test case.

**Table A.2: Test Options Declaration**

Item	Option	Status	Support	Mnemonic
1	Support of Toolkit Test Events (see note)	O		O_Toolkit_Test_Events
2	Support of seamless test APDU logging via Baseband (see note)	O		O_Seamless_APDU_Logging
3	Interface for file contents verification	O		O_File_Contents_Verification
NOTE: The support of the SSP Test Tool Interface (ETSI TS 103 834) is handled like the support of seamless test APDU logging via Baseband or for Test Toolkit Event based testing. Specific information may be added to test cases where needed.				

For details on these options see clauses 4.1.3, to 4.1.6 of the present document.

### 3.7.3 Applicability of the individual tests

Table B.1 lists the optional, conditional or mandatory features for which the supplier of the implementation states the support. As pre-condition the supplier of the implementation shall state the support of possible options in table A.1.

The "Release XY ME" columns shows the status of the entries as follows:

The following notations, defined in ISO/IEC 9646-7 [7], are used for the status column:

- M mandatory – the capability is required to be supported.
- O optional – the capability may be supported or not.
- N/A not applicable – in the given context, it is impossible to use the capability.
- X prohibited (excluded) – there is a requirement not to use this capability in the given context.
- O.i qualified optional – for mutually exclusive or selectable options from a set. "i" is an integer which identifies a unique group of related optional items and the logic of their selection which is defined immediately following the table.
- Ci conditional – the requirement on the capability ("M", "O", "X" or "N/A") depends on the support of other optional or conditional items. "i" is an integer identifying an unique conditional status expression which is defined immediately following the table. For nested conditional expressions, the syntax "IF ... THEN (IF ... THEN ... ELSE...) ELSE ..." shall be used to avoid ambiguities.

The "Additional test case execution recommendation" column shows the status of the entries as follows:

- A applicable - the test is applicable according to the corresponding entry in the "Rxx ME" column

- R redundant – the test has to be considered as redundant when the corresponding E-UTRAN/EPC related test of the present document has been validated and successfully executed. In that case the requirement may be verified by means of the E-UTRAN/EPC functionality only.
- AERi Additional test case Execution Recommendation – with respect to the above listed definitions of ("A") and ("R") the test is applicable ("A") or redundant ("R") depending on the support of other optional or conditional items. "i" is an integer identifying a unique conditional status expression which is defined immediately following the table. For nested conditional expressions, the syntax "IF ... THEN (IF ... THEN ... ELSE...) ELSE ..." shall be used to avoid ambiguities.

### References to items

For each possible item answer (answer in the support column) there exists a unique reference, used, for example, in the conditional expressions. It is defined as the table identifier, followed by a solidus character "/", followed by the item number in the table. If there is more than one support column in a table, the columns shall be discriminated by letters (a, b, etc.), respectively.

EXAMPLE: A.1/4 is the reference to the answer of item 4 in table A.1.

## 3.8 Applicability table

Table B.1: Applicability of tests

Test#	Title	from Rel	to Rel (see note)	Applicability	Network Dependency	Test Option	Support
5	Subscription related tests						
5.1	IMSI / TMSI handling						
5.1.6	UE identification by short IMSI when accessing E-UTRAN/EPC	Rel-13		C001	E-USS OR NB-SS	E.04	
5.1.7	UE identification by short IMSI using 2 digit MNC when accessing E-UTRAN/EPC	Rel-13		C001	E-USS OR NB-SS	I.01	
5.1.8	UE identification after changed IMSI with service "EMM Information" not available	Rel-13		C001	E-USS OR NB-SS	I.01	
5.1.9	UE identification by GUTI when using USIM with service "EMM Information" not available	Rel-13		C001	E-USS OR NB-SS	I.01	
5.1.10	UE identification by GUTI when using USIM with service "EMM Information" available	Rel-13		C001	E-USS OR NB-SS	E.04	
5.2	Access Control handling						
5.2.2	Access Control information handling for E-UTRAN/EPC	Rel-13		C003	E-USS	E.04	
5.2.3	Access Control information handling for NB-IoT	Rel-13		C002	NB-SS	E.04	
5.3	Handling subscription identifier privacy for 5G						
5.3.1	SUCI calculation by ME using null scheme	Rel-15		C004	NG-SS	E.04	
5.3.2	SUCI calculation by ME using Profile B	Rel-15		C004	NG-SS	I.01	
5.3.3	UE identification by SUCI during initial registration – SUCI calculation by USIM using profile B	Rel-15		C004	NG-SS	E.04	
5.3.4	UE identification by SUCI in response to IDENTITY REQUEST message	Rel-15		C004	NG-SS	E.04	
5.3.5	UE identification by SUCI in response to IDENTITY REQUEST message with T3519 timer expiry	Rel-15		C004	NG-SS	I.01	
5.3.6	UE identification by SUCI in response to IDENTITY REQUEST message and AUTHENTICATION REJECT	Rel-15		C004	NG-SS	I.01	
5.3.7	SUCI calculation by the ME using null scheme – missing parameters for subscription identifier privacy support by the USIM	Rel-15		C004	NG-SS	E.04	
5.3.8	UE identification by 5G-GUTI – Last Registered TAI stored on USIM	Rel-15		C004	NG-SS	E.04	
5.3.9	UE identification by 5G-GUTI – Last Registered TAI stored by ME	Rel-15		C004	NG-SS	E.04	
5.3.10	UE identification after SUPI is changed	Rel-15		C004	NG-SS	E.04	
5.3.11	SUCI calculation by ME using Profile A	Rel-15		C004	NG-SS	E.04	

Test#	Title	from Rel	to Rel (see note)	Applicability	Network Dependency	Test Option	Support
5.3.12	UE identification by SUCI during initial registration – SUCI calculation by USIM using profile A	Rel-15		C004	NG-SS	E.04	
5.3.13	SUCI calculation by ME using null scheme – no Protection Scheme Identifier provisioned in the USIM	Rel-15		C004	NG-SS	E.04	
5.3.14	SUCI calculation by ME using null scheme – no Home Network Public Key for supported protection scheme provisioned in the USIM	Rel-15		C004	NG-SS	E.04	
5.3.15	SUCI calculation by ME using null scheme with the E-UTRAN/EPC UICC	Rel-15		C004	NG-SS	I.01	
5.3.16	SUCI calculation by ME using the lower priority protection scheme when the higher priority protection scheme is not supported by the ME	Rel-15		C004	NG-SS	E.04	
5.3.17	SUCI calculation by ME using Profile B with compressed Home Network Public Key	Rel-15		C004	NG-SS	E.04	
5.4	Unified Access Control information handling for 5G-NR						
5.4.1	Unified Access Control – Access identity 0, no access identities indicated by USIM	Rel-15		C004	NG-SS	E.04	
5.4.1A	Unified Access Control – Access identity 0, no access identities indicated by USIM, Access Category 8	Rel-15		C005	NG-SS	E.04	
5.4.2	Unified Access Control – Access Identity 1 – MPS indicated by USIM	Rel-15		C004	NG-SS	E.04	
5.4.2A	Unified Access Control – Access Identity 1 – MPS indicated by USIM, Access Category 8	Rel-15		C005	NG-SS	E.04	
5.4.3	Unified Access Control – Access Identity 1 – no MPS indication by USIM and SUPI not changed	Rel-15		C004	NG-SS	E.04	
5.4.4	Unified Access Control – Access Identity 1 – no MPS indication by USIM and SUPI is changed	Rel-15		C004	NG-SS	E.04	
5.4.5	Unified Access Control – Access Identity 2 – MCS indicated by USIM	Rel-15		C004	NG-SS	E.04	
5.4.5A	Unified Access Control – Access Identity 2 – MCS indicated by USIM	Rel-15		C005	NG-SS	E.04	
5.4.6	Unified Access Control – Access Identity 2 – no MCS indication by USIM and SUPI is not changed	Rel-15		C004	NG-SS	E.04	
5.4.7	Unified Access Control – Access Identity 2 – no MCS indication by USIM and SUPI is changed	Rel-15		C004	NG-SS	E.04	
5.4.8	Unified Access Control – Access Identities 11 and 15 indicated by USIM	Rel-15		C004	NG-SS	E.04	
5.4.8A	Unified Access Control – Access Identities 11 and 15 indicated by USIM, Access Category 8	Rel-15		C005	NG-SS	E.04	
5.4.9	Unified Access Control – Access Identities 12, 13 and 14 indicated by USIM	Rel-15		C004	NG-SS	E.04	
5.4.9A	Unified Access Control – Access Identities 12, 13 and 14 indicated by USIM, Access Category 8	Rel-15		C005	NG-SS	E.04	
5.4.10	Unified Access Control – Operator-Defined Access Category	Rel-15		C004	NG-SS	E.04	
5.4.11	Unified Access Control – Operator-Defined Access Categories, no change in SUPI	Rel-15		C004	NG-SS	E.04	
5.4.12	Unified Access Control – Operator-Defined Access Categories, SUPI change	Rel-15		C004	NG-SS	E.04	
5.5	Handling of operator controlled features						
5.5.1	Display of registered 5G PLMN name from USIM	Rel-15		C006	NG-SS	I.01	
5.5.2	Display of registered 5G PLMN name from ME	Rel-15		C006	NG-SS	I.01	
5.6	Handling subscription identifier privacy for 5G - SUPI type in NAI format						
5.6.1	SUCI calculation by ME using null scheme	Rel-16		C007	NG-SS	E.07	
5.6.2	UE identification by SUCI during initial registration – SUCI calculation by USIM using profile A	Rel-16		C007	NG-SS	E.04	

Test#	Title	from Rel	to Rel (see note)	Applicability	Network Dependency	Test Option	Support
5.6.3	UE identification by SUCI during initial registration – SUCI calculation by USIM using profile B	Rel-16		C007	NG-SS	E.04	
5.6.4	UE identification after SUPI is changed	Rel-16		C007	NG-SS	E.04	
5.6.5	UE identification by SUCI during initial registration – SUCI calculation by ME using profile A	Rel-16		C007	NG-SS	E.04	
5.6.6	UE identification by SUCI during initial registration – SUCI calculation by ME using profile B	Rel-16		C007	NG-SS	E.04	
<b>6 Security related Tests</b>							
<b>6.1 PIN handling</b>							
6.1.1	Entry of PIN	Rel-13		M		E.04	
6.1.2	Change of PIN	Rel-13		M		E.04	
6.1.3	Unblock PIN	Rel-13		C008		E.04	
6.1.4	Entry of PIN2	Rel-13		C009		E.04	
6.1.5	Change of PIN2	Rel-13		C009		E.04	
6.1.6	Unblock PIN2	Rel-13		C010		E.04	
6.1.7	Replacement of PIN	Rel-13		O		E.04	
6.1.8	Change of Universal PIN	Rel-13		O		E.04	
6.1.9	Unblock Universal PIN	Rel-13		O		E.04	
6.1.10	Entry of PIN on multi-verification capable UICCs	Rel-13		O		E.04	
6.1.11	Change of PIN on multi-verification capable UICCs	Rel-13		O		E.04	
6.1.12	Unblock PIN on multi-verification capable UICCs	Rel-13		O		E.04	
6.1.13	Entry of PIN2 on multi-verification capable UICCs	Rel-13		O		E.04	
6.1.14	Change of PIN2 on multi-verification capable UICCs	Rel-13		O		E.04	
6.1.15	Unblock PIN2 on multi-verification capable UICCs	Rel-13		O		E.04	
6.1.16	Replacement of PIN with key reference "07"	Rel-13		O		E.04	
<b>7 PLMN related tests</b>							
<b>7.1 FPLMN handling</b>							
7.1.4	Adding FPLMN to the forbidden PLMN list when accessing E-UTRAN	Rel-13		C001	E-USS OR NB-SS	E.04	
7.1.5	UE updating forbidden PLMNs when accessing E-UTRAN	Rel-13		C001	E-USS OR NB-SS	E.04	
7.1.6	UE deleting forbidden PLMNs when accessing E-UTRAN	Rel-13		C001	E-USS OR NB-SS	E.04	
7.1.8	Updating the Forbidden PLMN list after receiving non-integrity protected reject message – E-UTRAN	Rel-13		C001	E-USS OR NB-SS	E.04	
<b>7.2 User controlled PLMN selector handling</b>							
7.2.1	UE updating the User controlled PLMN selector list	Rel-13		C011		E.07	
7.2.5	UE updating the User controlled PLMN selector list for E-UTRAN	Rel-13		C011 AND C012		E.07	
7.2.8	UE recognising the priority order of the User controlled PLMN selector list with the same access technology – E-UTRAN in NB-S1 mode	Rel-14		C011 AND C002	NB-SS	E.03	
7.2.9	UE recognising the priority order of the User controlled PLMN selector list using the ACT preference – E-UTRAN in WB-S1/E-UTRAN in NB-S1	Rel-14		C011 AND C012 AND C002	E_USS AND NB-SS	E.03	
<b>7.3 Operator controlled PLMN selector handling</b>							
7.3.3	UE recognising the priority order of the Operator controlled PLMN selector list when accessing E-UTRAN	Rel-13		C001	E-USS OR NB-SS	E.03	
7.3.4	UE recognising the priority order of the User controlled PLMN selector over the Operator controlled PLMN selector list – E-UTRAN	Rel-13		C001	E-USS OR NB-SS	E.03	
7.3.5	UE recognising the priority order of the Operator controlled PLMN selector list when accessing E-UTRAN in NB-S1 mode	Rel-14		C002	NB-SS	E.03	

Test#	Title	from Rel	to Rel (see note)	Applicability	Network Dependency	Test Option	Support
7.3.6	UE recognising the priority order of the User controlled PLMN selector over the Operator controlled PLMN selector list – E-UTRAN in NB-S1 mode	Rel-14		C011 AND C002	NB-SS	E.03	
7.3.7	UE recognising the priority order of the Operator controlled PLMN selector list using the ACT preference - E-UTRAN in NB-S1/ E-UTRAN in WB-S1 mode	Rel-14		C012 AND C002	E-USS AND NB-SS	E.03	
7.4	Higher priority PLMN search handling						
7.4.3	UE recognising the search period of the Higher priority PLMN – E-UTRAN	Rel-13		C001	E-USS OR NB-SS	E.03	
7.4.7	UE recognising the search period of the higher priority PLMN – NG-RAN	Rel-15		C004	NG-SS	E.03	
8	Subscription independent tests						
8.1	Phone book procedures						
8.1.2	Update of the Phonebook Synchronisation Counter (PSC)	Rel-13		C012		E.07	
8.1.3	Handling of BCD number/ SSC content extension	Rel-13		C013		E.07	
8.1.4	Phonebook selection	Rel-13		C014		E.07	
8.1.5	Local Phonebook handling	Rel-13		C012		E.07	
9	USIM service handling						
9.1	Access Point Name Control List handling						
9.1.4	Access Point Name Control List handling for UEs supporting ACL connected to E-UTRAN/EPC	Rel-13		C020	E-USS	I.01 (E.03)	
10	CSG list handling						
10.1	CSG list handling for E-UTRA						
10.1.1	Automatic CSG selection in E-UTRA with CSG list on USIM, success	Rel-13		C021	E-USS	E.04	
10.1.2	Automatic CSG selection in E-UTRA with CSG list on USIM, removal of CSG ID from the USIM	Rel-13		C021	E-USS	E.06	
10.1.3	Manual CSG selection in E-UTRA with CSG list on USIM, success	Rel-13		C022	E-USS	E.06	
10.1.4	Manual CSG selection in E-UTRA with CSG list on USIM, rejected	Rel-13		C022	E-USS	E.06	
10.1.5	CSG selection in E-UTRA with no CSG list on USIM, no IMSI change	Rel-13		C022	E-USS	I.01	
10.1.6	CSG selection in E-UTRA with no CSG list on USIM, with IMSI change	Rel-13		C022	E-USS	I.01	
10.1.7	Manual CSG selection without display restrictions in E-UTRA with ACSG list and OCSG list on USIM	Rel-13		C022	E-USS	E.04	
10.1.8	Manual CSG selection with display restrictions in E-UTRA with ACSG list and OCSG list on USIM	Rel-13		C022	E-USS	E.04	
10.2	CSG list handling for UTRA						
11	NAS security context parameter handling						
11.1	NAS security context parameter handling when service "EMM Information" is available	Rel-13		C001	E-USS OR NB-SS	E.04	
11.2	NAS security context parameter handling when service "EMM Information" is not available, no IMSI change	Rel-13		C001	E-USS OR NB-SS	E.04	
11.3	NAS security context parameter handling when service "EMM Information" is not available, IMSI changed	Rel-13		C001	E-USS OR NB-SS	E.04	
11.4	EPS NAS Security Context Storage	Rel-13		C001	E-USS OR NB-SS	E.04	
12	Non Access Stratum (NAS) Configuration parameter handling						
13	UICC interface during PSM						
13.1	UICC interface in PSM handling for E-UTRAN – No UICC deactivation in PSM	Rel-13	Rel-13	C023	E-USS OR NB-SS	see note 1	
		Rel-14					
13.2	UICC interface in PSM handling for E-UTRAN – PSM not accepted by E-USS/NB-SS	Rel-13	Rel-13	C023	E-USS OR NB-SS	see note 1	

Test#	Title	from Rel	to Rel (see note)	Applicability	Network Dependency	Test Option	Support
		Rel-14					
13.4	UICC interface in PSM for E-UTRAN – SUSPEND UICC	Rel-14		C023	E-USS OR NB-SS	see note 1	
14	UICC interface during eDRX						
14.1	UICC interface during eDRX for E-UTRAN – eDRX is not supported by the UICC	Rel-13	Rel-13	C024	E-USS OR NB-SS	see note 1	
		Rel-14					
14.2	UICC interface during eDRX for E-UTRAN – eDRX is not accepted by E-USS/NB-SS	Rel-13	Rel-13	C024	E-USS OR NB-SS	see note 1	
		Rel-14					
15	Authentication procedure and NAS security context handling for 5G						
15.1	Authentication procedure for EAP-AKA'						
15.1.1	Authentication procedure for EAP-AKA' - Authentication is successful	Rel-15	Rel-15	C004	NG-SS	E.07	
15.1A.1	Authentication procedure for EAP-AKA' - Authentication is successful	Rel-16		C004	NG-SS	E.04 (E.03)	
15.1.2	Authentication procedure for EAP-AKA' – Authentication is successful - GSM UICC	Rel-15		C004	NG-SS	I.01	
15.1.3	Authentication procedure for EAP-AKA' – AUTN fails on the USIM	Rel-15		C004	NG-SS	E.04	
15.1.4	Authentication procedure for EAP-AKA' - after SUPI is changed	Rel-15		C004	NG-SS	I.01	
15.2	Authentication procedure for 5G AKA						
15.2.1	Authentication procedure for 5G AKA - Authentication is successful	Rel-15	Rel-15	C004	NG-SS	E.04 (E.03)	
15.2A.1	Authentication procedure for 5G AKA - Authentication is successful	Rel-16		C004	NG-SS	E.04 (E.03)	
15.2.2	Authentication procedure for 5G AKA – Authentication is successful - GSM UICC	Rel-15		C004	NG-SS	I.01 (E.04)	
15.2A.2	Authentication procedure for 5G AKA – Authentication is successful	Rel-15	Rel-15	C004	NG-SS	I.01	
15.2.3	Authentication procedure 5G AKA – AUTN fails on the USIM	Rel-15		C004	NG-SS	E.04	
15.2.4	Authentication procedure for 5G AKA - after SUPI is changed	Rel-15		C004	NG-SS	I.01	
15.2.5	Authentication procedure for registrations on 3GPP access. successful 5G AKA - Authentication in different PLMNs	Rel-16		C028	NG-SS	E.04	
16	UE Route Selection Policy (URSP) procedure						
16.1	Pre-configured URSP rules						
16.1.1	Support for URSP by USIM	Rel-16		C026	NG-SS	E.04 (E.03)	
16.1.2	Support for URSP by ME	Rel-16		C026	NG-SS	E.04 (E.03)	
16.1.3	Support of Signalled URSP	Rel-16		C026	NG-SS	E.04 (E.03)	
17	CAG list handling						
17.1	CAG list handling for 5G						
17.1.1	Automatic CAG selection with preconfigured CAG list on USIM	Rel-17		C027	NG-SS	I.01	
18	NSSAA procedure with SSIM						
18.1	SSIM management procedures						
18.1.1	SSIM identification, S-NSSAI list request	Rel-18		C029	NG-SS		
18.2	SSIM commands						
18.2.1	AUTHENTICATE command, Identity EAP-Request/EAP-Response messages	Rel-18		C029	NG-SS		
18.2.2	AUTHENTICATE command, other EAP-Request/EAP-Response messages	Rel-18		C029	NG-SS		
18.2.3	AUTHENTICATE command, EAP-Success/EAP-Failure messages	Rel-18		C029	NG-SS		
NOTE:	Blank entries indicate the latest valid release at the time of publication of this specification						
NOTE 1:	Available methods are probably not sufficient. E.g. verification of electrical behaviour is needed						

Table B.2: Applicability conditions

Condition#	Info	Mnemonic
C001	IF A.1/20 OR A.1/21 OR A.1/37 THEN M ELSE N/A	-- O_eFDD OR O_eTDD OR O_NB-IoT
C002	IF A.1/37 THEN M ELSE N/A	-- O_NB-IoT
C003	IF (A.1/20 OR A.1/21) AND A.1/27 THEN M ELSE N/A	-- (O_eFDD OR O_eTDD) AND O_MULTIPLE_PDN
C004	IF A.1/43 AND A.1/44 THEN M ELSE N/A	-- O_5G_CN AND O_5G_NR
C005	IF A.1/43 AND A.1/44 AND A.1/47 THEN M ELSE N/A	-- O_5G_CN AND O_5G_NR AND O_INACTIVE
C006	IF A.1/43 AND A.1/44 AND A.1/31 THEN M ELSE N/A	-- O_5G_CN AND O_5G_NR AND O_DISPLAY
C007	IF A.1/43 AND A.1/44 AND A.1/46 THEN M ELSE N/A	-- O_5G_CN AND O_5G_NR AND O_SUPI_NAI
C008	IF A.1/19 THEN "Expected Sequence A" M ELSE "Expected Sequence B" M	-- O_PIN_MMI_STRING
C009	IF A.1/2 THEN M ELSE N/A	-- O_PIN2_ENTRY_FEAT
C010	IF A.1/2 AND A.1/19 THEN "Expected Sequence A" M ELSE N/A	-- O_PIN2_ENTRY_FEAT AND O_PIN_MMI_STRING
C011	IF A.1/17 THEN M ELSE N/A	-- O_EFPLMNwACT_NUM_ENTRY
C012	IF A.1/8 THEN M ELSE N/A	-- O_LOCAL_PB
C013	IF A.1/9 THEN M ELSE N/A	-- O_GLOBAL_PB
C014	IF A.1/8 AND A.1/9 THEN M ELSE N/A	-- O_LOCAL_PB AND O_GLOBAL_PB
C015	IF (A.1/10 AND A.1/23 AND (A.1/20 OR A.1/21)) THEN M ELSE N/A	-- O_STORE_CLASS2_SMS AND O_SM-OVER-IP_RECEIVER AND (O_eFDD OR O_eTDD)
C016	IF A.1/24 THEN M ELSE N/A	-- O_READ_USIM-EF_SMS_IF_USIM+ISIM
C017	IF A.1/11 AND A.1/13 THEN M ELSE N/A	-- O_MMS AND O_NO_USER_MMS_CONF_SELEC
C018	IF A.1/11 AND A.1/14 THEN M ELSE N/A	-- O_MMS AND O_MMS_NOTIF_STORAGE
C019	IF A.1/25 THEN M ELSE N/A	-- O_READ_ISIM-EF_SMS_IF_USIM+ISIM
C020	IF A.1/15 AND (A.1/20 OR A.1/21) THEN M ELSE N/A	-- O_ACL AND (O_eFDD OR O_eTDD)
C021	IF (A.1/20 OR A.1/21) AND A.1/22 THEN M ELSE N/A	-- (O_eFDD OR O_eTDD) AND O_CSG_LIST
C022	IF (A.1/20 OR A.1/21) AND A.1/22 AND A.1/29 THEN M ELSE N/A	-- (O_eFDD OR O_eTDD) AND O_CSG_LIST AND O_MANUAL_CSG_SELECTION
C023	IF (A.1/20 OR A.1/21 OR A.1/37) AND A.1/39 THEN M ELSE N/A	-- (O_eFDD OR O_eTDD OR O_NB-IoT) AND O_PSM_DEAC_UICC
C024	IF (A.1/20 OR A.1/21 OR A.1/37) AND A.1/40 THEN M ELSE N/A	-- (O_eFDD OR O_eTDD OR O_NB-IoT) AND O_eDRX_DEAC_UICC
C025	IF (A.1/20 OR A.1/21 OR A.1/37) AND A.1/42 THEN M ELSE N/A	-- (O_eFDD OR O_eTDD OR O_NB-IoT) AND O_eDRX_SUSPEND_UICC
C026	IF A.1/43 AND A.1/44 AND A.1/45 THEN M ELSE N/A	-- O_5G_CN AND O_5G_NR AND O_URSP_by_USIM
C027	IF A.1/43 AND A.1/44 AND A.1/49 THEN M ELSE N/A	-- O_5G_CN AND O_5G_NR AND pc_CAG
C028	IF A.1/43 AND A.1/44 AND A.1/54 THEN M ELSE N/A	-- O_5G_CN AND O_5G_NR AND O_multregs_by_USIM
C029	IF A.1/43 AND A.1/44 AND A.1/56 THEN M ELSE N/A	-- O_5G_CN AND O_5G_NR AND O_SSIM

Table B.3: Test option

Option#	Meaning	Info
I.01	Implicit verification	Only used if no explicit verification is needed within the test sequence
E.01	Explicit verification, method A.2/1 only	
E.02	Explicit verification, method A.2/2 only	
E.03	Explicit verification, method A.2/3 only	
E.04	Explicit verification, method A.2/1 or A.2/2	
E.05	Explicit verification, method A.2/1 or A.2/3	
E.06	Explicit verification, method A.2/2 or A.2/3	
E.07	Explicit verification, method A.2/1 or A.2/2 or A.2.3	

### 3.9 Rules for the representation of number systems and strings

For the representation of decimal numbers, binary numbers, hexadecimal numbers and strings in text of the present document the following rules apply:

Convention	Description
nnnnn	Decimal number, e.g.: PIN value or phone number
'b'	Single digit binary number ('0' or '1')
'bbb'/'bbb bbbb'	Multiple digit binary number, e.g.: '010' or '111 0101'
'bbbb bbbb'	8-bit binary number, e.g.: '0110 0001' (separator between MSB and LSB)
'hh'	Single octet hexadecimal number, e.g.: '2B'
'hh hh .. hh'	Multi-octet hexadecimal number, e.g.: 'FF 00 .. C3'
"SSSS"	Character string, e.g.: "FDN111"
NOTE:	Unless otherwise specified, a 'x' or 'X' present in a binary or hexadecimal number is "don't care"

In addition to the enclosing quotation marks, bit values should be clearly identifiable as such by means of additional information. E.g.: 100 (bit 5-7) or CAG only bit: 1.

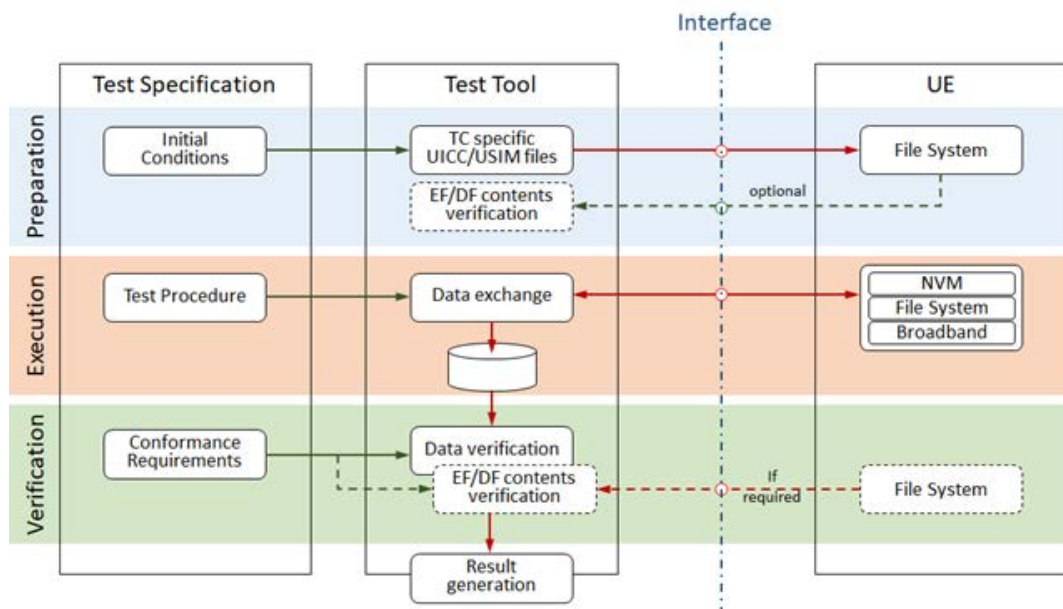
## 4 Test environment

### 4.1 Test environment description

#### 4.1.1 General test environment

Without having the UICC-Terminal interface accessible a direct verification of APDU/data timing and contents is not possible. Thus, alternative implementations and methods will be used to provide sufficient confidence in the result obtained. The present document will not specify an authoritative test environment. The following figure shows a test environment that allows the verification of test results for UEs with an integrated and not removable UICC/USIM (nrUSIM).

The present document shall provide a test environment and test methods that allow the verification of test results for UEs with an integrated and not removable UICC/USIM (nrUSIM).



**Figure 4.1: General test environment**

Figure 4.1 gives an overview on how a test case shall be executed.

Based on the identified test purpose and the related conformance requirements an appropriate test sequence is defined. The test itself can be split into three phases:

- In the preparation phase the initial set-up for the test case is performed. Test specific data is transferred to the nrUSIM. E.g. by provisioning a test specific profile.
- In the execution phase the test procedure is performed. It has to be ensured that all steps defined in the test procedure are executed and that they are executed in order. The data generated during this execution is stored in the TT and/or test EFs in the file system within the nrUICC.
- In the verification phase the data, procedures and processes identified and stored during execution are checked against given conformance requirements. A final verification of specific EF/DF contents might be required. The exchange of required data has to be ensured, even though the required data transfer is not necessarily listed in the test procedure.

### 4.1.2 Example - test environment for implicit testing

Implicit testing within the scope of the present document describes an end-to-end test method where the UICC/USIM file system of the DUT is prepared to contain specific data. During test execution the data transferred from the DUT to the TT is checked and compared to the expected result or value respectively.

Example:

- During preparation phase specific content for the  $EF_{IMSI}$  is updated in the nrUSIM;
- A registration to the network shall be executed using this value;
- The TT compares the initial value sent with the value returned during registration.

To ensure that no pre-configured value is used, the values to be verified in such a test procedure shall be generated as described in clause 4.3 of the present document.

NOTE: A test toolkit applet can be used for testing USAT specific test cases in TS 31.117 [35].

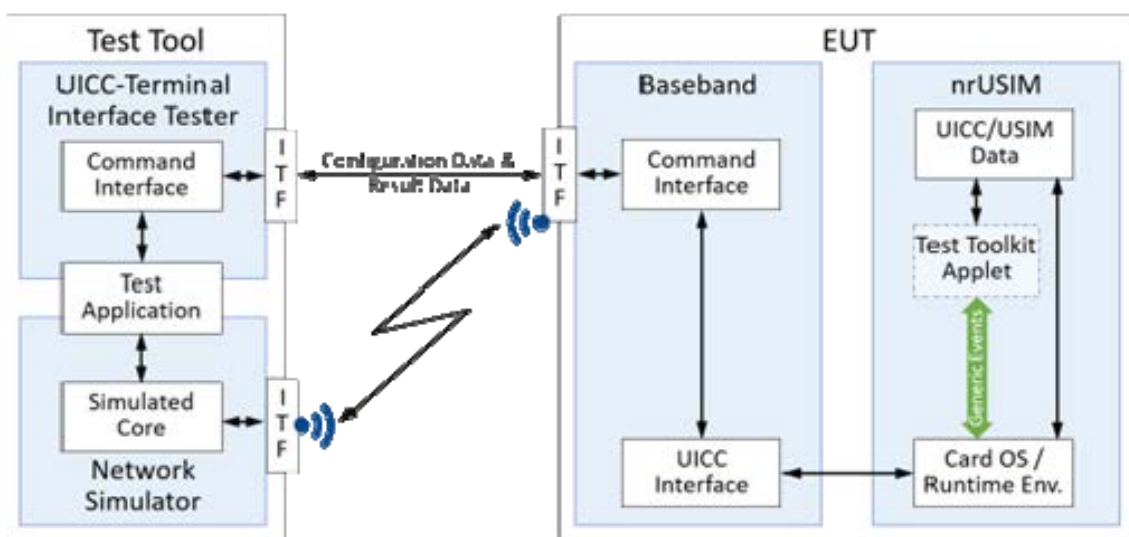


Figure 4.2: Test environment for implicit testing

### 4.1.3 Example - test environment for contents verification

Contents verification within the scope of the present document describes a procedure that allows the TT to compare contents of EFs/DFs available on the EUT with expected values defined in the present document.

Example:

- During preparation phase specific content for the  $EF_{FPLMN}$  is updated in the nrUSIM;
- During execution of the test the FPLMN value is modified;
- As the FPLMN value stored in  $EF_{FPLMN}$  is not transferred to the TT during test execution;
- The TT performs a read procedure on  $EF_{FPLMN}$  at test case end (not necessarily part of the test procedure);
- The TT compares the value read with the expected value stored in the TT.

The contents verification method described here is not applicable when a verification of EF/DF contents needs to be performed at a time other than the preparation or the verification phase.

NOTE: It is not expected that a reading procedure on EF contents can be performed whilst the test procedure is executed.

The test environment needed to perform contents verification is identical to the test environment shown for implicit testing.

#### 4.1.4 Example - test environment for seamless testing

Seamless testing within the scope of the present document relies on monitoring of data transfer between ME and nrUSIM traced by a software interface between nrUSIM and baseband implemented by the ME vendor.

The logged communication can be transferred to the TT and will be used to determine if conformance requirements are met (see example in Annex D).

NOTE: A test toolkit applet may be used for testing USAT specific test cases in TS 31.117 [35]. Refer to Annex B.1 for examples of test EFs required when using the test toolkit applet.

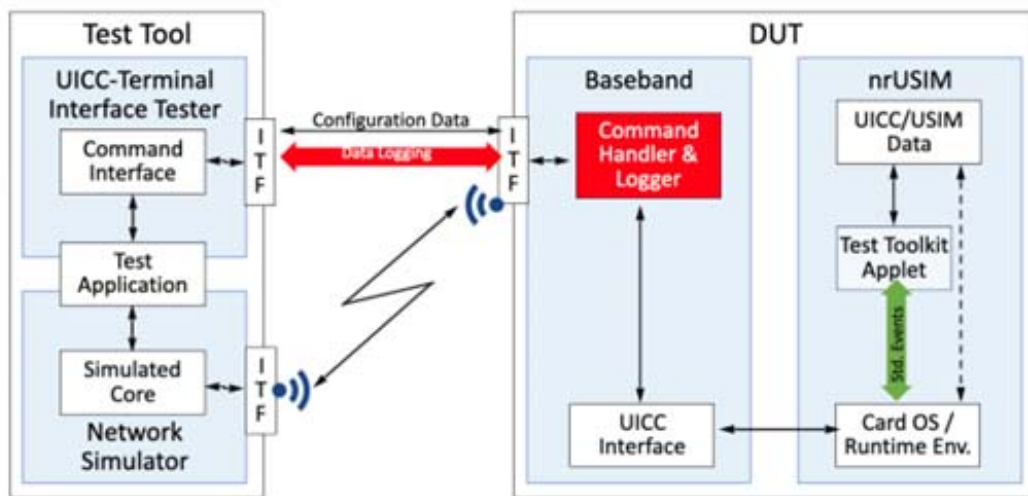


Figure 4.3: Test environment for seamless testing

#### 4.1.5 Example – test environment for test toolkit events based testing

Test toolkit events based testing within the scope of the present document is applicable for UEs supporting the required USIM application toolkit functionality. A toolkit applet is installed onto the nrUSIM, capable of handling test events internal to the card runtime environment and the applets to monitor APDUs received at the nrUICC.

NOTE: The same test toolkit applet may be used for testing USAT specific test cases in TS 31.117 [35]. Refer to Annex B.2 for examples of test EFs required when using the test toolkit applet.

The logged events can be stored in a test EF during the test execution phase and transferred to the TT during the verification phase to determine if conformance requirements are met.

ME may provide an interface for tester to monitor APDU communication during test execution through the TT.

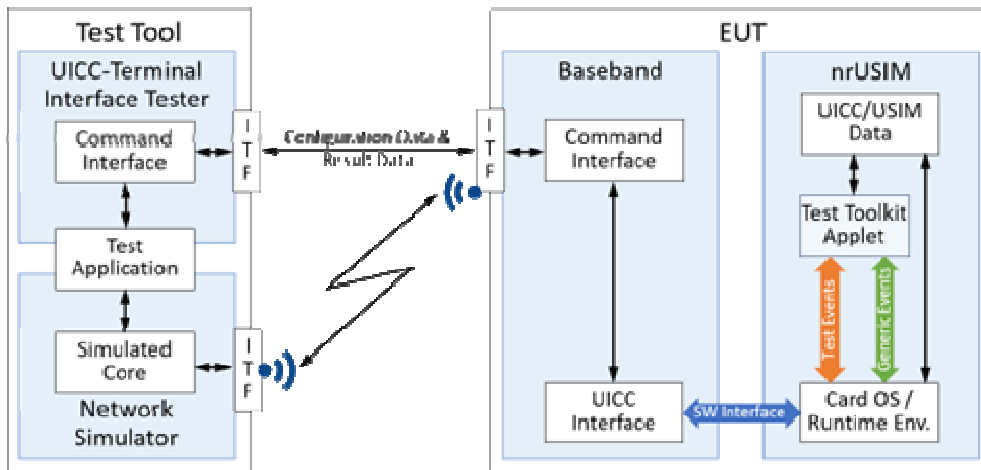


Figure 4.4: Test environment for test toolkit events based testing

Please see the required "Test configuration state" in Annex N and the "Examples of test configuration usage" in Annex O of ETSI TS 102 221 [8]

#### 4.1.6 Example – test environment for UEs with ETSI eSSP/iSSP

For testing UEs with an USIM functionality provided by an eSSP/iSSP as defined in ETSI TS 103 666-x specifications a test tool interface as defined in ETSI TS 103 834 has to be supported. For the usage within this specification the SSP test tool interface is handled like the test environment for seamless or for test toolkit event based testing. Specific execution requirements or setups may be added to this specification when required. Adaption needed to operate tests on UEs with an eSSP/iSSP, like e.g., an APDU gate are out of scope of the present document.

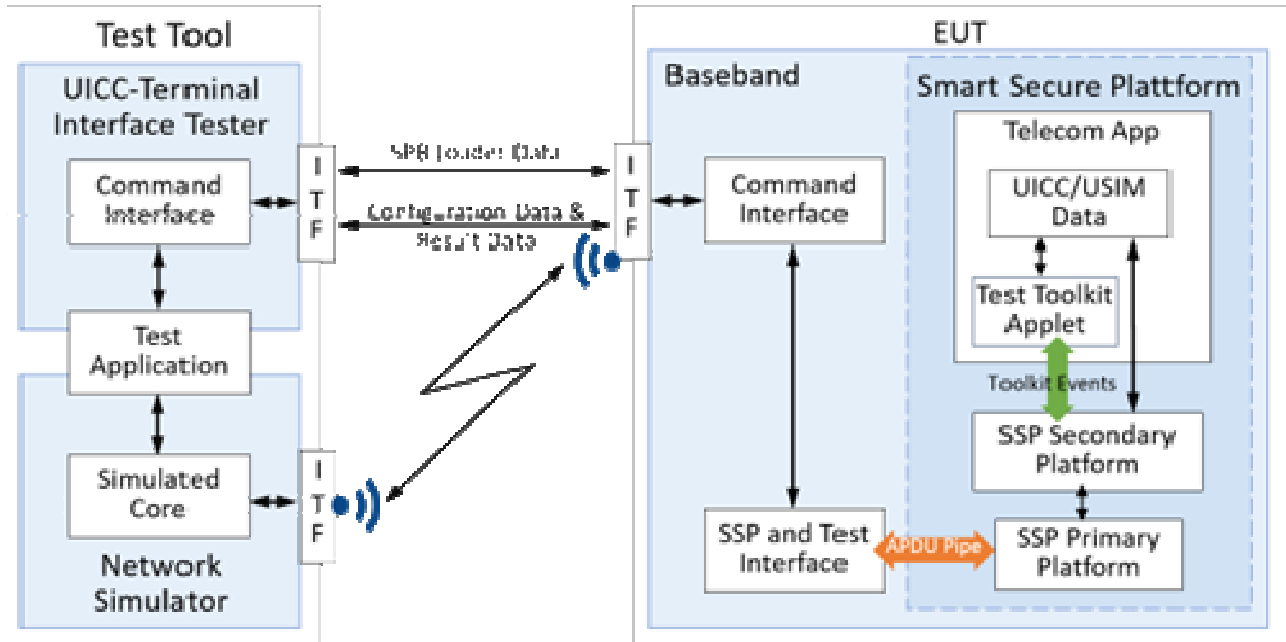


Figure 4.5: Test environment for UEs with ETSI eSSP/iSSP

## 4.2 Requirements to the EUT and the test environment

### 4.2.1 General Requirements

All tests defined in the subsequent clauses apply to UEs operating an nrUSIM, what implies that the UICC-Terminal interface cannot be exposed to a TT. Depending on the test method used, an explicit verification of APDUs or data sent via the UICC-Terminal interface might not be possible. If explicit verification of APDUs, data or file contents is needed to verify a conformance requirement the implementation and applicability has to be declared (see also clause 3.7.1).

The tests are not applicable for UEs providing a UICC-Terminal interface in accordance to interface form factors defined in ETSI TS 102 221 [8] or ETSI TS 102 671 [29].

The following sequence of tests confirms:

- a) the usage of the test specific UICC/USIM data;
- b) the correct interpretation of data read from the USIM (Universal Subscriber Identification Module) by the ME;
- c) the correct writing of data to the USIM by the ME;
- d) the initiation of appropriate procedures by the ME;
- e) the correct execution of functions

All tests apply to the USIM application on the UICC or an equivalent application implemented in accordance to the ETSI SSP specifications ETSI TS 103 666-1 [10], ETSI TS 103 666-2 [11] and ETSI TS 103 666-3 [12]

### 4.2.2 Requirements to the UE (EUT) – supported interfaces

The EUT has to support interfaces and administration methods to allow the TT or the User to set the initial conditions defined for the test cases. Where the EUT may be solely the UE or the UE connected to an interface device.

**NOTE:** The connection of the UE and an interface device is set up similar to what is described in the Companion Device scenario in GSMA SGP.22 [30], but not limited to remote SIM provisioning functionality.

#### **Suggested interfaces:**

- Wi-Fi (IEEE 802.11-2016 [13])
- USB (USB-IF, USB 2.0 or higher)

The UE has to support at least one of the following data transfer methods:

- RFM and OTA via ETSI TS 102 225 [14] and ETSI TS 102 226 [15]
- AT commands as defined in TS 27.007 [16]
- Java™Card as defined in TS 31.130 [17]

Even though the availability of at least one of the suggested interfaces and one of the suggested data transfer method is recommended, interfaces and methods for UICC/USIM preparation for testing purposes are to be provided by the UE vendor and are out of scope of the present document.

### 4.2.3 Supported RATs

UEs tested in accordance to the present document shall support any 3GPP defined RATs. Test cases defined in the present document may contain RAT or RAN specific conformance requirements and methods of test. The applicability of the individual test cases can be determined by using Table B.1.

Tests that would require 2G network access (GERAN) are out of scope of the present document.

## 4.2.4 Initial and final procedure steps

Initial and final procedure steps are out of scope of the current specification to not explicitly exclude methods that might be used to get a UE set up at test case start or to have it 'cleaned up' at the end of a test (if required).

The testing person has to ensure that the UE has installed test specific the UICC and USIM data in accordance to the definitions of the particular test (see note). The UE has to be accessible and is brought into a specific reception mode if required by the test case. It has to be ensured that interfaces that are used to verify file data or a specific functionality do not interfere or block the operation of the test procedure as defined within this specification.

For verification purposes an interaction with the UE is allowed even after ending the defined test procedure. If such interaction takes place it has to be reported to the TT. A verification of conformance requirements that is based on data or information that is generated during this post-procedure interaction has to be identifiable as a post process, but can be used for the result generation.

**NOTE:** For all EFs, DFs and ADFs building the UICC and USIM where no data is explicitly defined in the test or by reference, an appropriate test value can be used (e.g.: values from GSMA TS.48 [9]).

## 4.3 Random value generation

To ensure that the EUT provides EF values read from the UICC/USIM, identified EFs are to be used with random EF content.

If the test definition requires random test values to be used, the EF content is generated on test case initialization. An EF containing random values always is specified in the initial condition clause of the test case. At least the EF coding is showing one or more placeholders (characters x to z, highlighted in red) where a generated random value has to be inserted. To avoid ambiguities a codomain ( $D$ ) of possible values is defined for each random character.

### Example:

**EF<sub>IMSI</sub>** (International Mobile Subscriber Identity)

Logically:

24681357x

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9
Hex	05	29	64	18	53	x7	FF	FF	FF

$D: x \in \{0x0; \dots; 0x9\}$

### Explanation:

The random IMSI can become any logical value from 246813570 to 246813579.

**NOTE:** the verification method using the generated random value is described in Annex A.4

EF content randomization (e.g. last digit) is limited to the elementary files EF<sub>IMSI</sub>, EF<sub>LOCI</sub> (files), EF<sub>Routing\_Indicator</sub> and Home Network Public Key identifier in the EF<sub>SUCI\_Cal\_Info</sub> and it is done for a limited number of network-dependent test cases only.

## 4.4 Suitability assessment

### 4.4.1 Suitability assessment in present test procedures

For test procedures defined within the present document the step table holds a separate column for the "suitability assessment", abbreviated as "SA". It will show the identifier of any conformance requirement (CR) where gaining suitable verification requires the usage of an optional test method. Conformance requirements that can be verified by "implicit" methods, e.g. the usage of a specific value is sufficiently verified if the test proceeds correctly with the next step or if the expected value can be seen on the air interface, will not be listed in the SA column.

## 4.4.2 Suitability assessment in test descriptions

For each CR listed in the SA column of a test procedure available in the present document additional information about the SA shall be provided with the description of the CR verification.

Tests purposes, conformance requirements and/or procedures defined in TS 31.121 [2] may be referenced. Modifications needed to adopt a test from TS 31.121 [2] to use the random value generation for the implicit testing will not be explicitly mentioned. If it becomes necessary to add suitable test methods from Table A.2 to a particular CR this shall be done by adding the related information to the related CR in the Acceptance criteria clauses available in the present document.

## 4.4.3 Suitability assessment in the test protocol

Whenever a test is executed using additional methods to generate a result the method and the gained result shall be noted in the test protocol. If none of the indicated optional test methods is supported, it shall be clearly noted that the no verification took place. A test step to be verified by an explicit method that could not be verified has to be marked as "Inconclusive". In case any test step is marked as "Inconclusive", the overall test case verdict shall be set to "Inconclusive".

## 4.4.4 Justification of additional measures

Even if implicit verification is recognized as a suitable and appropriate verification method, additional methods to explicitly verify file contents and/or the file handling shall be used if supported. The verification result and the used verification method shall be noted in the test report. In case this additional measure leads to a deviating result, the result of the explicit check defined to this test case applies.

Conformance requirements that can be verified with such an additional measure are marked with an 'O' in the SA column. Possible optional verification methods are noted in the acceptance criteria for each test case if applicable.

# 4.5 Definition of default values

## 4.5.1 Introduction

### 4.5.1.1 Installation, provisioning or modification methods for EFs and DFs

Installation, provisioning or modification methods for EFs and DFs defined in the UICCs/USIMs used for testing or in the test cases are out of scope of the present document. Respective methods have to be provided by the UE vendor.

### 4.5.1.2 TS.48 Version and usage

Unless stated differently in the test description or in the specific UICC definition TS.48 eSIM GTP v5.0 is used

The usage of file values defined in GSMA TS.48 [9] does not imply that remote SIM provisioning as defined in GSMA or profiles as defined by the TCA have to be supported by the nrUSIM.

## 4.5.2 Definition of the Default UICC

The Default UICC for the present document is build from TS.48 eSIM GTP referenced in clause 4.5.1.2 with the following exceptions:

### EF<sub>AD</sub> (Administrative Data)

Logically:

Mode of operation:	normal operation
Additional information:	ciphering indicator feature disabled
Length of MNC in the IMSI:	3 digit

Coding:

Byte	B1	B2	B3	B4
Hex	00	00	00	03

**EF<sub>UST</sub>** (USIM Service Table)

Logically:

Service n°1:	Local Phone Book	available
Service n°2:	Fixed Dialling Numbers (FDN)	available
Service n°6:	Barred Dialling Numbers (BDN)	available
Service n°17:	Group Identifier Level 1	not available
Service n°18:	Group Identifier Level 2	not available
Service n°20:	User controlled PLMN selector with Access Technology	available
Service n°27:	GSM Access	available
Service n°33:	shall be set to '1'	available
Service n°34:	Enabled Services Table	available
Service n°85:	EPS Mobility Management Information	available
Service n°86:	Allowed CSG Lists and corresponding indications	available

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Binary	xx1x xx11	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxxx xxxx	xxxx xxxx	xxxx xxxx
	B9	B10	B11	B12				
	xxxx xxxx	xxxx xxxx	xx11 xxxx	0000 0xxx				

### 4.5.3 Definition of FDN UICC

The values of the FDN UICC are identical to the values of the Default UICC defined in clause 4.5.2 of the present document with the following exceptions:

**EF<sub>EST</sub>** (Enable Service Table)

Logically:

Service n°1:	Fixed Dialling Numbers (FDN)	activated
Service n°2:	Barred Dialling Numbers (BDN)	deactivated
Service n°3:	APN Control List (ACL)	deactivated

Coding:

Byte:	B1
Binary	xxxx x001

**EF<sub>FDN</sub>** (Fixed Dialling Numbers)

Logically:

Record 1:

Length of alpha identifier:	6 characters;
Alpha identifier:	"FDN111";
Length of BCD number:	6 bytes;
TON and NPI:	Telephony and International;
Dialled number:	+1357924680;
CCI2:	None;
Ext2:	None.

Coding for record 1:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	46	44	4E	31	31	31	06	91	31	75	29	64
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>				
	08	FF	FF	FF	FF	FF	FF	FF				

Record 2:

Length of alpha identifier: 6 characters;  
 Alpha identifier: "FDN222";  
 Length of BCD number: 4 bytes;  
 TON and NPI: Telephony and International;  
 Dialed number: 24680;  
 CCI2: None;  
 Ext2: None.

Coding for record 2:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	46	44	4E	32	32	32	04	81	42	86	F0	FF
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>				
	FF	FF	FF	FF	FF	FF	FF	FF				

Record 3:

Length of alpha identifier: 6 characters;  
 Alpha identifier: "FDN333";  
 Length of BCD number: 11 bytes;  
 TON and NPI: Telephony and International;  
 Dialed number: +12345678901234567890;  
 CCI2: None;  
 Ext2: None.

Coding for record 3:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	46	44	4E	33	33	33	0B	91	21	43	65	87
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>				
	09	21	43	65	87	09	FF	FF				

#### EF<sub>ECC</sub> (Emergency Call Codes)

Logically:

Emergency call code: 122;  
 Emergency call code alpha identifier: "TEST";  
 Emergency call Service Category: Mountain Rescue.

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	21	F2	FF	54	45	53	54	10

EF/DF definitions provided in the Initial condition clause of a test case/test sequence take precedence over values defined as default.

#### 4.5.4 Definition of E-UTRAN/EPC UICC

The values of the E-UTRAN/EPC UICC are identical to the values of the Default UICC defined in clause 4.5.2 of the present document with the following exceptions:

#### EF<sub>UST</sub> (USIM Service Table)

Logically:

Allow services up to Service n°120

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Binary	xx1x xx11	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxxx xxxx	xxxx xxxx	xxxx xxxx
	<b>B9</b>	<b>B10</b>	<b>B11</b>	<b>B12</b>	<b>B13</b>	<b>B14</b>	<b>B15</b>	
	xxxx xxxx	xxxx xxxx	xx11 xxxx	xxxx xxxx	xxxx xxxx	xxxx xxxx	xxxx xxxx	

**EF**<sub>EPSLOC</sub>I (EPS Location Information)

Logically:

GUTI: 24608100010266431122

Last visited registered TAI: 246/081/0001

EPS update status: not updated

Coding:

Byte:	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex:	0B	F6	42	16	80	00	01	02	66	43	11	22
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>						
	42	16	80	00	01	01						

**EF**<sub>PLMN<sub>WACT</sub></sub> (User Controlled PLMN Selector with Access Technology) is configured as defined in TS 31.121 [2] clause 4.8.3

**EF**<sub>OPLMN<sub>WACT</sub></sub> (Operator Controlled PLMN Selector with Access Technology) is configured as defined in TS 31.121 [2] clause 4.8.4

**EF**<sub>ACSGL</sub> (Allowed CSG Lists) is configured as defined in TS 31.121 [2] clause 4.8.5

**EF**<sub>CSGT</sub> (CSG Type) is configured as defined in TS 31.121 [2] clause 4.8.6

**EF**<sub>HNB</sub>N (Home (e)NodeB Name) is configured as defined in TS 31.121 [2] clause 4.8.7

**EF**<sub>EPSNSC</sub> (EPS NAS Security Context) is configured as defined in TS 31.121 [2] clause 4.8.8

**EF**<sub>NASCONFIG</sub> (Non Access Stratum Configuration) is configured as defined in TS 31.121 [2] clause 4.8.9

EF/DF definitions provided in the Initial condition clause of a test case/test sequence take precedence over values defined as default.

## 4.5.5 Definition of E-UTRAN/EPC ISIM-UICC

The E-UTRAN/EPC ISIM-UICC shall contain a USIM as defined in clause 4.5.4 of the present document and an ISIM for IMS access as defined in TS 31.121 [2], clause 4.5.3.

EF/DF definitions provided in the Initial condition clause of a test case/test sequence take precedence over values defined as default.

## 4.5.6 Definition of ACSGL/OCSGL E-UTRAN/EPC UICC

The values of the ACSGL/OCSGL E-UTRAN/EPC UICC are identical to the values of the Default UICC defined in clause 4.5.2 of the present document with the following exceptions:

**EF**<sub>UST</sub> (USIM Service Table)

Logically:

Service n°90:	Operator CSG Lists and corresponding indications	available
Service n°92:	Support of CSG Display Control	available

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Binary	xx1x xx11	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxxx xxxx	xxxx xxxx	xxxx xxxx
	B9	B10	B11	B12				
	xxxx xxxx	xxxx xxxx	xx11 xxxx	0000 1x1x				

**EF<sub>AD</sub>** (Administrative Data)

Logically:

Mode of operation: normal operation  
 Additional information: ciphering indicator feature disabled  
 all available CSGs can be displayed without any restriction (b2)  
 Length of MNC in the IMSI: 3 digit

Coding:

Byte	B1	B2	B3	B4
Hex	00	00	00	03

**EF<sub>OC</sub>SGL** (Operator CSG Lists)

For testing 2 CSG lists are defined and stored together in record one.

Logically:

1<sup>st</sup> CSG list

PLMN: 246 081 (MCC MNC)  
 1<sup>st</sup> CSG list 1<sup>st</sup> CSG Type indication 01  
 1<sup>st</sup> CSG list 1<sup>st</sup> CSG HNB Name indication 01  
 1<sup>st</sup> CSG list 1<sup>st</sup> CSG CSG ID: 01 (27bit)  
 1<sup>st</sup> CSG list 2<sup>nd</sup> CSG Type indication 05  
 1<sup>st</sup> CSG list 2<sup>nd</sup> CSG HNB Name indication 05  
 1<sup>st</sup> CSG list 2<sup>nd</sup> CSG CSG ID: 05 (27bit)  
 CSG display indicator: All available CSG IDs can be displayed during a manual CSGselection 00

2<sup>nd</sup> CSG list

PLMN: 244 081 (MCC MNC)  
 2<sup>nd</sup> CSG list 1<sup>st</sup> CSG Type indication 07  
 2<sup>nd</sup> CSG list 1<sup>st</sup> CSG HNB Name indication 07  
 2<sup>nd</sup> CSG list 1<sup>st</sup> CSG CSG ID: 07 (27bit)  
 CSG display indicator: All available CSG IDs can be displayed during a manual CSGselection 00

Coding:

Byte	B01	B02	B03	B04	B05	B06	B07	B08	B09	B10	B11	B12
Hex	A0	18	80	03	42	16	80	81	06	01	01	00
	B13	B14	B15	B16	B17	B18	B19	B20	B21	B22	B23	B24
	00	00	3F	81	06	05	05	00	00	00	BF	82
	B25	B26	B27	B28	B29	B30	B31	B32	B33	B34	B35	B36
	01	00	A0	10	80	03	42	14	80	81	06	07
	B37	B38	B39	B40	B41	B42	B43	B44				
	07	00	00	00	FF	82	01	00				

**E**F<sub>OCST</sub> (Operator CSG Type)

Record 1:

Logically: OMode ONE

Coding:

Byte	B01	B02	B03	B04	B05	B06	B07	B08	B09	B10	B11	B12
Hex	89	13	80	00	4F	00	4D	00	6F	00	64	00
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	65	00	20	00	4F	00	4E	00	45	FF	FF	FF
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>						
	FF	FF	FF	FF	FF	FF						

Record 2:

Logically: OMode TWO

Coding:

Byte	B01	B02	B03	B04	B05	B06	B07	B08	B09	B10	B11	B12
Hex	89	13	80	00	4F	00	4D	00	6F	00	64	00
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	65	00	20	00	54	00	57	00	4F	FF	FF	FF
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>						
	FF	FF	FF	FF	FF	FF						

Record 3:

Logically: OMode THREE

Coding:

Byte	B01	B02	B03	B04	B05	B06	B07	B08	B09	B10	B11	B12
Hex	89	17	80	00	4F	00	4D	00	6F	00	64	00
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	65	00	20	00	54	00	48	00	52	00	45	00
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>						
	45	FF	FF	FF	FF	FF						

Record 4:

Logically: OMode FOUR

Coding:

Byte	B01	B02	B03	B04	B05	B06	B07	B08	B09	B10	B11	B12
Hex	89	15	80	00	4F	00	4D	00	6F	00	64	00
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	65	00	20	00	46	00	4F	00	55	00	52	FF
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>						
	FF	FF	FF	FF	FF	FF						

Record 5:

Logically: Group FIVE

Coding:

Byte	B01	B02	B03	B04	B05	B06	B07	B08	B09	B10	B11	B12
Hex	89	15	80	00	47	00	72	00	6F	00	75	00
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	70	00	20	00	46	00	49	00	56	00	45	FF
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>						
	FF	FF	FF	FF	FF	FF						

Record 6:

Logically: Group SIX

Coding:

Byte	B01	B02	B03	B04	B05	B06	B07	B08	B09	B10	B11	B12
Hex	89	13	80	00	47	00	72	00	6F	00	75	00
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	70	00	20	00	53	00	49	00	58	FF	FF	FF
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>						
	FF	FF	FF	FF	FF	FF						

Record 7:

Logically: Group SEVEN

Coding:

Byte	B01	B02	B03	B04	B05	B06	B07	B08	B09	B10	B11	B12
Hex	89	17	80	00	47	00	72	00	6F	00	75	00
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	70	00	20	00	53	00	45	00	56	00	45	00
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>						
	4E	FF	FF	FF	FF	FF						

Record 8:

Logically: Group EIGHT

Coding:

Byte	B01	B02	B03	B04	B05	B06	B07	B08	B09	B10	B11	B12
Hex	89	17	80	00	47	00	72	00	6F	00	75	00
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	70	00	20	00	45	00	49	00	47	00	48	00
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>						
	54	FF	FF	FF	FF	FF						

All other records are empty.

**EF<sub>OHNB</sub>** (Operator Home (e)NodeB Name)

Record 1:

Logically: Home ONE

Coding:

Byte	B01	B02	B03	B04	B05	B06	B07	B08	B09	B10	B11	B12
Hex	80	11	80	00	48	00	6F	00	6D	00	65	00
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	20	00	4F	00	4E	00	45	FF	FF	FF	FF	FF
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>						
	FF	FF	FF	FF	FF	FF						

Record 2:

Logically: Home TWO

Coding:

Byte	B01	B02	B03	B04	B05	B06	B07	B08	B09	B10	B11	B12
Hex	80	11	80	00	48	00	6F	00	6D	00	65	00
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	20	00	54	00	57	00	4F	FF	FF	FF	FF	FF
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>						
	FF	FF	FF	FF	FF	FF						

Record 3:

Logically: Home THREE

Coding:

Byte	B01	B02	B03	B04	B05	B06	B07	B08	B09	B10	B11	B12
Hex	80	15	80	00	48	00	6F	00	6D	00	65	00
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	20	00	54	00	48	00	52	00	45	00	45	FF
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>						
	FF	FF	FF	FF	FF	FF						

Record 4:

Logically: Home FOUR

Coding:

Byte	B01	B02	B03	B04	B05	B06	B07	B08	B09	B10	B11	B12
Hex	80	13	80	00	48	00	6F	00	6D	00	65	00
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	20	00	46	00	4F	00	55	00	52	FF	FF	FF
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>						
	FF	FF	FF	FF	FF	FF						

Record 5:

Logically: Home FIVE

Coding:

Byte	B01	B02	B03	B04	B05	B06	B07	B08	B09	B10	B11	B12
Hex	80	13	80	00	48	00	6F	00	6D	00	65	00
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	20	00	46	00	49	00	56	00	45	FF	FF	FF
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>						
	FF	FF	FF	FF	FF	FF						

Record 6:

Logically: Home SIX

Coding:

Byte	B01	B02	B03	B04	B05	B06	B07	B08	B09	B10	B11	B12
Hex	80	11	80	00	48	00	6F	00	6D	00	65	00
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	20	00	53	00	49	00	58	FF	FF	FF	FF	FF
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>						
	FF	FF	FF	FF	FF	FF						

Record 7:

Logically: Home SEVEN

Coding:

Byte	B01	B02	B03	B04	B05	B06	B07	B08	B09	B10	B11	B12
Hex	80	15	80	00	48	00	6F	00	6D	00	65	00
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	20	00	53	00	45	00	56	00	45	00	4E	FF
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>						
	FF	FF	FF	FF	FF	FF						

Record 8:

Logically: Home EIGHT

Coding:

Byte	B01	B02	B03	B04	B05	B06	B07	B08	B09	B10	B11	B12
Hex	80	15	80	00	48	00	6F	00	6D	00	65	00
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	20	00	45	00	49	00	47	00	48	00	54	FF
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>						
	FF	FF	FF	FF	FF	FF						

EF/DF definitions provided in the Initial condition clause of a test case/test sequence take precedence over values defined as default.

## 4.5.7 Definition of Non-Access Stratum Configuration UICC

In general, the values of the Non-Access Stratum Configuration UICC are identical to the values of the Default UICC. Non-Access Stratum Configuration UICC specific configurations, as defined in TS 31.121 [2], clause 4.7 apply.

EF/DF definitions provided in the Initial condition clause of a test case/test sequence take precedence over values defined as default.

## 4.5.8 Definition of Non-Access Stratum Configuration of E-UTRAN/EPC UICC

In general, the values of the Non-Access Stratum Configuration of E-UTRAN/EPC UICC are identical to the values of the Default UICC. Non-Access Stratum Configuration of E-UTRAN/EPC UICC specific configurations, as defined in TS 31.121 [2], clause 4.8 apply.

EF/DF definitions provided in the Initial condition clause of a test case/test sequence take precedence over values defined as default.

## 4.5.9 Definition of 5G-NR UICC

The values of the 5G-NR UICC are identical to the values of the Default UICC defined in clause 4.5.2 of the present document with the following exceptions:

**EF<sub>UST</sub>** (USIM Service Table)

Logically:

Allow services up to Service n°131

Service n°122:	5GS Mobility Management Information	available
Service n°123:	5G Security Parameters	available
Service n°124:	Subscription identifier privacy support	available

Service n°125: SUCI calculation by the USIM not available

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Binary:	xx1x xx11	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxxx xxxx	xxxx xxxx	xxxx xxxx
	<b>B9</b>	<b>B10</b>	<b>B11</b>	...	<b>B16</b>	<b>B17</b>		
	xxxx xxxx	xxxx xxxx	xx11 xxxx	...	xxx0 111x	0000 0xxx		

**EF<sub>5GS3GPPLOC1</sub>** (5GS 3GPP location information)

Logically:

5G-GUTI: FF FF FF FF FF FF FF FF FF FF

TAI: 246 081 000000

5GS update status: 5U2 NOT UPDATED

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	FF	FF	FF	FF	FF	FF	FF	FF
	<b>B9</b>	<b>B10</b>	<b>B11</b>	<b>B12</b>	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>
	FF	FF	FF	FF	FF	42	16	80
	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>				
	00	00	00	01				

**EF<sub>SUCI\_Calc\_Info</sub>** (Subscription Concealed Identifier Calculation Information EF)

Logically:

Protection Scheme Identifier List data object

Protection Scheme Identifier 1 – ECIES scheme profile B

Key Index 1: 1

Protection Scheme Identifier 2 – ECIES scheme profile A

Key Index 2: 2

Protection Scheme Identifier 3 – null-scheme

Key Index 3: 0

Home Network Public Key List data object

Home Network Public Key 1 Identifier: 27

Home Network Public Key 1:

- 04 72 DA 71 97 62 34 CE 83 3A 69 07 42 58 67 B8 2E 07 4D 44 EF 90 7D FB 4B 3E 21 C1 C2 25 6E BC D1 5A 7D ED 52 FC BB 09 7A 4E D2 50 E0 36 C7 B9 C8 C7 00 4C 4E ED C4 F0 68 CD 7B F8 D3 F9 00 E3 B4

Home Network Public Key 2 Identifier: 30

Home Network Public Key 2:

- 5A 8D 38 86 48 20 19 7C 33 94 B9 26 13 B2 0B 91 63 3C BD 89 71 19 27 3B F8 E4 A6 F4 EE C0 A6 50

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
------	----	----	----	----	----	----	----	----

Hex	A0	06	02	01	01	02	00	00
	<b>B9</b>	<b>B10</b>	<b>B11</b>	<b>B12</b>	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>
	A1	6B	80	01	1B	81	41	04
	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	72	DA	71	97	62	34	CE	83
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>	<b>B31</b>	<b>B32</b>
	3A	69	07	42	58	67	B8	2E
	<b>B33</b>	<b>B34</b>	<b>B35</b>	<b>B36</b>	<b>B37</b>	<b>B38</b>	<b>B39</b>	<b>B40</b>
	07	4D	44	EF	90	7D	FB	4B
	<b>B41</b>	<b>B42</b>	<b>B43</b>	<b>B44</b>	<b>B45</b>	<b>B46</b>	<b>B47</b>	<b>B48</b>
	3E	21	C1	C2	25	6E	BC	D1
	<b>B49</b>	<b>B50</b>	<b>B51</b>	<b>B52</b>	<b>B53</b>	<b>B54</b>	<b>B55</b>	<b>B56</b>
	5A	7D	ED	52	FC	BB	09	7A
	<b>B57</b>	<b>B58</b>	<b>B59</b>	<b>B60</b>	<b>B61</b>	<b>B62</b>	<b>B63</b>	<b>B64</b>
	4E	D2	50	E0	36	C7	B9	C8
	<b>B65</b>	<b>B66</b>	<b>B67</b>	<b>B68</b>	<b>B69</b>	<b>B70</b>	<b>B71</b>	<b>B72</b>
	C7	00	4C	4E	ED	C4	F0	68
	<b>B73</b>	<b>B74</b>	<b>B75</b>	<b>B76</b>	<b>B77</b>	<b>B78</b>	<b>B79</b>	<b>B80</b>
	CD	7B	F8	D3	F9	00	E3	B4
	<b>B81</b>	<b>B82</b>	<b>B83</b>	<b>B84</b>	<b>B85</b>	<b>B86</b>	<b>B87</b>	<b>B88</b>
	80	01	1E	81	20	5A	8D	38
	<b>B89</b>	<b>B90</b>	<b>B91</b>	<b>B92</b>	<b>B93</b>	<b>B94</b>	<b>B95</b>	<b>B96</b>
	86	48	20	19	7C	33	94	B9
	<b>B97</b>	<b>B98</b>	<b>B99</b>	<b>B100</b>	<b>B101</b>	<b>B102</b>	<b>B103</b>	<b>B104</b>
	26	13	B2	0B	91	63	3C	BD
	<b>B105</b>	<b>B106</b>	<b>B107</b>	<b>B108</b>	<b>B109</b>	<b>B110</b>	<b>B111</b>	<b>B112</b>
	89	71	19	27	3B	F8	E4	A6
	<b>B113</b>	<b>B114</b>	<b>B115</b>	<b>B116</b>	<b>B117</b>			
	F4	EE	C0	A6	50			

**EF<sub>Routing\_Indicator</sub>** (Routing Indicator EF)

Logically:

Routing Indicator: 17

Coding:

Byte	B1	B2	B3	B4
Hex	71	FF	00	00

**EF<sub>5GS3GPPNSC</sub>** (5GS 3GPP Access NAS Security Context)

This file shall be available.

Logically:

ngKSI: '07'(no key available)  
 K<sub>AMF</sub>: 32 byte key, any value  
 Uplink NAS count: '00'  
 Downlink NAS count: '01'  
 Identifiers of selected NAS integrity  
 and encryption algorithms: '01'  
 Identifiers of selected EPS NAS  
 integrity and encryption algorithms  
 for use after mobility to EPS: '01'

Coding:

Byte:	B1	B2	B3	B4	B5	B6	B7	B8	...	B39
Hex	A0	37	80	01	07	81	20	xx	...	xx
	<b>B40</b>	<b>B41</b>	<b>B42</b>	<b>B43</b>	<b>B44</b>	<b>B45</b>	<b>B46</b>	<b>B47</b>	<b>B48</b>	<b>B49</b>
	82	04	00	00	00	00	83	04	00	00
	<b>B50</b>	<b>B51</b>	<b>B52</b>	<b>B53</b>	<b>B54</b>	<b>B55</b>	<b>B56</b>	<b>B57</b>		
	00	01	84	01	01	85	01	01		

**EF<sub>5GSN3GPPNSC</sub>** (5GS non-3GPP Access NAS Security Context)

This file shall be available.

Logically:

ngKSI: '07'(no key available)  
 K<sub>AMF</sub>: 32 byte key, any value  
 Uplink NAS count: '00'  
 Downlink NAS count: '01'  
 Identifiers of selected NAS integrity  
 and encryption algorithms: '01'  
 Identifiers of selected EPS NAS  
 integrity and encryption algorithms  
 for use after mobility to EPS: '01'

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	...	B39
Hex	A0	37	80	01	07	81	20	xx	...	xx
	<b>B40</b>	<b>B41</b>	<b>B42</b>	<b>B43</b>	<b>B44</b>	<b>B45</b>	<b>B46</b>	<b>B47</b>	<b>B48</b>	<b>B49</b>
	82	04	00	00	00	00	83	04	00	00
	<b>B50</b>	<b>B51</b>	<b>B52</b>	<b>B53</b>	<b>B54</b>	<b>B55</b>	<b>B56</b>	<b>B57</b>		
	00	01	84	01	01	85	01	01		

EF/DF definitions provided in the Initial condition clause of a test case/test sequence take precedence over values defined as default.

#### 4.5.10 Definition of 5G-NR UICC – non-IMSI SUPI Type

The values of the 5G-NR UICC – non-IMSI SUPI Type are identical to the values of the 5G-NR UICC defined in clause 4.5.9 of the present document with the following exceptions:

**EF<sub>AD</sub>** (Administrative Data)

Logically:

Mode of operation: normal operation  
 Additional information: ciphering indicator feature disabled  
 Length of MNC in the IMSI: 0

Coding:

Byte	B1	B2	B3	B4
Hex	00	00	00	00

**EF<sub>FUST</sub>** (USIM Service Table)

Logically:

Service n°130: Support for SUPI of type NSI or GLI or GCI available

Coding:

<b>Byte:</b>	<b>B1</b>	<b>B2</b>	<b>B3</b>	<b>B4</b>	<b>B5</b>	<b>B6</b>	<b>B7</b>	<b>B8</b>
Binary:	xx1x xx11	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxxx xxxx	xxxx xxxx	xxxx xxxx
	<b>B9</b>	<b>B10</b>	<b>B11</b>	...	<b>B16</b>	<b>B17</b>		
	xxxx xxxx	xxxx xxxx	xx11 xxxx	...	xxx0 111x	0000 0x1x		

**EF<sub>IMSI</sub>** (IMSI)

This file shall **not** be available.

**EF<sub>SUPI\_NAI</sub>** (SUPI as Network Access Identifier)

This file shall be available.

Logically: 00-00-5E-00-53-00@5gc.mnc012.mcc345.3gppnetwork.org

SUPI Type: GCI

Username: 00-00-5E-00-53-00

Realm: 5gc.mnc012.mcc345.3gppnetwork.org

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	82	33	30	30	2D	30	30	2D
	<b>B9</b>	<b>B10</b>	<b>B11</b>	<b>B12</b>	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>
	35	45	2D	30	30	2D	35	33
	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	2D	30	30	40	35	67	63	2E
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>	<b>B31</b>	<b>B32</b>
	6D	6E	63	30	31	32	2E	6D
	<b>B33</b>	<b>B34</b>	<b>B35</b>	<b>B36</b>	<b>B37</b>	<b>B38</b>	<b>B39</b>	<b>B40</b>
	63	63	33	34	35	2E	33	67
	<b>B41</b>	<b>B42</b>	<b>B43</b>	<b>B44</b>	<b>B45</b>	<b>B46</b>	<b>B47</b>	<b>B48</b>
	70	70	6E	65	74	77	6F	72
	<b>B49</b>	<b>B50</b>	<b>B51</b>	<b>B52</b>	<b>B53</b>			
	6B	2E	6F	72	67			

**EF<sub>SUCI\_Calc\_Info</sub>** (Subscription Concealed Identifier Calculation Information EF)

Logically:

Protection Scheme Identifier List data object

Protection Scheme Identifier 1 – ECIES scheme profile B

Key Index 1: 1

Protection Scheme Identifier 2 – ECIES scheme profile A

Key Index 2: 2

Protection Scheme Identifier 3 – null-scheme

Key Index 3: 0

Home Network Public Key List data object

Home Network Public Key 1 Identifier: 27

Home Network Public Key 1:

- 04 72 DA 71 97 62 34 CE 83 3A 69 07 42 58 67 B8 2E 07 4D 44 EF 90 7D FB 4B 3E 21 C1 C2 25 6E BC D1 5A 7D ED 52 FC BB 09 7A 4E D2 50 E0 36 C7 B9 C8 C7 00 4C 4E ED C4 F0 68 CD 7B F8 D3 F9 00 E3 B4

Home Network Public Key 2 Identifier: 30

Home Network Public Key 2:

- 5A 8D 38 86 48 20 19 7C 33 94 B9 26 13 B2 0B 91 63 3C BD 89 71 19 27 3B F8 E4 A6 F4 EE C0 A6 50

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	A0	06	02	01	01	02	00	00
	<b>B9</b>	<b>B10</b>	<b>B11</b>	<b>B12</b>	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>
	A1	6B	80	01	1B	81	41	04
	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	72	DA	71	97	62	34	CE	83
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>	<b>B31</b>	<b>B32</b>
	3A	69	07	42	58	67	B8	2E
	<b>B33</b>	<b>B34</b>	<b>B35</b>	<b>B36</b>	<b>B37</b>	<b>B38</b>	<b>B39</b>	<b>B40</b>
	07	4D	44	EF	90	7D	FB	4B
	<b>B41</b>	<b>B42</b>	<b>B43</b>	<b>B44</b>	<b>B45</b>	<b>B46</b>	<b>B47</b>	<b>B48</b>
	3E	21	C1	C2	25	6E	BC	D1
	<b>B49</b>	<b>B50</b>	<b>B51</b>	<b>B52</b>	<b>B53</b>	<b>B54</b>	<b>B55</b>	<b>B56</b>
	5A	7D	ED	52	FC	BB	09	7A
	<b>B57</b>	<b>B58</b>	<b>B59</b>	<b>B60</b>	<b>B61</b>	<b>B62</b>	<b>B63</b>	<b>B64</b>
	4E	D2	50	E0	36	C7	B9	C8
	<b>B65</b>	<b>B66</b>	<b>B67</b>	<b>B68</b>	<b>B69</b>	<b>B70</b>	<b>B71</b>	<b>B72</b>
	C7	00	4C	4E	ED	C4	F0	68
	<b>B73</b>	<b>B74</b>	<b>B75</b>	<b>B76</b>	<b>B77</b>	<b>B78</b>	<b>B79</b>	<b>B80</b>
	CD	7B	F8	D3	F9	00	E3	B4
	<b>B81</b>	<b>B82</b>	<b>B83</b>	<b>B84</b>	<b>B85</b>	<b>B86</b>	<b>B87</b>	<b>B88</b>
	80	01	1E	81	20	5A	8D	38
	<b>B89</b>	<b>B90</b>	<b>B91</b>	<b>B92</b>	<b>B93</b>	<b>B94</b>	<b>B95</b>	<b>B96</b>
	86	48	20	19	7C	33	94	B9
	<b>B97</b>	<b>B98</b>	<b>B99</b>	<b>B100</b>	<b>B101</b>	<b>B102</b>	<b>B103</b>	<b>B104</b>
	26	13	B2	0B	91	63	3C	BD
	<b>B105</b>	<b>B106</b>	<b>B107</b>	<b>B108</b>	<b>B109</b>	<b>B110</b>	<b>B111</b>	<b>B112</b>
	89	71	19	27	3B	F8	E4	A6
	<b>B113</b>	<b>B114</b>	<b>B115</b>	<b>B116</b>	<b>B117</b>			
	F4	EE	C0	A6	50			

EF/DF definitions provided in the Initial condition clause of a test case/test sequence take precedence over values defined as default.

#### 4.5.11 Definition of 5G-NR UICC – support of Rel-16 features

The values of the 5G-NR UICC – support of Rel-16 features are identical to the values of the 5G-NR UICC defined in clause 4.5.9 of the present document with the following exceptions:

**EF<sub>UST</sub>** (USIM Service Table)

Logically:

Allow services up to Service n°136

Service n°133:	5G Security Parameters extended	available
Service n°136	Support for multiple records of NAS security context storage for multiple registration	available

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Binary:	xx1x xx11	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxxx xxxx	xxxx xxxx	xxxx xxxx
	<b>B9</b>	<b>B10</b>	<b>B11</b>	...	<b>B16</b>	<b>B17</b>		
	xxxx xxxx	xxxx xxxx	xx11 xxxx	...	xxx0 111x	1xx1 xxx1		

**EF<sub>5GS3GPPNSC</sub>** (5GS 3GPP Access NAS Security Context)

This file shall be available and shall contain two records (see TS 31.102 [4]).

Logically:

First record:

ngKSI: '07'(no key available)  
 K<sub>AMF</sub>: 32 byte key, any value  
 Uplink NAS count: '00'  
 Downlink NAS count: '01'  
 Identifiers of selected NAS integrity  
 and encryption algorithms: '01'  
 Identifiers of selected EPS NAS  
 integrity and encryption algorithms  
 for use after mobility to EPS: '01'

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	...	B39
Hex	A0	37	80	01	07	81	20	xx	...	xx
	<b>B40</b>	<b>B41</b>	<b>B42</b>	<b>B43</b>	<b>B44</b>	<b>B45</b>	<b>B46</b>	<b>B47</b>	<b>B48</b>	<b>B49</b>
	82	04	00	00	00	00	83	04	00	00
	<b>B50</b>	<b>B51</b>	<b>B52</b>	<b>B53</b>	<b>B54</b>	<b>B55</b>	<b>B56</b>	<b>B57</b>		
	00	01	84	01	01	85	01	01		

Second record

ngKSI: '07'(no key available)  
 K<sub>AMF</sub>: 32 byte key, any value  
 Uplink NAS count: '00'  
 Downlink NAS count: '01'  
 Identifiers of selected NAS integrity  
 and encryption algorithms: '01'  
 Identifiers of selected EPS NAS  
 integrity and encryption algorithms  
 for use after mobility to EPS: '01'  
 PLMN identifier: '000000'

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	...	B39
Hex	A0	3C	80	01	07	81	20	xx	...	xx
	<b>B40</b>	<b>B41</b>	<b>B42</b>	<b>B43</b>	<b>B44</b>	<b>B45</b>	<b>B46</b>	<b>B47</b>	<b>B48</b>	<b>B49</b>
	82	04	00	00	00	00	83	04	00	00
	<b>B50</b>	<b>B51</b>	<b>B52</b>	<b>B53</b>	<b>B54</b>	<b>B55</b>	<b>B56</b>	<b>B57</b>	<b>B58</b>	<b>B59</b>
	00	01	84	01	01	85	01	01	86	03
	<b>B60</b>	<b>B61</b>	<b>B62</b>							
	00	00	00							

**EF<sub>5GSN3GPPNSC</sub>** (5GS non-3GPP Access NAS Security Context)

This file shall be available and shall contain two records (see TS 31.102 [4]).

Logically:

First record:

ngKSI: '07'(no key available)  
 K<sub>AMF</sub>: 32 byte key, any value  
 Uplink NAS count: '00'  
 Downlink NAS count: '01'

Identifiers of selected NAS integrity  
and encryption algorithms: '01'  
Identifiers of selected EPS NAS  
integrity and encryption algorithms  
for use after mobility to EPS: '01'

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	...	B39
Hex	A0	37	80	01	07	81	20	xx	...	xx
	<b>B40</b>	<b>B41</b>	<b>B42</b>	<b>B43</b>	<b>B44</b>	<b>B45</b>	<b>B46</b>	<b>B47</b>	<b>B48</b>	<b>B49</b>
	82	04	00	00	00	00	83	04	00	00
	<b>B50</b>	<b>B51</b>	<b>B52</b>	<b>B53</b>	<b>B54</b>	<b>B55</b>	<b>B56</b>	<b>B57</b>		
	00	01	84	01	01	85	01	01		

Second record

ngKSI: '07'(no key available)  
K<sub>AMF</sub>: 32 byte key, any value  
Uplink NAS count: '00'  
Downlink NAS count: '01'  
Identifiers of selected NAS integrity  
and encryption algorithms: '01'  
Identifiers of selected EPS NAS  
integrity and encryption algorithms  
for use after mobility to EPS: '01'  
PLMN identifier: '000000'

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	...	B39
Hex	A0	3C	80	01	07	81	20	xx	...	xx
	<b>B40</b>	<b>B41</b>	<b>B42</b>	<b>B43</b>	<b>B44</b>	<b>B45</b>	<b>B46</b>	<b>B47</b>	<b>B48</b>	<b>B49</b>
	82	04	00	00	00	00	83	04	00	00
	<b>B50</b>	<b>B51</b>	<b>B52</b>	<b>B53</b>	<b>B54</b>	<b>B55</b>	<b>B56</b>	<b>B57</b>	<b>B58</b>	<b>B59</b>
	00	01	84	01	01	85	01	01	86	03
	<b>B60</b>	<b>B61</b>	<b>B62</b>							
	00	00	00							

EF/DF definitions provided in the Initial condition clause of a test case/test sequence take precedence over values defined as default.

## 4.5.12 Definition of 5G-NR UICC – support of Rel-17 features

The values of the 5G-NR UICC – support of Rel-17 features are identical to the values of the 5G-NR UICC – support of Rel-16 features defined in clause 4.5.11 of the present document with the following exceptions:

**EF<sub>UST</sub>** (USIM Service Table)

Logically:

Allow services up to Service n°146

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Binary:	xx1x xx11	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxxx xxxx	xxxx xxxx	xxxx xxxx
	<b>B9</b>	<b>B10</b>	<b>B11</b>	...	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>
	xxxx xxxx	xxxx xxxx	xx11 xxxx	...	xxx0 111x	xxx1 xxx1	xxxx xxxx	0000 00xx

### 4.5.13 Definition 5G-NR UICC – CAG support

In general, the values of the 5G-NR UICC – CAG support are identical to the values of the of 5G-NR UICC as defined in clause 4.5.12 in addition the following exceptions apply:

#### EF<sub>UST</sub> (USIM Service Table)

Logically:

Service n°137: Preconfigured CAG information list available

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Binary:	xx1x xx11	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxxx xxxx	xxxx xxxx	xxxx xxxx
	<b>B9</b>	<b>B10</b>	<b>B11</b>	...	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>
	xxxx xxxx	xxxx xxxx	xx11 xxxx	...	xxx0 111x	xxxx xxxx	xxxx xxx1	0000 00xx

#### EF<sub>CAG</sub> (Pre-configured CAG information list EF)

Logically:

PLMN: 244 083 (MCC MNC)  
 CAG only bit: 1  
 Range indication bit: 1  
 CAG-ID range: '00 00 00 01' to '00 00 00 07'

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10
Hex	00	0D	0C	42	34	80	03	00	00	00
	<b>B11</b>	<b>B12</b>	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>
	01	00	00	00	07					

EF/DF definitions provided in the Initial condition clause of a test case/test sequence take precedence over values defined as default.

### 4.5.14 Definition of 5G-NR ISIM-UICC

The 5G-NR ISIM-UICC shall contain a USIM as defined in clause 4.5.9 of the present document and an ISIM for IMS access as defined in TS 31.121 [2], clause 4.5.3.

EF/DF definitions provided in the Initial condition clause of a test case/test sequence take precedence over values defined as default.

### 4.5.15 Definition of 5G-NR UICC – support of Rel-18 features

The values of the 5G-NR UICC – support of Rel-18 features are identical to the values of the 5G-NR UICC – support of Rel-17 features defined in clause 4.5.12 of the present document with the following exceptions:

#### EF<sub>UST</sub> (USIM Service Table)

Logically:

Allow services up to Service n°150

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Binary:	xx1x xx11	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxxx xxxx	xxxx xxxx	xxxx xxxx
	<b>B9</b>	<b>B10</b>	<b>B11</b>	...	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>
	xxxx xxxx	xxxx xxxx	xx11 xxxx	...	xxx0 111x	xxx1 xxx1	xxxx xxxx	00xx xxxx

## 4.5.16 Definition of 5G-NR SSIM-UICC

The 5G-NR SSIM-UICC shall contain a SSIM as defined in TS 31.105 [59], with an AID value build from a 3GPP RID, and PIX coding as defined for the '3GPP SSIM' application in ETSI TS 101 220 [60], Annex E and a USIM as defined in clause 4.5.y of the present document.

EF/DF definitions provided in the Initial condition clause of a test case/test sequence take precedence over values defined as default.

### EF<sub>EAPID</sub> (EAP Identifier)

Logically:

EAP Identifier: [verylongusername1@3gpp.com](mailto:verylongusername1@3gpp.com)  
 Username: verylongusername1  
 Realm: 3gpp.com

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	80	1A	76	65	72	79	6C	6F	6E	67	75	73
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	65	72	6E	61	6D	65	31	40	33	67	70	70
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>								
	2E	63	6F	6D								

### EF<sub>NSSAI</sub> (S-NSSAI List)

Logically:

Record 1:  
 S-NSSAI: 01 01 01 03 (SST: eMBB, SD: 010103)

Coding:

Byte	B1	B2	B3	B4
Hex	01	01	01	03

Record 2:  
 S-NSSAI: 01 01 01 02 (SST: eMBB, SD: 010102)

Coding:

Byte	B1	B2	B3	B4
Hex	01	01	01	02

## 4.6 Definition of default values for EFs commonly used with random value generation

### 4.6.1 EF<sub>IMSI</sub> with 3-digit MNC and random value

#### EF<sub>IMSI</sub> (International Mobile Subscriber Identity)

Logically:

2460813579135x

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9
Hex	08	21	64	80	31	75	19	53	Fx

D:  $x \in \{0x0; \dots; 0x9\}$

If the test/sequence is executed using an explicit test option as identified in Table A.2/1 or A.2/2, providing log data for all UICC-Terminal communication, x may be set to x=7.

#### 4.6.2 EF<sub>IMSI</sub> "short", with 3-digit MNC and random value

EF<sub>IMSI</sub> (International Mobile Subscriber Identity)

Logically:

24608135x

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9
Hex	05	29	64	80	31	x5	FF	FF	FF

D:  $x \in \{0x0; \dots; 0x9\}$

If the test/sequence is executed using an explicit test option as identified in Table A.2/1 or A.2/2, providing log data for all UICC-Terminal communication, x may be set to x=7.

#### 4.6.3 EF<sub>IMSI</sub> "short", with 2-digit MNC and random value

EF<sub>IMSI</sub> (International Mobile Subscriber Identity)

Logically:

24681357x

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9
Hex	05	29	64	18	53	x7	FF	FF	FF

D:  $x \in \{0x0; \dots; 0x9\}$

If the test/sequence is executed using an explicit test option as identified in Table A.2/1 or A.2/2, providing log data for all UICC-Terminal communication, x may be set to x=9.

#### 4.6.4 EF<sub>IMSI</sub> "long", with 3-digit MNC and random value

EF<sub>IMSI</sub> (International Mobile Subscriber Identity)

Logically:

24608111111111x

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9
Hex	08	29	64	80	11	11	11	11	x1

D:  $x \in \{0x0; \dots; 0x9\}$

If the test/sequence is executed using an explicit test option as identified in Table A.2/1 or A.2/2, providing log data for all UICC-Terminal communication, x may be set to x=1.

#### 4.6.5 EF<sub>IMSI</sub> for SUCI calculation tests

EF<sub>IMSI</sub> (International Mobile Subscriber Identity)

Logically:

24608135793579x

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9
Hex	08	29	64	80	31	75	39	75	x9

$D: x \in \{0x0; \dots; 0x9\}$

If the test/sequence is executed using an explicit test option as identified in Table A.2/1 or A.2/2, providing log data for all UICC-Terminal communication, x may be set to x=3.

#### 4.6.6 EF<sub>IMSI</sub> for "change IMSI" tests

EF<sub>IMSI</sub> (International Mobile Subscriber Identity)

Logically:

24608122223333x

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9
Hex	08	29	64	80	21	22	32	33	X3

$D: x \in \{0x0; \dots; 0x9\}$

If the test/sequence is executed using an explicit test option as identified in Table A.2/1 or A.2/2, providing log data for all UICC-Terminal communication, x may be set to x=3.

#### 4.6.7 EF<sub>Routing\_Indicator</sub> with 2-digit MNC and random value

EF<sub>Routing\_Indicator</sub> (Routing Indicator EF)

Logically:

1y

Coding:

Byte	B1	B2	B3	B4
Hex	y1	FF	FF	FF

$D: y \in \{0x0; \dots; 0x9, 0xF\}$

If the test/sequence is executed using an explicit test option as identified in Table A.2/1 or A.2/2, providing log data for all UICC-Terminal communication, y may be set to y=7.

#### 4.6.8 EF<sub>LOCi</sub> with "short" random TMSI value

EF<sub>LOCi</sub> (Location Information)

Logically:

LAI-MCC: 246  
 LAI-MNC: 081  
 LAI-LAC: 0001  
 TMSI: 0000214x

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11
Hex	00	00	21	4x	42	16	80	00	01	FF	00

$D: x \in \{0x0; \dots; 0x9\}$

If the test/sequence is executed using an explicit test option as identified in Table A.2/1 or A.2/2, providing log data for all UICC-Terminal communication, x may be set to x=3.

## 4.6.9 EF<sub>LOCI</sub> with "long" random TMSI value

### EF<sub>LOCI</sub> (Location Information)

Logically:

LAI-MCC: 246  
 LAI-MNC: 081  
 LAI-LAC: 0001  
 TMSI: 214x0000

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11
Hex	21	4x	00	00	42	16	80	00	01	FF	00

D:  $x \in \{0x0; \dots; 0x9\}$

If the test/sequence is executed using an explicit test option as identified in Table A.2/1 or A.2/2, providing log data for all UICC-Terminal communication, x may be set to x=3.

## 4.6.10 EF<sub>EPSLOCI</sub>

### EF<sub>EPSLOCI</sub> (EPS Location Information)

Logically:

GUTI: 24608100010266uvwxyz  
 Last visited registered TAI: 246/081/0001  
 EPS update status: not updated

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	0B	F6	42	16	80	00	01	02
	<b>B9</b>	<b>B10</b>	<b>B11</b>	<b>B12</b>	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>
	66	vu	xw	zy	42	16	80	00
	<b>B17</b>	<b>B18</b>						
	01	01						

D:  $u, v, w, x, y, z \in \{0x0; \dots; 0x9\}$

If the test/sequence is executed using an explicit test option as identified in Table A.2/1 or A.2/2, providing log data for all UICC-Terminal communication, the variables may be set to fixed values: u=3, v=4, w=5, x=6, y=7, z=8

## 4.6.11 EF<sub>FDN</sub>

### EF<sub>FDN</sub> (Fixed Dialling Numbers)

Logically:

Record 1:

Length of alpha identifier: 6 characters;  
 Alpha identifier: "FDN111";  
 Length of BCD number: 6 bytes;  
 TON and NPI: Telephony and International;  
 Dialed number: +135792468x;  
 CCI2: None;  
 Ext2: None.

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	46	44	4E	31	31	31	06	91
	B9	B10	B11	B12	B13	B14	B15	B16
	31	75	29	64	x8	FF	FF	FF
	B17	B18	B19	B20				
	FF	FF	FF	FF				

D:  $x \in \{0x0; \dots; 0x9\}$ 

Record 2:

Length of alpha identifier: 6 characters;  
Alpha identifier: "FDN222";  
Length of BCD number: 4 bytes;  
TON and NPI: Telephony and International;  
Dialled number: 2468y;  
CCI2: None;  
Ext2: None.

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	46	44	4E	32	32	32	04	91
	B9	B10	B11	B12	B13	B14	B15	B16
	42	86	Fy	FF	FF	FF	FF	FF
	B17	B18	B19	B20				
	FF	FF	FF	FF				

D:  $y \in \{0x0; \dots; 0x9\}$ 

Record 3:

Length of alpha identifier: 6 characters;  
Alpha identifier: "FDN333";  
Length of BCD number: 11 bytes;  
TON and NPI: Telephony and International;  
Dialled number: +1234567890123456789z;  
CCI2: None;  
Ext2: None.

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	46	44	4E	33	33	33	0B	91
	B9	B10	B11	B12	B13	B14	B15	B16
	21	43	65	87	09	21	43	65
	B17	B18	B19	B20				
	87	z9	FF	FF				

D:  $z \in \{0x0; \dots; 0x9\}$ 

If the test/sequence is executed using an explicit test option as identified in Table A.2/1 or A.2/2, providing log data for all UICC-Terminal communication, the variables may be set to fixed values:  $x, y, z = 0$

## 4.6.12 EF<sub>ECC</sub>

EF<sub>ECC</sub> (Emergency Call Codes)

Logically:

Emergency call code: 12x;  
Emergency call code alpha identifier: "TEST";  
Emergency call Service Category: Mountain Rescue.

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	21	Fx	FF	54	45	53	54	10

D:  $x \in \{0x0; \dots; 0x9\}$

If the test/sequence is executed using an explicit test option as identified in Table A.2/1 or A.2/2, providing log data for all UICC-Terminal communication, x may be set to x=2.

## 4.7 Default values for NG-SS and UE configurations

### 4.7.1 Default NG-SS and UE configuration for different usage settings

For 'voice centric' usage:

- The NG-SS shall support IMS voice over PS session over 3GPP access and the IMS SIP Registration procedure, in accordance with clauses 4.7.2 and 4.7.3.
- The UE shall use IMS specific configuration as defined in clause 4.7.4.

For 'data centric' usage:

- The NG-SS shall support the default NG-SS configuration for IMS Registration as defined in clause 4.7.2.1. It may support IMS voice over PS session over 3GPP access as defined in clause 4.7.2.2.
- The UE may attempt to initiate a PDU Session establishment for IMS and it is up to NG-SS implementation to accept it and to perform the IMS registration procedure as defined in clause 4.7.2 or to reject the PDU Session establishment. The IMS specific configuration as defined in clause 4.7.4 may be used in the UE.

In case the optional feature `pc_VOICE_CENTRIC`, as defined in table A.1 is supported, the TT shall operate the test case as defined for 'voice centric' usage. Else the 'data centric' configuration shall be used.

### 4.7.2 Default NG-SS configuration for 3GPP access with IMS service

#### 4.7.2.1 Default NG-SS configuration for IMS Registration support

The NG-SS is configured with the IMSI within the USIM application, the P-CSCF address, the home domain name, public and private user identities together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the ISIM.

- NG-SS is listening to SIP default port 5060 for both UDP and TCP protocols.
- NG-SS is able to perform IMS AKA authentication for the IMPI, according to TS 33.203 [57 clause 6.1.
- SIB 1 in NG-SS Cell shall not include `uac-BarringInfo` with `UAC_BarringInfo` for AccessCategory 9, IMS Signalling.

#### 4.7.2.2 Default NG-SS configuration for PS voice support

The following parameters apply to all 5G test cases in 'voice centric' usage.

- 5GS network feature support element includes 'IMS voice over PS session over 3GPP access indicator' (IMS-VoPS-3GPP) in the REGISTRATION ACCEPT.

### 4.7.3 Default NG-SS procedure for 5G Registration on 3GPP access with IMS service

The NG-SS and UE shall perform 5G Registration procedure and IMS SIP Registration procedure as per the generic procedure defined in this clause.

5G-NR generic procedure for 5G Registration on 3GPP access with IMS service defined in Annex C.1 shall be the default procedure for 5G Registration on 3GPP access with IMS service.

The procedure provided for a test case may include common test steps only. However, in 'voice centric' usage, NG-SS and UE shall support additional steps defined in the 'voice centric' procedure in Annex C.1.

#### 4.7.4 Default UE configuration for IMS service

UE shall be configured with the DNN type as 'ims' and DNN as IMS.

IMS private user identity, Home Network Domain Name, IMS public user identity, and P-CSCF Address required for IMS SIP Registration shall be configured in the 5G-NR ISIM-UICC as defined in clause 4.5.14.

---

## 5 Subscription related tests

### 5.1 IMSI/TMSI handling

#### 5.1.1 UE identification by short IMSI

GERAN/UTRAN test - not applicable

#### 5.1.2 UE identification by short IMSI using a 2-digit MNC

GERAN/UTRAN test - not applicable

#### 5.1.3 UE identification by "short" TMSI

GERAN/UTRAN test - not applicable

#### 5.1.4 UE identification by "long" TMSI

GERAN/UTRAN test - not applicable

#### 5.1.5 UE identification by long IMSI, TMSI updating and key set identifier assignment

GERAN/UTRAN test - not applicable

#### 5.1.6 UE identification by short IMSI when accessing E-UTRAN/EPC

##### 5.1.6.1 Definition and applicability

PAGING for EPS services using IMSI is an abnormal procedure used for error recovery in the network. The IMSI is used for unique identification of the UE by an E-UTRAN/EPC if there is no GUTI available. The IMSI is stored in the USIM and read during the UICC-Terminal initialisation procedure.

##### 5.1.6.2 Conformance requirement

CR 1 Only after reception of a PAGING message containing the IMSI stored in the USIM the UE shall send the RRC CONNECTION REQUEST message.

Reference:

- TS 31.102 [19], clauses 5.1.1 and 5.2.2;
- TS 24.301 [21], clause 5.6.2.2.2 and 5.6.2.4.

CR 2 For NB-IoT, the PAGING message shall include a CN domain indicator set to "PS". If the paging message includes a UE PAGING IDENTITY set to the UE's IMSI, the PAGING procedure is performed according to clause 5.6.2.2.2 of [21].

Reference:

- TS 31.102 [19], clauses 5.1.1 and 5.2.2;
- TS 24.301 [21], clause 5.6.2.2.2 and 5.6.2.4.

CR 3 The ME correctly performs the READ BINARY command on EF<sub>IMSI</sub>.

Reference:

- TS 31 101 [33], clause 11.1.3;
- ETSI TS 102 221 [8], clause 11.1.3 and 14.1.1.

### 5.1.6.3 Test purpose

The purpose of this test is to verify that:

- 1) the ME uses the IMSI stored in the USIM when attaching to the network;
- 2) the ME can handle an IMSI of less than the maximum length.
- 3) To verify that the READ EF<sub>IMSI</sub> command is performed correctly by the ME.
- 4) To verify that the UE does not respond to a paging message containing an IMSI not stored in the USIM.

### 5.1.6.4 Method of test

#### 5.1.6.4.1 Initial conditions

The values of the E-UTRAN/EPC UICC as defined in clause 4.5.4 of the present document are used with EF<sub>IMSI</sub> as defined in clause 4.6.2.

For Test Procedure A the TT (E-USS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001
- Access control: unrestricted

For Test Procedure B the TT (NB-SS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001
- Access control: unrestricted

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and runs an initial activation.

#### 5.1.6.4.2 Procedure

##### 5.1.6.4.2.1 Test procedure A

Step	Direction	Action	Information	REQ	SA
1	UE > TT	Send ATTACH REQUEST			
2	TT > UE	Send PAGING with IMSI 24608122222	The UE does not send an RCC CONNECTION REQUEST		
3	UE	READ EF <sub>IMSI</sub>		CR 3	A.2/1 OR A.2/2
4	TT > UE	Send PAGING with the IMSI stored in the USIM			

5	UE > TT	Send RRC CONNECTION REQUEST	The TT responds with a RRC CONNECTION SETUP	CR 1	
6	UE > TT	Send RRC CONNECTION SETUP COMPLETE	The UE performs the EPS attach procedure		
7	TT > UE	Send RRC CONNECTION RELEASE			

#### 5.1.6.4.2.2 Test procedure B

Step	Direction	Action	Information	REQ	SA
1	UE > TT	Send ATTACH REQUEST			
2	TT > UE	Send PAGING-NB with IMSI 24608122222	The UE does not send an RRC CONNECTION REQUEST-NB		
3	UE	READ EF <sub>IMSI</sub>		CR 3	A.2/1 OR A.2/2
4	TT > UE	Send PAGING-NB with the IMSI stored in the USIM			
5	UE > TT	Send RRC CONNECTION REQUEST-NB	The TT responds with a RRC CONNECTION SETUP-NB	CR 2	
6	UE > TT	Send RRC CONNECTION SETUP COMPLETE-NB	The UE performs the EPS attach procedure		
7	TT > UE	Send RRC CONNECTION RELEASE-NB			

### 5.1.6.5 Acceptance criteria

#### 5.1.6.5.1 Acceptance criteria for Test Procedure A

CR 1 is verified by analysing the IMSI value transferred by the UE in the RRC CONNECTION REQUEST. The conformance requirement CR 1 is met if the IMSI value stored on the USIM matches the IMSI value provided to the TT (USS).

#### 5.1.6.5.2 Acceptance criteria for Test Procedure B

CR 2 is verified by analysing the IMSI value transferred by the UE in the RRC CONNECTION REQUEST-NB. The conformance requirement CR 2 is met if the IMSI value stored on the USIM matches the IMSI value provided to the TT (NB-SS).

#### 5.1.6.4.3 Common acceptance criteria

CR 3 is explicitly verified in step 3) by analysing the READ command used to read the contents of EF<sub>IMSI</sub> (A.2/1 or A.2/2). CR 3 is met if the READ command is executed as defined in [28], clause 14.1.1.

## 5.1.7 UE identification by short IMSI using a 2-digit MNC when accessing E-UTRAN/EPC

### 5.1.7.1 Definition and applicability

In some networks the IMSI identifying the E-UTRAN/EPC can consist of a 2-digit MNC. PAGING for EPS services using IMSI is an abnormal procedure used for error recovery in the network. The IMSI is used for unique identification of the UE by an E-UTRAN/EPC if there is no GUTI available. The IMSI is stored in the USIM and read during the UICC-Terminal initialisation procedure.

### 5.1.7.2 Conformance requirement

CR 1 Only after reception of a PAGING message containing the IMSI stored in the USIM the UE shall send the RRC CONNECTION REQUEST message.

Reference:

- TS 31.102 [19], clause 5.1.1 and 5.2.2;
- ETSI TS 102 221 [8], clause 14.1.1;
- TS 24.301 [21], clause 5.6.2.2.2 and 5.6.2.4.

CR 2 The ME correctly handles the an IMSI that contains a 2-digit MNC.

Reference:

- TS 23 003 [34], clause 2.2;

### 5.1.7.3 Test purpose

The purpose of this test is to verify that:

- 1) the ME uses the IMSI stored in the USIM when attaching to the network;
- 2) the ME is capable of handling an IMSI with a 2-digit MNC;
- 3) the EF<sub>IMSI</sub> is correctly read by the ME;
- 4) the ME does not respond to a PAGING message containing an IMSI not stored in the USIM.

### 5.1.7.4 Method of test

#### 5.1.7.4.1 Initial conditions

The values of the E-UTRAN/EPC UICC as defined in clause 4.5.4 of the present document are used with EF<sub>IMSI</sub> as defined in clause 4.6.3, and the following exception:

**EF<sub>AD</sub>** (Administrative Data)

Logically:

UE operation mode: normal operation  
 Additional information: ciphering indicator feature disabled  
 MNC: 2 digits

Coding:

Byte	B1	B2	B3	B4
Hex	00	00	00	02

For Test Procedure A the TT (E-USS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/81/0001
- Access control: unrestricted

For Test Procedure B the TT (NB-SS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/81/0001
- Access control: unrestricted

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and runs an initial activation.

#### 5.1.7.4.2 Procedure

##### 5.1.7.4.2.1 Test procedure A

Step	Direction	Action	Information	REQ	SA
1	UE > TT	Send ATTACH REQUEST			

2	TT > UE	Send PAGING with IMSI 24608122222	The UE does not send an RRC CONNECTION REQUEST		
3	UE	READ EF <sub>IMSI</sub>			
4	TT > UE	Send PAGING with the IMSI stored in the USIM			
5	UE > TT	Send RRC CONNECTION REQUEST	The TT responds with a RRC CONNECTION SETUP	CR 1 CR 2	
6	UE > TT	Send RRC CONNECTION SETUP COMPLETE	The UE performs the EPS attach procedure		
7	TT > UE	Send RRC CONNECTION RELEASE			

#### 5.1.7.4.2.2 Test procedure B

Step	Direction	Action	Information	REQ	SA
1	UE > TT	Send ATTACH REQUEST			
2	TT > UE	Send PAGING-NB with IMSI 24608122222	The UE does not send an RRCConnectionRequest-NB		
3	UE	READ EF <sub>IMSI</sub>			
4	TT > UE	Send PAGING-NB with the IMSI stored in the USIM			
5	UE > TT	Send RRC CONNECTION REQUEST-NB	The TT responds with a RRC CONNECTION SETUP-NB	CR 1 CR 2	
6	UE > TT	Send RRC CONNECTION SETUP COMPLETE-NB	The UE performs the EPS attach procedure		
7	TT > UE	Send RRC CONNECTION RELEASE-NB			

#### 5.1.7.4 Acceptance criteria

For Procedure A, CR 1 is verified by analysing the RRC CONNECTION REQUEST. The conformance requirement CR 1 is met if the IMSI value stored on the USIM matches the IMSI value provided to the TT (E-USS)

For Procedure B, CR 1 is verified by analysing the RRC CONNECTION REQUEST-NB. The conformance requirement CR 1 is met if the IMSI value stored on the USIM matches the IMSI value provided to the TT (NB-SS).

CR 2 can be implicitly verified by assuring that the RRC CONNECTION REQUEST/RRC CONNECTION REQUEST-NB sent from the UE contains the IMSI value stored on the USIM.

NOTE: An explicit verification of the READ command is done in test 5.1.6 and another verification is not required. Nevertheless, it is optional to explicitly verify the READ EF<sub>IMSI</sub> command in step 2) using any of the test options A.2/1 or A.2/2.

### 5.1.8 UE identification after changed IMSI with service "EMM Information" not available

#### 5.1.8.1 Definition and applicability

The attach procedure is used to attach for packet services in EPS. With a successful attach procedure, a context is established for the UE in the MME, and a default bearer is established between the UE and the PDN GW, thus enabling always-on IP connectivity to the UE. The network may also initiate the activation of dedicated bearers as part of the attach procedure. For NB-IoT UEs the establishment of the PDN connection is optional.

#### 5.1.8.2 Conformance requirement

CR 1 The following EMM parameters shall be stored on the USIM if the corresponding file is present:

- GUTI;
- last visited registered TAI;

- EPS update status.

Reference:

- TS 31.102 [19], clause 5.1.1 and 5.2.2;
- TS 24.301 [21], clause 5.5.1.2.1, 5.5.1.2.2, 5.5.1.2.4 and Annex C.

CR 2 The UE includes the IMSI stored in the USIM during the attach procedure.

### 5.1.8.3 Test purpose

The purpose of this test is to verify that:

- 1) the UE deletes existing EMM parameters from the UE's non-volatile memory in case a different IMSI is activated;
- 2) the UE includes the IMSI stored in the USIM during the attach procedure.

### 5.1.8.4 Method of test

#### 5.1.8.4.1 Initial conditions

The values of the Default UICC as defined in clause 4.5.2 of the present document are used with the following exception:

**EF<sub>UST</sub>** (USIM Service Table)

Logically:

Service n°85:        EPS Mobility Management Information        not available

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Binary	xx1x xx11	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxxx xxxx	xxxx xxxx	xxxx xxxx
	<b>B9</b>	<b>B10</b>	<b>B11</b>	<b>B12</b>				
	xxxx xxxx	xxxx xxxx	xx10 xxxx	0000 0xxx				

The TT (E-USS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC):    246/081/0001
- Access control:        unrestricted

The TT (NB-SS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC):    246/081/0001
- Access control:        unrestricted

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and runs an initial activation.

#### 5.1.8.4.2 Procedure

##### 5.1.8.4.2.1 Test procedure A

Step	Direction	Action	Information	REQ	SA
1	UE > TT	Send RRC CONNECTION REQUEST	The TT responds with a RRC CONNECTION SETUP		
2	UE > TT	Send RRC CONNECTION SETUP COMPLETE			

3	UE > TT	Send ATTACH REQUEST	The TT responds with an ATTACH ACCEPT including the following values: - GUTI: "24608100010266345678" - TAI (MCC/MNC/TAC): 246/081/0001		
4	UE > TT	Send ATTACH COMPLETE	The TT responds with a RRC CONNECTION RELEASE		
5	USER/TT	Power off/deactivate the UE			
6	USER/TT	Reconfigure UICC in the UE	The values of the Default UICC as defined in clause 4.5.2 of the present document are used with EF <sub>IMSI</sub> as defined in clause 4.6.6		
7	USER/TT	Run activation of the UE			
8	UE > TT	Send RRC CONNECTION REQUEST	The TT responds with a RRC CONNECTION SETUP		
9	UE > TT	Send RRC CONNECTION SETUP COMPLETE			
10	UE > TT	Send ATTACH REQUEST	The UE sends an ATTACH REQUEST including the IMSI as generated in accordance to the definition in clause 4.6.6 but neither a GUTI nor the TAI	CR 1 CR 2	

#### 5.1.8.4.2.2 Test procedure B

Step	Direction	Action	Information	REQ	SA
1	UE > TT	Send RRC CONNECTION REQUEST-NB	The TT responds with a RRC CONNECTION SETUP-NB		
2	UE > TT	Send RRC CONNECTION SETUP COMPLETE-NB			
3	UE > TT	Send ATTACH REQUEST	The TT responds with an ATTACH ACCEPT including the following values: - GUTI: "24608100010266345678" - TAI (MCC/MNC/TAC): 246/081/0001		
4	UE > TT	Send ATTACH COMPLETE	The TT responds with a RRC CONNECTION RELEASE-NB		
5	USER/TT	Power off/deactivate the UE			
6	USER/TT	Reconfigure UICC in the UE	The values of the Default UICC as defined in clause 4.5.2 of the present document are used with EF <sub>IMSI</sub> as defined in clause 4.6.6		
7	USER/TT	Run activation of the UE			
8	UE > TT	Send RRC CONNECTION REQUEST-NB	The TT responds with a RRC CONNECTION SETUP COMPLETE-NB		
9	UE > TT	Send RRC CONNECTION SETUP COMPLETE-NB			
10	UE > TT	Send ATTACH REQUEST	The UE sends an ATTACH REQUEST including the IMSI as generated in accordance to the definition in clause 4.5.84.6.6 but neither a GUTI nor the TAI	CR 1 CR 2	

#### 5.1.8.5 Acceptance criteria

CR 1 and CR 2 can be implicitly verified by assuring that the ATTACH REQUEST sent from the UE in step 10) contains the IMSI value provided during reconfiguration (step 6)).

NOTE: As service n°85 is not available, no EMM parameters shall be stored on the USIM. Further verification of CR 1 is not needed.

## 5.1.9 UE identification by GUTI when using USIM with service "EMM Information" not available

### 5.1.9.1 Definition and applicability

The attach procedure is used to attach for packet services in EPS. With a successful attach procedure, a context is established for the UE in the MME, and a default bearer is established between the UE and the PDN GW, thus enabling always-on IP connectivity to the UE. The network may also initiate the activation of dedicated bearers as part of the attach procedure. For NB-IoT UEs the establishment of the PDN connection is optional.

### 5.1.9.2 Conformance requirement

CR 1 The following EMM parameters shall be stored on the USIM if the corresponding file is present:

- GUTI;
- last visited registered TAI;
- EPS update status

NOTE: If the corresponding file is not present on the USIM, these EMM parameters except allowed CSG list are stored in a non-volatile memory in the ME together with the IMSI from the USIM. These EMM parameters can only be used if the IMSI from the USIM matches the IMSI stored in the non-volatile memory; else the UE shall delete the EMM parameters.

Reference:

- TS 31.102 [19], clause 5.1.1 and 5.2.2;
- TS 24.301 [21], clause 5.5.1.2.1, 5.5.1.2.2, 5.5.1.2.4 and Annex C.

CR 2 The UE uses the GUTI and the TAI from the UE's non-volatile memory during the attach procedure if the IMSI stored in the UE's non-volatile memory and the IMSI stored in the USIM are identical.

### 5.1.9.3 Test purpose

The purpose of this test is to verify that:

- 1) the UE stores the GUTI and the TAI in the UE's non-volatile memory;
- 2) the UE includes the IMSI stored in the USIM during the attach procedure.

### 5.1.9.4 Method of test

#### 5.1.9.4.1 Initial conditions

The values of the Default UICC as defined in clause 4.5.2 of the present document are used with the following exception:

**EF<sub>UST</sub>** (USIM Service Table)

Logically:

Service n°85:          EPS Mobility Management Information          not available

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Binary	xx1x xx11	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxxx xxxx	xxxx xxxx	xxxx xxxx
	<b>B9</b>	<b>B10</b>	<b>B11</b>	<b>B12</b>				
	xxxx xxxx	xxxx xxxx	xx10 xxxx	0000 0xxx				

The TT (E-USS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001
- Access control: unrestricted

The TT (NB-SS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001
- Access control: unrestricted

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and runs an initial activation.

#### 5.1.9.4.2 Procedure

##### 5.1.9.4.2.1 Test procedure A

Step	Direction	Action	Information	REQ	SA
1	UE > TT	Send RRC CONNECTION REQUEST	The TT responds with a RRC CONNECTION SETUP		
2	UE > TT	Send RRC CONNECTION SETUP COMPLETE			
3	UE > TT	Send ATTACH REQUEST	The UE sends an ATTACH ACCEPT including the following values: - GUTI: "24608100010266345678" - TAI (MCC/MNC/TAC): 246/081/0001		
4	UE > TT	Send ATTACH COMPLETE	The TT responds with a RRC CONNECTION RELEASE		
5	USER/TT	Power off/deactivate the UE, then run activation of the UE			
6	UE > TT	Send RRC CONNECTION REQUEST	The TT responds with a RRC CONNECTION SETUP		
7	UE > TT	Send RRC CONNECTION SETUP COMPLETE			
8	UE > TT	Send ATTACH REQUEST	The sent ATTACH ACCEPT includes the following values: - GUTI: "24608100010266345678" - TAI (MCC/MNC/TAC): 246/081/0001	CR 1 CR 2	

##### 5.1.9.4.2.2 Test procedure B

Step	Direction	Action	Information	REQ	SA
1	UE > TT	Send RRC CONNECTION REQUEST-NB	The TT responds with a RRC CONNECTION SETUP-NB		
2	UE > TT	Send RRC CONNECTION SETUP COMPLETE-NB			
3	UE > TT	Send ATTACH REQUEST	The TT sends an ATTACH ACCEPT including the following values: - GUTI: "24608100010266345678" - TAI (MCC/MNC/TAC): 246/081/0001		
4	UE > TT	Send ATTACH COMPLETE			
5	TT > UE	Send RRC CONNECTION RELEASE-NB			
6	USER/TT	Power off/deactivate the UE, then run activation of the UE			
7	UE > TT	Send RRC CONNECTION REQUEST-NB	The TT responds with a RRC CONNECTION SETUP-NB		
8	UE > TT	Send RRC CONNECTION SETUP COMPLETE-NB			
9	UE > TT	Send ATTACH REQUEST	The sent ATTACH ACCEPT includes the following values: - GUTI: "24608100010266345678" - TAI (MCC/MNC/TAC): 246/081/0001	CR 1 CR 2	

### 5.1.9.5 Acceptance criteria

CR 1 and CR 2 can be implicitly verified by assuring that the ATTACH REQUEST sent from the UE in step 10) contains the GUTI and TAI values provided during the first attach procedure.

NOTE: As service n°85 is not available, no EMM parameters shall be stored on the USIM. Further verification of CR 1 is not needed.

## 5.1.10 UE identification by GUTI when using USIM with service "EMM Information" available

### 5.1.10.1 Definition and applicability

The attach procedure is used to attach for packet services in EPS. With a successful attach procedure, a context is established for the UE in the MME, and a default bearer is established between the UE and the PDN GW, thus enabling always-on IP connectivity to the UE. The network may also initiate the activation of dedicated bearers as part of the attach procedure. For NB-IoT UEs the establishment of the PDN connection is optional.

### 5.1.10.2 Conformance requirement

CR 1 The following EMM parameters shall be stored on the USIM if the corresponding file is present:

- GUTI;
- last visited registered TAI;
- EPS update status

NOTE: The presence and format of corresponding files on the USIM is specified in TS 31.102 [19].

Reference:

- TS 31.102 [19], clause 5.1.1 and 5.2.2;
- TS 24.301 [21], clause 5.5.1.2.1, 5.5.1.2.2, 5.5.1.2.4 and Annex C.

CR 2 The UE uses the GUTI and the TAI stored in EF<sub>EPSLOC1</sub> on the USIM during the attach procedure.

### 5.1.10.3 Test purpose

The purpose of this test is to verify that:

- 1) the UE stores the GUTI and the TAI in in EF<sub>EPSLOC1</sub> if service n°85 is available in EF<sub>UST</sub>;
- 2) the UE uses GUTI and the TAI values stored in EF<sub>EPSLOC1</sub> during the attach procedure.

### 5.1.10.4 Method of test

#### 5.1.10.4.1 Initial conditions

The values of the E-UTRAN/EPC UICC as defined in clause 4.5.4 of the present document are used with EF<sub>EPSLOC1</sub> as defined in clause 4.6.10 and the following exception:

EF<sub>EPSNSC</sub> (EPS NAS Security Context)

Logically:

Key Set Identifier KSI <sub>ASME</sub> :	'07' (no key available)
ASME Key (KSI <sub>ASME</sub> ):	32 byte key, any value
Uplink NAS count:	'00'
Downlink NAS count:	'01'
Identifiers of selected NAS integrity and encryption algorithm:	'01'

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	...	B39	B40
Hex	A0	34	80	01	07	81	20	xx	...	xx	82
	<b>B41</b>	<b>B42</b>	<b>B43</b>	<b>B44</b>	<b>B45</b>	<b>B46</b>	<b>B47</b>	<b>B48</b>	<b>B49</b>	<b>B50</b>	<b>B51</b>
	04	00	00	00	00	83	04	00	00	00	01
	<b>B52</b>	<b>B53</b>	<b>B54</b>								
	84	01	01								

The TT (E-USS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0002
- Access control: unrestricted

The TT (NB-SS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0002
- Access control: unrestricted

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and runs an initial activation.

#### 5.1.10.4.2 Procedure

##### 5.1.10.4.2.1 Test procedure A

Step	Direction	Action	Information	REQ	SA
1	UE > TT	Send RRC CONNECTION REQUEST	The TT responds with a RRC CONNECTION SETUP		
2	UE > TT	Send RRC CONNECTION SETUP COMPLETE			
3	UE > TT	Send ATTACH REQUEST	Receiving the ATTACH REQUEST including the values available from EF <sub>EPSLOC1</sub> as defined in clause 4.6.10, the TT sends an ATTACH ACCEPT including the following values: - GUTI: "24608100010266436587" - TAI (MCC/MNC/TAC): 246/081/0002	CR 2	
4	UE > TT	Send ATTACH COMPLETE	The TT responds with a RRC CONNECTION RELEASE		

##### 5.1.10.4.2.2 Test procedure B

Step	Direction	Action	Information	REQ	SA
1	UE > TT	Send RRC CONNECTION REQUEST-NB	The TT responds with a RRC CONNECTION SETUP-NB		
2	UE > TT	Send RRC CONNECTION SETUP COMPLETE_NB			
3	UE > TT	Send ATTACH REQUEST	Receiving the ATTACH REQUEST including the values available from EF <sub>EPSLOC1</sub> as defined in clause 4.6.10, the TT sends an ATTACH ACCEPT including the following values: - GUTI: "24608100010266436587" - TAI (MCC/MNC/TAC): 246/081/0002	CR 2	
4	UE > TT	Send ATTACH COMPLETE	The TT responds with a RRC CONNECTION RELEASE-NB		

##### 5.1.10.4.2.3 Common final Test Procedure

Step	Direction	Action	Information	REQ	SA
------	-----------	--------	-------------	-----	----

5 OR 5+x	UE	READ EF <sub>EPSLOC1</sub>	The TT is enabled to verify the contents of EF <sub>EPSLOC1</sub> either while executing step 4) or in an additional action that might be executed after ending the test	CR 1	A.2/1 OR A.2/2 OR A.2/3
-------------	----	----------------------------	--	------	-------------------------------------

### 5.1.10.5 Acceptance criteria

CR 2 can be implicitly verified by assuring that the ATTACH REQUEST sent from the UE in step 3) contains the GUTI and TAI values provided from the EF<sub>EPSLOC1</sub> stored on the USIM during configuration.

CR 1 shall be explicitly verified using any of the methods identified in clause 3.7.2 of the present document. CR 1 is met if EF<sub>EPSLOC1</sub> contains the following data:

#### EF<sub>EPSLOC1</sub> (EPS Location Information)

Logically:

GUTI: 24608100010266436587  
 Last visited registered TAI: 246/081/0002  
 EPS update status: updated

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	0B	F6	42	16	80	00	01	02
	<b>B9</b>	<b>B10</b>	<b>B11</b>	<b>B12</b>	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>
	66	34	56	78	42	16	80	00
	<b>B17</b>	<b>B18</b>						
	02	00						

## 5.2 Access Control handling

### 5.2.1 Access Control information handling

GERAN/UTRAN test - not applicable

### 5.2.2 Access Control information handling for E-UTRAN/EPC

#### 5.2.2.1 Definition and applicability

Access Control allows restriction of EPS bearer context activation access attempts. All user equipment (UE) are assigned to one out of ten randomly allocated classes, and optionally (for priority uses) also to one or more special categories.

An Access Class of the special categories is only valid in the HPLMN or HPLMN country. Otherwise, the randomly allocated class is used.

The classes are programmed on the USIM. The network controls which classes at any time may be barred.

Emergency call handling is FFS.

#### 5.2.2.2 Conformance requirement

CR 1 The ME shall read the access control value as part of the USIM-Terminal initialisation procedure and subsequently adopt this value.

Reference:

- TS 31.102 [19], clause 5.1.1.

CR 2 If the UE is a member of at least one access class which corresponds to the permitted classes as signalled over the air interface, and the access class is applicable in the serving network, access attempts are allowed. Otherwise access attempts are not allowed.

Reference:

- TS 22.011 [6], clauses 4.3 and 4.4,
- TS 24.301 [26], clause 5.5.1.2.6,

NOTE: All options are shown in figure 5-2 of [2] and are referenced to the tests.

### 5.2.2.3 Test purpose

The purpose of this test is to verify that:

- 1) the ME reads the access control value as part of the USIM-Terminal initialisation procedure, and subsequently adopts this value;
- 2) the UE controls its network access in accordance with its access control class and the conditions imposed by the serving network.

The tests verify ME performance for the following:

- Tests (a) and (b): UE with access class 0 to 9,
- Tests (c): UE with access class 11 and 15 not in HPLMN, and  
UE with access class 12,13 and 14 not in HPLMN country;
- Test (d) and (e): UE with access class 11 and 15 not in HPLMN, and  
UE with access class 12,13 and 14 not in HPLMN country;
- Test (g) and (h): UE with access class 11 and 15 in HPLMN, and  
UE with access class 12,13 and 14 in HPLMN country.

Each of the above are tested against all relevant combinations of access control bits signalled by the network, as shown in table 5-2 of TS 31.121 [2].

### 5.2.2.4 Method of test

#### 5.2.2.4.1 Initial conditions

The values of the Default UICC as defined in clause 4.5.2 of the present document are used with the exceptions given in TS 31.121 [2] clauses 5.2.2.4.1 and 5.2.2.4.2.

The TT (E-USS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): MCC, MNC: see table 5-2 of [2], TAC="0001".
- Access control: see table 5-2 of [2].

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case with an IMSI and access control values as given in table 5-2 of [2] and runs an initial activation.

NOTE: Depending on the initial value of the EF<sub>EPSLOC1</sub>, the UE may perform a location update. This shall be accepted by the E-USS.

#### 5.2.2.4.2 Coding details

The coding details defined in TS 31.121 [2] clause 5.2.2.4.2 apply.

#### 5.2.2.4.3 Procedure

Execute the test procedure as defined in TS 31.121 [2] clause 5.2.2.4.3.

#### 5.2.2.5 Acceptance criteria

CR 1 is implicitly verified after step a) if the ME has adopted the access control parameters as requested.

CR 2 is verified after step b) if the ME accesses the network, or makes no access attempt, in accordance with the Test Result entries given in table 5-2 of [2].

NOTE 1: barred = yes, in these sub-sequences, the UE shall not establish a connection  
barred = no, the UE shall establish a connection.

NOTE 2: For conformance testing, to limit testing, in test (a), (b) and (c) it is only necessary that one of the access classes is tested. This access class may be chosen randomly.

### 5.2.3 Access Control information handling for NB-IoT

#### 5.2.3.1 Definition and applicability

Access Control allows restriction RRC connection establishment attempts. All user equipment (UE) are assigned to one out of ten randomly allocated classes, and optionally (for priority uses) also to one or more special categories.

An Access Class of the special categories is only valid in the HPLMN or HPLMN country. Otherwise, the randomly allocated class is used.

The classes are programmed on the USIM. The network controls which classes at any time may be barred.

#### 5.2.3.2 Conformance requirement

CR 1 The ME shall read the access control value as part of the USIM-Terminal initialisation procedure and subsequently adopt this value.

Reference:

- TS 31.102 [19], clause 5.1.1.

CR 2 If the UE is a member of at least one access class which corresponds to the permitted classes as signalled over the air interface, and the access class is applicable in the serving network, access attempts are allowed. Otherwise access attempts are not allowed.

Reference:

- TS 22.011 [6], clauses 4.3 and 4.4,
- TS 24.301 [26], clause 5.5.1.2.6,

#### 5.2.3.3 Test purpose

The purpose of this test is to verify that:

- 1) the ME reads the access control value as part of the USIM-Terminal initialisation procedure, and subsequently adopts this value;
- 2) the UE controls its network access in accordance with its access control class and the conditions imposed by the serving network.

The tests verify ME performance for the following:

Tests (a) and (b): UE with access class 0 to 9,

Tests (c): UE with access class 11 and 15 not in HPLMN, and  
UE with access class 12,13 and 14 not in HPLMN country;

Test (d) and (e): UE with access class 11 and 15 not in HPLMN, and  
UE with access class 12,13 and 14 not in HPLMN country.

Each of the above are tested against all relevant combinations of access control bits signalled by the network, as shown in table 5-3 of TS 31.121 [2].

### 5.2.3.4 Method of test

#### 5.2.3.4.1 Initial conditions

The values of the Default UICC as defined in clause 4.5.2 of the present document are used with the exceptions given in TS 31.121 [2] clauses 5.2.3.4.1 and 5.2.3.4.2.

The TT (E-USS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): MCC, MNC: see table 5-3 of [2], TAC="0001".
- Access control: see table 5-3 of [2].

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case with an IMSI and access control values as given in table 5-3 of [2] and runs an initial activation.

NOTE: Depending on the initial value of the EF<sub>EPSLOCI</sub>, the UE may perform a location update. This shall be accepted by the TT (NB-SS).

#### 5.2.3.4.2 Coding details

The coding details defined in TS 31.121 [2] clause 5.2.3.4.2 apply.

#### 5.2.3.4.3 Procedure

Execute the test procedure as defined in TS 31.121 [2] clause 5.2.3.4.3.

### 5.2.3.5 Acceptance criteria

CR 1 is implicitly verified after step a) if the ME has adopted the access control parameters as requested.

CR 2 is verified after step a) if the ME accesses the network, or makes no access attempt, in accordance with the Test Result entries given in table 5-3 of [2].

NOTE 1: barred = yes, in these sub-sequences, the UE shall not establish a connection  
barred = no, the UE shall establish a connection.

NOTE 2: For conformance testing, to limit testing, in test (a), (b) and (c) it is only necessary that one of the access classes is tested. This access class may be chosen randomly.

## 5.3 Handling subscription identifier privacy for 5G

### 5.3.1 SUCI calculation by ME using null scheme

#### 5.3.1.1 Definition and applicability

If the operator's decision is that ME shall calculate the SUCI, the home network operator shall provision a list of the Protection Scheme Identifiers in the USIM that the operator allows. The list of Protection Scheme Identifiers in the USIM may contain one or more Protection Scheme Identifiers in the order of their priority. The ME shall read the SUCI calculation information from the USIM, including the SUPI, the Home Network Public Key, the Home Network Public

Key Identifier, and the list of Protection Scheme Identifiers. The ME shall select the protection scheme from its supported schemes that has the highest priority in the list obtained from the USIM.

The ME shall calculate the SUCI using the null-scheme if the highest priority of the protection schemes listed in the USIM is the null-scheme.

### 5.3.1.2 Conformance requirement

CR 1 The SUCI calculation procedure shall be performed by the ME if Service n°124 is available and Service n°125 is not available in EF<sub>UST</sub>.

Reference:

- TS 31.102 [19], clauses 4.4.11.8 and 4.4.11.11

CR 2 The ME shall read the SUCI calculation information from the USIM, including the SUPI, the Home Network Public Key, the Home Network, Public Key Identifier, and the list of Protection Scheme Identifiers.

Reference:

- TS 31.102 [19], clauses 4.4.11.8 and 4.4.11.11 and clauses 5.3.47 and 5.3.51.

CR 3 The ME shall calculate the SUCI including the SUCI calculation information procedure and the routing indicator procedure, using the null-scheme if highest priority of the protection schemes listed in the USIM is the null-scheme.

Reference:

- TS 31.102 [19], clauses 5.3.47 and 5.3.51;
- TS 33.501 [24], clause Annex C.

CR 4 The UE shall successfully authenticate and perform an initial registration on the network.

Reference:

- TS 24.501 [25], clause 5.5.1.2.4.

### 5.3.1.3 Test purpose

The purpose of this test is to verify that:

- 1) the ME correctly reads EF<sub>SUCI\_Calc\_Info</sub>, EF<sub>Routing\_indicator</sub> and EF<sub>IMSI</sub> from the USIM,
- 2) the SUCI calculation procedure is performed by the ME if Service n°124 is available and Service n°125 is not available in EF<sub>UST</sub>,
- 3) the ME selects the protection scheme that has the highest priority from the list obtained by the USIM,
- 4) the ME is calculating the SUCI using the null-scheme\*,
- 5) the UE successfully registers to the network.

NOTE: In the used configuration the null-scheme is the protection scheme with the highest priority listed in the USIM.

### 5.3.1.4 Method of test

#### 5.3.1.4.1 Initial conditions

The values of the 5G-NR UICC as defined in clause 4.5.9 of the present document are used with EF<sub>IMSI</sub> as defined in clause 4.6.5, EF<sub>Routing\_Indicator</sub> as defined in clause 4.6.7, and the following exception:

EF<sub>SUCI\_Calc\_Info</sub> (Subscription Concealed Identifier Calculation Information EF)

Logically:

Protection Scheme Identifier List data object:

Protection Scheme Identifier 1 – null-scheme

Key Index 1: 0

Protection Scheme Identifier 2 – ECIES scheme profile B

Key Index 2: 1

Protection Scheme Identifier 3 – ECIES scheme profile A

Key Index 3: 2

Home Network Public Key List data object:

Home Network Public Key 1 Identifier:27

Home Network Public Key 1:

04 72 DA 71 97 62 34 CE 83 3A 69 07 42 58 67 B8 2E 07 4D 44 EF 90 7D FB 4B 3E 21 C1 C2 25 6E  
BC D1 5A 7D ED 52 FC BB 09 7A 4E D2 50 E0 36 C7 B9 C8 C7 00 4C 4E ED C4 F0 68 CD 7B F8 D3  
F9 00 E3 B4

Home Network Public Key 2 Identifier: 30

Home Network Public Key 2:

5A 8D 38 86 48 20 19 7C 33 94 B9 26 13 B2 0B 91 63 3C BD 89 71 19 27 3B F8 E4 A6 F4 EE C0 A6  
50

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	A0	06	00	00	02	01	01	02
	<b>B9</b>	<b>B10</b>	<b>B11</b>	<b>B12</b>	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>
	A1	6B	80	01	1B	81	41	04
	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	72	DA	71	97	62	34	CE	83
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>	<b>B31</b>	<b>B32</b>
	3A	69	07	42	58	67	B8	2E
	<b>B33</b>	<b>B34</b>	<b>B35</b>	<b>B36</b>	<b>B37</b>	<b>B38</b>	<b>B39</b>	<b>B40</b>
	07	4D	44	EF	90	7D	FB	4B
	<b>B41</b>	<b>B42</b>	<b>B43</b>	<b>B44</b>	<b>B45</b>	<b>B46</b>	<b>B47</b>	<b>B48</b>
	3E	21	C1	C2	25	6E	BC	D1
	<b>B49</b>	<b>B50</b>	<b>B51</b>	<b>B52</b>	<b>B53</b>	<b>B54</b>	<b>B55</b>	<b>B56</b>
	5A	7D	ED	52	FC	BB	09	7A
	<b>B57</b>	<b>B58</b>	<b>B59</b>	<b>B60</b>	<b>B61</b>	<b>B62</b>	<b>B63</b>	<b>B64</b>
	4E	D2	50	E0	36	C7	B9	C8
	<b>B65</b>	<b>B66</b>	<b>B67</b>	<b>B68</b>	<b>B69</b>	<b>B70</b>	<b>B71</b>	<b>B72</b>
	C7	00	4C	4E	ED	C4	F0	68
	<b>B73</b>	<b>B74</b>	<b>B75</b>	<b>B76</b>	<b>B77</b>	<b>B78</b>	<b>B79</b>	<b>B80</b>
	CD	7B	F8	D3	F9	00	E3	B4
	<b>B81</b>	<b>B82</b>	<b>B83</b>	<b>B84</b>	<b>B85</b>	<b>B86</b>	<b>B87</b>	<b>B88</b>
	80	01	1E	81	20	5A	8D	38
	<b>B89</b>	<b>B90</b>	<b>B91</b>	<b>B92</b>	<b>B93</b>	<b>B94</b>	<b>B95</b>	<b>B96</b>
	86	48	20	19	7C	33	94	B9
	<b>B97</b>	<b>B98</b>	<b>B99</b>	<b>B100</b>	<b>B101</b>	<b>B102</b>	<b>B103</b>	<b>B104</b>
	26	13	B2	0B	91	63	3C	BD
	<b>B105</b>	<b>B106</b>	<b>B107</b>	<b>B108</b>	<b>B109</b>	<b>B110</b>	<b>B111</b>	<b>B112</b>
	89	71	19	27	3B	F8	E4	A6
	<b>B113</b>	<b>B114</b>	<b>B115</b>	<b>B116</b>	<b>B117</b>			
	F4	EE	C0	A6	50			

The TT (NG-SS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/083/000001
- Access control: unrestricted.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and runs an initial activation.

### 5.3.1.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	READ EF <sub>UST</sub>	(Evaluation of service settings)	CR 1	
2	UE	READ EF <sub>IMSI</sub> , EF <sub>SUCI_Calc_Info</sub> , EF <sub>Routing_indicator</sub>		CR 2	A.2/1 OR A.2/2
3	ME	Perform SUCI calculation	The ME performs a SUCI calculation using null scheme	CR 3	
4	UE > TT	Send REGISTRATION REQUEST	The UE sends a REGISTRATION REQUEST with 5GS registration type IE as "initial registration" and 5GS mobile identity information element type "SUCI"		
5	TT > UE	Send REGISTRATION ACCEPT	The TT sends a REGISTRATION ACCEPT with 5G-GUTI		
6	UE > TT	Send REGISTRATION COMPLETE		CR 4	

### 5.3.1.5 Acceptance criteria

CR 1 and CR 3 are implicitly verified in step 4). The conformance requirements are met if the 5GS mobile identity IE in the REGISTRATION REQUEST performed in step 4) includes the following values:

- SUPI format: 0
- Home Network Identifier: 246/081
- Routing Indicator: 1<sub>y</sub>
- Protection Scheme Identifier: 00
- Home Network Public Key Identifier: 0
- Scheme output: 35793579<sub>x</sub>

CR 2 can be verified by a method explicitly verifying the correct execution of the READ commands on the listed EFs (A.2/1 or A.2/2). CR 2 is met if the READ procedure on EF<sub>SUCI\_Calc\_Info</sub>, EF<sub>Routing\_indicator</sub> and EF<sub>IMSI</sub> has been executed as defined in [28], clause 14.1.1.

CR 4 is met if the UE sends REGISTRATION COMPLETE message to the TT (NG-SS) in step 6).

NOTE: It is optional to explicitly verify CR 1 in step 1) using any of the test options A.2/1 or A.2/2, checking the service options set in EF<sub>UST</sub>.

## 5.3.2 SUCI calculation by ME using Profile B

### 5.3.2.1 Definition and applicability

If the operator's decision is that ME shall calculate the SUCI, the home network operator shall provision a list of the Protection Scheme Identifiers that the operator allows in the USIM. The list of Protection Scheme Identifiers in the USIM may contain one or more Protection Scheme Identifiers in order of their priority. The ME shall read the SUCI calculation information from the USIM, including the SUPI, the Home Network Public Key, the Home Network Public Key Identifier, and the list of Protection Scheme Identifiers. The ME shall select the protection scheme from its supported schemes that has the highest priority in the list obtained from the USIM.

### 5.3.2.2 Conformance requirement

CR 1 SUCI calculation procedure shall be performed by the ME if Service n°124 is available and Service n°125 is not available in EF<sub>UST</sub>

Reference:

- TS 31.102 [19], clause 4.4.11.8

CR 2 As part of the SUCI calculation performed by the ME, the ME performs the reading procedure with  $EF_{SUCI\_Calc\_Info}$ .

Reference:

- TS 31.102 [19], clause 4.4.11.8 and 5.3.47

CR 3 The ME shall calculate the SUCI using the ECIES scheme profile B if highest priority of the protection schemes listed in the USIM is the ECIES scheme profile B.

Reference:

- TS 31.102 [19], clause 4.4.11.8
- TS 33.501 [24], Annex C, clause C.3 and C.4
- TS 24.501 [25], clause 9.11.3

CR 4 The UE shall successfully authenticate and perform an initial registration on the network.

Reference:

- TS 24.501 [25], clause 5.5.1.2.4.

### 5.3.2.3 Test purpose

The purpose of this test is to verify that:

- 1) the ME reads the SUCI calculation information from the USIM, including the SUPI, the Home Network Public Key, the Home Network Public Key Identifier, and the list of Protection Scheme Identifiers,
- 2) the ME selects the protection scheme from its supported schemes that has the highest priority in the list obtained from the USIM (i.e. ECIES scheme profile B and the home network public key),
- 3) the UE successfully registers to the network.

NOTE: In the used configuration profile B is the protection scheme with the highest priority listed in the USIM.

### 5.3.2.4 Method of test

#### 5.3.2.4.1 Initial conditions

The values of the default 5G-NR UICC defined in clause 4.5.9 of the present document are used with  $EF_{IMSI}$  as defined in clause 4.6.5,  $EF_{Routing\_Indicator}$  as defined in clause 4.6.7.

The TT (NG-SS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/083/000001.
- Access control: unrestricted.

The TT (NG-SS) shall be configured with Home Network Private Key as following:

Coding:

<b>Byte</b>	<b>B1</b>	<b>B2</b>	<b>B3</b>	<b>B4</b>	<b>B5</b>	<b>B6</b>	<b>B7</b>	<b>B8</b>
Hex	F1	AB	10	74	47	7E	BC	C7
	<b>B9</b>	<b>B10</b>	<b>B11</b>	<b>B12</b>	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>
	5F	54	EA	1C	5F	C3	68	B1
	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	61	67	30	15	5E	00	41	AC
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>	<b>B31</b>	<b>B32</b>
	44	7D	63	01	97	5F	EC	DA

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and runs an initial activation.

#### 5.3.2.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	READ EF <sub>UST</sub>	(Evaluation of service settings)	CR 1	
2	UE	READ EF <sub>SUCI_Calc_Info</sub>		CR 2	
3	ME	Perform SUCI calculation	The ME performs a SUCI calculation using Profile B	CR 3	
4	UE > TT	Send REGISTRATION REQUEST	The UE sends a REGISTRATION REQUEST with 5GS registration type IE as "initial registration" and 5GS mobile identity information element type "SUCI"		
5	TT > UE	Send REGISTRATION ACCEPT	The TT sends a REGISTRATION ACCEPT with a new 5G-GUTI		
6	UE > TT	Send REGISTRATION COMPLETE		CR 4	

#### 5.3.2.5 Acceptance criteria

Actions required to fulfil CR 1, CR 2 and CR 3 are executed by the ME. The implicitly verification of these requirements is done in step 4). The conformance requirements are met if the 5GS mobile identity IE in the REGISTRATION REQUEST performed in step 4) includes the following values:

- SUPI format: 0
- Home Network Identifier: 246/081
- Routing Indicator: 1y
- Protection Scheme Identifier: 02
- Home Network Public Key Identifier: 27
- Scheme output: ECC ephemeral public key, encryption of 35793579x and MAC tag value

CR 4 is met if the UE sends REGISTRATION COMPLETE message to the TT (NG-SS) in step 6).

NOTE: It is optional to explicitly verify CR 1 and CR 2 using any of the test options A.2/1 or A.2/2, checking the READ commands on EF<sub>SUCI\_Calc\_Info</sub> (CR 2) and evaluating the service options settings in EF<sub>UST</sub> (CR 1).

### 5.3.3 UE identification by SUCI during initial registration – SUCI calculation by USIM using profile B

#### 5.3.3.1 Definition and applicability

If the operator's decision, indicated by the USIM, is that the USIM shall calculate the SUCI, then the USIM shall not give the ME any parameter for the calculation of the SUCI including the Home Network Public Key Identifier, the Home Network Public Key, and the Protection Scheme Identifier. If the ME determines that the calculation of the SUCI, indicated by the USIM, shall be performed by the USIM, the ME shall delete any previously received or locally cached parameters for the calculation of the SUCI including the Routing Indicator, the Home Network Public Key Identifier, the Home Network Public Key and the Protection Scheme Identifier.

#### 5.3.3.2 Conformance requirement

CR 1 SUCI calculation procedure shall be performed by the USIM if services n°124 and n°125 are available in EF<sub>UST</sub>.

Reference:

- TS 31.102 [19], clause 4.4.11.8

CR 2 The ME shall use the GET IDENTITY command in SUCI context to retrieve the SUCI calculated by the USIM.

Reference:



Home Network Public Key:

Byte:	B1	B2	B3	B4	B5	B6	B7	B8
Hex	04	72	DA	71	97	62	34	CE
	<b>B9</b>	<b>B10</b>	<b>B11</b>	<b>B12</b>	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>
	83	3A	69	07	42	58	67	B8
	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	2E	07	4D	44	EF	90	7D	FB
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>	<b>B31</b>	<b>B32</b>
	4B	3E	21	C1	C2	25	6E	BC
	<b>B33</b>	<b>B34</b>	<b>B35</b>	<b>B36</b>	<b>B37</b>	<b>B38</b>	<b>B39</b>	<b>B40</b>
	D1	5A	7D	ED	52	FC	BB	09
	<b>B41</b>	<b>B42</b>	<b>B43</b>	<b>B44</b>	<b>B45</b>	<b>B46</b>	<b>B47</b>	<b>B48</b>
	7A	4E	D2	50	E0	36	C7	B9
	<b>B49</b>	<b>B50</b>	<b>B51</b>	<b>B52</b>	<b>B53</b>	<b>B54</b>	<b>B55</b>	<b>B56</b>
	C8	C7	00	4C	4E	ED	C4	F0
	<b>B57</b>	<b>B58</b>	<b>B59</b>	<b>B60</b>	<b>B61</b>	<b>B62</b>	<b>B63</b>	<b>B64</b>
	68	CD	7B	F8	D3	F9	00	E3
	<b>B65</b>							
	B4							

EF<sub>SUCI\_Calc\_Info</sub>: Not available to the ME

The TT (NG-SS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/083/000001.
- Access control: unrestricted.

The TT (NG-SS) shall be configured with Home Network Private Key for profile B:

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	F1	AB	10	74	47	7E	BC	C7
	<b>B9</b>	<b>B10</b>	<b>B11</b>	<b>B12</b>	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>
	5F	54	EA	1C	5F	C3	68	B1
	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	61	67	30	15	5E	00	41	AC
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>	<b>B31</b>	<b>B32</b>
	44	7D	63	01	97	5F	EC	DA

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and runs an initial activation.

#### 5.3.3.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	READ EF <sub>UST</sub>	(Evaluation of service settings)		
2	USIM	Perform SUCI calculation	The USIM performs a SUCI calculation using Profile B	CR 1	
3	ME > USIM	Send GET IDENTITY	The USIM returns the calculated SUCI. The GET IDENTITY command is sent with Identity Context in P2 as SUCI (0x01)	CR 2 CR 3	A.2/1 OR A.2/2
4	UE > TT	Send REGISTRATION REQUEST	The UE sends a REGISTRATION REQUEST with 5GS registration type IE as "initial registration" and 5GS mobile identity information element type "SUCI"		
5	TT > UE	Send REGISTRATION ACCEPT	The TT sends a REGISTRATION ACCEPT with a new 5G-GUTI		
6	UE > TT	Send REGISTRATION COMPLETE		CR 4	

### 5.3.3.5 Acceptance criteria

CR 1 is implicitly verified. The requirement is met if the expected SUCI is included in the REGISTRATION REQUEST in step 4). The SUCI in the 5GS mobile identity IE. The REGISTRATION REQUEST shall include the following values:

- SUPI format: 0
- Home Network Identifier: 246/081
- Routing Indicator: 1y
- Protection Scheme Identifier: 02
- Home Network Public Key Identifier: 27
- Scheme output: ECC ephemeral public key, encryption of 35793579x and MAC tag value

CR 2 and CR 3 can be verified by a method explicitly verifying the correct execution of the GET IDENTITY command using the expected values (A.2/1 or A.2/2).

CR 4 is met if the UE sends REGISTRATION COMPLETE message to the NG-SS in step 6).

## 5.3.4 UE identification by SUCI in response to IDENTITY REQUEST message

### 5.3.4.1 Definition and applicability

The identification procedure is specified to request a particular UE to provide specific identification parameters, e.g. the SUCI or the IMEI. The SUCI is a privacy preserving identifier containing the concealed SUPI and IMEI is a format of PEI.

The network initiates the identification procedure by sending an IDENTITY REQUEST message to the UE and starting timer T3570. The IDENTITY REQUEST message specifies the requested identification parameters in the Identity type information element and the UE shall be ready to respond to an IDENTITY REQUEST message at any time whilst in 5GMM-CONNECTED mode.

### 5.3.4.2 Conformance requirement

CR 1 A UE shall be ready to respond to an IDENTITY REQUEST message at any time whilst in 5GMM-CONNECTED mode.

CR 2 Upon receipt of the IDENTITY REQUEST message, if the Identity type IE in the IDENTITY REQUEST message is set to "SUCI", the UE shall:

- if timer T3519 is not running, generate a fresh SUCI as specified in TS 33.501 [41], send an IDENTITY RESPONSE message with the SUCI, start timer T3519 and store the value of the SUCI sent in the IDENTITY RESPONSE message; and
- if timer T3519 is running, send an IDENTITY RESPONSE message with the stored SUCI.

CR 3 If the REGISTRATION ACCEPT message contained a 5G-GUTI, the UE shall return a REGISTRATION COMPLETE message to the AMF to acknowledge the received 5G-GUTI, stop timer T3519 if running, and delete any stored SUCI.

Reference:

- TS 31.102 [19], clauses 5.3.47 and 5.3.51;
- TS 33.501 [24], clause Annex C.

CR 4 The ME shall correctly read  $EF_{SUCI\_Calc\_Info}$ ,  $EF_{Routing\_indicator}$  and  $EF_{IMSI}$  from the USIM.

Reference:

- TS 31.102 [19], clause 4.4.11.8 and 5.3.47
- TS 24.501 [25], clause 5.5.1.2.4.

### 5.3.4.3 Test purpose

The purpose of this test is to verify that:

- 1) the ME correctly performs the READ commands for EF<sub>SUCI\_Calc\_Info</sub>, EF<sub>Routing\_indicator</sub> and EF<sub>IMSI</sub> from the USIM,
- 2) the UE will perform SUCI calculation procedure correctly;
- 3) upon reception of the IDENTITY REQUEST message with Identity type IE set to "SUCI", the UE will:
  - if timer T3519 is not running, generate a fresh SUCI, send an IDENTITY RESPONSE message with the SUCI, start timer T3519 and store the value of the SUCI sent in the IDENTITY RESPONSE message; and
  - if timer T3519 is running, send an IDENTITY RESPONSE message with the stored SUCI;
- 4) upon reception of the REGISTRATION ACCEPT message containing a 5G-GUTI UE deletes the stored SUCI and stops timer T3519 if running.

### 5.3.4.4 Method of test

#### 5.3.4.4.1 Initial conditions

The values of the default 5G-NR UICC defined in clause 4.5.9 of the present document are used with EF<sub>IMSI</sub> as defined in clause 4.6.5, EF<sub>Routing\_Indicator</sub> as defined in clause 4.6.7 and the following exception:

**EF<sub>5GS3GPPLOC1</sub>** (5GS 3GPP Location Information)

Logically:

5G-GUTI: 244 083 00010266436587  
 TAI (MCC/MNC/TAC): 244/083/000001  
 5GS update status: 5U2 NOT UPDATED

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	00	0B	F2	42	34	80	00	01
	<b>B9</b>	<b>B10</b>	<b>B11</b>	<b>B12</b>	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>
	02	66	43	65	87	42	34	80
	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>				
	00	00	01	01				

The TT (NG-SS) transmits on the BCCH, with the following network parameters:

Cell A:

- TAI (MCC/MNC/TAC): 244/083/000001
- Access control: unrestricted.

Cell B:

- TAI (MCC/MNC/TAC): 244/084/000001
- Access control: unrestricted.

The Cell A on the TT (NG-SS) is activated and transmits on the BCCH.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and runs an initial activation.

## 5.3.4.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	READ EF <sub>IMSI</sub> , EF <sub>SUCI_Calc_Info</sub> , EF <sub>Routing_indicator</sub>		CR 4	A.2/1 OR A.2/2
2	UE > TT	Send REGISTRATION REQUEST	The UE sends a REGISTRATION REQUEST to Cell A with 5GS registration type IE as "initial registration" and 5GS mobile identity information element type "5G-GUTI" and starts the timer T3519		
3	TT > UE	Send IDENTITY REQUEST	The TT sends an IDENTITY REQUEST indicating that the Identity type information element is "SUCI" and starts the timer T3570		
4	UE > TT	Send IDENTITY RESPONSE	The UE sends an IDENTITY RESPONSE message with a fresh generated SUCI, starts the timer T3519 and stores the new SUCI	CR 1 CR 2	
5	TT > UE	Send IDENTITY REQUEST	The TT ignores the IDENTITY RESPONSE sent by the UE and re-sends the IDENTITY REQUEST indicating that the Identity type information element is "SUCI" before the expiry of T3519		
6	UE > TT	Send IDENTITY RESPONSE	The UE sends an IDENTITY RESPONSE message with the stored SUCI	CR 1 CR 2	
7	TT > UE	Send REGISTRATION ACCEPT	The TT sends a REGISTRATION ACCEPT message with a 5G-GUTI and stops timer T3570 (if running)		
8	UE > TT	Send REGISTRATION COMPLETE	The UE stops the timers T3510 (if running) and T3519 and deletes the stored SUCI	CR 3	
9	TT	Deactivate Cell A on BCCH then activate Cell B on BCCH			
10	UE > TT	Send REGISTRATION REQUEST	The UE sends a REGISTRATION REQUEST to Cell B with 5GS registration type IE as "mobility registration updating" or as "initial registration" and 5GS mobile identity information element type "5G-GUTI" and starts timer T3510		
11	TT > UE	Send IDENTITY REQUEST	The TT sends an IDENTITY REQUEST indicating that the Identity type information element is "SUCI" and starts timer T3570		
12	UE > TT	Send IDENTITY RESPONSE	The UE sends an IDENTITY RESPONSE message with a fresh generated SUCI, starts timer T3519 and stores the new SUCI	CR 1 CR 2	
13	TT > UE	Send REGISTRATION ACCEPT	The TT sends a REGISTRATION ACCEPT message with a 5G-GUTI and stops the timer T3570 (if running)		
14	UE > TT	Send REGISTRATION COMPLETE	The UE sends a REGISTRATION COMPLETE message, stops the timers T3510 (if running) and T3519 and deletes the stored SUCI	CR 3	

## 5.3.4.5 Acceptance criteria

CR 1 and CR 2 are implicitly verified in step 4), step 6) and step 12). The conformance requirements are met if the UE sends an IDENTITY RESPONSE message with:

- a fresh generated SUCI if timer T3519 is not running;
- the stored SUCI if timer T3519 is running.

CR 3 is implicitly verified in step 8) and step 14). The conformance requirement is met if the UE sent a REGISTRATION COMPLETE message after receiving the 5G-GUTI.

CR 4 can be verified in step 1) by a method explicitly verifying the correct execution of the READ commands on the listed EFs (A.2/1 or A.2/2). CR 4 is met if the READ procedure on EF<sub>SUCI\_Calc\_Info</sub>, EF<sub>Routing\_indicator</sub> and EF<sub>IMSI</sub> has been executed as defined in [28], clause 14.1.1.

## 5.3.5 UE identification by SUCI in response to IDENTITY REQUEST message with T3519 timer expiry

### 5.3.5.1 Definition and applicability

The identification procedure is specified to request a particular UE to provide specific identification parameters, e.g. the SUCI or the IMEI. The SUCI is a privacy preserving identifier containing the concealed SUPI and IMEI is a format of PEI.

The network initiates the identification procedure by sending an IDENTITY REQUEST message to the UE and starting timer T3570. The IDENTITY REQUEST message specifies the requested identification parameters in the Identity type information element and the UE shall be ready to respond to an IDENTITY REQUEST message at any time whilst in 5GMM-CONNECTED mode.

### 5.3.5.2 Conformance requirement

CR 1 A UE shall be ready to respond to an IDENTITY REQUEST message at any time whilst in 5GMM-CONNECTED mode.

CR 2 Upon receipt of the IDENTITY REQUEST message, if the Identity type IE in the IDENTITY REQUEST message is set to "SUCI", the UE shall:

- if timer T3519 is not running, generate a fresh SUCI as specified in TS 33.501 [41], send an IDENTITY RESPONSE message with the SUCI, start timer T3519 and store the value of the SUCI sent in the IDENTITY RESPONSE message; and
- if timer T3519 is running, send an IDENTITY RESPONSE message with the stored SUCI.

CR 3 If the REGISTRATION ACCEPT message contained a 5G-GUTI, the UE shall return a REGISTRATION COMPLETE message to the AMF to acknowledge the received 5G-GUTI, stop timer T3519 if running, and delete any stored SUCI.

Reference:

- TS 31.102 [19], clauses 5.3.47 and 5.3.51;
- TS 33.501 [24], clause Annex C.

CR 4 On expiry of timer T3519 (60s) the UE shall delete the stored SUCI

Reference:

- TS 24.501 [25], Table 10.2.1.

CR 5 During initial registration the UE handles the 5GS mobile identity IE in the following order as defined in TS 24.501 [25] clause 5.5.1.2.2:

- a) a valid 5G-GUTI assigned by the same PLMN;
- b) a valid 5G-GUTI assigned by an equivalent PLMN;
- c) a valid 5G-GUTI assigned by any other PLMN;

- d) a SUCI is available in the UE.

### 5.3.5.3 Test purpose

The purpose of this test is to verify that:

- 1) the ME correctly performs the READ commands for EF<sub>SUCI\_Calc\_Info</sub>, EF<sub>Routing\_indicator</sub> and EF<sub>IMSI</sub> from the USIM,
- 2) upon reception of the IDENTITY REQUEST message with Identity type IE set to "SUCI", the UE will:
  - if timer T3519 is not running, generate a fresh SUCI, send an IDENTITY RESPONSE message with the SUCI, start timer T3519 and store the value of the SUCI sent in the IDENTITY RESPONSE message; and
  - if timer T3519 is running, send an IDENTITY RESPONSE message with the stored SUCI,
- 3) upon expiry of T3519 UE deletes the stored SUCI,
- 4) the UE handles the 5GS mobile identity IE in the correct order during initial registration and use 5G-GUTI as identity when it has both, a valid 5G-GUTI and the SUCI.

### 5.3.5.4 Method of test

#### 5.3.5.4.1 Initial conditions

The values of the default 5G-NR UICC defined in clause 4.5.9 of the present document are used with EF<sub>IMSI</sub> as defined in clause 4.6.5, EF<sub>Routing\_Indicator</sub> as defined in clause 4.6.7 and the following exception:

**EF<sub>5GS3GPPLOC</sub>** (5GS 3GPP Location Information)

Logically:

5G-GUTI: 244 083 00010266436587  
 TAI (MCC/MNC/TAC): 244/083/000001  
 5GS update status: 5U2 NOT UPDATED

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	00	0B	F2	42	34	80	00	01
	<b>B9</b>	<b>B10</b>	<b>B11</b>	<b>B12</b>	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>
	02	66	43	65	87	42	34	80
	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>				
	00	00	01	01				

The TT (NG-SS) transmits on the BCCH, with the following network parameters:

Cell A:

- TAI (MCC/MNC/TAC): 244/083/000001
- CellIdentity: 000000001
- Access control: unrestricted.

Cell B :

- TAI (MCC/MNC/TAC): 244/084/000001
- CellIdentity: 000000002
- Access control: unrestricted.

The Cell A on the TT (NG-SS) is activated and transmits on the BCCH.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and runs an initial activation.

## 5.3.5.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE > TT	Send REGISTRATION REQUEST	The UE sends a REGISTRATION REQUEST to Cell A with 5GS registration type IE as "initial registration" and 5GS mobile identity information element type "5G-GUTI" and starts timer T3510	CR 5	
2	TT > UE	Send IDENTITY REQUEST	The TT sends an IDENTITY REQUEST message indicating that the Identity type information element is "SUCI"	CR 1 CR 2	
3	UE > TT	Send IDENTITY RESPONSE	The UE sends an IDENTITY RESPONSE message with a fresh generated SUCI, starts the timer T3519 and stores the new SUCI		
4	TT	Deactivate Cell A on BCCH and then activate Cell B on BCCH	Execute before the expiry of timer T3519 and the UE stops timer T3510		
5	UE > TT	Send REGISTRATION REQUEST	While timer T3519 is running the UE sends a REGISTRATION REQUEST to Cell B with 5GS registration type IE as "initial registration" and 5GS mobile identity information element type "5G-GUTI" and starts timer T3510	CR 5	
6	TT > UE	Send IDENTITY REQUEST	The TT sends an IDENTITY REQUEST indicating that the Identity type information element is "SUCI"		
7	UE > TT	Send IDENTITY RESPONSE	The UE sends an IDENTITY RESPONSE message with the stored SUCI		
8	TT	Deactivate Cell B on BCCH and then activate Cell A on BCCH	Execute after 70 sec (after timer T3519 expires) and the UE stops timer T3510		
9	UE > TT	Send REGISTRATION REQUEST	The UE sends a REGISTRATION REQUEST to Cell A with 5GS registration type IE as "initial registration" and 5GS mobile identity information element type "5G-GUTI" and starts timer T3510	CR 5	
10	TT > UE	Send IDENTITY REQUEST	The TT sends an IDENTITY REQUEST indicating that the Identity type information element is "SUCI"		
11	UE > TT	Send IDENTITY RESPONSE	The UE sends an IDENTITY RESPONSE message with the freshly generated SUCI, starts timer T3519 and stores the new SUCI	CR 1 CR 2	
12	TT > UE	Send REGISTRATION ACCEPT	The TT sends a REGISTRATION ACCEPT message with a 5G-GUTI		
13	UE > TT	Send REGISTRATION COMPLETE	The UE sends the REGISTRATION COMPLETE message, stops timers T3510 and T3519 (if running) and deletes the stored SUCI	CR 3 CR 4	

## 5.3.5.5 Acceptance criteria

CR 1 and CR 2 are implicitly verified in step 2) and step 11). The conformance requirements are met if the UE sends an IDENTITY RESPONSE message with:

- a fresh generated SUCI if timer T3519 is not running;
- the stored SUCI if timer T3519 is running.

CR 3 is implicitly verified in step 13). The conformance requirement is met if the UE sent a REGISTRATION COMPLETE message after receiving the 5G-GUTI.

CR 4 is verified in step 13). The conformance requirement is met if no SUCI is stored on the UE, i.e., no two successive GET IDENTITY commands in steps 3), 7) and 11) are identical.

CR 5 is implicitly verified in step 1), step 5) and step 9). The conformance requirement is met if the expected 5GS mobile identity IE is sent in the REGISTRATION REQUEST during initial registration.

## 5.3.6 UE identification by SUCI in response to IDENTITY REQUEST message and AUTHENTICATION REJECT

### 5.3.6.1 Definition and applicability

The identification procedure is specified to request a particular UE to provide specific identification parameters, e.g. the SUCI or the IMEI. The SUCI is a privacy preserving identifier containing the concealed SUPI and IMEI is a format of PEI.

The network initiates the identification procedure by sending an IDENTITY REQUEST message to the UE and starting timer T3570. The IDENTITY REQUEST message specifies the requested identification parameters in the Identity type information element and the UE shall be ready to respond to an IDENTITY REQUEST message at any time whilst in 5GMM-CONNECTED mode.

### 5.3.6.2 Conformance requirement

CR 1 A UE shall be ready to respond to an IDENTITY REQUEST message at any time whilst in 5GMM-CONNECTED mode.

Reference:

- TS 24.501 [25], clause 5.4.3.3
- TS 31.102 [19], clauses 4.4.11.8, 4.4.11.11, 5.3.47 and 5.3.51

CR 2 Upon receipt of the IDENTITY REQUEST message, if the Identity type IE in the IDENTITY REQUEST message is set to "SUCI", the UE shall:

- if timer T3519 is not running, generate a fresh SUCI as specified in TS 33.501 [24], send an IDENTITY RESPONSE message with the SUCI, start timer T3519 and store the value of the SUCI sent in the IDENTITY RESPONSE message;

and

- if timer T3519 is running, send an IDENTITY RESPONSE message with the stored SUCI. The UE shall use the GET IDENTITY command in SUCI context to retrieve the SUCI calculated by the USIM.

Reference:

- TS 24.501 [25], clause 5.4.3.3

CR 3 If the REGISTRATION ACCEPT message contained a 5G-GUTI, the UE shall return a REGISTRATION COMPLETE message to the AMF to acknowledge the received 5G-GUTI, stop timer T3519 if running, and delete any stored SUCI

Reference:

- TS 24.501 [25], clause 5.5.1.2.4

CR 4 If the AUTHENTICATION REJECT message is received by the UE, the UE shall abort any 5GMM signalling procedure, stop any of the timers T3510, T3516, T3517, T3519 or T3521 (if they were running), delete stored SUCI and enter state 5GMM-DEREGISTERED.

Reference:

- TS 24.501 [25], clause 8.2.5

### 5.3.6.3 Test purpose

The purpose of this test is to verify that:

- 1) the READ EF<sub>SUCI\_Calc\_Info</sub>, EF<sub>Routing\_Indicator</sub> and EF<sub>MSI</sub> commands are performed correctly by the ME;
- 2) the ME will perform SUCI calculation procedure correctly;
- 3) upon reception of the IDENTITY REQUEST message with Identity type IE set to "SUCI", the UE will:
  - if timer T3519 is not running, generate a fresh SUCI as specified in TS 33.501 [24], send an IDENTITY RESPONSE message with the SUCI, start timer T3519 and store the value of the SUCI sent in the IDENTITY RESPONSE message;
- and
- if timer T3519 is running, send an IDENTITY RESPONSE message with the stored SUCI;
- 4) upon receiving the AUTHENTICATION REJECT the UE deletes the stored SUCI.

### 5.3.6.4 Method of test

#### 5.3.6.4.1 Initial conditions

The values of the default 5G-NR UICC defined in clause 4.5.9 of the present document are used with EF<sub>MSI</sub> as defined in clause 4.6.5 and the following exceptions:

**EF<sub>5GS3GPPLOC</sub>** (5GS 3GPP Location Information)

Logically:

5G-GUTI: 244 083 00010266436587  
 TAI (MCC/MNC/TAC): 244/083/000001  
 5GS update status: 5U2 NOT UPDATED

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	00	0B	F2	42	34	80	00	01
	B9	B10	B11	B12	B13	B14	B15	B16
	02	66	43	65	87	42	34	80
	B17	B18	B19	B20				
	00	00	01	01				

The TT (NG-SS) transmits on the BCCH, with the following network parameters:

Cell A:

- TAI (MCC/MNC/TAC): 244/083/000001
- Access control: unrestricted.

Cell B:

- TAI (MCC/MNC/TAC): 244/084/000001
- Access control: unrestricted.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and runs an initial activation.

## 5.3.6.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	TT	Bring up Cell A			
2	UE > TT	Send REGISTRATION REQUEST	The UE sends a REGISTRATION REQUEST to Cell A with 5GS registration type IE as "initial registration" and 5GS mobile identity information element type "5G-GUTI" and starts the timer T3519		
3	TT > UE	Send IDENTITY REQUEST	The IDENTITY REQUEST is indicating that the Identity type information element is "SUCI"		
4	UE > TT	Send IDENTITY RESPONSE	The UE sends an IDENTITY RESPONSE containing the fresh generated SUCI and starts the timer T3519	CR 1 CR 2 CR 3	
5	TT > UE	Send AUTHENTICATION REQUEST			
6	UE > TT	Send AUTHENTICATION RESPONSE			
7	TT > UE	Send AUTHENTICATION REJECT			
8	UE	Stop timer T3510 Stop timer T3519 Delete stored SUCI Abort any 5GMM signalling procedure	Enter state 5GMM-DEREGISTERED	CR 4	
9	TT	Bring down Cell A Bring up Cell B			
10	USER/TT	Power off/deactivate the UE, then run activation of the UE			
11	UE > TT	Send REGISTRATION REQUEST	The UE sends a REGISTRATION REQUEST to Cell B with 5GS registration type IE as "initial registration" and 5GS mobile identity information element type "SUCI" containing the fresh generated SUCI, starts the timers T3510 and T3519 and delete the stored SUCI		
12	TT > UE	Send REGISTRATION ACCEPT	The REGISTRATION ACCEPT message contains a 5G-GUTI		
13	UE > TT	Send REGISTRATION COMPLETE	The UE i.a. acknowledges the received 5G-GUTI, stops the timers T3510 and T3519 if running and delete the stored SUCI		
NOTE: a verification of timer states as indicated in steps 2), 4), 11) and 13) is not required. An explicit verification may be possible on MEs providing the related information.					

## 5.3.6.5 Acceptance criteria

CR 1, CR 2 and CR 3 are implicitly verified if the UE returns an IDENTITY RESPONSE containing the expected SUCI in step 4).

CR 4 can be verified on the TT. The requirement is met if no signalling is received from the UE during step 8).

## 5.3.7 SUCI calculation by the ME using null scheme – missing parameters for subscription identifier privacy support by the USIM

## 5.3.7.1 Definition and applicability

If the operator's decision is that ME shall calculate the SUCI, the home network operator shall provision a list of the Protection Scheme Identifiers that the operator allows in the USIM. The list of Protection Scheme Identifiers in the USIM may contain one or more Protection Scheme Identifiers in order of their priority. The ME shall read the SUCI calculation information from the USIM, including the SUPI, the Home Network Public Key, the Home Network Public Key Identifier, and the list of Protection Scheme Identifiers. The ME shall select the protection scheme from its supported schemes that has the highest priority in the list obtained from the USIM.

The ME shall calculate the SUCI using the null-scheme if one or more parameters (i.e. Home Network Public Key, Protection Scheme Identifier) required for the calculation of the SUCI are not provisioned in the USIM.

### 5.3.7.2 Conformance requirement

CR 1 SUCI calculation procedure shall be performed by the ME if Service n°124 is available and Service n°125 is "not available" in EF<sub>UST</sub>

Reference:

- TS 31.102 [19], clause 5.3.47

CR 2 As part of the SUCI calculation performed by the ME, the ME shall perform reading procedure on EF<sub>SUCI\_Calc\_Info</sub> and EF<sub>Routing\_Indicator</sub>.

Reference:

- TS 31.102 [19], clauses 4.4.11.8, 4.4.11.11, 5.3.47 and 5.3.51

CR 3 The ME shall calculate the SUCI using the null-scheme if no Protection Scheme Identifier is provisioned in the USIM or if there is no Home Network Public Key configured in the USIM for the highest priority protection scheme configured in the USIM that the ME supports

Reference:

- TS 33.501 [24], Annex C

### 5.3.7.3 Test purpose

The purpose of this test is to verify that:

- 1) the READ EF<sub>SUCI\_Calc\_Info</sub>, EF<sub>Routing\_Indicator</sub> and EF<sub>IMSI</sub> commands are performed correctly by the ME;
- 2) the ME correctly performs the SUCI calculation procedure using null-scheme.

### 5.3.7.4 Method of test

#### 5.3.7.4.1 Initial conditions

The values of the default 5G-NR UICC defined in clause 4.5.9 of the present document are used with EF<sub>IMSI</sub> as defined in clause 4.6.5 and the following exceptions:

The USIM does not have the Home Network Public Key configured for the highest priority protection scheme configured in the USIM that the ME supports.

EF<sub>SUCI\_Calc\_Info</sub> (Subscription Concealed Identifier Calculation Information EF)

Logically:

null

Coding:

Byte	B1	B2	B3	B4	B5	B6
Hex	A0	02	01	01	A1	00

The TT (NG-SS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/083/000001,
- Access control: unrestricted.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and runs an initial activation.

### 5.3.7.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	READ EF <sub>IMSI</sub> , EF <sub>UST</sub> , EF <sub>SUCI_Calc_Info</sub> , EF <sub>Routing_Indicator</sub>	(Evaluation of service settings)	CR 1	A.2/1 OR A.2/2
2	UE > TT	Send REGISTRATION REQUEST	The UE sends a REGISTRATION REQUEST to Cell A with 5GS registration type IE as "initial registration" and 5GS mobile identity information element type "SUCI"	CR 2	
3	TT > UE	Send REGISTRATION ACCEPT	The REGISTRATION ACCEPT message contains a 5G-GUTI		
4	UE > TT	Send REGISTRATION COMPLETE	i.a. acknowledge the received 5G-GUTI		

### 5.3.7.5 Acceptance criteria

CR 1 can be verified by a method explicitly verifying the correct execution of the READ commands on the listed EFs (A.2/1 or A.2/2).

CR 2 is met if the 5GS mobile identity IE in the REGISTRATION REQUEST contains the SUCI as coded below:

SUPI format: 0  
 Home Network Identifier: 246/081  
 Routing indicator: 17  
 Protection scheme id: 00  
 Home network public key Id: 0  
 Scheme output: 357935793

## 5.3.8 UE identification by 5G-GUTI – Last Registered TAI stored on USIM

### 5.3.8.1 Definition and applicability

A globally unique temporary user identity for 5GS-based services, the 5G globally unique temporary identity (5G-GUTI), is used for identification within the signalling procedures. A UE supporting N1 mode includes a valid 5G-GUTI, if any is available, in the REGISTRATION REQUEST and DEREGISTRATION REQUEST messages.

### 5.3.8.2 Conformance requirement

CR 1 The following 5GMM parameters shall be stored on the USIM if the corresponding file is present:

- 5G-Globally Unique Temporary Identifier (5G-GUTI);
- Last visited registered Tracking Area Identity in 5GS (TAI);
- 5GS update status.

Reference:

- TS 31.102 [19], clauses 4.4.11.2

CR 2 If the corresponding file is not present on the USIM, these 5GMM parameters are stored in a non-volatile memory in the ME together with the SUPI from the USIM. These 5GMM parameters can only be used if the SUPI from the USIM matches the SUPI stored in the non-volatile memory; else the UE shall delete the 5GMM parameters.

Reference:

- TS 24.501 [25], clauses 5.3.3, 5.5.1.2 and Annex C.

### 5.3.8.3 Test purpose

The purpose of this test is to verify that:

1. the READ EF<sub>5GS3GPPLOC1</sub> and EF<sub>IMSI</sub> commands are performed correctly by the ME;
2. the ME correctly uses the 5G-GUTI in the REGISTRATION REQUEST.

### 5.3.8.4 Method of test

#### 5.3.8.4.1 Initial conditions

The values of the default 5G-NR UICC defined in clause 4.5.9 of the present document are used with EF<sub>IMSI</sub> as defined in clause 4.6.5 and the following exceptions:

#### EF<sub>5GS3GPPLOC1</sub>

Logically:

5G-GUTI: 244 083 00010266436587  
 TAI (MCC/MNC/TAC): 244/083/000001  
 5GS update status: 5U2 NOT UPDATED

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	00	0B	F2	42	34	80	00	01
	B9	B10	B11	B12	B13	B14	B15	B16
	02	66	43	65	87	42	34	80
	B17	B18	B19	B20				
	00	00	01	01				

The TT (NG-SS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/083/000002
- Access control: unrestricted.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and runs an initial activation.

#### 5.3.8.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	TT	Bring up the NG-SS			
2	UE	READ EF <sub>IMSI</sub> , EF <sub>5GS3GPPLOC1</sub>		CR 1	A.2/1 OR A.2/2
3	UE > TT	Send REGISTRATION REQUEST	The UE sends a REGISTRATION REQUEST to the NG-SS with 5GS registration type IE as "initial registration" and 5GS mobile identity information element type "5G-GUTI"		
4	TT > UE	Send REGISTRATION ACCEPT	The REGISTRATION ACCEPT message contains: - 5G-GUTI: "2440830001026655555" - 5GS TAI list with TAI with: - TAI: 244/083/000002		
5	UE > TT	Send REGISTRATION COMPLETE	The UE i.a. acknowledges the received 5G-GUTI, sends the REGISTRATION COMPLETE message and stops timers T3510 (if running)		

6	USER/TT	Power off/deactivate the UE, then run activation of the UE	The UE updates the USIM with valid NAS security context		
7	UE	READ EF <sub>IMSI</sub> , EF <sub>5GS3GPPLOCI</sub>		CR 1	A.2/1 OR A.2/2
8	UE > TT	Send REGISTRATION REQUEST	The UE sends a REGISTRATION REQUEST to the NG-SS with 5GS registration type IE as "initial registration" and 5GS mobile identity information element type "5G-GUTI" and starts the timer T3510	CR 2	
9	TT > UE	Send REGISTRATION ACCEPT	The REGISTRATION ACCEPT message contains a 5G-GUTI. The UE i.a. acknowledge the received 5G-GUTI		
NOTE: a verification of timer states as indicated in steps 5) and 8) is not required. An explicit verification may be possible on MEs providing the related information.					

### 5.3.8.5 Acceptance criteria

CR 1 can be verified by a method explicitly verifying the correct execution of the READ commands in steps 2) and 7) on the listed EFs (A.2/1 or A.2/2).

CR 2 is implicitly verified if the REGISTRATION REQUEST in step 7) contains the new 5G-GUTI and the last visited TAI:

SUPI format: 244 083 00010266555555

TAI (MCC/MNC/TAC): 244/083/000002

## 5.3.9 UE identification by 5G-GUTI – Last Registered TAI stored by ME

### 5.3.9.1 Definition and applicability

A globally unique temporary user identity for 5GS-based services, the 5G globally unique temporary identity (5G-GUTI), is used for identification within the signalling procedures. A UE supporting N1 mode includes a valid 5G-GUTI, if any is available, in the REGISTRATION REQUEST and DEREGISTRATION REQUEST messages.

### 5.3.9.2 Conformance requirement

CR 1 The following 5GMM parameters shall be stored on the USIM if the corresponding file is present:

- 5G-Globally Unique Temporary Identifier (5G-GUTI);
- Last visited registered Tracking Area Identity in 5GS (TAD);
- 5GS update status.

Reference:

- TS 31.102 [19], clauses 4.4.11.2

CR 2 If the corresponding file is not present on the USIM, these 5GMM parameters are stored in a non-volatile memory in the ME together with the SUPI from the USIM. These 5GMM parameters can only be used if the SUPI from the USIM matches the SUPI stored in the non-volatile memory; else the UE shall delete the 5GMM parameters.

Reference:

- TS 24.501 [25], clauses 5.3.3, 5.5.1.2 and Annex C.

### 5.3.9.3 Test purpose

The purpose of this test is to verify that:

- 1) the READ EF<sub>IMSI</sub> commands are performed correctly by the ME;
- 2) the ME correctly uses the 5G-GUTI in the REGISTRATION REQUEST;
- 3) the ME stores the new 5G-GUTI in its non-volatile memory if the corresponding file is not present in the USIM.

### 5.3.9.4 Method of test

#### 5.3.9.4.1 Initial conditions

The values of the default 5G-NR UICC defined in clause 4.5.9 of the present document are used with EF<sub>IMSI</sub> as defined in clause 4.6.5.

The TT (NG-SS) transmits on the BCCH, with the following network parameters:

Cell A:

- TAI (MCC/MNC/TAC): 244/083/000001
- Access control: unrestricted.

Cell B:

- TAI (MCC/MNC/TAC): 244/084/000001
- Access control: unrestricted.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and runs an initial activation.

#### 5.3.9.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	TT	Bring up the Cell A			
2	UE	READ EF <sub>IMSI</sub>		CR 1	A.2/1 OR A.2/2
3	UE > TT	Send REGISTRATION REQUEST	The UE sends a REGISTRATION REQUEST to the NG-SS with 5GS registration type IE as "initial registration"		
4	TT > UE	Send REGISTRATION ACCEPT	The REGISTRATION ACCEPT message contains: - 5G-GUTI: "24408300010266436587" - 5GS TAI list with TAI with: - TAI: 244/083/000002		
5	UE > TT	Send REGISTRATION COMPLETE			
6	USER/TT	Power off/deactivate the UE, then run activation of the UE			
7	UE > TT	Send REGISTRATION REQUEST	The UE sends a REGISTRATION REQUEST to the NG-SS with 5GS registration type IE as "initial registration" and 5GS mobile identity information element type "5G-GUTI" and starts the timer T3510	CR 2	
8	TT > UE	Send REGISTRATION ACCEPT	The REGISTRATION ACCEPT message contains: - 5G-GUTI: "24408300010266434444" - 5GS TAI list with TAI with: - TAI: 244/083/000001		
9	UE > TT	Send REGISTRATION COMPLETE	The UE sends a REGISTRATION COMPLETE and stops the timer T3510		
10	TT	Bring down Cell A Bring up Cell B			

11	UE > TT	Send REGISTRATION REQUEST	The UE sends a REGISTRATION REQUEST to the NG-SS with 5GS registration type IE as "mobility registration updating" or as "initial registration" and 5GS mobile identity information element type "5G-GUTI" and starts the timer T3510	CR 2	
NOTE: a verification of timer states as indicated in steps 7), 9) and 11) is not required. An explicit verification may be possible on MEs providing the related information.					

### 5.3.9.5 Acceptance criteria

CR 1 can be verified by a method explicitly verifying the correct execution of the READ commands in step 2) on the listed EFs (A.2/1 or A.2/2).

CR 2 is implicitly verified if the REGISTRATION REQUEST in step 7) contains the following parameters:

5G-GUTI: 244 083 00010266436587

Last visited registered TAI: 244/083/000002

and in step 11):

5G-GUTI: 244 083 00010266434444

Last visited registered TAI: 244/083/000001

## 5.3.10 UE identification after SUPI is changed

### 5.3.10.1 Definition and applicability

A globally unique temporary user identity for 5GS-based services, the 5G globally unique temporary identity (5G-GUTI), is used for identification within the signalling procedures. A UE supporting N1 mode includes a valid 5G-GUTI, if any is available, in the REGISTRATION REQUEST and DEREGISTRATION REQUEST messages.

### 5.3.10.2 Conformance requirement

CR 1 The following 5GMM parameters shall be stored on the USIM if the corresponding file is present:

- 5G-Globally Unique Temporary Identifier (5G-GUTI);
- Last visited registered Tracking Area Identity in 5GS (TAI);
- 5GS update status;
- 5G NAS security context parameters from a full native 5G NAS security context.

NOTE: The presence and format of corresponding files on the USIM is specified in TS 31.102 [4].

Reference:

- TS 31.102 [19], clauses 4.4.11.2

CR 2 If the corresponding file is not present on the USIM, these 5GMM parameters are stored in a non-volatile memory in the ME together with the SUPI from the USIM. These 5GMM parameters can only be used if the SUPI from the USIM matches the SUPI stored in the non-volatile memory; else the UE shall delete the 5GMM parameters.

Reference:

- TS 24.501 [25], clauses 5.3.3, 5.5.1.2 and Annex C.

CR 3 The ME correctly performs the READ BINARY command on EF<sub>IMSI</sub>.

References:

- TS 31 101 [33], clause 11.1.3;
- ETSI TS 102 221 [8], clause 11.1.3 and 14.1.1.

### 5.3.10.3 Test purpose

The purpose of this test is to verify that:

- 1) the READ EF<sub>IMSI</sub> commands are performed correctly by the ME;
- 2) the ME deletes the 5GMM parameters from non-volatile memory in case SUPI is changed.

### 5.3.10.4 Method of test

#### 5.3.10.4.1 Initial conditions

The values of the E-UTRAN UICC defined in clause 4.5.3 of the present document are used with EF<sub>IMSI</sub> as defined in clause 4.6.5.

The TT (NG-SS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/083/000001
- Access control: unrestricted.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and runs an initial activation.

#### 5.3.10.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	READ EF <sub>IMSI</sub>		CR 3	A.2/1 OR A.2/2
2	UE > TT	Send REGISTRATION REQUEST	The UE sends a REGISTRATION REQUEST to the NG-SS with 5GS registration type IE as "initial registration"		
3	TT > UE	Send REGISTRATION ACCEPT	The REGISTRATION ACCEPT message contains: - 5G-GUTI: "24408300010266436587" - 5GS TAI list with TAI with: - TAI: 244/083/000001		
4	UE > TT	Send REGISTRATION COMPLETE			
5	USER/TT	Power off/deactivate the UE			
6	UE	Change UICC configuration	The IMSI is set to: "246081685533963"		
7	USER/TT	Run activation of the UE			
8	UE > TT	Send REGISTRATION REQUEST	The UE sends a REGISTRATION REQUEST to the NG-SS	CR 1 CR 2	

### 5.3.10.5 Acceptance criteria

CR 1 and CR 2 are implicitly verified in the REGISTRATION REQUESTs in step 8). The used E-UTRAN UICC shall not be capable to store any 5G related information. Therefore, none of the information provided in step 3) shall be available second REGISTRATION REQUEST.

## 5.3.11 SUCI calculation by ME using Profile A

### 5.3.11.1 Definition and applicability

If the operator's decision is that the ME shall calculate the SUCI, the Home Network Operator shall provision a list of the Protection Scheme Identifiers that the operator allows in the USIM. The list of Protection Scheme Identifiers in the USIM may contain one or more Protection Scheme Identifiers in order of their priority. The ME shall read the SUCI calculation information from the USIM, including the SUPI, the Home Network Public Key, the Home Network Public Key Identifier, and the list of Protection Scheme Identifiers. The ME shall select the protection scheme from its supported schemes that has the highest priority in the list obtained from the USIM.

### 5.3.11.2 Conformance requirement

CR 1 SUCI calculation procedure shall be performed by the ME if Service n°124 is available and Service n°125 is not available in EF<sub>UST</sub>

Reference:

- TS 31.102 [19], clause 5.3.47

CR 2 As part of the SUCI calculation performed by the ME, the ME performs the reading procedure with EF<sub>SUCI\_Calc\_Info</sub>.

Reference:

- TS 31.102 [19], clauses 4.4.11.8 and 5.3.47.

CR 3 The ME shall calculate the SUCI using the ECIES scheme profile A if highest priority of the protection schemes listed in the USIM is the ECIES scheme profile A.

References:

- TS 31 101 [33], clause 11.1.3;
- ETSI TS 102 221 [8], clause 11.1.3 and 14.1.1.

### 5.3.11.3 Test purpose

The purpose of this test is to verify that:

- 1) the READ EF<sub>Routing\_Indicator</sub>, EF<sub>SUCI\_Calc\_Info</sub> and EF<sub>MSI</sub> commands are performed correctly by the ME;
- 2) To verify that the ME performs SUCI calculation procedure using the profile with the highest priority (i.e. ECIES scheme profile A and the Home Network Public Key).

### 5.3.11.4 Method of test

#### 5.3.11.4.1 Initial conditions

The values of the default 5G-NR UICC defined in clause 4.5.9 of the present document are used with EF<sub>MSI</sub> as defined in clause 4.6.5 and the following exceptions:

EF<sub>SUCI\_Calc\_Info</sub> (Subscription Concealed Identifier Calculation Information EF)

Logically:

Protection Scheme Identifier List data object:

Protection Scheme Identifier 1 – ECIES scheme profile A  
 Key Index 1: 1  
 Protection Scheme Identifier 2 – ECIES scheme profile B  
 Key Index 2: 2  
 Protection Scheme Identifier 3 – null-scheme  
 Key Index 3: 0

## Home Network Public Key List data object

Home Network Public Key 1 Identifier: 30

Home Network Public Key 1:

- 5A 8D 38 86 48 20 19 7C 33 94 B9 26 13 B2 0B 91 63 3C BD 89 71 19 27 3B F8 E4 A6 F4 EE C0 A6 50

Home Network Public Key 2 Identifier: 27

Home Network Public Key 2:

- 04 72 DA 71 97 62 34 CE 83 3A 69 07 42 58 67 B8 2E 07 4D 44 EF 90 7D FB 4B 3E 21 C1 C2 25 6E BC D1 5A 7D ED 52 FC BB 09 7A 4E D2 50 E0 36 C7 B9 C8 C7 00 4C 4E ED C4 F0 68 CD 7B F8 D3 F9 00 E3 B4

The NG-SS shall be configured with Home Network Private Key as following (for Profile A):

Coding:	B1	B2	B3	B4	B5	B6	B7	B8
Hex	C5	3C	22	20	8B	61	86	0B
	<b>B9</b>	<b>B10</b>	<b>B11</b>	<b>B12</b>	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>
	06	C6	2E	54	06	A7	B3	30
	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	C2	B5	77	AA	55	58	98	15
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>	<b>B31</b>	<b>B32</b>
	10	D1	28	24	7D	38	BD	1D

The TT (NG-SS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/083/000001
- Access control: unrestricted.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and runs an initial activation.

## 5.3.11.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	READ EF <sub>IMSI</sub> , EF <sub>UST</sub> , EF <sub>Routing_Indicator</sub> and EF <sub>SUCI_Calc_Info</sub>	(Evaluation of service settings)	CR 2	A.2/1 OR A.2/2
2	ME	Perform SUCI calculation	The ME performs a SUCI calculation using Profile A	(CR 3)	
3	UE > TT	Send REGISTRATION REQUEST	The UE sends a REGISTRATION REQUEST to the NG-SS with 5GS registration type IE as "initial registration" and 5GS mobile identity information element type "SUCI"	CR 1	
4	TT > UE	Send REGISTRATION ACCEPT			
5	UE > TT	Send REGISTRATION COMPLETE			

## 5.3.11.5 Acceptance criteria

CR 1 and CR 3 are implicitly verified in the REGISTRATION REQUEST in step 3). The requirements are met if the REGISTRATION REQUEST sent to the NG-SS contains:

- SUPI format: 0
- Home Network Identifier: 246/081
- Routing indicator: 17
- Protection scheme id: 01
- Home network public key Id: 30
- Scheme output: ECC ephemeral public key, encryption of 357935793 and MAC tag value

CR 2 can be verified by a method explicitly verifying the correct execution of the READ commands in step 1) on the listed EFs (A.2/1 or A.2/2).

## 5.3.12 UE identification by SUCI during initial registration – SUCI calculation by USIM using profile A

### 5.3.12.1 Definition and applicability

If the operator's decision, indicated by the USIM, is that the USIM shall calculate the SUCI, then the USIM shall not give the ME any parameter for the calculation of the SUCI including the Home Network Public Key Identifier, the Home Network Public Key, and the Protection Scheme Identifier. If the ME determines that the calculation of the SUCI, indicated by the USIM, shall be performed by the USIM, the ME shall delete any previously received or locally cached parameters for the calculation of the SUCI including the Routing Indicator, the Home Network Public Key Identifier, the Home Network Public Key and the Protection Scheme Identifier.

### 5.3.12.2 Conformance requirement

CR 1 SUCI calculation procedure shall be performed by the USIM if Services n°124 and n°125 are available in EF<sub>UST</sub>.

Reference:

- TS 31.102 [19], clause 5.3.48;
- TS 33.501 [24], clause Annex C.

CR 2 The ME shall use the GET IDENTITY command in SUCI context to retrieve the SUCI calculated by the USIM.

Reference:

- TS 31.102 [19], clause 5.3.48 and 7.5;
- TS 24.501 [42], clause 5.5.1.2.2.

CR 3 This GET IDENTITY command shall be as per 7.5.2 in TS 31.102

Reference:

- TS 31.102 [4], clause 7.5.

### 5.3.12.3 Test purpose

The purpose of this test is to verify that:

- 1) the GET IDENTITY command is performed correctly by the ME.
- 2) the UE includes the SUCI received from the 5G-NR UICC within GET IDENTITY response in the 5GS mobile identity IE.

### 5.3.12.4 Method of test

#### 5.3.12.4.1 Initial conditions

The values of the default 5G-NR UICC defined in clause 4.5.9 of the present document are used with EF<sub>IMSI</sub> as defined in clause 4.6.5 with the following exceptions:

EF<sub>UST</sub> (USIM Service Table)

Logically:

Service n°125:	SUCI calculation by the USIM	available
----------------	------------------------------	-----------

Coding:

Byte:	B1	B2	B3	B4	B5	B6	B7	B8
Binary:	xxxx xx1x	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxxx xxxx	xxxx xxxx	xxxx xxxx
	<b>B9</b>	<b>B10</b>	<b>B11</b>	...	<b>B16</b>			
	xxxx xxxx	xxxx xxxx	xx11 xxxx	...	xxx1 111x			

5G-NR UICC is configured with:

Protection Scheme Identifier: ECIES scheme profile A  
 Key Index: 1  
 Home Network Public Key Identifier: 30

Home Network Public Key:

Byte:	B1	B2	B3	B4	B5	B6	B7	B8
Hex	5A	8D	38	86	48	20	19	7C
	<b>B9</b>	<b>B10</b>	<b>B11</b>	<b>B12</b>	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>
	33	94	B9	26	13	B2	0B	91
	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	63	3C	BD	89	71	19	27	3B
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>	<b>B31</b>	<b>B32</b>
	F8	E4	A6	F4	EE	C0	A6	50

**EF**<sub>SUCI\_Calc\_Info</sub> (Subscription Concealed Identifier Calculation Information EF): Not available to the ME

The NG-SS shall be configured with Home Network Private Key for profile A:

Coding:	B1	B2	B3	B4	B5	B6	B7	B8
Hex	C5	3C	22	20	8B	61	86	0B
	<b>B9</b>	<b>B10</b>	<b>B11</b>	<b>B12</b>	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>
	06	C6	2E	54	06	A7	B3	30
	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	C2	B5	77	AA	55	58	98	15
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>	<b>B31</b>	<b>B32</b>
	10	D1	28	24	7D	38	BD	1D

The TT (NG-SS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/083/000001
- Access control: unrestricted.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and runs an initial activation.

#### 5.3.12.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	READ EF <sub>UST</sub>	(Evaluation of service settings)		
2	USIM	Perform SUCI calculation	The USIM performs a SUCI calculation using Profile A	(CR 1)	
3	ME > USIM	Send GET IDENTITY	The GET IDENTITY command is sent with Identity Context in P2 as SUCI (0x01). The USIM returns the calculated SUCI	(CR 1) CR 2 CR 3	A.2/1 OR A.2/2
4	UE > TT	Send REGISTRATION REQUEST	The UE sends a REGISTRATION REQUEST with 5GS registration type IE as "initial registration" and 5GS mobile identity information element type "SUCI"	CR 1 (CR 2) (CR 3)	
5	TT > UE	Send REGISTRATION ACCEPT	The TT sends a REGISTRATION ACCEPT with a 5G-GUTI		
6	UE > TT	Send REGISTRATION COMPLETE			

### 5.3.12.5 Acceptance criteria

CR 1 is implicitly verified if the REGISTRATION REQUEST in step 4). The requirements are met if the REGISTRATION REQUEST sent to the NG-SS contains:

SUPI format:	0
Home Network Identifier:	246/081
Routing indicator:	17
Protection scheme id:	01
Home network public key Id:	30
Scheme output:	ECC ephemeral public key, encryption of 357935793 and MAC tag value

CR 2 and CR 3 are explicitly verified in step 3). The requirements are met if the GET IDENTITY command in step 3) is performed correctly.

An implicit verification of CR 2 and CR 3 can be done in step 4). The requirements are met if the REGISTRATION REQUEST sent to the NG-SS contains what is defined to fulfil CR 1.

## 5.3.13 SUCI calculation by ME using null scheme– no Protection Scheme Identifier provisioned in the USIM

### 5.3.13.1 Definition and applicability

If the operator's decision is that ME shall calculate the SUCI, and the home network operator has not provisioned any Protection Scheme Identifier definition in the list of Protection Scheme Identifiers in the USIM, the ME shall calculate the SUCI using the null-scheme.

### 5.3.13.2 Conformance requirement

CR 1 SUCI calculation procedure shall be performed by the ME if Service n°124 is available and Service n°125 is not available in EF<sub>UST</sub>

Reference:

- TS 31.102 [19], clause 5.3.47

CR 2 As part of the SUCI calculation performed by the ME, the ME performs the reading procedure with EF<sub>Routing\_Indicator</sub>

Reference:

- TS 31.102 [19], clauses 4.4.11.11 and 5.3.51.

CR 3 The ME shall calculate the SUCI using the null-scheme if no Protection Scheme Identifier is provisioned in the USIM.

References:

- TS 33.501 [24], clause 6.12.2 and Annex C

### 5.3.13.3 Test purpose

The purpose of this test is to verify that:

- 1) the READ EF<sub>SUCI\_Calc\_Info</sub>, EF<sub>Routing\_Indicator</sub> and EF<sub>IMSI</sub> commands are performed correctly by the ME.
- 2) the ME performs the SUCI calculation procedure using null-scheme.

### 5.3.13.4 Method of test

#### 5.3.13.4.1 Initial conditions

The values of the default 5G-NR UICC defined in clause 4.5.9 of the present document are used with EF<sub>IMSI</sub> as defined in clause 4.6.5 with the following exceptions:

EF<sub>SUCI\_Calc\_Info</sub> (Subscription Concealed Identifier Calculation Information EF)

Logically:

null

Coding:

Byte:	B1	B2
Hex	A0	00

The TT (NG-SS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/083/000001
- Access control: unrestricted.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and runs an initial activation.

#### 5.3.13.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	READ EF <sub>UST</sub> , EF <sub>Routing_Indicator</sub> and EF <sub>SUCI_Calc_Info</sub>	(Evaluation of data and service settings)	CR 1 (CR 2)	A.2/1 OR A.2/2
2	ME	Perform SUCI calculation	The ME performs a SUCI calculation using the null scheme	(CR 2)	
3	UE > TT	Send REGISTRATION REQUEST	The UE sends a REGISTRATION REQUEST with 5GS registration type IE as "initial registration" and 5GS mobile identity information element type "SUCI"	(CR 1) CR 2 CR 3	
4	TT > UE	Send REGISTRATION ACCEPT	The TT sends a REGISTRATION ACCEPT with a 5G-GUTI		
5	UE > TT	Send REGISTRATION COMPLETE			

### 5.3.13.5 Acceptance criteria

CR 1 can be verified by a method explicitly verifying the correct execution of the READ commands in step 1) on the listed EFs (A.2/1 or A.2/2). CR 2 may optionally be verified by the used explicit method too.

CR 2 and CR 3 (and CR 1) are implicitly verified in the REGISTRATION REQUEST in step 3). The requirements are met if the REGISTRATION REQUEST sent to the NG-SS contains:

SUPI format: 0  
 Home Network Identifier: 246/081  
 Routing indicator: 17  
 Protection scheme id: 00  
 Home network public key Id: 0  
 Scheme output: 357935793

## 5.3.14 SUCI calculation by ME using null scheme – no Home Network Public Key for supported protection scheme provisioned in the USIM

### 5.3.14.1 Definition and applicability

If the operator's decision is that ME shall calculate the SUCI, and the home network operator has not provisioned the Home Network Public Key for the protection scheme configured in the USIM that the ME supports, the ME shall calculate the SUCI using the null-scheme.

### 5.3.14.2 Conformance requirement

CR 1 SUCI calculation procedure shall be performed by the ME if Service n°124 is available and Service n°125 is not available in EF<sub>UST</sub>.

Reference:

- TS 31.102 [19], clause 5.3.47

CR 2 As part of the SUCI calculation performed by the ME, the ME performs the reading procedure with EF<sub>SUCI\_Calc\_Info</sub> and EF<sub>Routing\_Indicator</sub>

Reference:

- TS 31.102 [19], clauses 4.4.11.8, 4.4.11.11, 5.3.47 and 5.3.51.

CR 3 The ME shall calculate the SUCI using the null scheme if no Home Network Public Key configured in the USIM for the protection scheme configured in the USIM that the ME supports.

References:

- TS 33.501 [24], clause 6.12.2 and Annex C
- TS 24.501 [25], clause 5.5.1.2.4.

### 5.3.14.3 Test purpose

The purpose of this test is to verify that:

- 1) the READ EF<sub>SUCI\_Calc\_Info</sub>, EF<sub>Routing\_Indicator</sub> and EF<sub>IMSI</sub> commands are performed correctly by the ME.
- 2) the ME performs the SUCI calculation procedure using null-scheme.

### 5.3.14.4 Method of test

#### 5.3.14.4.1 Initial conditions

The values of the default 5G-NR UICC defined in clause 4.5.9 of the present document are used with EF<sub>IMSI</sub> as defined in clause 4.6.5 with the following exceptions:

EF<sub>SUCI\_Calc\_Info</sub> (Subscription Concealed Identifier Calculation Information EF)

Logically:

Protection Scheme Identifier List data object

Protection Scheme Identifier 1 – ECIES scheme profile B  
Key Index 1: 0

Coding:

Byte:	B1	B2	B3	B4
Hex	A0	02	02	00

The TT (NG-SS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/083/000001
- Access control: unrestricted.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and runs an initial activation.

#### 5.3.14.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	READ EF <sub>UST</sub> , EF <sub>Routing_Indicator</sub> and EF <sub>SUCI_Calc_Info</sub>	(Evaluation of data and service settings)	CR 1 (CR 2)	A.2/1 OR A.2/2
2	ME	Perform SUCI calculation	The ME performs a SUCI calculation using the null scheme	(CR 2)	
3	UE > TT	Send REGISTRATION REQUEST	The UE sends a REGISTRATION REQUEST with 5GS registration type IE as "initial registration" and 5GS mobile identity information element type "SUCI"	(CR 1) CR 2 CR 3	
4	TT > UE	Send REGISTRATION ACCEPT	The TT sends a REGISTRATION ACCEPT with a 5G-GUTI		
5	UE > TT	Send REGISTRATION COMPLETE			

#### 5.3.14.5 Acceptance criteria

CR 1 can be verified by a method explicitly verifying the correct execution of the READ commands in step 1) on the listed EFs (A.2/1 or A.2/2). CR 2 may optionally be verified by the used explicit method too.

CR 2 and CR 3 (and CR 1) are implicitly verified in the REGISTRATION REQUEST in step 3). The requirements are met if the REGISTRATION REQUEST sent to the NG-SS contains:

SUPI format: 0  
 Home Network Identifier: 246/081  
 Routing indicator: 17  
 Protection scheme id: 00  
 Home network public key Id: 0  
 Scheme output: 357935793

### 5.3.15 SUCI calculation by ME using null scheme with the E-UTRAN/EPC UICC

#### 5.3.15.1 Definition and applicability

If the operator's decision is that ME shall calculate the SUCI, the home network operator shall provision the Protection Scheme and public key in the USIM that the operator allows. But if the SUCI calculation indication is not present, the calculation is in the ME. If the Home Network Public Key or the priority list are not provisioned in the USIM, the ME shall calculate the SUCI using the null-scheme. The Routing Indicator shall be stored in the USIM. If the Routing Indicator is not present in the USIM, the ME shall set it to a default value 0.

#### 5.3.15.2 Conformance requirement

CR 1 SUCI calculation procedure shall be performed by the ME if the SUCI calculation indication is not present in the USIM.

Reference:

- TS 33.501 [24], clause 5.2.5, 6.12.2, Annex C.

CR 2 The ME shall calculate the SUCI using the null-scheme if E-UTRAN/EPC UICC is installed into the ME.

- TS 33.501 [24], clause 6.12.2 and Annex C;
- TS 24.501 [25], clause 5.5.1.2.4 and 9.11.3.4.

### 5.3.15.3 Test purpose

The purpose of this test is to verify that the ME performs the SUCI calculation procedure using null-scheme.

### 5.3.15.4 Method of test

#### 5.3.15.4.1 Initial conditions

The values of the E-UTRAN UICC defined in clause 4.5.4 of the present document are used with the following exceptions:

**EF<sub>IMSI</sub>** (International Mobile Subscriber Identity)

Logically:

246081357935793

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9
Hex	08	29	64	80	31	75	39	75	39

If activated, the TT (NG-SS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/083/000001
- Access control: unrestricted.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and runs an initial activation. The TT (NG-SS) activates Cell A.

#### 5.3.15.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	READ EF <sub>UST</sub>	(Evaluation of service settings)		
2	UE > TT	Send REGISTRATION REQUEST	The UE sends a REGISTRATION REQUEST to the NG-SS		
3	TT > UE	Send REGISTRATION REJECT	The TT sends a REGISTRATION REJECT with cause: <i>Roaming not allowed in this tracking area</i>		
4	UE	Deactivate and then re-activate the UE			
5	UE	READ EF <sub>UST</sub> , EF <sub>IMSI</sub>	(Evaluation of data and service settings)		
6	ME	Perform SUCI calculation	The ME performs a SUCI calculation using the null scheme	(CR 1) (CR 2)	
7	UE > TT	Send REGISTRATION REQUEST	The UE sends a REGISTRATION REQUEST with 5GS registration type IE as "initial registration" and 5GS mobile identity information element type "SUCI"	CR 1 CR 2	
8	TT > UE	Send REGISTRATION ACCEPT	The TT sends a REGISTRATION ACCEPT with a 5G-GUTI		
9	UE > TT	Send REGISTRATION COMPLETE			

### 5.3.15.5 Acceptance criteria

CR 1 and CR 2 are implicitly verified in the REGISTRATION REQUEST in step 7). The requirements are met if the REGISTRATION REQUEST sent to the NG-SS contains:

SUPI format: 0  
Home Network Identifier: 246/081

Routing indicator: 0  
Protection scheme id: 00  
Home network public key Id: 0  
Scheme output: 357935793

### 5.3.16 SUCI calculation by ME using the lower priority protection scheme when the higher priority protection scheme is not supported by the ME

#### 5.3.16.1 Definition and applicability

If the operator's decision is that the ME shall calculate the SUCI, the Home Network Operator shall provision a list of the Protection Scheme Identifiers that the operator allows in the USIM. The list of Protection Scheme Identifiers in the USIM may contain one or more Protection Scheme Identifiers in order of their priority. The ME shall read the SUCI calculation information from the USIM, including the SUPI, the Home Network Public Key, the Home Network Public Key Identifier, and the list of Protection Scheme Identifiers. The ME shall select the protection scheme from its supported schemes that has the highest priority in the list obtained from the USIM. If the higher priority protection scheme is not supported by the ME, the ME should use the lower priority protection scheme to calculate the SUCI.

#### 5.3.16.2 Conformance requirement

CR 1 SUCI calculation procedure shall be performed by the ME if Service n°124 is available and Service n°125 is not available in EF<sub>UST</sub>.

Reference:

- TS 31.102 [19], clause 5.3.47 and 5.3.51.

CR 2 As part of the SUCI calculation performed by the ME, the ME performs the reading procedure with EF<sub>SUCI\_Calc\_Info</sub>.

Reference:

- TS 31.102 [19], clauses 4.4.11.8 and 5.3.47.

CR 3 The ME shall select the protection scheme from its supported schemes that has the highest priority in the list are obtained from the USIM. If the higher priority protection scheme is not supported by the ME, the ME should use the lower priority protection scheme to calculate the SUCI.

References:

- TS 31.102 [19], clauses 4.4.11.8;
- TS 33.501 [24], clause 6.12.2 and Annex C
- TS 24.501 [25], clause 5.5.1.2.4.

#### 5.3.16.3 Test purpose

The purpose of this test is to verify that:

- 1) the READ EF<sub>Routing\_Indicator</sub>, EF<sub>SUCI\_Calc\_Info</sub> and EF<sub>IMSI</sub> commands are performed correctly by the ME.
- 2) if the higher priority protection scheme is not supported by the ME, the ME should use the lower priority protection scheme to calculate the SUCI.

## 5.3.16.4 Method of test

### 5.3.16.4.1 Initial conditions

The values of the default 5G-NR UICC defined in clause 4.5.9 of the present document are used with  $EF_{\text{MSI}}$  as defined in clause 4.6.5 with the following exceptions:

$EF_{\text{SUCI\_Calc\_Info}}$  (Subscription Concealed Identifier Calculation Information EF)

Logically:

Protection Scheme Identifier List data object

Protection Scheme Identifier	1 – any value of the reserved range (i.e 0x3 - 0xB) that is not standardized
Key Index 1:	1
Protection Scheme Identifier	2 – ECIES scheme profile A
Key Index 1:	2
Protection Scheme Identifier	3 – null-scheme
Key Index 3:	0

Home Network Public Key List data object

Home Network Public Key 1 Identifier: 16

Home Network Public Key 1:

- 2E 85 DA EC 6A C9 B5 2B 5D 2D 58 02 33 29 57 75 49 44 5A 39 3D 2A 68 E6 12 14 27 34 95 AD  
BE 65

Home Network Public Key 2 Identifier: 30

Home Network Public Key 2:

- 5A 8D 38 86 48 20 19 7C 33 94 B9 26 13 B2 0B 91 63 3C BD 89 71 19 27 3B F8 E4 A6 F4 EE C0  
A6 50

Coding:

Byte:	B1	B2	B3	B4	B5	B6	B7	B8
Hex	A0	06	NOTE	01	01	02	00	00
	<b>B9</b>	<b>B10</b>	<b>B11</b>	<b>B12</b>	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>
	A1	4A	80	01	10	81	20	2E
	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	85	DA	EC	6A	C9	B5	2B	5D
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>	<b>B31</b>	<b>B32</b>
	2D	58	02	33	29	57	75	49
	<b>B33</b>	<b>B34</b>	<b>B35</b>	<b>B36</b>	<b>B37</b>	<b>B38</b>	<b>B39</b>	<b>B40</b>
	44	5A	39	3D	2A	68	E6	12
	<b>B41</b>	<b>B42</b>	<b>B43</b>	<b>B44</b>	<b>B45</b>	<b>B46</b>	<b>B47</b>	<b>B48</b>
	14	27	34	95	AD	BE	65	80
	<b>B49</b>	<b>B50</b>	<b>B51</b>	<b>B52</b>	<b>B53</b>	<b>B54</b>	<b>B55</b>	<b>B56</b>
	01	1E	81	20	5A	8D	38	86
	<b>B57</b>	<b>B58</b>	<b>B59</b>	<b>B60</b>	<b>B61</b>	<b>B62</b>	<b>B63</b>	<b>B64</b>
	48	20	19	7C	33	94	B9	26
	<b>B65</b>	<b>B66</b>	<b>B67</b>	<b>B68</b>	<b>B69</b>	<b>B70</b>	<b>B71</b>	<b>B72</b>
	13	B2	0B	91	63	3C	BD	89
	<b>B73</b>	<b>B74</b>	<b>B75</b>	<b>B76</b>	<b>B77</b>	<b>B78</b>	<b>B79</b>	<b>B80</b>
	71	19	27	3B	F8	E4	A6	F4
	<b>B81</b>	<b>B82</b>	<b>B83</b>	<b>B84</b>				
	EE	C0	A6	50				

NOTE: Any value of the reserved range (i.e 0x3 - 0xB) that is not standardized (e.g. 0xB).

The NG-SS shall be configured with Home Network Private Key as following (for Profile A):

<b>Coding:</b>	<b>B1</b>	<b>B2</b>	<b>B3</b>	<b>B4</b>	<b>B5</b>	<b>B6</b>	<b>B7</b>	<b>B8</b>
Hex	C5	3C	22	20	8B	61	86	0B
	<b>B9</b>	<b>B10</b>	<b>B11</b>	<b>B12</b>	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>
	06	C6	2E	54	06	A7	B3	30
	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	C2	B5	77	AA	55	58	98	15
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>	<b>B31</b>	<b>B32</b>
	10	D1	28	24	7D	38	BD	1D

The TT (NG-SS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/083/000001
- Access control: unrestricted.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and runs an initial activation.

#### 5.3.16.4.2 Procedure

<b>Step</b>	<b>Direction</b>	<b>Action</b>	<b>Information</b>	<b>REQ</b>	<b>SA</b>
1	UE	READ EF <sub>IMSI</sub> , EF <sub>UST</sub> , EF <sub>Routing_Indicator</sub> and EF <sub>SUCI_Calc_Info</sub>	(Evaluation of data and service settings)	CR 2	A.2/1 OR A.2/2
2	ME	Perform SUCI calculation	The ME performs a SUCI calculation	(CR 1) (CR 3)	
3	UE > TT	Send REGISTRATION REQUEST	The UE sends a REGISTRATION REQUEST with 5GS registration type IE as "initial registration" and 5GS mobile identity information element type "SUCI"	CR 1 CR 3	
4	TT > UE	Send REGISTRATION ACCEPT	The TT sends a REGISTRATION ACCEPT with a 5G-GUTI		
5	UE > TT	Send REGISTRATION COMPLETE			

#### 5.3.16.5 Acceptance criteria

CR 1 can be verified by a method explicitly verifying the correct execution of the READ commands in step 1) on the listed EFs (A.2/1 or A.2/2).

CR 1 and CR 3 are implicitly verified in the REGISTRATION REQUEST in step 3). The requirements are met if the REGISTRATION REQUEST sent to the NG-SS contains:

- SUPI format: 0
- Home Network Identifier: 246/081
- Routing indicator: 17
- Protection scheme id: 01
- Home network public key Id: 30
- Scheme output: ECC ephemeral public key, encryption of 357935793 and MAC tag value

## 5.3.17 SUCI calculation by ME using Profile B with compressed Home Network Public Key

### 5.3.17.1 Definition and applicability

If the operator's decision is that ME shall calculate the SUCI, the home network operator shall provision a list of the Protection Scheme Identifiers that the operator allows in the USIM. The list of Protection Scheme Identifiers in the USIM may contain one or more Protection Scheme Identifiers in order of their priority. The ME shall read the SUCI calculation information from the USIM, including the SUPI, the Home Network Public Key, the Home Network Public Key Identifier, and the list of Protection Scheme Identifiers. The ME shall select the protection scheme from its supported schemes that has the highest priority in the list obtained from the USIM.

### 5.3.17.2 Conformance requirement

CR 1 SUCI calculation procedure shall be performed by the ME if Service n°124 is available and Service n°125 is not available in EF<sub>UST</sub>.

Reference:

- TS 31.102 [19], clause 5.3.47 and 5.3.51.

CR 2 As part of the SUCI calculation performed by the ME, the ME performs the reading procedure with EF<sub>SUCI\_Calc\_Info</sub>.

Reference:

- TS 31.102 [19], clauses 4.4.11.8 and 5.3.47.

CR 3 The ME shall calculate the SUCI using the highest priority supported protection scheme and the home network public key stored on the USIM.

References:

- TS 31.102 [19], clauses 4.4.11.8;
- TS 33.501 [24], clause 6.12.2 and Annex C
- TS 24.501 [25], clause 5.5.1.2.4.

CR 4 The ME shall be capable to calculate the SUCI using Profile B with the ECC public key provided in compressed format.

References:

- TS 33.501 [24], Annex C.3.4.2 and Annex C.4.4
- RFC 5480 [51], clause 2.2.

### 5.3.17.3 Test purpose

The purpose of this test is to verify that:

- 1) the READ EF<sub>Routing\_Indicator</sub>, EF<sub>SUCI\_Calc\_Info</sub> and EF<sub>IMSI</sub> commands are performed correctly by the ME.
- 2) the ME performs the SUCI calculation procedure using the profile with the highest priority (i.e. ECIES scheme profile B and the home network public key)

### 5.3.17.4 Method of test

#### 5.3.17.4.1 Initial conditions

The values of the default 5G-NR UICC defined in clause 4.5.9 of the present document are used with EF<sub>IMSI</sub> as defined in clause 4.6.5 with the following exceptions:

EF<sub>SUCI\_Calc\_Info</sub> (Subscription Concealed Identifier Calculation Information EF)

Logically:

Protection Scheme Identifier List data object

Protection Scheme Identifier 1 – ECIES scheme profile B  
 Key Index 1: 1  
 Protection Scheme Identifier 2 – ECIES scheme profile A  
 Key Index 1: 2  
 Protection Scheme Identifier 3 – null-scheme  
 Key Index 3: 0

Home Network Public Key List data object

Home Network Public Key 1 Identifier: 27

Home Network Public Key 1 (see note):

- 02 72 DA 71 97 62 34 CE 83 3A 69 07 42 58 67 B8 2E 07 4D 44 EF 90 7D FB 4B 3E 21 C1 C2 25  
 6E BC D1

Home Network Public Key 2 Identifier: 30

Home Network Public Key 2:

- 5A 8D 38 86 48 20 19 7C 33 94 B9 26 13 B2 0B 91 63 3C BD 89 71 19 27 3B F8 E4 A6 F4 EE C0  
 A6 50

- Coding:

Byte:	B1	B2	B3	B4	B5	B6	B7	B8
Hex	A0	06	02	01	01	02	00	00
	<b>B9</b>	<b>B10</b>	<b>B11</b>	<b>B12</b>	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>
	A1	4B	80	01	1B	81	21	02
	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	72	DA	71	97	62	34	CE	83
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>	<b>B31</b>	<b>B32</b>
	3A	69	07	42	58	67	B8	2E
	<b>B33</b>	<b>B34</b>	<b>B35</b>	<b>B36</b>	<b>B37</b>	<b>B38</b>	<b>B39</b>	<b>B40</b>
	07	4D	44	EF	90	7D	FB	4B
	<b>B41</b>	<b>B42</b>	<b>B43</b>	<b>B44</b>	<b>B45</b>	<b>B46</b>	<b>B47</b>	<b>B48</b>
	3E	21	C1	C2	25	6E	BC	D1
	<b>B49</b>	<b>B50</b>	<b>B51</b>	<b>B52</b>	<b>B53</b>	<b>B54</b>	<b>B55</b>	<b>B56</b>
	80	01	1E	81	20	5A	8D	38
	<b>B57</b>	<b>B58</b>	<b>B59</b>	<b>B60</b>	<b>B61</b>	<b>B62</b>	<b>B63</b>	<b>B64</b>
	86	48	20	19	7C	33	94	B9
	<b>B65</b>	<b>B66</b>	<b>B67</b>	<b>B68</b>	<b>B69</b>	<b>B70</b>	<b>B71</b>	<b>B72</b>
	26	13	B2	0B	91	63	3C	BD
	<b>B73</b>	<b>B74</b>	<b>B75</b>	<b>B76</b>	<b>B77</b>	<b>B78</b>	<b>B79</b>	<b>B80</b>
	89	71	19	27	3B	F8	E4	A6
	<b>B81</b>	<b>B82</b>	<b>B83</b>	<b>B84</b>	<b>B85</b>			
	F4	EE	C0	A6	50			

- NOTE: EF<sub>SUCL\_Calc\_Info</sub> contains the compressed form of the ECC public key for Profile B.

The NG-SS shall be configured with Home Network Private Key as following:

Coding:	B1	B2	B3	B4	B5	B6	B7	B8
Hex	F1	AB	10	74	47	7E	BC	C7
	<b>B9</b>	<b>B10</b>	<b>B11</b>	<b>B12</b>	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>
	F5	54	EA	1C	5F	C3	68	B1
	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	61	67	30	15	5E	00	41	AC
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>	<b>B31</b>	<b>B32</b>
	44	7D	63	01	97	5F	EC	DA

The TT (NG-SS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/083/000001
- Access control: unrestricted.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and runs an initial activation.

#### 5.3.17.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	READ EF <sub>IMSI</sub> , EF <sub>UST</sub> , EF <sub>Routing_Indicator</sub> and EF <sub>SUCI_Calc_Info</sub>	(Evaluation of data and service settings)	CR 2	A.2/1 OR A.2/2
2	ME	Perform SUCI calculation	The ME performs a SUCI calculation	(CR 1) (CR 3) (CR 4)	
3	UE > TT	Send REGISTRATION REQUEST	The UE sends a REGISTRATION REQUEST with 5GS registration type IE as "initial registration" and 5GS mobile identity information element type "SUCI"	CR 1 CR 3 CR 4	
4	TT > UE	Send REGISTRATION ACCEPT	The TT sends a REGISTRATION ACCEPT with a 5G-GUTI		
5	UE > TT	Send REGISTRATION COMPLETE			

#### 5.3.17.5 Acceptance criteria

CR 1 can be verified by a method explicitly verifying the correct execution of the READ commands in step 1) on the listed EFs (A.2/1 or A.2/2).

CR 1 and CR 3 are implicitly verified in the REGISTRATION REQUEST in step 3). The requirements are met if the REGISTRATION REQUEST sent to the NG-SS contains:

SUPI format: 0  
 Home Network Identifier: 246/081  
 Routing indicator: 17  
 Protection scheme id: 02  
 Home network public key Id: 27  
 Scheme output: ECC ephemeral public key, encryption of 357935793 and MAC tag value

## 5.4 Unified Access Control information handling for 5G-NR

### 5.4.1 Unified Access Control – Access identity 0, no access identities indicated by USIM

#### 5.4.1.1 Definition and applicability

The purpose of Unified Access Control procedure is to perform access barring check for a 5GS access attempt associated with a given Access Category and one or more Access Identities upon request from upper layers or the RRC layer.

The 5G network shall be able to broadcast barring control information (i.e. a list of barring parameters associated with an Access Identity and an Access Category) in SIB1.

If no Access Identities are configured in EF<sub>UAC\_AIC</sub> and in EF<sub>ACC</sub>, Access Identity 0 is applicable. The UE shall read EF<sub>UAC\_AIC</sub> and EF<sub>ACC</sub> as part of USIM Initialization procedure.

The UE shall be able to determine whether or not a particular new access attempt is allowed based on barring parameters that the UE receives from the broadcast barring control information and the configuration in the USIM.

When the NAS detects an access event, the NAS shall perform the mapping of the kind of request to one or more access identities and one access category and lower layers will perform access barring checks for that request based on the determined access identities and access category.

### 5.4.1.2 Conformance requirement

CR 1 The ME shall read the access control value as part of the USIM-ME initialization procedure, and subsequently adopt this value.

Reference:

- TS 31.102 [19], clause 5.1.1.2.

CR 2 Access Identities are configured at the UE as listed in TS 22.261 [36] Table 6.22.2.2-1. Access Categories are defined by the combination of conditions related to UE and the type of access attempt as listed in TS 22.261 [36] Table 6.22.2.3-1. One or more Access Identities and only one Access Category are selected and tested for an access attempt.

Reference:

- TS 22.261 [36], clause 6.22.2.

CR 3 The UE shall be able to determine whether or not a particular new access attempt is allowed based on uac-BarringInfo broadcast in SIB1. Access Control check shall be performed as per the information received in uac-BarringInfoSetList.

Reference:

- TS 38.331 [37], clause 5.3.14.

### 5.4.1.3 Test purpose

The purpose of this test is to verify that:

- 1) the ME reads the access control value from  $EF_{UAC\_AIC}$  and  $EF_{ACC}$  as part of the USIM-ME initialisation procedure, and subsequently adopts this value.
- 2) the UE maps the kind of request to one or more access identities and one access category and lower layers performs access barring checks for that request based on the determined access identities and access category.

### 5.4.1.4 Method of test

#### 5.4.1.4.1 Initial conditions

The values of the 5G-NR UICC as defined in clause 4.5.9 of the present document are used with  $EF_{IMSI}$  as defined in clause 4.6.5 and the following exceptions:

$EF_{UAC\_AIC}$  and  $EF_{ACC}$

No Access Identities configured in  $EF_{UAC\_AIC}$  and no Access Classes configured in  $EF_{ACC}$  as shown in table 5.4.1-1.

$EF_{UST}$  (USIM Service Table)

Logically:

Settings from clause 4.5.9 (5G-NR UICC) of the present document apply with the following changes:

Service n°124	Subscription identifier privacy support	not available
Service n°126	UAC Access Identities support	available

Coding:

Byte:	B1	B2	B3	B4	B5	B6	B7	B8
Binary:	xxxx xx1x	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxx1 xx1x	xxxx xxxx	xxxx xxxx
	B9	B10	B11	...	B16			
	xxxx xxxx	xxxx xxxx	xx11 xxxx	...	xx10 011x			

The NG-SS is configured to transmit on the BCCH with the following parameters:

Cell A:

- TAI (MCC/MNC/TAC): MCC, MNC: see table 5.4.1-1, TAC: 000001.
- CellIdentity: 000000001

For the table 5.4.1-1:

uac-BarringInfo in SIB1 should be set as in the table:

- Refer to Annex A for the Methods UAC\_BarringInfo\_xxxxxx() in the table.

If present in the *REGISTRATION ACCEPT*, the 5GS network feature support IE indicates Access identities 1 and 2 are not valid.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case.

#### 5.4.1.4.2 Test sequence settings

**Table 5.4.1-1**

TC Seq#	Access Category	USIM		SIB1 on Cell A		REGISTRATION ACCEPT (5GS network feature support IE)		Result	
		EF <sub>UAC-AIC</sub>	EF <sub>ACC</sub> (Byte 1 b8-b4)	uac-BarringInfo	PLMN-Identity (MCC/MNC)	MPS indicator Bit	MCS indicator Bit	Registration successful?	MO Data call successful?
1.1	7	0x00 00 00 00	00000	Not Present	246 / 081	0	0	Yes	Yes
1.2	3	0x00 00 00 00	00000	UAC_BarringInfo_Common (3,0x0000000'B)	246 / 081	0	0	No	N/A
1.3	3	0x00 00 00 00	00000	UAC_BarringInfo_PerPLMN (3,0x0000000'B)	246 / 081	0	0	No	N/A
1.4	3	0x00 00 00 00	00000	UAC_BarringInfo_PerPLMN (3,0x1000000'B)	246 / 081	0	0	No	N/A
1.5	7	0x00 00 00 00	00000	UAC_BarringInfo_Common (7,0x0000000'B)	246 / 081	0	0	Yes	No
1.6	7	0x00 00 00 00	00000	UAC_BarringInfo_PerPLMN (7,0x0000000'B)	246 / 081	0	0	Yes	No
1.7	3	0x00 00 00 00	00000	UAC_BarringInfo_Common2 (7,0x1000000'B, 3,0x0000000'B)	244 / 081	0	0	No	N/A

#### 5.4.1.4.3 Procedure

Procedure/steps to be repeated for all sequences listed in table 5.4.1-1:

Step	Direction	Action	Information	REQ	SA
1	TT	SIB1 of Cell A is transmitted as defined in the initial conditions for tests from table 5.4.1-1	Barring info is set as in table 5.4.1-1 See Annex A for the Methods UAC_BarringInfo_xxxxxx() in the table		
2	UE	Power UE on	The UE performs a SIM initialisation. (includes reading of EF <sub>UAC-AIC</sub> and EF <sub>ACC</sub> )	CR 1	A.2/1 OR A.2/2

#### If cell access is not allowed:

3	UE > TT	REGISTRATION REQUEST in not sent	See column 'Registration successful?' for the result	CR 2 CR 3	
4	User	End test sequence			

#### If cell access is allowed:

3	UE > TT	Send REGISTRATION REQUEST	See column 'Registration successful?' for the result	CR 2 CR 3	
4	TT > UE	Send REGISTRATION ACCEPT	For simplicity other signalling is not shown		

#### If MO Data call is not allowed:

5	UE	Attempt to set up MO Data call	To set up the MO Data call the MMI or EMMI is used	CR 2 CR 3	
6	User	End test sequence			
<b>If MO Data call is allowed:</b>					
5	UE > TT	Set up MO Data call ( <i>PDU Session Establishment</i> )	To set up the MO Data call the MMI or EMMI is used	CR 2 CR 3	
6	User	End test sequence			

### 5.4.1.5 Acceptance criteria

For the scenarios in table 5.4.1-1:

CR 1 is explicitly verified at step 2) by analysing the file READ commands for EF<sub>UAC-AIC</sub> and EF<sub>ACC</sub> during the USIM-ME initialisation procedure.

CR 2 and CR 3 are verified at:

- steps 3) and 5) by analysing if the UE shall make a successful or unsuccessful Registration to the network in accordance with the result indicated in the table and
- steps 4) and 5) by analysing if the UE shall make a successful or unsuccessful MO Data call in accordance with the result indicated in the table if the step is applicable.

## 5.4.1A Unified Access Control – Access identity 0, no access identities indicated by USIM, Access Category 8

### 5.4.1A.1 Definition and applicability

The purpose of Unified Access Control procedure is to perform access barring check for a 5GS access attempt associated with a given Access Category and one or more Access Identities upon request from upper layers or the RRC layer.

The 5G network shall be able to broadcast barring control information (i.e. a list of barring parameters associated with an Access Identity and an Access Category) in SIB1.

If no Access Identities are configured in EF<sub>UAC-AIC</sub> and in EF<sub>ACC</sub>, Access Identity 0 is applicable. The UE shall read EF<sub>UAC-AIC</sub> and EF<sub>ACC</sub> as part of USIM Initialization procedure.

The UE shall be able to determine whether or not a particular new access attempt is allowed based on barring parameters that the UE receives from the broadcast barring control information and the configuration in the USIM.

When the NAS detects an access event, the NAS shall perform the mapping of the kind of request to one or more access identities and one access category and lower layers will perform access barring checks for that request based on the determined access identities and access category.

If RRC state is RRC\_INACTIVE and the resumption of the RRC connection is triggered due to an RNA Update, RRC layer shall select Access Category as '8' and perform unified access control procedure in case there is no ongoing emergency service.

### 5.4.1A.2 Conformance requirement

CR 1 The ME shall read the access control value as part of the USIM-ME initialization procedure, and subsequently adopt this value.

Reference:

- TS 31.102 [19], clause 5.1.1.2.

CR 2 Access Identities are configured at the UE as listed in TS 22.261 [36] Table 6.22.2.2-1. Access Categories are defined by the combination of conditions related to UE and the type of access attempt as listed in TS 22.261 [36] Table 6.22.2.3-1. One or more Access Identities and only one Access Category are selected and tested for an access attempt.

Reference:

- TS 22.261 [36], clause 6.22.2.

CR 3 The UE shall be able to determine whether or not a particular new access attempt is allowed based on uac-BarringInfo broadcast in SIB1. Access Control check shall be performed as per the information received in uac-BarringInfoSetList.

Reference:

- TS 38.331 [37], clause 5.3.14.

CR 4 If the resumption of the RRC connection is triggered due to an RNA update and there is no ongoing emergency service RRC shall select '8' as the Access Category and perform the unified access control procedure.

Reference:38.331 [37], clause 5.3.13.2.

### 5.4.1A.3 Test purpose

The purpose of this test is to verify that:

- 1) the ME reads the access control value from  $EF_{UAC\_AIC}$  and  $EF_{ACC}$  as part of the USIM-ME initialisation procedure, and subsequently adopts this value.
- 2) the UE maps the kind of request to one or more access identities and one access category and lower layers performs access barring checks for that request based on the determined access identities and access category.
- 3) the UE performs unified access control procedure if RNA Update procedure is triggered.

### 5.4.1A.4 Method of test

#### 5.4.1A.4.1 Initial conditions

The values of the 5G-NR UICC as defined in clause 4.5.9 of the present document are used with  $EF_{IMSI}$  as defined in clause 4.6.5 and the following exceptions:

#### $EF_{UAC\_AIC}$ and $EF_{ACC}$

No Access Identities configured in  $EF_{UAC\_AIC}$  and no Access Classes configured in  $EF_{ACC}$  as shown in table 5.4.1A-1.

#### $EF_{UST}$ (USIM Service Table)

Logically:

Settings from clause 4.5.9 (5G-NR UICC) of the present document apply with the following changes:

Service n°124	Subscription identifier privacy support	not available
Service n°126	UAC Access Identities support	available

Coding:

Byte:	B1	B2	B3	B4	B5	B6	B7	B8
Binary:	xxxx xx1x	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxx1 xx1x	xxxx xxxx	xxxx xxxx
	<b>B9</b>	<b>B10</b>	<b>B11</b>	...	<b>B16</b>			
	xxxx xxxx	xxxx xxxx	xx11 xxxx	...	xx10 011x			

The TT (NG-SS) is configured to transmit on the BCCH with the following parameters:

Cell A:

- TAI (MCC/MNC/TAC): MCC, MNC: see table 5.4.1A-1, TAC: 000001.
- CellIdentity: 000000001

For the table 5.4.1A-1:

No uac-BarringInfo in SIB1.

If present in the REGISTRATION ACCEPT, the 5GS network feature support IE indicates Access identities 1 and 2 are not valid.

Cell B:

- TAI (MCC/MNC/TAC): MCC, MNC: see table 5.4.1A-1, TAC 000001.
- CellIdentity: 000000002

For the table 5.4.1A-1:

uac-BarringInfo in SIB1 should be set as in the table:

- Refer to Annex A for the Methods UAC\_BarringInfo\_XXXXXX() in the table.

If present in the REGISTRATION ACCEPT, the 5GS network feature support IE indicates Access identities 1 and 2 are not valid.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case.

### 5.4.1A.4.2 Test sequence settings

**Table 5.4.1A-1**

TC Seq#	Access Category	USIM		SIB1 on Cell A		REGISTRATION ACCEPT (5GS network feature support IE)		Result
		EF <sub>UAC_AIC</sub>	EF <sub>ACC</sub> (Byte 1 b8-b4)	uac-BarringInfo	PLMN-Identity (MCC/MNC)	MPS indicator Bit	MCS indicator Bit	
2.1	8	0x00 00 00 00	00000	Not Present	246 / 081	0	0	Yes
2.2	8	0x00 00 00 00	00000	UAC_BarringInfo_Common (8,0x00000000'B)	246 / 081	0	0	No
2.3	8	0x00 00 00 00	00000	UAC_BarringInfo_PerPLMN (8,0x00000000'B)	246 / 081	0	0	No
2.4	8	0x00 00 00 00	00000	UAC_BarringInfo_Common2 (7,0x10000000'B, 8,0x00000000'B)	244 / 081	0	0	No

### 5.4.1A.4.3 Procedure

Procedure/steps to be repeated for all sequences listed in table 5.4.1A-1:

Step	Direction	Action	Information	REQ	SA
1	TT	SIB1 of Cell A is transmitted as defined in the initial conditions for tests from table 5.4.1A-1	No barring info is provided to Cell A		
2	UE	Power UE on	The UE performs a SIM initialisation (includes reading of EF <sub>UAC_AIC</sub> and EF <sub>ACC</sub> )	CR 1	A.2/1 OR A.2/2
3	UE > TT	Send REGISTRATION REQUEST			
4	TT > UE	Send REGISTRATION ACCEPT	The registration is successful		
5	UE > TT	Set up MO Data call (PDU SessionEstablishment)	To set up the MO Data call the MMI or EMMI is used. The MO Data call is set up successfully		
6	TT > UE	Send RRC RELEASE with suspendConfig in criticalExtensions (with the choice rrcRelease)	ran-NotificationAreaInfo in suspendConfig contains the cellList with cellIdentity of Cell A: cellList { plmn-Identity {mcc, mnc}, -- see table 5.4.1A-1 for MCC/MNC ran-AreaCells 000000001'B }		
7	TT	Deactivate Cell A and activate Cell B			

8	TT	SIB1 of Cell B is transmitted as defined in table 5.4.1A-1	Barring info is as in the table. See Annex A for the Methods UAC_BarringInfo_xxxxxx() in the table		
9	UE > TT	Initiate RRC RESUME REQUEST procedure with <i>resumeCause</i> set to <i>rna-Update</i> .	See the column 'RRC RESUME REQUEST with <i>resumeCause</i> set to <i>rna-Update</i> successful?' for the result	CR 2 CR 3 CR 4	

### 5.4.1A.5 Acceptance criteria

For the scenarios in table 5.4.1A-1:

CR 1 is explicitly verified at step 2) by analysing the file READ commands for  $EF_{UAC-AIC}$  and  $EF_{ACC}$  during the USIM-Terminal initialisation procedure.

CR 2, CR 3, and CR 4 are verified at steps 9) and 10) by analysing if the UE shall make a successful or unsuccessful RRC Resumption for RNA Update in accordance with the result indicated in the table.

## 5.4.2 Unified Access Control – Access Identity 1 – MPS indicated by USIM

### 5.4.2.1 Definition and applicability

The purpose of Unified Access Control procedure is to perform access barring check for a 5GS access attempt associated with a given Access Category and one or more Access Identities upon request from upper layers or the RRC layer.

The 5G network shall be able to broadcast barring control information (i.e. a list of barring parameters associated with an Access Identity and an Access Category) in SIB1.

The  $EF_{UAC-AIC}$  in the USIM contains the configuration information pertaining to access identity 1 allocated for high priority services MPS.

The UE shall be able to determine whether or not a particular new access attempt is allowed based on barring parameters that the UE receives from the broadcast barring control information and the configuration in the USIM.

When the NAS detects an access event, the NAS shall perform the mapping of the kind of request to one or more access identities and one access category and lower layers will perform access barring checks for that request based on the determined access identities and access category.

### 5.4.2.2 Conformance requirement

CR 1 The ME shall read the access control value as part of the USIM-ME initialization procedure, and subsequently adopt this value.

Reference:

- TS 31.102 [19], clause 5.1.1.2.

CR 2 Access Identities are configured at the UE as listed in TS 22.261 [36] Table 6.22.2.2-1. Access Categories are defined by the combination of conditions related to UE and the type of access attempt as listed in TS 22.261 [36] Table 6.22.2.3-1. One or more Access Identities and only one Access Category are selected and tested for an access attempt.

Reference:

- TS 22.261 [36], clause 6.22.2

CR 3 Access Identity 1 is valid if the RPLMN is the HPLMN, EHPLMN or visited PLMN of the home country.

Reference:

- TS 24.501 [25], clause 4.5.2

CR 4 The UE shall be able to determine whether or not a particular new access attempt is allowed based on uac-BarringInfo broadcast in SIB1. Access Control check shall be performed as per the information received in uac-BarringInfoSetList.

Reference:

- TS 38.331 [37], clauses 5.3.14

### 5.4.2.3 Test purpose

The purpose of this test is to verify that:

- 1) the ME reads the access control value from  $EF_{UAC\_AIC}$  and  $EF_{ACC}$  as part of the USIM-ME initialisation procedure, and subsequently adopts this value.
- 2) the UE maps the kind of request to one or more access identities and one access category and lower layers performs access barring checks for that request based on the determined access identities and access category.
- 3) the UE determines whether or not a particular access attempt is allowed based on uac-BarringInfo broadcast in SIB1 and if the RPLMN is the HPLMN, EHPLMN or visited PLMN of the home country.

### 5.4.2.4 Method of test

#### 5.4.2.4.1 Initial conditions

The values of the 5G-NR UICC as defined in clause 4.5.9 of the present document are used with  $EF_{IMSI}$  as defined in clause 4.6.5 and the following exceptions:

#### $EF_{UAC\_AIC}$ and $EF_{ACC}$

No Access Identities configured in  $EF_{UAC\_AIC}$  and no Access Classes configured in  $EF_{ACC}$  as also shown in table 5.4.2-1.

#### $EF_{UST}$ (USIM Service Table)

Logically:

Settings from clause 4.5.9 (5G-NR UICC) of the present document apply with the following changes:

Service n°124	Subscription identifier privacy support	not available
Service n°126	UAC Access Identities support	available

Coding:

Byte:	B1	B2	B3	B4	B5	B6	B7	B8
Binary:	xxxx xx1x	xxxx xxxx	xxx1 1x00	xxxx x1xx	xxxx xx11	xxx1 xx1x	xxxx xxxx	xxxx xxxx
	<b>B9</b>	<b>B10</b>	<b>B11</b>	...	<b>B16</b>			
	xxxx xxxx	xxxx xxxx	xx11 xxxx	...	xx10 011x			

The TT (NG-SS) is configured to transmit on the BCCH with the following parameters:

Cell A:

- TAI (MCC/MNC/TAC): MCC, MNC: see table 5.4.2-1, TAC: 000001.
- CellIdentity: 000000001

For the table 5.4.2-1:

uac-BarringInfo in SIB1 should be set as in the table:

- Refer to Annex A for the Methods  $UAC\_BarringInfo\_xxxxxx()$  in the table.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case.

## 5.4.2.4.2 Test sequence settings

Table 5.4.2-1

TC Seq#	Access Category	USIM		SIB1 on Cell A		REGISTRATION ACCEPT (5GS network feature support IE)		Result	
		EF <sub>UAC_AIC</sub>	EF <sub>ACC</sub> (Byte 1 b8-b4)	uac-BarringInfo	PLMN-Identity (MCC/MNC)	MPS indicator Bit	MCS indicator Bit	Registration successful?	MO Data call successful?
1.1	7	0x01 00 00 00	00000	Not Present	246 / 081	0	0	Yes	Yes
1.2	3	0x01 00 00 00	00000	UAC_BarringInfo_Common (3,0x1000000'B)	246 / 081	0	0	No	NA
1.3	3	0x01 00 00 00	00000	UAC_BarringInfo_PerPLMN (3,0x1000000'B)	246 / 081	0	0	No	NA
1.4	3	0x01 00 00 00	00000	UAC_BarringInfo_Common (3,0x1000000'B)	246 / 082	0	0	No	NA
1.5	3	0x01 00 00 00	00000	UAC_BarringInfo_Common (3,0x0100000'B)	246 / 081	0	0	Yes	Yes
1.6	3	0x03 00 00 00	00000	UAC_BarringInfo_Common (3,0x0100000'B)	246 / 081	0	0	Yes	Yes
1.7	7	0x01 00 00 00	00000	UAC_BarringInfo_Common (7,0x0000000'B)	246 / 081	0	0	Yes	Yes
1.8	3	0x01 00 00 00	00000	UAC_BarringInfo_Common (3,0x0000000'B)	244 / 081	0	0	No	NA
1.9	7	0x01 00 00 00	00000	UAC_BarringInfo_Common (7,0x1000000'B)	246 / 081	0	0	Yes	No
1.10	7	0x01 00 00 00	00000	UAC_BarringInfo_PerPLMN (7,0x1000000'B)	246 / 081	0	0	Yes	No
1.11	7	0x01 00 00 00	00000	UAC_BarringInfo_Common (7,0x1000000'B)	246 / 082	0	0	Yes	No
1.12	7	0x01 00 00 00	00000	UAC_BarringInfo_Common (7,0x0000000'B)	244 / 081	0	0	Yes	No
1.13	7	0x01 00 00 00	00000	UAC_BarringInfo_Common (7,0x0100000'B)	244 / 081	1	0	Yes	Yes
1.14	7	0x02 00 00 00	00000	UAC_BarringInfo_Common (7,0x0100000'B)	244 / 081	1	0	Yes	Yes
1.15	7	0x01 00 00 00	00000	UAC_BarringInfo_Common2 (3,0x0100000'B, 7,0x1000000'B)	246 / 081	0	0	Yes	No
1.16	3	0x01 00 00 00	00000	UAC_BarringInfo_Common2 (7,0x1000000'B, 3,0x0000000'B)	244 / 081	0	0	No	NA
2.5	8	0x01 00 00 00	00000	UAC_BarringInfo_Common2 (7,0x1000000'B, 8,0x0000000'B)	244 / 081	0	0	No	
2.6	8	0x01 00 00 00	00000	UAC_BarringInfo_Common (8,0x0000000'B)	246 / 081	0	0	Yes	

## 5.4.2.4.3 Procedure

Procedure/steps to be repeated for all sequences listed in table 5.4.2-1:

Step	Direction	Action	Information	REQ	SA
1	TT	SIB1 of Cell A is transmitted as defined in the initial conditions for tests from table 5.4.2-1	Barring info is set as in table 5.4.2-1 See Annex A for the Methods UAC_BarringInfo_XXXXXX() in the table		
2	UE	Power UE on	The UE performs a SIM initialisation. (includes reading of EF <sub>UAC_AIC</sub> and EF <sub>ACC</sub> )	CR 1	A.2/1 OR A.2/2
<b>If cell access is not allowed:</b>					
3	UE > TT	REGISTRATION REQUEST is not sent	See column 'Registration successful?' for the result	CR 2 CR 3 CR 4	
4	User	End test sequence			

If cell access is allowed:					
3	UE > TT	Send REGISTRATION REQUEST	See column 'Registration successful?' for the result	CR 2 CR 3 CR 4	
4	TT > UE	Send REGISTRATION ACCEPT	For simplicity other signalling is not shown		
If MO Data call is not allowed:					
5	UE	Attempt to set up MO Data call	To set up the MO Data call the MMI or EMMI is used	CR 2 CR 3 CR 4	
6	User	End test sequence			
If MO Data call is allowed:					
5	UE > TT	Set up MO Data call ( <i>PDU SessionEstablishment</i> )	To set up the MO Data call the MMI or EMMI is used	CR 2 CR 3 CR 4	
6	User	End test sequence			

### 5.4.2.5 Acceptance criteria

For the scenarios in table 5.4.2-1:

CR 1 is explicitly verified at step 2) by analysing the file READ commands for EF<sub>UAC-AIC</sub> and EF<sub>ACC</sub> during the USIM-ME initialisation procedure.

CR 2, CR 3, and CR 4 are verified at:

- step 3) by analysing if the UE shall make a successful or unsuccessful registration to the network in accordance with the result indicated in the table and
- step 5) by analysing if the UE shall make a successful or unsuccessful MO Data call in accordance with the result indicated in the table if the step is applicable.

## 5.4.2A Unified Access Control – Access Identity 1 – MPS indicated by USIM, Access Category 8

### 5.4.2A.1 Definition and applicability

The purpose of Unified Access Control procedure is to perform access barring check for a 5GS access attempt associated with a given Access Category and one or more Access Identities upon request from upper layers or the RRC layer.

The 5G network shall be able to broadcast barring control information (i.e. a list of barring parameters associated with an Access Identity and an Access Category) in SIB1.

The EF<sub>UAC-AIC</sub> in the USIM contains the configuration information pertaining to access identity 1 allocated for high priority services MPS.

The UE shall be able to determine whether or not a particular new access attempt is allowed based on barring parameters that the UE receives from the broadcast barring control information and the configuration in the USIM.

When the NAS detects an access event, the NAS shall perform the mapping of the kind of request to one or more access identities and one access category and lower layers will perform access barring checks for that request based on the determined access identities and access category.

If RRC state is RRC\_INACTIVE and the resumption of the RRC connection is triggered due to an RNA Update RRC layer shall select Access Category as '8' and perform unified access control procedure in case there is no ongoing emergency service.

### 5.4.2A.2 Conformance requirement

CR 1 The ME shall read the access control value as part of the USIM-ME initialization procedure, and subsequently adopt this value.

Reference:

- TS 31.102 [19], clause 5.1.1.2.

CR 2 Access Identities are configured at the UE as listed in TS 22.261 [36] Table 6.22.2.2-1. Access Categories are defined by the combination of conditions related to UE and the type of access attempt as listed in TS 22.261 [36] Table 6.22.2.3-1. One or more Access Identities and only one Access Category are selected and tested for an access attempt.

Reference:

- TS 22.261 [36], clause 6.22.2

CR 3 Access Identity 1 is valid if the RPLMN is the HPLMN, EHPLMN or visited PLMN of the home country.

Reference:

- TS 24.501 [25], clause 4.5.2

CR 4 The UE shall be able to determine whether or not a particular new access attempt is allowed based on uac-BarringInfo broadcast in SIB1. Access Control check shall be performed as per the information received in uac-BarringInfoSetList.

Reference:

- TS 38.331 [37], clauses 5.3.14

CR 5 If the resumption of the RRC connection is triggered due to an RNA update and there is no ongoing emergency service RRC shall select '8' as the Access Category and perform the unified access control procedure.

Reference:

- TS 38.331 [37], clauses 5.3.13.2

### 5.4.2A.3 Test purpose

The purpose of this test is to verify that:

- 1) the ME reads the access control value from  $EF_{UAC\_AIC}$  and  $EF_{ACC}$  as part of the USIM-ME initialisation procedure, and subsequently adopts this value.
- 2) the UE maps the kind of request to one or more access identities and one access category and lower layers performs access barring checks for that request based on the determined access identities and access category.
- 3) the UE determines whether or not a particular access attempt is allowed based on uac-BarringInfo broadcast in SIB1 and if the RPLMN is the HPLMN, EHPLMN or visited PLMN of the home country.
- 4) the UE performs unified access control procedure if RNA Update procedure is triggered.

### 5.4.2A.4 Method of test

#### 5.4.2A.4.1 Initial conditions

The values of the 5G-NR UICC as defined in clause 4.5.9 of the present document are used with  $EF_{IMSI}$  as defined in clause 4.6.5 and the following exceptions:

**$EF_{UAC\_AIC}$**  and  **$EF_{ACC}$**

No Access Identities configured in  $EF_{UAC\_AIC}$  and no Access Classes configured in  $EF_{ACC}$  as also shown in table 5.4.2A-2.

**EF<sub>UST</sub>** (USIM Service Table)

Logically:

Service n°124	Subscription identifier privacy support	not available
Service n°126	UAC Access Identities support	available

Coding:

Byte:	B1	B2	B3	B4	B5	B6	B7	B8
Binary:	xxxx xx1x	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxx1 xx1x	xxxx xxxx	xxxx xxxx
	<b>B9</b>	<b>B10</b>	<b>B11</b>	...	<b>B16</b>			
	xxxx xxxx	xxxx xxxx	xx11 xxxx	...	xx10 011x			

The TT (NG-SS) is configured to transmit on the BCCH with the following parameters:

Cell A:

- TAI (MCC/MNC/TAC): MCC, MNC: see table 5.4.2A-1, TAC: 000001.
- CellIdentity: 000000001

For the table 5.4.2A-1:

No uac-BarringInfo in SIB1.

Cell B:

- TAI (MCC/MNC/TAC): MCC, MNC: see table 5.4.2A-1, TAC: 000001.
- CellIdentity: 000000002

For the table 5.4.2A-1:

uac-BarringInfo in SIB1 should be set as in the table:

- Refer to Annex A for the Methods UAC\_BarringInfo\_xxxxxx() in the table.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case.

**5.4.2A.4.2 Test sequence settings**

**Table 5.4.2A-1**

TC Seq#	Access Category	USIM		SIB1 on Cell B		REGISTRATION ACCEPT (5GS network feature support IE)		Result
		EF <sub>UAC_AIC</sub>	EF <sub>ACC</sub> (Byte 1 b8-b4)	uac-BarringInfo	PLMN-Identity (MCC/MNC)	MPS indicator Bit	MCS indicator Bit	
2.1	8	0x01 00 00 00	00000	Not Present	246 / 081	0	0	Yes
2.2	8	0x01 00 00 00	00000	UAC_BarringInfo_Common (8,0x1000000'B)	246 / 081	0	0	No
2.3	8	0x01 00 00 00	00000	UAC_BarringInfo_PerPLMN (8,0x0000000'B)	246 / 081	0	0	Yes
2.4	8	0x01 00 00 00	00000	UAC_BarringInfo_Common (8,0x1000000'B)	244 / 081	1	0	No
2.5	8	0x01 00 00 00	00000	UAC_BarringInfo_Common2 (7,0x1000000'B, 8,0x0000000'B)	244 / 081	0	0	No
2.6	8	0x01 00 00 00	00000	UAC_BarringInfo_Common (8,0x0000000'B)	246 / 081	0	0	Yes

**5.4.2A.4.3 Procedure**

Procedure/steps to be repeated for all sequences listed in table 5.4.2A-1:

Step	Direction	Action	Information	REQ	SA
1	TT	SIB1 of Cell A is transmitted as defined in the initial conditions and in table 5.4.2A-1	No barring info is provided to Cell A		
2	UE	Power UE on	The UE performs a SIM initialisation	CR 1	A.2/1 OR A.2/2
3	UE > TT	Send REGISTRATION REQUEST			
4	TT > UE	Send REGISTRATION ACCEPT	The registration is successful		
5	UE > TT	Set up MO Data call (PDU SessionEstablishment)	To set up the MO Data call the MMI or EMMI is used. The MO Data call is set up successfully		
6	TT > UE	Send RRC RELEASE with <i>suspendConfig</i> in <i>criticalExtensions</i> (with the choice <i>rrcRelease</i> )	ran-NotificationAreaInfo in <i>suspendConfig</i> contains the <i>cellList</i> with <i>cellIdentity</i> of Cell A: <pre> cellList {   plmn-Identity {mcc, mnc},   -- see table 5.4.2A-1 for   MCC/MNC   ran-AreaCells 000000001'B } </pre>		
7	TT	Deactivate Cell A and activate Cell B			
8	TT	SIB1 of Cell B is transmitted as defined in table 5.4.2A-1	Barring info is as in the table. See Annex A for the Methods <i>UAC_BarringInfo_XXXXX()</i> in the table		
9	UE > TT	Initiate RRC RESUME REQUEST procedure with <i>resumeCause</i> set to <i>rna-Update</i> .	See the column 'RRC RESUME REQUEST with <i>resumeCause</i> set to <i>rna-Update</i> successful?' for the result	CR 2 CR 3 CR 4 CR 5	

### 5.4.2A.5 Acceptance criteria

For the scenarios in table 5.4. 2A-1:

CR 1 is explicitly verified at step 2) by analysing the file READ commands for  $EF_{UAC\_AIC}$  and  $EF_{ACC}$  during the USIM-Terminal initialisation procedure.

CR 2, CR 3, CR 4, and CR 5 are verified at step 9) by analysing if the UE shall make a successful or unsuccessful RRC Resumption for RNA Update in accordance with the result indicated in the table.

## 5.4.3 Unified Access Control – Access Identity 1 – no MPS indication by USIM and SUPI not changed

### 5.4.3.1 Definition and applicability

The purpose of Unified Access Control procedure is to perform access barring check for a 5GS access attempt associated with a given Access Category and one or more Access Identities upon request from upper layers or the RRC layer.

The 5G network shall be able to broadcast barring control information (i.e. a list of barring parameters associated with an Access Identity and an Access Category) in SIB1.

When the UE is in the country of its HPLMN or in an EHPLMN (if the EHPLMN list is present), and the USIM file  $EF_{UAC\_AIC}$  does not indicate the UE is configured for access identity 1, the UE uses the MPS indicator bit of the 5GS network feature support IE in the REGISTRATION ACCEPT message to determine if access identity 1 is valid.

The UE shall not consider access identity 1 to be valid when the UE is not in the country of its HPLMN prior to receiving the MPS indicator bit of the 5GS network feature support IE in the REGISTRATION ACCEPT message being set to "Access identity 1 valid in RPLMN or equivalent PLMN".

The UE shall be able to determine whether or not a particular new access attempt is allowed based on barring parameters that the UE receives from the broadcast barring control information and the configuration in the USIM.

When the NAS detects an access event, the NAS shall perform the mapping of the kind of request to one or more access identities and one access category and lower layers will perform access barring checks for that request based on the determined access identities and access category.

#### 5.4.3.2 Conformance requirement

CR 1 The USIM file EF<sub>UAC\_AIC</sub> does not indicate the UE is configured for access identity 1, the UE uses the MPS indicator bit of the 5GS network feature support IE in the REGISTRATION ACCEPT message to determine if access identity 1 is valid. shall read the access control value as part of the USIM-ME initialization procedure, and subsequently adopt this value.

Reference:

- TS 24.501 [25], clause 4.5.2.

CR 2 The UE shall not consider access identity 1 to be valid when the UE is not in the country of its HPLMN prior to receiving the MPS indicator bit of the 5GS network feature support IE in the REGISTRATION ACCEPT message being set to "Access identity 1 valid in RPLMN or equivalent PLMN".

Reference:

- TS 24.501 [25], clause 4.5.2.

CR 3 The MPS indicator is stored together with a PLMN identity of the PLMN that provided it, and is valid in that RPLMN or equivalent PLMN. The MPS indicator can only be used if the SUPI from the USIM matches the SUPI stored in the non-volatile memory of the ME, else the UE shall delete the MPS indicator.

Reference:

- TS 24.501 [25], Annex C.

CR 4 Access Identity 1 is valid if the RPLMN is the HPLMN, EHPLMN or visited PLMN of the home country.

Reference:

- TS 24.501 [25], clause 4.5.2

CR 5 Upon receiving a REGISTRATION ACCEPT message with the MPS indicator bit set to "Access identity 1 valid", the UE shall act as a UE with access identity 1 configured for MPS in all NG-RAN of the registered PLMN and its equivalent PLMNs. The MPS indicator bit in the 5GS network feature support IE provided in the REGISTRATION ACCEPT message is valid until the UE receives a REGISTRATION ACCEPT message with the MPS indicator bit set to "Access identity 1 not valid" or until the UE selects a non-equivalent PLMN. Access identity 1 is only applicable while the UE is in N1 mode.

Reference:

- TS 24.501 [25], clause 5.5.1.3.4

CR 6 The UE shall be able to determine whether or not a particular new access attempt is allowed based on uac-BarringInfo broadcast in SIB1. Access Control check shall be performed as per the information received in uac-BarringInfoSetList.

Reference:

- TS38.331 [37], clauses 5.3.14

#### 5.4.3.3 Test purpose

The purpose of this test is to verify that:

- 1) if the RPLMN is the HPLMN, EHPLMN or visited PLMN of the home country and the USIM file EF<sub>UAC\_AIC</sub> does not indicate the UE is configured for access identity 1 and the MPS indicator bit of the 5GS network feature support IE in the REGISTRATION ACCEPT message is received, UE considers access identity as 1 for access barring;

- 2) the MPS indicator is stored together with a PLMN identity of the PLMN that provided it, and the MPS indicator can only be used if the SUPI from the USIM matches the SUPI stored in the non-volatile memory of the ME;
- 3) the UE maps the kind of request to one or more access identities and one access category and lower layers performs access barring checks for that request based on the determined access identities and access category;
- 4) the UE determines whether or not a particular access attempt is allowed based on uac-BarringInfo broadcast in SIB1 and if the RPLMN is the HPLMN, EHPLMN or visited PLMN of the home country;
- 5) a UE operated with a USIM where the file EF<sub>UAC\_AIC</sub> does not indicate access identity 1, after a change of the REGISTRATION ACCEPT message with the MPS indicator bit set to "Access identity 1 not valid", or when the UE has selected a non-equivalent PLMN, the UE is acting as if it is configured for access identity 0.

#### 5.4.3.4 Method of test

##### 5.4.3.4.1 Initial conditions

The values of the 5G-NR UICC as defined in clause 4.5.9 of the present document are used with EF<sub>IMSI</sub> as defined in clause 4.6.5 and the following exceptions:

##### EF<sub>UAC\_AIC</sub> and EF<sub>ACC</sub>

No Access Identity is configured in EF<sub>UAC\_AIC</sub> and no Access Classes are configured in EF<sub>ACC</sub> as given in table 5.4.3-1.

##### EF<sub>UST</sub> (USIM Service Table)

Logically:

Service n°124	Subscription identifier privacy support	not available
Service n°126	UAC Access Identities support	available

Coding:

Byte:	B1	B2	B3	B4	B5	B6	B7	B8
Binary:	xxxx xx1x	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxxx xxxx	xxxx xxxx	xxxx xxxx
	<b>B9</b>	<b>B10</b>	<b>B11</b>	...	<b>B16</b>			
	xxxx xxxx	xxxx xxxx	xx11 xxxx	...	xx10 011x			

The TT (NG-SS) is configured to transmit on the BCCH with the following parameters:

Cell A:

- TAI (MCC/MNC/TAC): 246/081/000001.
- CellIdentity: 00000001

For Table 5.4.3-1:

After turning on the cell for the 2<sup>nd</sup> time, uac-BarringInfo in SIB1 should be set as in the table:

- Refer to Annex A for the Methods UAC\_BarringInfo\_xxxxxx() in the table.

Cell B:

- TAI (MCC/MNC/TAC): MCC, MNC: see table 5.4.3-1, TAC: 000002.
- CellIdentity: 00000002

For Table 5.4.3-1:

uac-BarringInfo in SIB1 should be set as in the table:

- Refer to Annex A for the Methods UAC\_BarringInfo\_xxxxxx() in the table.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case.

5.4.3.4.2 Test sequence settings

Table 5.4.3-1

TC Seq#	Access Category	USIM		REGISTRATION ACCEPT (5GS network feature support IE) on Cell A at 1 <sup>st</sup> power up of the ME		SIB1 of Cell A or B after the 2 <sup>nd</sup> power up of the ME			Result	
		EF <sub>UAC-AIC</sub>	EF <sub>ACC</sub> (Byte 1 b8-b4)	MPS indicator Bit	MCS indicator Bit	Cell A or B	uac-BarringInfo	PLMN-Identity (MCC/MNC)	Registration successful?	MO Data call successful?
1.1	3	0x00 00 00 00	00000	1	0	Cell A	Not Present	246 / 081	Yes	Yes
1.2	3	0x00 00 00 00	00000	1	0	Cell A	UAC_BarringInfo_Common (3,0x1000000'B)	246 / 081	No	N/A
1.3	7	0x00 00 00 00	00000	1	0	Cell A	UAC_BarringInfo_Common (7,0x0100000'B)	246 / 081	Yes	No
1.4	3	0x00 00 00 00	00000	1	0	Cell A	UAC_BarringInfo_Common (3,0x0100000'B)	246 / 081	Yes	Yes
1.5	3	0x00 00 00 00	00000	1	0	Cell B	UAC_BarringInfo_PerPLMN (3,0x0100000'B)	246 / 082	No	N/A
1.6	3	0x00 00 00 00	00000	1	0	Cell B	UAC_BarringInfo_Common (3,0x0000000'B)	244 / 081	No	N/A
1.7	7	0x00 00 00 00	00000	1	0	Cell B	UAC_BarringInfo_Common (7,0x0100000'B)	244 / 081	Yes	No
1.8	7	0x00 00 00 00	00000	1	1	Cell B	UAC_BarringInfo_Common (7,0x0100000'B)	244 / 081	Yes	No

5.4.3.4.3 Procedure

Procedure/steps to be repeated for all sequences listed in table 5.4.3-1:

Step	Direction	Action	Information	REQ	SA
1	TT	SIB1 of Cell A is transmitted without uac-BarringInfo in SIB1.			
2	UE	Power UE on	The UE performs a SIM initialisation. (includes reading of EF <sub>UAC-AIC</sub> and EF <sub>ACC</sub> )	CR 1	A.2/1 OR A.2/2
3	UE > TT	REGISTRATION REQUEST is sent			
4	TT > UE	Send REGISTRATION ACCEPT	The MPS indicator bit set to "Access identity 1 valid". For simplicity other signalling is not shown		
5	UE	Power UE off			
6	TT	Deactivates Cell A			
7	TT	Activates Cell A or B with SIB1 as specified in the table 5.4.3-1	See the column 'SIB1 of Cell A or B after the 2nd power up of the ME' for the SIB 1 and the column 'Cell A or B' to find the cell to be activated for this test step.		
8	UE	Power UE on	The UE performs a SIM initialisation again.		
<b>If cell access is not allowed:</b>					
9	UE > TT	REGISTRATION REQUEST in not sent	See column 'Registration successful?' for the result	CR 2 through CR 6	
10	USER	End test sequence			

If cell access is allowed:					
9	UE > TT	Send REGISTRATION REQUEST	See column 'Registration successful?' for the result	CR 2 through CR 6	
10	TT > UE	Send REGISTRATION ACCEPT	MPS and MCS indicator bits are set to zero in 5GS network feature support IE. For simplicity other signalling is not shown		
If MO Data call is not allowed:					
11	UE	Attempt to set up MO Data call	To set up the MO Data call the MMI or EMMI is used	CR 2 through CR 6	
12	USER	End test sequence			
If MO Data call is allowed:					
11	UE > TT	Set up MO Data call ( <i>PDU SessionEstablishment</i> )	To set up the MO Data call the MMI or EMMI is used	CR 2 through CR 6	
12	USER	End test sequence			

#### 5.4.3.5 Acceptance criteria

For the scenarios in table 5.4.3-1:

CR 1 is explicitly verified at step 2) by analysing the file READ commands for EF<sub>UAC-AIC</sub> and EF<sub>ACC</sub> during the USIM-Terminal initialisation procedure.

CR 2, CR 3, CR 4, CR 5, and CR 6 are verified

- at steps 9) and 10) by analysing if the UE shall make a successful or unsuccessful Registration to the network in accordance with the result indicated in the table and
- at steps 11) and 12) by analysing if the UE shall make a successful or unsuccessful MO Data call in accordance with the result indicated in the table if the step is applicable.

### 5.4.4 Unified Access Control – Access Identity 1 – no MPS indication by USIM and SUPI is changed

#### 5.4.4.1 Definition and applicability

The purpose of Unified Access Control procedure is to perform access barring check for a 5GS access attempt associated with a given Access Category and one or more Access Identities upon request from upper layers or the RRC layer.

The 5G network shall be able to broadcast barring control information (i.e. a list of barring parameters associated with an Access Identity and an Access Category) in SIB1.

When the UE is in the country of its HPLMN or in an EHPLMN (if the EHPLMN list is present), and the USIM file EF<sub>UAC\_AIC</sub> does not indicate the UE is configured for access identity 1, the UE uses the MPS indicator bit of the 5GS network feature support IE in the REGISTRATION ACCEPT message to determine if access identity 1 is valid.

The MPS indicator is stored together with a PLMN identity of the PLMN that provided it and is valid in that RPLMN or equivalent PLMN. The MPS indicator can only be used if the SUPI from the USIM matches the SUPI stored in the non-volatile memory of the ME, else the UE shall delete the MPS indicator.

The UE shall be able to determine whether or not a particular new access attempt is allowed based on barring parameters that the UE receives from the broadcast barring control information and the configuration in the USIM.

When the NAS detects an access event, the NAS shall perform the mapping of the kind of request to one or more access identities and one access category and lower layers will perform access barring checks for that request based on the determined access identities and access category.

#### 5.4.4.2 Conformance requirement

CR 1 When the UE is in the country of its HPLMN, and the USIM file  $EF_{UAC\_AIC}$  does not indicate the UE is configured for access identity 1, the UE uses the MPS indicator bit of the 5GS network feature support IE in the REGISTRATION ACCEPT message to determine if access identity 1 is valid.

Reference:

- TS 24.501 [25], clause 4.5.2.

CR 2 The UE shall not consider access identity 1 to be valid when the UE is not in the country of its HPLMN prior to receiving the MPS indicator bit of the 5GS network feature support IE in the REGISTRATION ACCEPT message being set to "Access identity 1 valid" in RPLMN or equivalent PLMN.

Reference:

- TS 24.501 [25], clause 4.5.2.

CR 3 Upon receiving a REGISTRATION ACCEPT message with the MPS indicator bit set to "Access identity 1 valid" in RPLMN or equivalent PLMN, the UE shall act as a UE with access identity 1 configured for MPS in all NG-RAN of the registered PLMN and its equivalent PLMNs. The MPS indicator bit in the 5GS network feature support IE provided in the REGISTRATION ACCEPT message is valid until the UE receives a REGISTRATION ACCEPT message with the MPS indicator bit set to "Access identity 1 not valid in RPLMN or equivalent PLMN" or until the UE selects a non-equivalent PLMN. Access identity 1 is only applicable while the UE is in N1 mode.

Reference:

- TS 24.501 [25], clause 5.5.1.2.4.

CR 4 The MPS indicator is stored together with a PLMN identity of the PLMN that provided it, and is valid in that RPLMN or equivalent PLMN. The MPS indicator can only be used if the SUPI from the USIM matches the SUPI stored in the non-volatile memory of the ME, else the UE shall delete the MPS indicator.

Reference:

- TS 24.501 [25], Annex C.

CR 5 The UE shall be able to determine whether or not a particular new access attempt is allowed based on uac BarringInfo broadcast in SIB1. Access Control check shall be performed as per the information received in uac BarringInfoSetList.

Reference:

- TS 38.331 [37], clause 5.3.14

#### 5.4.4.3 Test purpose

The purpose of this test is to verify that:

- 1) if the RPLMN is the HPLMN, EHPLMN or visited PLMN of the home country and the USIM file  $EF_{UAC\_AIC}$  does not indicate the UE is configured for access identity 1 and the MPS indicator bit of the 5GS network feature support IE in the REGISTRATION ACCEPT message is received, UE considers access identity as 1 for access barring;
- 2) the MPS indicator bit in the 5GS network feature support IE provided in the REGISTRATION ACCEPT message is valid until the UE receives a REGISTRATION ACCEPT message with the MPS indicator bit set to "Access identity 1 not valid" or until the UE selects a non-equivalent PLMN;
- 3) the MPS indicator is stored together with a PLMN identity of the PLMN that provided it, and the MPS indicator can only be used if the SUPI from the USIM matches the SUPI stored in the non-volatile memory of the ME;
- 4) the UE maps the kind of request to one or more access identities and one access category and lower layers performs access barring checks for that request based on the determined access identities and access category;

- 5) a UE operated with a USIM where the file EF<sub>UAC\_AIC</sub> does not indicate access identity 1, after a change of the REGISTRATION ACCEPT message with the MPS indicator bit set to "Access identity 1 not valid", or when the UE has selected a non-equivalent PLMN, the UE is acting as if it is configured for access identity 0.

5.4.4.4 Method of test

5.4.4.4.1 Initial conditions

The values of the 5G-NR UICC as defined in clause 4.5.9 of the present document are used with EF<sub>IMSI</sub> as defined in clause 4.6.5 and the following exceptions:

EF<sub>UAC\_AIC</sub> and EF<sub>ACC</sub>

No Access Identity is configured in EF<sub>UAC\_AIC</sub> and no Access Classes are configured in EF<sub>ACC</sub> as given in table 5.4.4-1.

EF<sub>UST</sub> (USIM Service Table)

Logically:

Service n°124	Subscription identifier privacy support	not available
Service n°126	UAC Access Identities support	available

Coding:

<b>Byte:</b>	<b>B1</b>	<b>B2</b>	<b>B3</b>	<b>B4</b>	<b>B5</b>	<b>B6</b>	<b>B7</b>	<b>B8</b>
Binary:	xxxx xx1x	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxxx xxxx	xxxx xxxx	xxxx xxxx
	<b>B9</b>	<b>B10</b>	<b>B11</b>	...	<b>B16</b>			
	xxxx xxxx	xxxx xxxx	xx11 xxxx	...	xx10 011x			

The defined UICC/USIM data is installed on the UE.

The TT (NG-SS) is configured to transmit on the BCCH with the following parameters:

Cell A:

- TAI (MCC/MNC/TAC): 246/081/000001.
- CellIdentity: 000000001

For Table 5.4.4-1:

After turning on the cell for the 2<sup>nd</sup> time, uac-BarringInfo in SIB1 should be set as in the table:

- Refer to Annex A for the Methods UAC\_BarringInfo\_xxxxxx() in the table.

Cell B:

Transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): MCC, MNC: see table 5.4.4-1, TAC: 000002.
- CellIdentity: 000000002

For Table 5.4.4-1:

uac-BarringInfo in SIB1 should be set as in the table:

- Refer to Annex A for the Methods UAC\_BarringInfo\_xxxxxx() in the table.

5.4.4.4.2 Test sequence settings

Table 5.4.4-1

TC Seq#	Acc	USIM	REGISTRATION ACCEPT	SIB1 of Cell A or B after the 2 <sup>nd</sup> power up of the ME	Result
---------	-----	------	---------------------	--	--------

				(5GS network feature support IE) on Cell A at 1 <sup>st</sup> power up of the ME						
		EF <sub>UAC_AIC</sub>	EF <sub>ACC</sub> (Byte 1 b8-b4)	MPS indicator Bit	MCS indicator Bit	Cell A or B	uac-BarringInfo	PLMN-Identity (MCC/MNC)	Registration successful?	MO Data call successful?
1.1	3	0x00 00 00 00	00000	1	0	Cell A	Not Present	246 / 081	Yes	Yes
1.2	3	0x00 00 00 00	00000	1	0	Cell A	UAC_BarringInfo_Common (3,0x0100000'B)	246 / 081	No	NA
1.3	7	0x00 00 00 00	00000	1	0	Cell A	UAC_BarringInfo_Common (7,0x0100000'B)	246 / 081	Yes	No
1.4	3	0x00 00 00 00	00000	1	0	Cell A	UAC_BarringInfo_Common (3,0x0000000'B)	246 / 081	No	NA
1.5	3	0x00 00 00 00	00000	1	0	Cell B	UAC_BarringInfo_Common (3,0x0100000'B)	246 / 082	No	NA
1.6	3	0x00 00 00 00	00000	1	0	Cell B	UAC_BarringInfo_PerPLMN (3,0x01000001'B)	244 / 081	No	NA
1.7	7	0x00 00 00 00	00000	1	0	Cell B	UAC_BarringInfo_Common (7,0x0000000'B)	244 / 081	Yes	No

#### 5.4.4.4.3 Procedure

Procedure/steps to be repeated for all sequences listed in table 5.4.3-1:

Step	Direction	Action	Information	REQ	SA
1	TT	SIB1 of Cell A is transmitted without uac-BarringInfo in SIB1.			
2	UE	Power UE on	The UE performs a SIM initialisation. (includes reading of EF <sub>UAC_AIC</sub> and EF <sub>ACC</sub> )	CR 1	A.2/1 OR A.2/2
3	UE > TT	REGISTRATION REQUEST is sent			
4	TT > UE	Send REGISTRATION ACCEPT	The MPS indicator bit set to "Access identity 1 valid".  For simplicity other signalling is not shown		
5	UE	Power UE on			
6	TT	Deactivates Cell A			
7	TT	Activates Cell A or B with SIB1 as specified in the table 5.4.3-1	See the column 'SIB1 of Cell A or B after the 2nd power up of the ME' for the SIB 1 and the column 'Cell A or B' to find the cell to be activated for this test step.		
8	UE	Power UE on	Power on with a different USIM (e.g.: IMSI set to 24681685533963) The UE performs a SIM initialisation again.		
<b>If cell access is not allowed:</b>					
9	UE > TT	REGISTRATION REQUEST in not sent	See column 'Registration successful?' for the result	CR 2 through CR 5	
10	USER	End test sequence			
<b>If cell access is allowed:</b>					
9	UE > TT	Send REGISTRATION REQUEST	See column 'Registration successful?' for the result	CR 2 through CR 5	

10	TT > UE	Send REGISTRATION ACCEPT	MPS and MCS indicator bits are set to zero in 5GS network feature support IE. For simplicity other signalling is not shown		
<b>If MO Data call is not allowed:</b>					
11	UE	Attempt to set up MO Data call	To set up the MO Data call the MMI or EMMI is used	CR 2 through CR 5	
12	USER	End test sequence			
<b>If MO Data call is allowed:</b>					
11	UE > TT	Set up MO Data call ( <i>PDU Session Establishment</i> )	To set up the MO Data call the MMI or EMMI is used	CR 2 through CR 5	
12	USER	End test sequence			

#### 5.4.4.5 Acceptance criteria

For the scenarios in table 5.4.4-1:

CR 1 is explicitly verified at step 2) by analysing the file READ commands for  $EF_{UAC-AIC}$  and  $EF_{ACC}$  during the USIM-Terminal initialisation procedure.

CR 2, CR 3, CR 4, and CR 5 are verified:

- at steps 9) and 10) by analysing if the UE shall make a successful or unsuccessful Registration to the network in accordance with the result indicated in the table and
- at steps 11) and 12) by analysing if the UE shall make a successful or unsuccessful MO Data call in accordance with the result indicated in the table if the step is applicable.

### 5.4.5 Unified Access Control – Access Identity 2 – MCS indicated by USIM

#### 5.4.5.1 Definition and applicability

The purpose of Unified Access Control procedure is to perform access barring check for a 5GS access attempt associated with a given Access Category and one or more Access Identities upon request from upper layers or the RRC layer.

The 5G network shall be able to broadcast barring control information (i.e. a list of barring parameters associated with an Access Identity and an Access Category) in SIB1.

The  $EF_{UAC-AIC}$  in the USIM contains the configuration information pertaining to access identity 2 allocated for high priority services MCS.

The UE shall be able to determine whether or not a particular new access attempt is allowed based on barring parameters that the UE receives from the broadcast barring control information and the configuration in the USIM.

When the NAS detects an access event, the NAS shall perform the mapping of the kind of request to one or more access identities and one access category and lower layers will perform access barring checks for that request based on the determined access identities and access category.

#### 5.4.5.2 Conformance requirement

CR 1 The UE shall read the access control value as part of the USIM-Terminal initialization procedure, and subsequently adopt this value.

Reference:

- TS 31.102 [19], clause 5.1.1.2.

CR 2 Access Identities are configured at the UE as listed in TS 22.261 [36] Table 6.22.2.2-1. Access Categories are defined by the combination of conditions related to UE and the type of access attempt as listed in TS 22.261 [36] Table 6.22.2.3-1. One or more Access Identities and only one Access Category are selected and tested for an access attempt.

Reference:

- TS 22.261 [36], clause 6.22.2

CR 3 Access Identity 2 is valid if the RPLMN is the HPLMN, EHPLMN or visited PLMN of the home country.

Reference:

- TS 24.501 [25], clause 4.5.2

CR 4 The UE shall be able to determine whether or not a particular new access attempt is allowed based on uac-BarringInfo broadcast in SIB1. Access Control check shall be performed as per the information received in uac-BarringInfoSetList.

Reference:

- TS 38.331 [37], clauses 5.3.14

### 5.4.5.3 Test purpose

The purpose of this test is to verify that:

- 1) the ME reads the access control value from  $EF_{UAC\_AIC}$  and  $EF_{ACC}$  as part of the USIM-Terminal initialisation procedure, and subsequently adopts this value
- 2) the UE maps the kind of request to one or more access identities and one access category and lower layers performs access barring checks for that request based on the determined access identities and access category;
- 3) the UE determines whether or not a particular access attempt is allowed based on uac-BarringInfo broadcast in SIB1 and if the RPLMN is the HPLMN, EHPLMN or visited PLMN of the home country.

### 5.4.5.4 Method of test

#### 5.4.5.4.1 Initial conditions

The values of the 5G-NR UICC as defined in clause 4.5.9 of the present document are used with  $EF_{IMSI}$  as defined in clause 4.6.5 and the following exceptions:

#### $EF_{UAC\_AIC}$ and $EF_{ACC}$

No Access Identity is configured in  $EF_{UAC\_AIC}$  and no Access Classes are configured in  $EF_{ACC}$  as given in table 5.4.5-1.

#### $EF_{UST}$ (USIM Service Table)

Logically:

Service n°124	Subscription identifier privacy support	not available
Service n°126	UAC Access Identities support	available

Coding:

Byte:	B1	B2	B3	B4	B5	B6	B7	B8
Binary:	xxxx xx1x	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxxx xxxx	xxxx xxxx	xxxx xxxx
	B9	B10	B11	...	B16			
	xxxx xxxx	xxxx xxxx	xx11 xxxx	...	xx10 011x			

The defined UICC/USIM data is installed on the UE.

The TT (NG-SS) is configured to transmit on the BCCH with the following parameters:

Cell A:

- TAI (MCC/MNC/TAC): MCC, MNC: see tables 5.4.5-x, TAC: 000001.
- CellIdentity: 000000001

For Table 5.4.5-1:

uac-BarringInfo in SIB1 should be set as in the table:

- Refer to Annex A for the Methods UAC\_BarringInfo\_xxxxxx() in the table.

#### 5.4.5.4.2 Test sequence settings

Table 5.4.5-1

TC Seq#	Access Category	USIM		SIB1		REGISTRATION ACCEPT (5GS network feature support IE)		Result	
		EF <sub>UAC_AIC</sub>	EF <sub>ACC</sub> (Byte 1 b8-b4)	uac-BarringInfo	PLMN-Identity (MCC/MNC)	MPS indicator Bit	MCS indicator Bit	Registration successful?	MO Data call successful?
1.1	7	0x02 00 00 00	00000	Not Present	246 / 081	0	0	Yes	Yes
1.2	3	0x02 00 00 00	00000	UAC_BarringInfo_Common (3,0x0100000'B)	246 / 081	0	0	No	NA
1.3	3	0x02 00 00 00	00000	UAC_BarringInfo_PerPLMN (3,0x0100000'B)	246 / 081	0	0	No	NA
1.4	3	0x02 00 00 00	00000	UAC_BarringInfo_Common (3,0x0100000'B)	246 / 082	0	0	No	NA
1.5	3	0x02 00 00 00	00000	UAC_BarringInfo_Common (3,0x1000000'B)	246 / 081	0	0	Yes	Yes
1.6	3	0x03 00 00 00	00000	UAC_BarringInfo_Common (3,0x1000000'B)	246 / 081	0	0	Yes	Yes
1.7	7	0x02 00 00 00	00000	UAC_BarringInfo_Common (7,0x0000000'B)	246 / 081	0	0	Yes	Yes
1.8	3	0x02 00 00 00	00000	UAC_BarringInfo_Common (3,0x0000000'B)	244 / 081	0	0	No	NA
1.9	7	0x02 00 00 00	00000	UAC_BarringInfo_Common (7,0x0100000'B)	246 / 081	0	0	Yes	No
1.10	7	0x02 00 00 00	00000	UAC_BarringInfo_PerPLMN (7,0x0100000'B)	246 / 081	0	0	Yes	No
1.11	7	0x02 00 00 00	00000	UAC_BarringInfo_Common (7,0x0100000'B)	246 / 082	0	0	Yes	No
1.12	7	0x02 00 00 00	00000	UAC_BarringInfo_Common (7,0x0000000'B)	244 / 081	0	0	Yes	No
1.13	7	0x02 00 00 00	00000	UAC_BarringInfo_Common (7,0x1000000'B)	244 / 081	0	1	Yes	Yes
1.14	7	0x01 00 00 00	00000	UAC_BarringInfo_Common (7,0x1000000'B)	244 / 081	0	1	Yes	Yes
1.15	7	0x02 00 00 00	00000	UAC_BarringInfo_Common2 (3,0x1000000'B, 7,0x0100000'B)	246 / 081	0	0	Yes	No
1.16	3	0x02 00 00 00	00000	UAC_BarringInfo_Common2 (7,0x0100000'B, 3,0x0000000'B)	244 / 081	0	0	No	NA

#### 5.4.5.4.3 Procedure

Procedure/steps to be repeated for all sequences listed in table 5.4.5-1:

Step	Direction	Action	Information	REQ	SA
1	TT	SIB1 of Cell A is transmitted as defined in the initial conditions for tests from table 5.4.5-1	Barring info is set as in table 5.4.5-1 See Annex A for the Methods UAC_BarringInfo_xxxxxx() in the table		
2	UE	Power UE on	The UE performs a SIM initialisation. (includes reading of EF <sub>UAC-AIC</sub> and EF <sub>ACC</sub> )	CR 1	A.2/1 OR A.2/2
<b>If cell access is not allowed:</b>					
3	UE > TT	REGISTRATION REQUEST is not sent	See column 'Registration successful?' for the result	CR 2 CR 3 CR 4	
4	User	End test sequence			
<b>If cell access is allowed:</b>					
3	UE > TT	Send REGISTRATION REQUEST	See column 'Registration successful?' for the result	CR 2 CR 3 CR 4	
4	TT > UE	Send REGISTRATION ACCEPT	For simplicity other signalling is not shown		
<b>If MO Data call is not allowed:</b>					
5	UE	Attempt to set up MO Data call	To set up the MO Data call the MMI or EMMI is used	CR 2 CR 3 CR 4	
6	User	End test sequence			
<b>If MO Data call is allowed:</b>					
5	UE > TT	Set up MO Data call ( <i>PDU SessionEstablishment</i> )	To set up the MO Data call the MMI or EMMI is used	CR 2 CR 3 CR 4	
6	User	End test sequence			

### 5.4.5.5 Acceptance criteria

For the scenarios in table 5.4.5-1:

CR 1 is explicitly verified at step 2) by analysing the file READ commands for EF<sub>UAC-AIC</sub> and EF<sub>ACC</sub> during the USIM-ME initialisation procedure.

CR 2, CR 3, and CR 4 are verified

- step 3) by analysing if the UE shall make a successful or unsuccessful registration to the network in accordance with the result indicated in the table and
- step 5) by analysing if the UE shall make a successful or unsuccessful MO Data call in accordance with the result indicated in the table if the step is applicable.

## 5.4.5A Unified Access Control – Access Identity 2 – MCS indicated by USIM

### 5.4.5A.1 Definition and applicability

The purpose of Unified Access Control procedure is to perform access barring check for a 5GS access attempt associated with a given Access Category and one or more Access Identities upon request from upper layers or the RRC layer.

The 5G network shall be able to broadcast barring control information (i.e. a list of barring parameters associated with an Access Identity and an Access Category) in SIB1.

The EF<sub>UAC-AIC</sub> in the USIM contains the configuration information pertaining to access identity 2 allocated for high priority services MCS.

The UE shall be able to determine whether or not a particular new access attempt is allowed based on barring parameters that the UE receives from the broadcast barring control information and the configuration in the USIM.

When the NAS detects an access event, the NAS shall perform the mapping of the kind of request to one or more access identities and one access category and lower layers will perform access barring checks for that request based on the determined access identities and access category.

If RRC state is RRC\_INACTIVE and the resumption of the RRC connection is triggered due to an RNA Update RRC layer shall select Access Category as 8 and perform unified access control procedure in case there is no ongoing emergency service.

### 5.4.5A.2 Conformance requirement

CR 1 The ME shall read the access control value as part of the USIM-Terminal initialization procedure, and subsequently adopt this value.

Reference:

- TS 31.102 [19], clause 5.1.1.2.

CR 2 Access Identities are configured at the UE as listed in TS 22.261 [36] Table 6.22.2.2-1. Access Categories are defined by the combination of conditions related to UE and the type of access attempt as listed in TS 22.261 [36] Table 6.22.2.3-1. One or more Access Identities and only one Access Category are selected and tested for an access attempt.

Reference:

- TS 22.261 [36], clause 6.22.2

CR 3 Access Identity 2 is valid if the RPLMN is the HPLMN, EHPLMN or visited PLMN of the home country.

Reference:

- TS 24.501 [25], clause 4.5.2

CR 4 The UE shall be able to determine whether or not a particular new access attempt is allowed based on uac-BarringInfo broadcast in SIB1. Access Control check shall be performed as per the information received in uac-BarringInfoSetList.

Reference:

- TS 38.331 [37], clauses 5.3.14

CR 5 If the resumption of the RRC connection is triggered due to an RNA update and there is no ongoing emergency service RRC shall select '8' as the Access Category and perform the unified access control procedure.

Reference:

- TS 38.331 [37], clauses 5.3.13.2

### 5.4.5A.3 Test purpose

The purpose of this test is to verify that:

- 1) the ME reads the access control value from  $EF_{UAC-AIC}$  and  $EF_{ACC}$  as part of the USIM-Terminal initialisation procedure, and subsequently adopts this value;
- 2) the UE maps the kind of request to one or more access identities and one access category and lower layers performs access barring checks for that request based on the determined access identities and access category;
- 3) the UE determines whether or not a particular access attempt is allowed based on uac-BarringInfo broadcast in SIB1 and if the RPLMN is the HPLMN, EHPLMN or visited PLMN of the home country;
- 4) the UE performs unified access control procedure if RNA Update procedure is triggered.

5.4.5A.4 Method of test

5.4.5A.4.1 Initial conditions

The values of the 5G-NR UICC as defined in clause 4.5.9 of the present document are used with EF<sub>IMSI</sub> as defined in clause 4.6.5 and the following exceptions:

**EF<sub>UAC\_AIC</sub>** and **EF<sub>ACC</sub>**

No Access Identities configured in EF<sub>UAC\_AIC</sub> and no Access Classes configured in EF<sub>ACC</sub> as also shown in table 5.4.5A-1.

**EF<sub>UST</sub>** (USIM Service Table)

Logically:

Service n°124	Subscription identifier privacy support	not available
Service n°126	UAC Access Identities support	available

Coding:

Byte:	B1	B2	B3	B4	B5	B6	B7	B8
Binary:	xxxx xx1x	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxxx xxxx	xxxx xxxx	xxxx xxxx
	B9	B10	B11	...	B16			
	xxxx xxxx	xxxx xxxx	xx11 xxxx	...	xx10 011x			

The defined UICC/USIM data is installed on the UE.

The TT (NG-SS) is configured to transmit on the BCCH with the following parameters:

Cell A:

- TAI (MCC/MNC/TAC): MCC, MNC: see table 5.4.5A-1, TAC: 000001.
- CellIdentity: 000000001

For Table 5.4.5A-1:

No uac-BarringInfo in SIB1.

Cell B:

Transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): MCC, MNC: see table 5.4.5A-1, TAC: 000001.
- CellIdentity: 000000002

For Table 5.4.5A-1:

uac-BarringInfo in SIB1 should be set as in the table:

- Refer to Annex A for the Methods UAC\_BarringInfo\_xxxxxx() in the table.

5.4.5A.4.2 Test sequence settings

**Table 5.4.5A-1**

TC Seq#	Access Categor	USIM	SIB1	REGISTRATION ACCEPT (5GS network feature support IE)	Result
---------	----------------	------	------	--	--------

		EF <sub>UAC_AIC</sub>	EF <sub>ACC</sub> (Byte 1, b8-b4)	uac-BarringInfo	PLMN- Identity (MCC/MNC)	MPS indicator Bit	MCS indicator Bit	RRCResume Request - rna-Update successful?
2.1	8	0x02 00 00 00	00000	Not Present	246 / 081	0	0	Yes
2.2	8	0x02 00 00 00	00000	UAC_BarringInfo_Common (8,0x0100000'B)	246 / 081	0	0	No
2.3	8	0x02 00 00 00	00000	UAC_BarringInfo_PerPLMN (8,0x0000000'B)	246 / 081	0	0	Yes
2.4	8	0x02 00 00 00	00000	UAC_BarringInfo_Common (8,0x0100000'B)	244 / 081	0	1	No
2.5	8	0x02 00 00 00	00000	UAC_BarringInfo_Common2 (7,0x0100000'B, 8,0x0000000'B)	244 / 081	0	0	No

#### 5.4.5A.4.2 Procedure

Procedure/steps to be repeated for all sequences listed in table 5.4.5A-1:

Step	Direction	Action	Information	REQ	SA
1	TT	SIB1 of Cell A is transmitted as defined in the initial conditions and in table 5.4.5A-1	No barring info is provided to Cell A		
2	UE	Power UE on	The UE performs a SIM initialisation	CR 1	A.2/1 OR A.2/2
3	UE > TT	Send REGISTRATION REQUEST			
4	TT > UE	Send REGISTRATION ACCEPT	The registration is successful		
5	UE > TT	Set up MO Data call ( <i>PDU SessionEstablishment</i> )	To set up the MO Data call the MMI or EMMI is used. The MO Data call is set up successfully		
6	TT > UE	Send RRC RELEASE with <i>suspendConfig</i> in <i>criticalExtensions</i> (with the choice <i>rrcRelease</i> )	ran-NotificationAreaInfo in <i>suspendConfig</i> contains the cellList with cellIdentity of Cell A: <pre> cellList {   plmn-Identity {mcc, mnc},   -- see table 5.4.5A-1 for   MCC/MNC   ran-AreaCells 000000001'B } </pre>		
7	TT	Deactivate Cell A and activate Cell B			
8	TT	SIB1 of Cell B is transmitted as defined in table 5.4.5A-1	Barring info is as in the table. See Annex A for the Methods <i>UAC_BarringInfo_xxxxxx()</i> in the table		
9	UE > TT	Initiate RRC RESUME REQUEST procedure with <i>resumeCause</i> set to <i>rna-Update</i> .	See the column 'RRC RESUME REQUEST with <i>resumeCause</i> set to <i>rna-Update</i> successful?' for the result	CR 2 CR 3 CR 4 CR 5	

#### 5.4.5A.5 Acceptance criteria

For the scenarios in table 5.4.5A-1:

CR 1 is explicitly verified at step 2) by analysing the file READ commands for EF<sub>UAC\_AIC</sub> and EF<sub>ACC</sub> during the USIM-Terminal initialisation procedure.

CR 2, CR 3, CR 4, and CR 5 are verified at step 9) by analysing if the UE shall make a successful or unsuccessful RRC Resumption for RNA Update in accordance with the result indicated in the table.

## 5.4.6 Unified Access Control – Access Identity 2 – no MCS indication by USIM and SUPI is not changed

### 5.4.6.1 Definition and applicability

The purpose of Unified Access Control procedure is to perform access barring check for a 5GS access attempt associated with a given Access Category and one or more Access Identities upon request from upper layers or the RRC layer.

The 5G network shall be able to broadcast barring control information (i.e. a list of barring parameters associated with an Access Identity and an Access Category) in SIB1.

When the UE is in the country of its HPLMN or in an EHPLMN (if the EHPLMN list is present), and the USIM file  $EF_{UAC\_AIC}$  does not indicate the UE is configured for access identity 2, the UE uses the MCS indicator bit of the 5GS network feature support IE in the REGISTRATION ACCEPT message to determine if access identity 2 is valid.

The UE shall not consider access identity 2 to be valid when the UE is not in the country of its HPLMN prior to receiving the MCS indicator bit of the 5GS network feature support IE in the REGISTRATION ACCEPT message being set to "Access identity 2 valid in RPLMN or equivalent PLMN".

The UE shall be able to determine whether or not a particular new access attempt is allowed based on barring parameters that the UE receives from the broadcast barring control information and the configuration in the USIM.

When the NAS detects an access event, the NAS shall perform the mapping of the kind of request to one or more access identities and one access category and lower layers will perform access barring checks for that request based on the determined access identities and access category.

### 5.4.6.2 Conformance requirement

CR 1 The USIM file  $EF_{UAC\_AIC}$  does not indicate the UE is configured for access identity 2, the UE uses the MCS indicator bit of the 5GS network feature support IE in the REGISTRATION ACCEPT message to determine if access identity 2 is valid.

Reference:

- TS 24.501 [25], clause 4.5.2.

CR 2 The UE shall not consider access identity 2 to be valid when the UE is not in the country of its HPLMN prior to receiving the MCS indicator bit of the 5GS network feature support IE in the REGISTRATION ACCEPT message being set to "Access identity 2 valid in RPLMN or equivalent PLMN".

Reference:

- TS 24.501 [25], clause 4.5.2.

CR 3 The MCS indicator is stored together with a PLMN identity of the PLMN that provided it, and is valid in that RPLMN or equivalent PLMN. The MCS indicator can only be used if the SUPI from the USIM matches the SUPI stored in the non-volatile memory of the ME, else the UE shall delete the MCS indicator.

Reference:

- TS 24.501 [25], Annex C.

CR 4 Access Identity 2 is valid if the RPLMN is the HPLMN, EHPLMN or visited PLMN of the home country.

Reference:

- TS 24.501 [25], clause 4.5.2

CR 5 Upon receiving a REGISTRATION ACCEPT message with the MCS indicator bit set to "Access identity 2 valid", the UE shall act as a UE with access identity 2 configured for MCS in all NG-RAN of the registered PLMN and its equivalent PLMNs. The MCS indicator bit in the 5GS network feature support IE provided in the REGISTRATION ACCEPT message is valid until the UE receives a REGISTRATION ACCEPT message with

the MCS indicator bit set to "Access identity 2 not valid" or until the UE selects a non-equivalent PLMN. Access identity 2 is only applicable while the UE is in N1 mode.

Reference:

- TS 24.501 [25], clause 5.5.1.3.4

CR 6 The UE shall be able to determine whether or not a particular new access attempt is allowed based on uac-BarringInfo broadcast in SIB1. Access Control check shall be performed as per the information received in uac-BarringInfoSetList.

Reference:

- TS 38.331 [37], clauses 5.3.14

### 5.4.6.3 Test purpose

The purpose of this test is to verify that:

- 1) if the RPLMN is the HPLMN, EHPLMN or visited PLMN of the home country and the USIM file EF<sub>UAC\_AIC</sub> does not indicate the UE is configured for access identity 2 and the MCS indicator bit of the 5GS network feature support IE in the REGISTRATION ACCEPT message is received, UE considers access identity as 2 for access barring;
- 2) the MCS indicator is stored together with a PLMN identity of the PLMN that provided it, and the MCS indicator can only be used if the SUPI from the USIM matches the SUPI stored in the non-volatile memory of the ME;
- 3) the UE maps the kind of request to one or more access identities and one access category and lower layers performs access barring checks for that request based on the determined access identities and access category;
- 4) the UE determines whether or not a particular access attempt is allowed based on uac-BarringInfo broadcast in SIB1 and if the RPLMN is the HPLMN, EHPLMN or visited PLMN of the home country;
- 5) a UE operated with a USIM where the file EF<sub>UAC\_AIC</sub> does not indicate access identity 2, after a change of the REGISTRATION ACCEPT message with the MCS indicator bit set to "Access identity 2 not valid", or when the UE has selected a non-equivalent PLMN, the UE is acting as if it is configured for access identity 0.

### 5.4.6.4 Method of test

#### 5.4.6.4.1 Initial conditions

The values of the 5G-NR UICC as defined in clause 4.5.9 of the present document are used with EF<sub>IMSI</sub> as defined in clause 4.6.5 and the following exceptions:

#### EF<sub>UAC\_AIC</sub> and EF<sub>ACC</sub>

No Access Identities configured in EF<sub>UAC\_AIC</sub> and no Access Classes configured in EF<sub>ACC</sub> as also shown in table 5.4.6-1.

#### EF<sub>UST</sub> (USIM Service Table)

Logically:

Service n°124	Subscription identifier privacy support	not available
Service n°126	UAC Access Identities support	available

Coding:

Byte:	B1	B2	B3	B4	B5	B6	B7	B8
Binary:	xxxx xx1x	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxxx xxxx	xxxx xxxx	xxxx xxxx
	B9	B10	B11	...	B16			
	xxxx xxxx	xxxx xxxx	xx11 xxxx	...	xx10 011x			

The defined UICC/USIM data is installed on the UE.

The TT (NG-SS) is configured to transmit on the BCCH with the following parameters:

Cell A:

- MCC, MNC: 246/081
- TAC: = 000001
- CellIdentity: 000000001

For Table 5.4.6-1:

After turning on the cell for the 2<sup>nd</sup> time, uac-BarringInfo in SIB1 should be set as in the table:

Refer to Annex A for the Methods UAC\_BarringInfo\_xxxxxx() in the table.

Cell B:

- TAI (MCC/MNC/TAC): MCC, MNC: see table 5.4.6-1, TAC: 000002.
- CellIdentity: 000000002

For Table 5.4.6-1:

uac-BarringInfo in SIB1 should be set as in the table:

Refer to Annex A for the Methods UAC\_BarringInfo\_xxxxxx() in the table.

#### 5.4.6.4.2 Test sequence settings

**Table 5.4.6-1**

TC Seq#	Access Category	USIM		REGISTRATION ACCEPT (5GS network feature support IE) on Cell A at 1 <sup>st</sup> power up of the ME		SIB1 of Cell A or B after the 2 <sup>nd</sup> power up of the ME			Result	
		EF <sub>UAC_AIC</sub>	EF <sub>ACC</sub> (Byte 1 b8-b4)	MPS indicator Bit	MCS indicator Bit	Cell A or B	uac-BarringInfo	PLMN-Identity (MCC/MNC)	Registration successful?	MO Data call successful?
1.1	3	0x00 00 00 00	00000	0	1	Cell A	Not Present	246 / 081	Yes	Yes
1.2	3	0x00 00 00 00	00000	0	1	Cell A	UAC_BarringInfo_Common (3,0x01000000'B)	246 / 081	No	NA
1.3	7	0x00 00 00 00	00000	0	1	Cell A	UAC_BarringInfo_Common (7,0x10000000'B)	246 / 081	Yes	No
1.4	3	0x00 00 00 00	00000	0	1	Cell A	UAC_BarringInfo_Common (3,0x10000000'B)	246 / 081	Yes	Yes
1.5	3	0x00 00 00 00	00000	0	1	Cell B	UAC_BarringInfo_Common (3,0x10000000'B)	246 / 082	No	NA
1.6	3	0x00 00 00 00	00000	0	1	Cell B	UAC_BarringInfo_PerPLMN (3,0x10000000'B)	244 / 081	No	NA
1.7	7	0x00 00 00 00	00000	0	1	Cell B	UAC_BarringInfo_Common (7,0x00000000'B)	244 / 081	Yes	No

#### 5.4.6.4.3 Procedure

Procedure/steps to be repeated for all sequences listed in table 5.4.6-1:

Step	Direction	Action	Information	REQ	SA
1	TT	SIB1 of Cell A is transmitted without uac-BarringInfo in SIB1.			

2	UE	Power UE on	The UE performs a SIM initialisation. (includes reading of EF <sub>UAC-AIC</sub> and EF <sub>ACC</sub> )	CR 1	A.2/1 OR A.2/2
3	UE > TT	REGISTRATION REQUEST is sent			
4	TT > UE	Send REGISTRATION ACCEPT	The MCS indicator bit set to "Access identity 2 valid". For simplicity other signalling is not shown		
5	UE	Power UE off			
6	TT	Deactivate Cell A			
7	TT	Activate Cell A or B with SIB1 as specified in the table 5.4.6-1	See the column 'SIB1 of Cell A or B after the 2nd power up of the ME' for the SIB 1 and the column 'Cell A or B' to find the cell to be activated for this test step.		
8	UE	Power UE on	The UE performs a SIM initialisation again.		
<b>If cell access is not allowed:</b>					
9	UE > TT	REGISTRATION REQUEST in not sent	See column 'Registration successful?' for the result	CR 2 through CR 6	
10	USER	End test sequence			
<b>If cell access is allowed:</b>					
9	UE > TT	Send REGISTRATION REQUEST	See column 'Registration successful?' for the result	CR 2 through CR 6	
10	TT > UE	Send REGISTRATION ACCEPT	MPS and MCS indicator bits are set to zero in 5GS network feature support IE. For simplicity other signalling is not shown		
<b>If MO Data call is not allowed:</b>					
11	UE	Attempt to set up MO Data call	To set up the MO Data call the MMI or EMMI is used	CR 2 through CR 6	
12	USER	End test sequence			
<b>If MO Data call is allowed:</b>					
11	UE > TT	Set up MO Data call (PDU SessionEstablishment)	To set up the MO Data call the MMI or EMMI is used	CR 2 through CR 6	
12	USER	End test sequence			

#### 5.4.6.4.3 Acceptance criteria

For the scenarios in table 5.4.6-1:

CR 1 is explicitly verified at step 2) by analysing the file READ commands for EF<sub>UAC-AIC</sub> and EF<sub>ACC</sub> during the USIM-Terminal initialisation procedure.

CR 2, CR 3, CR 4, CR 5, and CR 6 are verified at:

- steps 9) and 10) by analysing if the UE shall make a successful or unsuccessful Registration to the network in accordance with the result indicated in the table and
- steps 11) and 12) by analysing if the UE shall make a successful or unsuccessful MO Data call in accordance with the result indicated in the table if the step is applicable.

## 5.4.7 Unified Access Control – Access Identity 2 – no MCS indication by USIM and SUPI is changed

### 5.4.7.1 Definition and applicability

The purpose of Unified Access Control procedure is to perform access barring check for a 5GS access attempt associated with a given Access Category and one or more Access Identities upon request from upper layers or the RRC layer.

The 5G network shall be able to broadcast barring control information (i.e. a list of barring parameters associated with an Access Identity and an Access Category) in SIB1.

When the USIM file EF<sub>UAC\_AIC</sub> does not indicate the UE is configured for access identity 2, the UE uses the MCS indicator bit of the 5GS network feature support IE in the REGISTRATION ACCEPT message to determine if access identity 2 is valid.

The MCS indicator is stored together with a PLMN identity of the PLMN that provided it, and is valid in that RPLMN or equivalent PLMN. The MCS indicator can only be used if the SUPI from the USIM matches the SUPI stored in the non-volatile memory of the ME, else the UE shall delete the MCS indicator.

The UE shall be able to determine whether or not a particular new access attempt is allowed based on barring parameters that the UE receives from the broadcast barring control information and the configuration in the USIM.

When the NAS detects an access event, the NAS shall perform the mapping of the kind of request to one or more access identities and one access category and lower layers will perform access barring checks for that request based on the determined access identities and access category.

### 5.4.7.2 Conformance requirement

CR 1 When the UE is in the country of its HPLMN, and the USIM file EF<sub>UAC\_AIC</sub> does not indicate the UE is configured for access identity 2, the UE uses the MCS indicator bit of the 5GS network feature support IE in the REGISTRATION ACCEPT message to determine if access identity 2 is valid.

Reference:

- TS 24.501 [25], clause 4.5.2.

CR 2 The UE shall not consider access identity 2 to be valid when the UE is not in the country of its HPLMN prior to receiving the MCS indicator bit of the 5GS network feature support IE in the REGISTRATION ACCEPT message being set to "Access identity 2 valid in RPLMN or equivalent PLMN".

Reference:

- TS 24.501 [25], clause 4.5.2.

CR 3 The UE shall consider access identity 2 to be valid when the network informs the UE that the use of access identity 2 is valid in the RPLMN or equivalent PLMN by setting the MCS indicator bit of the 5GS network feature support IE to "Access identity 2 valid", in the REGISTRATION ACCEPT message, the UE shall act as a UE with access identity 2 configured for MCS in all NG-RAN of the registered PLMN and its equivalent PLMNs, until the UE receives a REGISTRATION ACCEPT message with the MCS indicator bit set to "Access identity 2 not valid" or until the UE selects a non-equivalent PLMN. Access identity 2 is only applicable while the UE is in N1 mode.

Reference:

- TS 24.501 [25], clause 5.5.1.2.4.

CR 4 The MCS indicator is stored together with a PLMN identity of the PLMN that provided it, and is valid in that RPLMN or equivalent PLMN. The MCS indicator can only be used if the SUPI from the USIM matches the SUPI stored in the non-volatile memory of the ME, else the UE shall delete the MCS indicator.

Reference:

- TS 24.501 [25], Annex C.

CR 5 The UE shall be able to determine whether or not a particular new access attempt is allowed based on uac-BarringInfo broadcast in SIB1. Access Control check shall be performed as per the information received in uac-BarringInfoSetList.

Reference:

- TS 38.331 [37], clauses 5.3.14

### 5.4.7.3 Test purpose

The purpose of this test is to verify that:

- 1) if the RPLMN is the HPLMN, EHPLMN or visited PLMN of the home country and the USIM file EF<sub>UAC\_AIC</sub> does not indicate the UE is configured for access identity 2 and the MCS indicator bit of the 5GS network feature support IE in the REGISTRATION ACCEPT message is received, UE considers access identity as 2 for access barring.
- 2) the MCS indicator bit in the 5GS network feature support IE provided in the REGISTRATION ACCEPT message is valid until the UE receives a REGISTRATION ACCEPT message with the MCS indicator bit set to "Access identity 2 not valid" or until the UE selects a non-equivalent PLMN.
- 3) the MCS indicator is stored together with a PLMN identity of the PLMN that provided it, and the MCS indicator can only be used if the SUPI from the USIM matches the SUPI stored in the non-volatile memory of the ME.
- 4) the UE maps the kind of request to one or more access identities and one access category and lower layers performs access barring checks for that request based on the determined access identities and access category.
- 5) a UE operated with a USIM where the file EF<sub>UAC\_AIC</sub> does not indicate access identity 2, after a change of the REGISTRATION ACCEPT message with the MCS indicator bit set to "Access identity 2 not valid", or when the UE has selected a non-equivalent PLMN, the UE is acting as if it is configured for access identity 0.

### 5.4.7.4 Method of test

#### 5.4.7.4.1 Initial conditions

The values of the 5G-NR UICC as defined in clause 4.5.9 of the present document are used with EF<sub>IMSI</sub> as defined in clause 4.6.5 and the following exceptions:

#### EF<sub>UAC\_AIC</sub> and EF<sub>ACC</sub>

No Access Identities configured in EF<sub>UAC\_AIC</sub> and no Access Classes configured in EF<sub>ACC</sub> as also shown in table 5.4.7-1.

#### EF<sub>UST</sub> (USIM Service Table)

Logically:

Service n°124	Subscription identifier privacy support	not available
Service n°126	UAC Access Identities support	available

Coding:

Byte:	B1	B2	B3	B4	B5	B6	B7	B8
Binary:	xxxx xx1x	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxxx xxxx	xxxx xxxx	xxxx xxxx
	B9	B10	B11	...	B16			
	xxxx xxxx	xxxx xxxx	xx11 xxxx	...	xx10 011x			

The defined UICC/USIM data is installed on the UE.

The TT (NG-SS) is configured to transmit on the BCCH with the following parameters:

Cell A:

- TAI (MCC/MNC/TAC): 246/081/000001

- CellIdentity: 000000001

For Table 5.4.7-1:

After turning on the cell for the 2<sup>nd</sup> time, uac-BarringInfo in SIB1 should be set as in the table:

- Refer to Annex A for the Methods UAC\_BarringInfo\_xxxxxx() in the table.

Cell B:

- TAI (MCC/MNC/TAC): MCC, MNC: see table 5.4.7-1, TAC: 000002.
- CellIdentity: 000000002

For Table 5.4.7-1:

uac-BarringInfo in SIB1 should be set as in the table:

### 5.4.7.4.2 Test sequence settings

Table 5.4.7-1

TC Seq#	Access Category	USIM		REGISTRATION ACCEPT (5GS network feature support IE) on Cell A at 1 <sup>st</sup> power up of the ME		SIB1 of Cell A or B after the 2 <sup>nd</sup> power up of the ME			Result	
		EF <sub>UAC_AIC</sub>	EF <sub>ACC</sub> (Byte 1 b8-b4)	MPS indicator Bit	MCS indicator Bit	Cell A or B	uac-BarringInfo	PLMN-Identity (MCC/MNC)	Registration successful?	MO Data call successful?
1.1	3	0x00 00 00 00	00000	0	1	Cell A	Not Present	246 / 081	Yes	Yes
1.2	3	0x00 00 00 00	00000	0	1	Cell A	UAC_BarringInfo_Common (3,0x1000000'B)	246 / 081	No	NA
1.3	7	0x00 00 00 00	00000	0	1	Cell A	UAC_BarringInfo_Common (7,0x1000000'B)	246 / 081	Yes	No
1.4	3	0x00 00 00 00	00000	0	1	Cell A	UAC_BarringInfo_Common (3,0x0000000'B)	246 / 081	No	NA
1.5	3	0x00 00 00 00	00000	0	1	Cell B	UAC_BarringInfo_Common (3,0x1000000'B)	246 / 082	No	NA
1.6	3	0x00 00 00 00	00000	0	1	Cell B	UAC_BarringInfo_PerPLMN (3,0x1000000'B)	244 / 081	No	NA
1.7	7	0x00 00 00 00	00000	0	1	Cell B	UAC_BarringInfo_Common (7,0x0000000'B)	244 / 081	Yes	No

### 5.4.7.4.3 Procedure

Procedure/steps to be repeated for all sequences listed in table 5.4.7-1:

Step	Direction	Action	Information	REQ	SA
1	TT	SIB1 of Cell A is transmitted without uac-BarringInfo in SIB1.			
2	UE	Power UE on	The UE performs a SIM initialisation. (includes reading of EFUAC-AIC and EFACC)	CR 1	A.2/1 OR A.2/2
3	UE > TT	REGISTRATION REQUEST is sent			
4	TT > UE	Send REGISTRATION ACCEPT	The MCS indicator bit set to "Access identity 2 valid". For simplicity other signalling is not shown		

5	UE	Power UE on			
6	TT	Deactivates Cell A			
7	TT	Activates Cell A or B with SIB1 as specified in the table 5.4.7-1	See the column 'SIB1 of Cell A or B after the 2nd power up of the ME' for the SIB 1 and the column 'Cell A or B' to find the cell to be activated for this test step.		
8	UE	Power UE on	Power on with a different USIM (e.g.: IMSI set to 24681685533963)  The UE performs a SIM initialisation again.		
<b>If cell access is not allowed:</b>					
9	UE > TT	REGISTRATION REQUEST in not sent	See column 'Registration successful?' for the result	CR 2 through CR 5	
10	USER	End test sequence			
<b>If cell access is allowed:</b>					
9	UE > TT	Send REGISTRATION REQUEST	See column 'Registration successful?' for the result	CR 2 through CR 5	
10	TT > UE	Send REGISTRATION ACCEPT	MPS and MCS indicator bits are set to zero in 5GS network feature support IE. For simplicity other signalling is not shown		
<b>If MO Data call is not allowed:</b>					
11	UE	Attempt to set up MO Data call	To set up the MO Data call the MMI or EMMI is used	CR 2 through CR 5	
12	USER	End test sequence			
<b>If MO Data call is allowed:</b>					
11	UE > TT	Set up MO Data call ( <i>PDU Session Establishment</i> )	To set up the MO Data call the MMI or EMMI is used	CR 2 through CR 5	
12	USER	End test sequence			

### 5.4.7.5 Acceptance criteria

For the scenarios in table 5.4.7-1:

CR 1 is explicitly verified at step 2) by analysing the file READ commands for  $EF_{UAC-AIC}$  and  $EF_{ACC}$  during the USIM-Terminal initialisation procedure.

CR 2, CR 3, CR 4, and CR 5 are verified at:

- steps 9) and 10) by analysing if the UE shall make a successful or unsuccessful Registration to the network in accordance with the result indicated in the table and
- steps 11) and 12) by analysing if the UE shall make a successful or unsuccessful MO Data call in accordance with the result indicated in the table if the step is applicable.

## 5.4.8 Unified Access Control – Access Identities 11 and 15 indicated by USIM

### 5.4.8.1 Definition and applicability

The purpose of Unified Access Control procedure is to perform access barring check for a 5GS access attempt associated with a given Access Category and one or more Access Identities upon request from upper layers or the RRC layer.

The 5G network shall be able to broadcast barring control information (i.e. a list of barring parameters associated with an Access Identity and an Access Category) in SIB1.

The EF<sub>ACC</sub> in the USIM contains the configuration information pertaining to access identities 11 and 15.

The UE shall be able to determine whether or not a particular new access attempt is allowed based on barring parameters that the UE receives from the broadcast barring control information and the configuration in the USIM.

When the NAS detects an access event, the NAS shall perform the mapping of the kind of request to one or more access identities and one access category and lower layers will perform access barring checks for that request based on the determined access identities and access category.

### 5.4.8.2 Conformance requirement

CR 1 The ME shall read the access control value as part of the USIM-Terminal initialization procedure, and subsequently adopt this value.

Reference:

- TS 31.102 [19], clause 5.1.1.2.

CR 2 Access Identities are configured at the UE as listed in TS 22.261 [43] Table 6.22.2.2-1. Access Categories are defined by the combination of conditions related to UE and the type of access attempt as listed in TS 22.261 [43] Table 6.22.2.3-1. One or more Access Identities and only one Access Category are selected and tested for an access attempt.

Reference:

- TS 22.261 [36], clause 6.22.2.

CR 3 Access Identity 11 and 15 are valid in HPLMN (if the EHPLMN list is not present or is empty) or EHPLMN (if the EHPLMN list is present).

Reference:

- TS 24.501 [25], clause 4.5.2.

CR 4 The UE shall be able to determine whether or not a particular new access attempt is allowed based on uac-BarringInfo broadcast in SIB1. Access Control check shall be performed as per the information received in uac-BarringInfoSetList.

Reference:

- TS 38.331 [37], clauses 5.3.14.

### 5.4.8.3 Test purpose

The purpose of this test is to verify that:

- 1) the ME reads the access control value from EF<sub>UAC-AIC</sub> and EF<sub>ACC</sub> as part of the USIM-Terminal initialisation procedure, and subsequently adopts this value.
- 2) the UE maps the kind of request to one or more access identities and one access category and lower layers performs access barring checks for that request based on the determined access identities and access category.
- 3) the UE determines whether or not a particular access attempt is allowed based on uac-BarringInfo broadcast in SIB1 and if the RPLMN is the HPLMN, EHPLMN or visited PLMN of the home country.

### 5.4.8.4 Method of test

#### 5.4.8.4.1 Initial conditions

The values of the 5G-NR UICC as defined in clause 4.5.9 of the present document are used with EF<sub>IMSI</sub> as defined in clause 4.6.5 and the following exceptions:

**EF<sub>UAC\_AIC</sub>** and **EF<sub>ACC</sub>**

No Access Identities configured in EF<sub>UAC\_AIC</sub> and no Access Classes configured in EF<sub>ACC</sub> as also shown in table 5.4.8-1.

**EF<sub>UST</sub>** (USIM Service Table)

Logically:

Service n°126 UAC Access Identities support available

Coding:

<b>Byte:</b>	<b>B1</b>	<b>B2</b>	<b>B3</b>	<b>B4</b>	<b>B5</b>	<b>B6</b>	<b>B7</b>	<b>B8</b>
Binary:	xxxx xx1x	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxxx xxxx	xxxx xxxx	xxxx xxxx
	<b>B9</b>	<b>B10</b>	<b>B11</b>	...	<b>B16</b>	<b>B17</b>		
	xxxx xxxx	xxxx xxxx	xx11 xxxx	...	xx10 11xx	0000 0xxx		

The defined UICC/USIM data is installed on the UE.

The TT (NG-SS) is configured to transmit on the BCCH with the following parameters:

Cell A:

- TAI (MCC/MNC/TAC):MCC, MNC: see tables 5.4.8-x, TAC: 000001.
- CellIdentity: 00000001

For Table 5.4.8-1:

uac-BarringInfo in SIB1 should be set as in the table:

- Refer to Annex A for the Methods UAC\_BarringInfo\_xxxxxx() in the table.

5.4.8.4.2 Test sequence settings

**Table 5.4.8-1**

TC Seq#	Access Category	USIM			SIB1		Result	
		EF <sub>UAC_AIC</sub>	EF <sub>ACC</sub> (Byte 1 b8-b4)	Access Identities	uac-BarringInfo	PLMN-Identity (MCC/MNC)	Registration successful?	MO Data call successful?
1.1	7	0x00 00 00 00	00001	11	Not Present	246 / 081	Yes	Yes
1.2	3	0x00 00 00 00	00001	11	UAC_BarringInfo_Common (3,0x0010000'B)	246 / 081	No	NA
1.3	3	0x00 00 00 00	00001	11	UAC_BarringInfo_PerPLMN (3,0x0010000'B)	246 / 081	No	NA
1.4	3	0x00 00 00 00	00001	11	UAC_BarringInfo_Common (3,0x0000000'B)	246 / 082	No	NA
1.5	3	0x00 00 00 00	00001	11	UAC_BarringInfo_Common (3,0x0001000'B)	246 / 081	Yes	Yes
1.6	3	0x00 00 00 00	10001	11, 15	UAC_BarringInfo_Common (3,0x0000001'B)	246 / 081	Yes	Yes
1.7	7	0x00 00 00 00	00001	11	UAC_BarringInfo_Common (7,0x0010000'B)	246 / 081	Yes	No
1.8	7	0x00 00 00 00	00001	11	UAC_BarringInfo_Common (7,0x0000000'B)	246 / 082	Yes	No
1.9	7	0x00 00 00 00	00001	11	UAC_BarringInfo_Common (7,0x0000000'B)	244 / 081	Yes	No
1.10	7	0x00 00 00 00	00001	11	UAC_BarringInfo_Common2 (3,0x0001000'B, 7,0x0010000'B)	246 / 081	Yes	No

1.11	3	0x00 00 00 00	10000	15	UAC_BarringInfo_Common (3,0x0000001'B)	246 / 081	No	NA
1.12	3	0x00 00 00 00	10000	15	UAC_BarringInfo_PerPLMN (3,0x0000001'B)	246 / 081	No	NA
1.13	3	0x00 00 00 00	10000	15	UAC_BarringInfo_Common (3,0x0000000'B)	246 / 082	No	NA
1.14	3	0x00 00 00 00	10000	15	UAC_BarringInfo_Common (3,0x0010000'B)	246 / 081	Yes	Yes
1.15	7	0x00 00 00 00	10000	15	UAC_BarringInfo_Common (7,0x0000001'B)	246 / 081	Yes	No
1.16	7	0x00 00 00 00	10000	15	UAC_BarringInfo_Common (7,0x0000000'B)	246 / 082	Yes	No
1.17	7	0x00 00 00 00	10000	15	UAC_BarringInfo_Common (7,0x0000000'B)	244 / 081	Yes	No
1.18	7	0x00 00 00 00	10000	15	UAC_BarringInfo_Common2 (3,0x0001000'B, 7,0x0000001'B)	246 / 081	Yes	No

#### 5.4.8.4.3 Procedure

Procedure/steps to be repeated for all sequences listed in table 5.4.8-1:

Step	Direction	Action	Comment	REQ	SA
1	TT	SIB1 of Cell A is transmitted as defined in the initial conditions for tests from table 5.4.8-1	Barring info is set as in table 5.4.8-1 See Annex A for the Methods UAC_BarringInfo_XXXXX() in the table		
2	UE	Power UE on	The UE performs a SIM initialisation. (includes reading of EF <sub>UAC-AIC</sub> and EF <sub>ACC</sub> )	CR 1	A.2/1 OR A.2/2

If cell access is not allowed:					
3	UE > TT	REGISTRATION REQUEST is not sent	See column 'Registration successful?' for the result	CR 2 CR 3 CR 4	
4	Tester	End test sequence			

If cell access is allowed:					
3	UE > TT	Send REGISTRATION REQUEST	See column 'Registration successful?' for the result	CR 2 CR 3 CR 4	
4	TT > UE	Send REGISTRATION ACCEPT	For simplicity other signalling is not shown		

If MO Data call is not allowed:					
5	UE	Attempt to set up MO Data call	To set up the MO Data call the MMI or EMMI is used	CR 2 CR 3 CR 4	
6	Tester	End test sequence			

If MO Data call is allowed:					
5	UE > TT	Set up MO Data call (PDU SessionEstablishment)	To set up the MO Data call the MMI or EMMI is used	CR 2 CR 3 CR 4	
6	Tester	End test sequence			

#### 5.4.8.5 Acceptance criteria

For the scenarios in table 5.4.8-1:

CR 1 is explicitly verified at step 2) by analysing the file READ commands for EF<sub>UAC-AIC</sub> and EF<sub>ACC</sub> during the USIM-ME initialisation procedure.

CR 2, CR 3, and CR 4 are verified

- at step 3) by analysing if the UE shall make a successful or unsuccessful registration to the network in accordance with the result indicated in the table and
- at step 5) by analysing if the UE shall make a successful or unsuccessful MO Data call in accordance with the result indicated in the table if the step is applicable.

## 5.4.8A Unified Access Control – Access Identities 11 and 15 indicated by USIM, Access Category 8

### 5.4.8A.1 Definition and applicability

The purpose of Unified Access Control procedure is to perform access barring check for a 5GS access attempt associated with a given Access Category and one or more Access Identities upon request from upper layers or the RRC layer.

The 5G network shall be able to broadcast barring control information (i.e. a list of barring parameters associated with an Access Identity and an Access Category) in SIB1.

The EF<sub>ACC</sub> in the USIM contains the configuration information pertaining to access identities 11 and 15.

The UE shall be able to determine whether or not a particular new access attempt is allowed based on barring parameters that the UE receives from the broadcast barring control information and the configuration in the USIM.

When the NAS detects an access event, the NAS shall perform the mapping of the kind of request to one or more access identities and one access category and lower layers will perform access barring checks for that request based on the determined access identities and access category.

If RRC state is RRC\_INACTIVE and the resumption of the RRC connection is triggered due to an RNA Update RRC layer shall select Access Category as 8 and perform unified access control procedure in case there is no ongoing emergency service.

### 5.4.8A.2 Conformance requirement

CR 1 The ME shall read the access control value as part of the USIM-Terminal initialization procedure, and subsequently adopt this value.

Reference:

- TS 31.102 [19], clause 5.1.1.2.

CR 2 Access Identities are configured at the UE as listed in TS 22.261 [36] Table 6.22.2.2-1. Access Categories are defined by the combination of conditions related to UE and the type of access attempt as listed in TS 22.261 [36] Table 6.22.2.3-1. One or more Access Identities and only one Access Category are selected and tested for an access attempt.

Reference:

- TS 22.261 [36], clause 6.22.2.

CR 3 Access Identity 11 and 15 are valid in HPLMN (if the EHPLMN list is not present or is empty) or EHPLMN (if the EHPLMN list is present).

Reference:

- TS 24.501 [25], clause 4.5.2.

CR 4 The UE shall be able to determine whether or not a particular new access attempt is allowed based on uac-BarringInfo broadcast in SIB1. Access Control check shall be performed as per the information received in uac-BarringInfoSetList.

Reference:

- TS 38.331 [37], clauses 5.3.14.

CR 5 If the resumption of the RRC connection is triggered due to an RNA update and there is no ongoing emergency service RRC shall select '8' as the Access Category and perform the unified access control procedure.

Reference:

- TS 38.331 [37], clauses 5.3.13.2.

### 5.4.8A.3 Test purpose

The purpose of this test is to verify that:

- 1) the ME reads the access control value from  $EF_{UAC\_AIC}$  and  $EF_{ACC}$  as part of the USIM-Terminal initialisation procedure, and subsequently adopts this value.
- 2) the UE maps the kind of request to one or more access identities and one access category and lower layers performs access barring checks for that request based on the determined access identities and access category.
- 3) the UE determines whether or not a particular access attempt is allowed based on uac-BarringInfo broadcast in SIB1 and if the RPLMN is the HPLMN, EHPLMN or visited PLMN of the home country.
- 4) the UE performs unified access control procedure if RNA Update procedure is triggered.

### 5.4.8A.4 Method of test

#### 5.4.8A.4.1 Initial conditions

The values of the 5G-NR UICC as defined in clause 4.5.9 of the present document are used with  $EF_{IMSI}$  as defined in clause 4.6.5 and the following exceptions:

$EF_{UAC\_AIC}$  and  $EF_{ACC}$

No Access Identities configured in  $EF_{UAC\_AIC}$  and no Access Classes configured in  $EF_{ACC}$  as also shown in table 5.4.8A-1.

$EF_{UST}$  (USIM Service Table)

Logically:

Service n°126      UAC Access Identities support      available

Coding:

Byte:	B1	B2	B3	B4	B5	B6	B7	B8
Binary:	xxxx xx1x	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxxx xxxx	xxxx xxxx	xxxx xxxx
	B9	B10	B11	...	B16	B17		
	xxxx xxxx	xxxx xxxx	xx11 xxxx	...	xx10 11xx	0000 0xxx		

The defined UICC/USIM data is installed on the UE.

The TT (NG-SS) is configured to transmit on the BCCH with the following parameters:

Cell A:

- TAI (MCC/MNC/TAC):MCC, MNC: see table 5.4.8A-1, TAC: 000001.
- CellIdentity: 000000001

For Table 5.4.8A-1:

No uac-BarringInfo in SIB1.

Cell B:

Transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC):MCC, MNC: see table 5.4.8A-1, TAC: 000001.
- CellIdentity: 00000002

For Table 5.4.8A-1:

uac-BarringInfo in SIB1 should be set as in the table:

- Refer to Annex A for the Methods UAC\_BarringInfo\_xxxxxx() in the table.

#### 5.4.8A.4.2 Test sequence settings

Table 5.4.8A-1

TC Seq#	Access Category	USIM			SIB1		Result
		EF <sub>UAC_AIC</sub>	EF <sub>ACC</sub> (Byte 1, b8-b4)	Access identity	uac-BarringInfo	PLMN-Identity (MCC/MNC)	
2.1	8	0x00 00 00 00	00001	11	Not Present	246 / 081	Yes
2.2	8	0x00 00 00 00	00001	11	UAC_BarringInfo_Common (8,0x0010000'B)	246 / 081	No
2.3	8	0x00 00 00 00	00001	11	UAC_BarringInfo_PerPLMN (8,0x0000000'B)	246 / 081	Yes
2.4	8	0x00 00 00 00	00001	11	UAC_BarringInfo_Common (8,0x0000000'B)	246 / 082	No
2.5	8	0x00 00 00 00	00001	11	UAC_BarringInfo_Common2 (7,0x0000001'B, 8,0x0000000'B)	244 / 081	No
2.6	8	0x00 00 00 00	10000	15	UAC_BarringInfo_Common (8,0x0000001'B)	246 / 081	No
2.7	8	0x00 00 00 00	10000	15	UAC_BarringInfo_PerPLMN (8,0x0000000'B)	246 / 081	Yes
2.8	8	0x00 00 00 00	10000	15	UAC_BarringInfo_Common (8,0x0000000'B)	246 / 082	No
2.9	8	0x00 00 00 00	10000	15	UAC_BarringInfo_Common2 (7,0x0000001'B, 8,0x0000000'B)	244 / 081	No

#### 5.4.8A.4.3 Procedure

Procedure/steps to be repeated for all sequences listed in table 5.4.8A-1:

Step	Direction	Action	Comment	REQ	SA
1	TT	SIB1 of Cell A is transmitted as defined in the initial conditions and in table 5.4.8A-1	No barring info is provided to Cell A		
2	UE	Power UE on	The UE performs a SIM initialisation	CR 1	A.2/1 OR A.2/2
3	UE > TT	Send RegistrationRequest			
4	TT > UE	Send RegistrationAccept	The registration is successful		
5	UE > TT	Set up MO Data call (PDU SessionEstablishment)	To set up the MO Data call the MMI or EMMI is used. The MO Data call is set up successfully		
6	TT > UE	Send RRC RELEASE with suspendConfig in criticalExtensions (with the choice rrcRelease)	ran-NotificationAreaInfo in suspendConfig contains the cellList with cellIdentity of Cell A: cellList { plmn-Identity {mcc, mnc}, -- see table 5.4.8A-1 for MCC/MNC ran-AreaCells 000000001'B		

			}		
7	TT	Deactivate Cell A and activate Cell B			
8	TT	SIB1 of Cell B is transmitted as defined in table 5.4.8A-1	Barring info is as in the table. See Annex A for the Methods UAC_BarringInfo_xxxxxx() in the table		
9	UE > TT	Initiate RRC RESUME REQUEST procedure with resumeCause set to rna-Update.	See the column 'RRCResumeRequest with resumeCause set to rna-Update successful?' for the result	CR 2 CR 3 CR 4 CR 5	

### 5.4.8A.5 Acceptance criteria

For the scenarios in table 5.4.8A-1:

CR 1 is explicitly verified at step 2) by analysing the file READ commands for  $EF_{UAC-AIC}$  and  $EF_{ACC}$  during the USIM-Terminal initialisation procedure.

CR 2, CR 3, CR 4, and CR 5 are verified

- at step 9) by analysing if the UE shall make a successful or unsuccessful RRC Resumption for RNA Update in accordance with the result indicated in the table.

## 5.4.9 Unified Access Control – Access Identities 12, 13 and 14 indicated by USIM

### 5.4.9.1 Definition and applicability

The purpose of Unified Access Control procedure is to perform access barring check for a 5GS access attempt associated with a given Access Category and one or more Access Identities upon request from upper layers or the RRC layer.

The 5G network shall be able to broadcast barring control information (i.e. a list of barring parameters associated with an Access Identity and an Access Category) in SIB1.

The  $EF_{ACC}$  in the USIM contains the configuration information pertaining to access identities 12, 13 and 14.

The UE shall be able to determine whether or not a particular new access attempt is allowed based on barring parameters that the UE receives from the broadcast barring control information and the configuration in the USIM.

When the NAS detects an access event, the NAS shall perform the mapping of the kind of request to one or more access identities and one access category and lower layers will perform access barring checks for that request based on the determined access identities and access category.

### 5.4.9.2 Conformance requirement

CR 1 The ME shall read the access control value as part of the USIM-Terminal initialization procedure, and subsequently adopt this value.

Reference:

- TS 31.102 [19], clause 5.1.1.2.

CR 2 Access Identities are configured at the UE as listed in TS 22.261 [43] Table 6.22.2.2-1. Access Categories are defined by the combination of conditions related to UE and the type of access attempt as listed in TS 22.261 [43] Table 6.22.2.3-1. One or more Access Identities and only one Access Category are selected and tested for an access attempt.

Reference:

- TS 22.261 [43], clause 6.22.2.

CR 3 Access Identities 12, 13 and 14 are valid in HPLMN and visited PLMNs of home country only.

Reference:

- TS 24.501 [42], clause 4.5.2.

CR 4 The UE shall be able to determine whether or not a particular new access attempt is allowed based on uac-BarringInfo broadcast in SIB1. Access Control check shall be performed as per the information received in uac-BarringInfoSetList.

Reference:

- TS 38.331 [44], clauses 5.3.14.

### 5.4.9.3 Test purpose

The purpose of this test is to verify that:

- 1) the ME reads the access control value from  $EF_{UAC\_AIC}$  and  $EF_{ACC}$  as part of the USIM-Terminal initialisation procedure, and subsequently adopts this value.
- 2) the UE maps the kind of request to one or more access identities and one access category and lower layers performs access barring checks for that request based on the determined access identities and access category.
- 3) the UE determines whether or not a particular access attempt is allowed based on uac-BarringInfo broadcast in SIB1 and if the RPLMN is the HPLMN, EHPLMN or visited PLMN of the home country.

### 5.4.9.4 Method of test

#### 5.4.9.4.1 Initial conditions

The values of the 5G-NR UICC as defined in clause 4.5.9 of the present document are used with  $EF_{IMSI}$  as defined in clause 4.6.5 and the following exceptions:

$EF_{UAC\_AIC}$  and  $EF_{ACC}$

No Access Identities configured in  $EF_{UAC\_AIC}$  and no Access Classes configured in  $EF_{ACC}$  as also shown in table 5.4.9-1.

$EF_{UST}$  (USIM Service Table)

Logically:

Service n°126      UAC Access Identities support      available

Coding:

Byte:	B1	B2	B3	B4	B5	B6	B7	B8
Binary:	xxxx xx1x	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxxx xxxx	xxxx xxxx	xxxx xxxx
	<b>B9</b>	<b>B10</b>	<b>B11</b>	...	<b>B16</b>	<b>B17</b>		
	xxxx xxxx	xxxx xxxx	xx11 xxxx	...	xx10 11xx	0000 0xxx		

The defined UICC/USIM data is installed on the UE.

The NG-SS is configured to transmit on the BCCH with the following parameters:

Cell A:

- TAI (MCC/MNC/TAC):MCC, MNC: see table 5.4.9-1, TAC: 000001.
- CellIdentity : 000000001

For Table 5.4.9-1:

uac-BarringInfo in SIB1 should be set as in the table:

- Refer to Annex A for the Methods UAC\_BarringInfo\_XXXXXX() in the table.

## 5.4.9.4.2 Tables related to the test case

Table 5.4.9-1

TC Seq#	Access Category	USIM			SIB1		Result	
		EF <sub>UAC_AIC</sub>	EF <sub>ACC</sub> (Byte 1 b8-b4)	Access Identity	uac-BarringInfo	PLMN-Identity (MCC/MNC)	Registration successful?	MO Data call successful?
1.1	7	0x00 00 00 00	00010	12	Not Present	246 / 081	Yes	Yes
1.2	3	0x00 00 00 00	00010	12	UAC_BarringInfo_Common (3,0x0001000'B)	246 / 081	No	NA
1.3	3	0x00 00 00 00	00010	12	UAC_BarringInfo_PerPLMN (3,0x0001000'B)	246 / 081	No	NA
1.4	3	0x00 00 00 00	00010	12	UAC_BarringInfo_Common (3,0x0000000'B)	246 / 082	Yes	Yes
1.5	3	0x00 00 00 00	00010	12	UAC_BarringInfo_Common (3,0x0001000'B)	246 / 082	No	NA
1.6	3	0x00 00 00 00	00010	12	UAC_BarringInfo_Common (3,0x0000000'B)	244 / 081	No	NA
1.7	3	0x00 00 00 00	00010	12	UAC_BarringInfo_Common (3,0x0000100'B)	246 / 081	Yes	Yes
1.8	3	0x00 00 00 00	01110	12,13,14	UAC_BarringInfo_Common (3,0x0000110'B)	246 / 081	Yes	Yes
1.9	7	0x00 00 00 00	00010	12	UAC_BarringInfo_Common (7,0x0001000'B)	246 / 081	Yes	No
1.10	7	0x00 00 00 00	00010	12	UAC_BarringInfo_Common (7,0x0000000'B)	246 / 082	Yes	Yes
1.11	7	0x00 00 00 00	00010	12	UAC_BarringInfo_Common (7,0x0000000'B)	244 / 081	Yes	No
1.12	7	0x00 00 00 00	00010	12	UAC_BarringInfo_Common2 (3,0x0000100'B, 7,0x0001000'B)	246 / 081	Yes	No
1.13	3	0x00 00 00 00	00100	13	UAC_BarringInfo_Common (3,0x0000100'B)	246 / 081	No	NA
1.14	3	0x00 00 00 00	00100	13	UAC_BarringInfo_PerPLMN (3,0x0000100'B)	246 / 081	No	NA
1.15	3	0x00 00 00 00	00100	13	UAC_BarringInfo_Common (3,0x0000000'B)	246 / 082	Yes	Yes
1.16	3	0x00 00 00 00	00100	13	UAC_BarringInfo_Common (3,0x0000100'B)	246 / 082	No	NA
1.17	3	0x00 00 00 00	00100	13	UAC_BarringInfo_Common (3,0x0000010'B)	246 / 082	Yes	Yes
1.18	7	0x00 00 00 00	00100	13	UAC_BarringInfo_Common (7,0x0000100'B)	246 / 081	Yes	No
1.19	7	0x00 00 00 00	00100	13	UAC_BarringInfo_Common (7,0x0000000'B)	244 / 081	Yes	No
1.20	7	0x00 00 00 00	00100	13	UAC_BarringInfo_Common2 (3,0x0000010'B, 7,0x0000100'B)	246 / 081	Yes	No
1.21	3	0x00 00 00 00	01000	14	UAC_BarringInfo_Common (3,0x0000010'B)	246 / 081	No	NA
1.22	3	0x00 00 00 00	01000	14	UAC_BarringInfo_PerPLMN (3,0x0000010'B)	246 / 081	No	NA
1.23	3	0x00 00 00 00	01000	14	UAC_BarringInfo_Common (3,0x0000000'B)	246 / 082	Yes	Yes
1.24	3	0x00 00 00 00	01000	14	UAC_BarringInfo_Common (3,0x0000010'B)	246 / 082	No	NA
1.25	3	0x00 00 00 00	01000	14	UAC_BarringInfo_Common (3,0x0001100'B)	246 / 082	Yes	Yes
1.26	7	0x00 00 00 00	01000	14	UAC_BarringInfo_Common (7,0x0000010'B)	246 / 081	Yes	No

1.27	7	0x00 00 00 00	01000	14	UAC_BarringInfo_Common (7,0x0000000'B)	244 / 081	Yes	No
1.28	7	0x00 00 00 00	01000	14	UAC_BarringInfo_Common2 (3,0x0000100'B, 7,0x0000010'B)	246 / 081	Yes	No

#### 5.4.9.4.3 Procedure

Procedure/steps to be repeated for all sequences listed in table 5.4.9-1:

Step	Direction	Action	Comment	REQ	SA
1	TT	SIB1 of Cell A is transmitted as defined in the initial conditions for tests from table 5.4.9-1	Barring info is set as in table 5.4.9-1 See Annex A for the Methods UAC_BarringInfo_XXXXXX() in the table		
2	UE	Power UE on	The UE performs a SIM initialisation. (includes reading of EF <sub>UAC-AIC</sub> and EF <sub>ACC</sub> )	CR 1	A.2/1 OR A.2/2

If cell access is not allowed:					
3	UE > TT	REGISTRATION REQUEST is not sent	See column 'Registration successful?' for the result	CR 2 CR 3 CR 4	
4	Tester	End test sequence			

If cell access is allowed:					
3	UE > TT	Send REGISTRATION REQUEST	See column 'Registration successful?' for the result	CR 2 CR 3 CR 4	
4	TT > UE	Send REGISTRATION ACCEPT	For simplicity other signalling is not shown		

If MO Data call is not allowed:					
5	UE	Attempt to set up MO Data call	To set up the MO Data call the MMI or EMMI is used	CR 2 CR 3 CR 4	
6	Tester	End test sequence			

If MO Data call is allowed:					
5	UE > TT	Set up MO Data call ( <i>PDU Session Establishment</i> )	To set up the MO Data call the MMI or EMMI is used	CR 2 CR 3 CR 4	
6	Tester	End test sequence			

#### 5.4.9.5 Acceptance criteria

For the scenarios in table 5.4.9-1:

CR 1 is explicitly verified at step 2) by analysing the file READ commands for EF<sub>UAC-AIC</sub> and EF<sub>ACC</sub> during the USIM-ME initialisation procedure.

CR 2, CR 3, and CR 4 are verified

- at step 3) by analysing if the UE shall make a successful or unsuccessful registration to the network in accordance with the result indicated in the table and
- at step 5) by analysing if the UE shall make a successful or unsuccessful MO Data call in accordance with the result indicated in the table if the step is applicable.

## 5.4.9A Unified Access Control – Access Identities 12, 13 and 14 indicated by USIM, Access Category 8

### 5.4.9A.1 Definition and applicability

The purpose of Unified Access Control procedure is to perform access barring check for a 5GS access attempt associated with a given Access Category and one or more Access Identities upon request from upper layers or the RRC layer.

The 5G network shall be able to broadcast barring control information (i.e. a list of barring parameters associated with an Access Identity and an Access Category) in SIB1.

The EF<sub>ACC</sub> in the USIM contains the configuration information pertaining to access identities 12, 13 and 14.

The UE shall be able to determine whether or not a particular new access attempt is allowed based on barring parameters that the UE receives from the broadcast barring control information and the configuration in the USIM.

When the NAS detects an access event, the NAS shall perform the mapping of the kind of request to one or more access identities and one access category and lower layers will perform access barring checks for that request based on the determined access identities and access category.

If RRC state is RRC\_INACTIVE and the resumption of the RRC connection is triggered due to an RNA Update RRC layer shall select Access Category as 8 and perform unified access control procedure in case there is no ongoing emergency service.

### 5.4.9A.2 Conformance requirement

CR 1 The ME shall read the access control value as part of the USIM-Terminal initialization procedure, and subsequently adopt this value.

Reference:

- TS 31.102 [19], clause 5.1.1.2.

CR 2 Access Identities are configured at the UE as listed in TS 22.261 [43] Table 6.22.2.2-1. Access Categories are defined by the combination of conditions related to UE and the type of access attempt as listed in TS 22.261 [43] Table 6.22.2.3-1. One or more Access Identities and only one Access Category are selected and tested for an access attempt.

Reference:

- TS 22.261 [43], clause 6.22.2.

CR 3 Access Identities 12, 13 and 14 are valid in HPLMN and visited PLMNs of home country only.

Reference:

- TS 24.501 [42], clause 4.5.2.

CR 4 The UE shall be able to determine whether or not a particular new access attempt is allowed based on uac-BarringInfo broadcast in SIB1. Access Control check shall be performed as per the information received in uac-BarringInfoSetList.

Reference:

- TS 38.331 [44], clauses 5.3.14.

CR 5 If the resumption of the RRC connection is triggered due to an RNA update and there is no ongoing emergency service RRC shall select '8' as the Access Category and perform the unified access control procedure.

Reference:

- TS 38.331 [44], clauses 5.3.13.2.

### 5.4.9A.3 Test purpose

The purpose of this test is to verify that:

- 1) the ME reads the access control value from  $EF_{UAC-AIC}$  and  $EF_{ACC}$  as part of the USIM-Terminal initialisation procedure, and subsequently adopts this value.
- 2) the UE maps the kind of request to one or more access identities and one access category and lower layers performs access barring checks for that request based on the determined access identities and access category.
- 3) the UE determines whether or not a particular access attempt is allowed based on  $uac-BarringInfo$  broadcast in SIB1 and if the RPLMN is the HPLMN, EHPLMN or visited PLMN of the home country.
- 4) the UE performs unified access control procedure if RNA Update procedure is triggered.

### 5.4.9A.4 Method of test

#### 5.4.9A.4.1 Initial conditions

The values of the 5G-NR UICC as defined in clause 4.5.9 of the present document are used with  $EF_{IMSI}$  as defined in clause 4.6.5 and the following exceptions:

#### $EF_{UAC-AIC}$ and $EF_{ACC}$

No Access Identities configured in  $EF_{UAC-AIC}$  and no Access Classes configured in  $EF_{ACC}$  as also shown in table 5.4.9-1.

#### $EF_{UST}$ (USIM Service Table)

Logically:

Service n°126      UAC Access Identities support      available

Coding:

Byte:	B1	B2	B3	B4	B5	B6	B7	B8
Binary:	xxxx xx1x	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxxx xxxx	xxxx xxxx	xxxx xxxx
	<b>B9</b>	<b>B10</b>	<b>B11</b>	...	<b>B16</b>	<b>B17</b>		
	xxxx xxxx	xxxx xxxx	xx11 xxxx	...	xx10 11xx	0000 0xxx		

The defined UICC/USIM data is installed on the UE.

The TT (NG-SS) is configured to transmit on the BCCH with the following parameters:

Cell A:

- TAI (MCC/MNC/TAC):MCC, MNC: see table 5.4.9A-1, TAC: 000001.
- CellIdentity: 000000001

For Table 5.4.9A-1:

No  $uac-BarringInfo$  in SIB1.

Cell B:

- TAI (MCC/MNC/TAC):MCC, MNC: see table 5.4.9A-1, TAC: 000001.
- CellIdentity: 000000002

For Table 5.4.9A-1:

$uac-BarringInfo$  in SIB1 should be set as in the table:

- Refer to Annex A for the Methods  $UAC\_BarringInfo\_xxxxxx()$  in the table.

## 5.4.9A.4.2 Tables related to the test case

Table 5.4.9A-1

TC Seq#	Access Category	USIM			SIB1		Result
		EF <sub>UAC_AIC</sub>	EF <sub>ACC</sub> (Byte 1 b8-b4)	Access Identity	uac-BarringInfo	PLMN-Identity (MCC/MNC)	RRCResumeRequest with resumeCause set to rna-Update successful?
2.1	8	0x00 00 00 00	00010	12	Not Present	246 / 081	Yes
2.2	8	0x00 00 00 00	00010	12	UAC_BarringInfo_Common(8,0x0001000'B)	246 / 081	No
2.3	8	0x00 00 00 00	00010	12	UAC_BarringInfo_PerPLMN(8,0x0000000'B)	246 / 081	Yes
2.4	8	0x00 00 00 00	00010	12	UAC_BarringInfo_Common(8,0x0010000'B)	246 / 082	Yes
2.5	8	0x00 00 00 00	00010	12	UAC_BarringInfo_Common2 (7,0x0010000'B, 8,0x0000000'B)	244 / 081	No
2.6	8	0x00 00 00 00	00100	13	UAC_BarringInfo_Common(8,0x0000100'B)	246 / 081	No
2.7	8	0x00 00 00 00	00100	13	UAC_BarringInfo_PerPLMN(8,0x0000000'B)	246 / 081	Yes
2.8	8	0x00 00 00 00	00100	13	UAC_BarringInfo_Common(8,0x0000100'B)	246 / 082	No
2.9	8	0x00 00 00 00	00100	13	UAC_BarringInfo_Common2 (7,0x0001000'B, 8,0x0000000'B)	244 / 081	No
2.10	8	0x00 00 00 00	01000	14	UAC_BarringInfo_Common(8,0x0000010'B)	246 / 081	No
2.11	8	0x00 00 00 00	01000	14	UAC_BarringInfo_PerPLMN(8,0x0000000'B)	246 / 081	Yes
2.12	8	0x00 00 00 00	01000	14	UAC_BarringInfo_Common(8,0x0000010'B)	246 / 082	No
2.13	8	0x00 00 00 00	01000	14	UAC_BarringInfo_Common2 (7,0x0000100'B, 8,0x0000000'B)	244 / 081	No

## 5.4.9A.4.3 Procedure

Procedure/steps to be repeated for all sequences listed in table 5.4.9A-1:

Step	Direction	Action	Comment	REQ	SA
1	TT	SIB1 of Cell A is transmitted as defined in the initial conditions and in table 5.4.9A-1	No barring info is provided to Cell A		
2	UE	Power UE on	The UE performs a SIM initialisation	CR 1	A.2/1 OR A.2/2
3	UE > TT	Send REGISTRATION REQUEST			
4	TT > UE	Send REGISTRATION ACCEPT	The registration is successful		
5	UE > TT	Set up MO Data call (PDU SessionEstablishment)	To set up the MO Data call the MMI or EMMI is used. The MO Data call is set up successfully		
6	TT > UE	Send RRC RELEASE with suspendConfig in criticalExtensions (with the choice rrcRelease)	ran-NotificationAreaInfo in suspendConfig contains the cellList with cellIdentity of Cell A: cellList { plmn-Identity {mcc, mnc}, -- see table 5.4.9A-1 for MCC/MNC ran-AreaCells 000000001'B }		

Step	Direction	Action	Comment	REQ	SA
7	TT	Deactivate Cell A and activate Cell B			
8	TT	SIB1 of Cell B is transmitted as defined in table 5.4.9A-1	Barring info is as in the table. See Annex A for the Methods <code>UAC_BarringInfo_xxxxxx()</code> in the table		
9	UE > TT	Initiate RRC RESUME REQUEST procedure with <i>resumeCause</i> set to <i>rna-Update</i> .	See the column ' <i>RRCResumeRequest</i> with <i>resumeCause</i> set to <i>rna-Update</i> successful?' for the result	CR 2 CR 3 CR 4 CR 5	

### 5.4.9A.5 Acceptance criteria

For the scenarios in table 5.4.9A-1:

CR 1 is explicitly verified at step 2) by analysing the file READ commands for  $EF_{UAC\_AIC}$  and  $EF_{ACC}$  during the USIM-Terminal initialisation procedure.

CR 2, CR 3, CR 4, and CR 5 are verified

- at step 9) by analysing if the UE shall make a successful or unsuccessful RRC Resumption for RNA Update in accordance with the result indicated in the table.

## 5.4.10 Unified Access Control – Operator-Defined Access Category

### 5.4.10.1 Definition and applicability

The purpose of Unified Access Control procedure is to perform access barring check for a 5GS access attempt associated with a given Access Category and one or more Access Identities upon request from upper layers or the RRC layer.

The 5G network shall be able to broadcast barring control information a list of barring parameters associated with an Access Identity and an Access Category in SIB1. Access category numbers in the 32-63 range are used for operator-defined Access Categories.

The  $EF_{UAC\_AIC}$  in the USIM contains the configuration information pertaining to access identities allocated for high priority services that can be used by the subscriber.

The UE shall be able to determine whether or not a particular new access attempt is allowed based on barring parameters that the UE receives from the broadcast barring control information and the configuration in the USIM.

When the NAS detects an access event, the NAS shall perform the mapping of the kind of request to one or more access identities and one access category and lower layers will perform access barring checks for that request based on the determined access identities and access category.

Operator-defined access category definitions can be signaled to the UE using NAS signaling. Each operator-defined access category definition consists of the parameters a precedence value, an operator-defined access category number, one or more access category criteria type and optionally, a standardized access category.

When the UE needs to initiate an access attempt that triggers access barring check, the UE shall determine one or more access identities from the set of standardized access identities, and one access category from the set of standardized access categories and operator-defined access categories, to be associated with that access attempt.

In order to determine the access category applicable for the access attempt, the NAS shall check the Access category mapping rules, and use the access category of the lowest rule number for which there is a match for barring check. In the case of operator-defined access categories, the UE shall select the access category from the operator-defined access category definition with the lowest precedence value.

### 5.4.10.2 Conformance requirement

CR 1 The ME shall read the access control value as part of the USIM initialization procedure, and subsequently adopt this value.

Reference:

- TS 31.102 [19], clause 5.1.1.2.

CR 2 Access Identities are configured at the UE as listed in Table 6.22.2.2-1. Access Categories are defined by the combination of conditions related to UE and the type of access attempt as listed in Table 6.22.2.3-1.

Reference:

- TS 22.261 [43], clause 6.22.2

CR 3 Operator may provide one or more PLMN-specific Operator-defined access category definitions to the UE using NAS signalling (Operator-defined access category definitions information element), and the UE handles the Operator-defined access category definitions stored for the Registered PLMN, as specified in TS 24.501.

References:

- TS 23.501 [39], clause 5.2.5
- TS 24.501 [25] clause 9.11.3.38

CR 4 When the UE needs to initiate an access attempt in one of the events listed in clause 4.5.1, the UE shall determine one or more access identities from the set of standardized access identities, and one access category from the set of standardized access categories and operator-defined access categories, to be associated with that access attempt.

Reference:

- TS 24.501 [25], clause 4.5.2

CR 5 An access attempt matches the criteria of an operator-defined access category definition, if the access attempt matches all access category criteria types included in the criteria with any of the associated access criteria type values.

Reference:

- TS 24.501 [25], clause 4.5.3

CR 6 In order to determine the access category applicable for the access attempt, the NAS shall check the rules in table 4.5.2.2, and use the access category for which there is a match for barring check. If the access attempt matches more than one rule, the access category of the lowest rule number shall be selected. If the access attempt matches more than one operator-defined access category definition, the UE shall select the access category from the operator-defined access category definition with the lowest precedence value (see clause 4.5.3).

Reference:

- TS 24.501 [25], clause 4.5.2

CR 7 If the UE receives Operator-defined access category definitions IE in the REGISTRATION ACCEPT message and the Operator-defined access category definitions IE contains one or more operator-defined access category definitions, the UE shall delete any operator-defined access category definitions stored for the RPLMN and shall store the received operator-defined access category definitions for the RPLMN. If the UE receives the Operator-defined access category definitions IE in the REGISTRATION ACCEPT message and the Operator-defined access category definitions IE contains no operator-defined access category definitions, the UE shall delete any operator-defined access category definitions stored for the RPLMN. If the REGISTRATION ACCEPT message does not contain the Operator-defined access category definitions IE, the UE shall not delete the operator-defined access category definitions stored for the RPLMN.

Reference:

- TS 24.501 [25], clause 5.5.1.2.4

CR 8 The UE shall be able to determine whether or not a particular new access attempt is allowed based on uac-BarringInfo broadcast in SIB1. Access Control check shall be performed as per the information received in uac-BarringInfoSetList.

Reference:

- TS 38.331 [37], clauses 5.3.14

### 5.4.10.3 Test purpose

The purpose of this test is to verify that:

- 1) the ME reads the access control value from EF<sub>UAC\_AIC</sub> and EF<sub>ACC</sub> as part of the USIM initialisation procedure, and subsequently adopts this value.
- 2) if the UE uses operator-defined access categories received within Operator-defined access category definitions information element in the REGISTRATION ACCEPT.
- 3) the UE checks the access category applicable for the access attempt, as per the Access category mapping rules and chooses the matching lowest rule.
- 4) the UE checks operator-defined access category parameters precedence value, operator-defined access category number and access category criteria type associated with the Operator-defined Access Category when determining the Access Category for the access attempt.
- 5) the UE stops using the operator-defined access category definitions stored for the previously selected PLMN.
- 6) the UE maps the kind of request to one or more access identities and one access category and lower layers performs access barring checks for that request based on the determined access identities and access category.
- 7) the UE determines whether or not a particular access attempt is allowed based on uac-BarringInfo broadcast in SIB1 and if the RPLMN is the HPLMN, EHPLMN or visited PLMN of the home country.

### 5.4.10.4 Method of test

#### 5.4.10.4.1 Initial conditions

The values of the 5G-NR UICC as defined in clause 4.5.9 of the present document are used with EF<sub>IMSI</sub> as defined in clause 4.6.5 and the following exceptions:

#### EF<sub>UAC\_AIC</sub> and EF<sub>ACC</sub>

No Access Identities configured in EF<sub>UAC\_AIC</sub> and no Access Classes configured in EF<sub>ACC</sub> as also shown in table 5.4.10-1.

#### EF<sub>UST</sub> (USIM Service Table)

Logically:

Service n°126      UAC Access Identities support      available

Coding:

Byte:	B1	B2	B3	B4	B5	B6	B7	B8
Binary:	xxxx xx1x	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxxx xxxx	xxxx xxxx	xxxx xxxx
	<b>B9</b>	<b>B10</b>	<b>B11</b>	...	<b>B16</b>	<b>B17</b>		
	xxxx xxxx	xxxx xxxx	xx11 xxxx	...	xx10 11xx	0000 0xxx		

ME shall be configured with following URSP rules:

Rule Precedence = 1

Traffic Descriptor:

DNN=TestGp.rs1

Route Selection Descriptor:

Precedence = 1

Network Slice Selection, S-NSSAI: '01 01 01 01' (ST: MBB, SD: 010101)

SSC Mode Selection:                      SSC Mode 1

Access Type preference:                      3GPP access

Rule Precedence = 2

Traffic Descriptor:

DNN = TestGp.rs2

Route Selection Descriptor:

Precedence = 1

Network Slice Selection, S-NSSAI: '01 01 01 02' (ST: MBB, SD: 010102)

SSC Mode Selection: SSC Mode 1

Rule Precedence = 3

Traffic Descriptor:

DNN = TestGp.rs3

Route Selection Descriptor:

Precedence = 1

Network Slice Selection, S-NSSAI: '01 01 01 02' (ST: MBB, SD: 010102)

SSC Mode Selection: SSC Mode 1

The TT (NG-SS) is configured to transmit on the BCCH with the following parameters:

Cell A:

- MCC, MNC: 246/081
- TAC: 000001
- CellIdentity: 000000001

For Table 5.4.10-1:

After turning on the cell for the 2<sup>nd</sup> time, uac-BarringInfo in SIB1 should be set as in the table:

- Refer to Annex A for the Methods UAC\_BarringInfo\_xxxxxx() in the table.

REGISTRATION ACCEPT IEIs.

- Operator-Defined Access Category Definitions IEI is configured as defined in Table 5.4.10-1
- Refer to Annex A tables A4-A5 for Methods ODAC\_definitions1() and ODAC\_definitions2().
- For HPLMN Cells: Allowed S-NSSAI IEI is configured to include S-NSSAIs '01 01 01 01', '01 01 01 02' and '01 01 01 03'.

For VPLMN Cells:

- Allowed S-NSSAI IEI is configured to include S-NSSAIs ('01 01 01 01', '01 01 01 01'), ('01 01 01 02', '01 01 01 02'), and ('01 01 01 03', '01 01 01 03').

#### 5.4.10.4.2 Tables related to the test case

**Table 5.4.10-1**

TC Seq#	Access Category for Call 1&2	USIM		SIB1 of Cell A		REGISTRATION ACCEPT	Result	
		EF <sub>UAC_AIC</sub>	EF <sub>ACC</sub> (Byte 1 b8-b4)	uac-BarringInfo	PLMN-Identity (MCC/MNC)	(Operator-defined access category definitions IE)	MO Data call 1 successful?	MO Data call 2 successful?
1.1	32,7	0x00 00 00 00	00000	Not Present	246 / 081	ODAC_definitions1(0)	Yes	Yes
1.2	32,7	0x00 00 00 00	00000	UAC_BarringInfo_Common (32,0x00000000'B)	246 / 081	ODAC_definitions1(0)	No	Yes
1.3	50,7	0x00 00 00 00	00000	UAC_BarringInfo_Common (50,0x01000000'B)	246 / 081	ODAC_definitions1(18)	No	Yes
1.4	63,7	0x01 00 00 00	00000	UAC_BarringInfo_Common (7,0x10000000'B)	246 / 082	ODAC_definitions1(31)	Yes	No

1.5	63,7	0x02 00 00 00	00000	UAC_BarringInfo_Common (63,0x0100000'B)	246 / 081	ODAC_definitions1(31)	No	Yes
1.6	48,7	0x01 00 00 00	00000	UAC_BarringInfo_Common2 (7,0x1000000'B, 48,0x1000000'B)	246 / 082	ODAC_definitions1(16)	No	No
1.7	48,7	0x02 00 00 00	00000	UAC_BarringInfo_Common (48,0x1000000'B)	246 / 082	ODAC_definitions1(16)	Yes	Yes
1.8	50,7	0x02 00 00 00	00000	UAC_BarringInfo_PerPLMN (50,0x1100000'B)	244 / 081	ODAC_definitions1(18)	No	Yes
1.9	50,7	0x00 00 00 00	00001	UAC_BarringInfo_Common (50,0x0001000'B)	244 / 081	ODAC_definitions1(18)	No	Yes
1.10	33,7	0x02 00 00 00	00000	UAC_BarringInfo_Common2 (33,0x0100000'B, 7,0x1000000'B)	246 / 082	ODAC_definitions1(1)	No	Yes
1.11	34,7	0x01 00 00 00	00000	UAC_BarringInfo_Common2 (7,0x1000000'B, 34,0x0100000'B)	246 / 082	ODAC_definitions1(2)	Yes	No
1.12	7,34	0x01 00 00 00	00000	UAC_BarringInfo_Common2 (32,0x1000000'B, 34,0x0100000'B)	246 / 081	ODAC_definitions2(2,0)	Yes	Yes
1.13	7,32	0x00 00 00 00	01000	UAC_BarringInfo_Common2 (32,0x0000000'B, 34,0x0000010'B)	246 / 082	ODAC_definitions2(0,2)	Yes	Yes
1.14	7,48	0x00 00 00 00	00100	UAC_BarringInfo_Common2 (48,0x0100000'B, 7,0x0000100'B)	246 / 082	ODAC_definitions2(16,31)	No	Yes
1.15	7,32	0x01 00 00 00	00000	UAC_BarringInfo_Common2 (32,0x1000000'B, 34,0x0100000'B)	246 / 081	ODAC_definitions2(2,0)	Yes	No
1.16	7,34	0x00 00 00 00	01000	UAC_BarringInfo_Common2 (32,0x0000000'B, 34,0x0000010'B)	246 / 082	ODAC_definitions2(0,2)	Yes	No
1.17	7,63	0x00 00 00 00	00100	UAC_BarringInfo_Common2 (48,0x0100000'B, 7,0x0000100'B)	246 / 082	ODAC_definitions2(16,31)	No	Yes

#### 5.4.10.4.3 Procedure

Procedure/steps to be repeated for all sequences listed in table 5.4.10-1:

Step	Direction	Action	Information	REQ	SA
1	TT	SIB1 of Cell A is transmitted as defined in the initial conditions for tests from table 5.4.10-1	Barring info is set as in table 5.4.10-1 See Annex A for the Methods UAC_BarringInfo_XXXXXX() in the table		
2	USER	Power UE on	The UE performs a SIM initialisation. (includes reading of EF <sub>UAC-AIC</sub> and EF <sub>ACC</sub> )	CR 1	A.2/1 OR A.2/2
3	UE > TT	Send REGISTRATION REQUEST			
4	TT > UE	Send REGISTRATION ACCEPT	REGISTRATION ACCEPT with the Operator-Defined Access Category Definitions IEI as defined in the table 5.4.10-1.  For simplicity other signalling is not shown		
<b>If 1<sup>st</sup> MO Data call is not allowed:</b>					
5	UE > TT	Attempt to set up 1 <sup>st</sup> MO Data call	Attempt to set up the MO Data call the MMI or EMMI is used	CR 2 to CR 8	

If 1 <sup>st</sup> MO Data call is allowed:					
5	UE > TT	Set up MO Data call ( <i>PDU SessionEstablishment</i> )	To set up the MO Data call the MMI or EMMI is used	CR 2 to CR 8	
For sequences 1.1 – 1.14:					
If 2 <sup>nd</sup> MO Data call is not allowed:					
6	UE > TT	Attempt to set up 2 <sup>nd</sup> MO Data call	Attempt to set up the MO Data call to DNN TestGp.rs2/S-NSSAI '01 01 01 02' using the MMI or EMMI.	CR 2 to CR 8	
7	USER	End test sequence			
For sequences 1.1 – 1.14:					
If 2 <sup>nd</sup> MO Data call is allowed:					
6	UE > TT	Set up MO Data call ( <i>PDU SessionEstablishment</i> )	To set up the MO Data call to DNN TestGp.rs2/S-NSSAI '01 01 01 02' using the MMI or EMMI.	CR 2 to CR 8	
7	USER	End test sequence			
For sequences 1.15 – 1.17:					
If 2 <sup>nd</sup> MO Data call is not allowed:					
6	UE > TT	Attempt to set up 2 <sup>nd</sup> MO Data call	Attempt to set up the MO Data call to DNN TestGp.rs3/S-NSSAI '01 01 01 02' using the MMI or EMMI.	CR 2 to CR 8	
7	USER	End test sequence			
For sequences 1.15 – 1.17:					
If 2 <sup>nd</sup> MO Data call is allowed:					
6	UE > TT	Set up MO Data call ( <i>PDU SessionEstablishment</i> )	To set up the MO Data call to DNN TestGp.rs3/S-NSSAI '01 01 01 02' using the MMI or EMMI.	CR 2 to CR 8	
7	USER	End test sequence			

#### 5.4.10.5 Acceptance criteria

For the scenarios in table 5.4.10-1:

CR 1 is explicitly verified at step 2) by analysing the file READ commands for EF<sub>UAC-AIC</sub> and EF<sub>ACC</sub> during the USIM-Terminal initialisation procedure.

CR 2, through CR 8 are verified

- at steps 5) by analysing if the UE shall make a successful or unsuccessful 1<sup>st</sup> MO Data call in accordance with the result indicated in the table if the step is applicable and
- at steps 6) and 7) by analysing if the UE shall make a successful or unsuccessful 2<sup>nd</sup> MO Data call in accordance with the result indicated in the table if the step is applicable.

### 5.4.11 Unified Access Control – Operator-Defined Access Categories, no change in SUPI

#### 5.4.11.1 Definition and applicability

The purpose of Unified Access Control procedure is to perform access barring check for a 5GS access attempt associated with a given Access Category and one or more Access Identities upon request from upper layers or the RRC layer.

The 5G network shall be able to broadcast barring control information a list of barring parameters associated with an Access Identity and an Access Category in SIB1. Access category numbers in the 32-63 range are used for operator-defined Access Categories.

The EF<sub>UAC-AIC</sub> in the USIM contains the configuration information pertaining to access identities allocated for high priority services that can be used by the subscriber.

The UE shall be able to determine whether or not a particular new access attempt is allowed based on barring parameters that the UE receives from the broadcast barring control information and the configuration in the USIM.

Operator-defined access category definitions can be signalled to the UE using NAS signalling. Each operator-defined access category definition consists of the parameters: a precedence value, an operator-defined access category number, one or more access category criteria type and optionally, a standardized access category.

Operator-defined access category definitions are stored together with a PLMN identity of the PLMN that provided them, and is valid in that PLMN or equivalent PLMN. The operator-defined access category definitions can only be used if the SUPI from the USIM matches the SUPI stored in the non-volatile memory of the ME, else the UE shall delete the operator-defined access category definitions.

In order to determine the access category applicable for the access attempt, the NAS shall check the Access category mapping rules, and use the access category of the lowest rule number for which there is a match for barring check. In the case of operator-defined access categories, the UE shall select the access category from the operator-defined access category definition with the lowest precedence value.

#### 5.4.11.2 Conformance requirement

CR 1 The ME shall read the access control value as part of the USIM initialization procedure, and subsequently adopt this value.

Reference:

- TS 31.102 [19], clause 5.1.1.2.

CR 2 Access Identities are configured at the UE as listed in TS 22.261 [43] Table 6.22.2.2-1. Access Categories are defined by the combination of conditions related to UE and the type of access attempt as listed in TS 22.261 [36] Table 6.22.2.3-1.

Reference:

- TS 22.261 [36], clause 6.22.2

CR 3 Operator may provide one or more PLMN-specific Operator-defined access category definitions to the UE using NAS signalling (Operator-defined access category definitions information element), and the UE handles the Operator-defined access category definitions stored for the Registered PLMN, as specified in TS 24.501.

References:

- TS 23.501 [39], clause 5.2.5
- TS 24.501 [25] clause 9.11.3.38

CR 4 Operator-defined access category definitions are stored together with a PLMN identity of the PLMN that provided them, and is valid in that PLMN or equivalent PLMN. The operator-defined access category definitions can only be used if the SUPI from the USIM matches the SUPI stored in the non-volatile memory of the ME, else the UE shall delete the operator-defined access category definitions.

Reference:

- TS 24.501 [25], Annex C

CR 5 In order to determine the access category applicable for the access attempt, the NAS shall check the rules in TS 24.501 [42] Table 4.5.2.2, and use the access category for which there is a match for barring check. If the access attempt matches more than one rule, the access category of the lowest rule number shall be selected. If the access attempt matches more than one operator-defined access category definition, the UE shall select the access category from the operator-defined access category definition with the lowest precedence value (see TS 24.501 [42] clause 4.5.3).

Reference:

- TS 24.501 [25], clause 4.5.2

CR 6 If the UE receives Operator-defined access category definitions IE in the REGISTRATION ACCEPT message and the Operator-defined access category definitions IE contains one or more operator-defined access category definitions, the UE shall delete any operator-defined access category definitions stored for the RPLMN and shall store the received operator-defined access category definitions for the RPLMN. If the UE receives the Operator-defined access category definitions IE in the REGISTRATION ACCEPT message and the Operator-defined access category definitions IE contains no operator-defined access category definitions, the UE shall delete any operator-defined access category definitions stored for the RPLMN. If the REGISTRATION ACCEPT message does not contain the Operator-defined access category definitions IE, the UE shall not delete the operator-defined access category definitions stored for the RPLMN.

Reference:

- TS 24.501 [25], clause 5.5.1.2.4

CR 7 The UE shall be able to determine whether or not a particular new access attempt is allowed based on uac-BarringInfo broadcast in SIB1. Access Control check shall be performed as per the information received in uac-BarringInfoSetList.

Reference:

- TS 38.331 [37], clauses 5.3.14

### 5.4.11.3 Test purpose

The purpose of this test is to verify that:

- 1) the ME reads the access control value from  $EF_{UAC\_AIC}$  and  $EF_{ACC}$  as part of the USIM-Terminal initialisation procedure, and subsequently adopts this value.
- 2) if UE uses operator-defined access categories received within Operator-defined access category definitions information element in the REGISTRATION ACCEPT.
- 3) the UE checks the access category applicable for the access attempt, as per the Access category mapping rules and chooses the matching lowest rule.
- 4) the UE checks operator-defined access category parameters precedence value, operator-defined access category number and access category criteria type associated with the Operator-defined Access Category when determining the Access Category for the access attempt.
- 5) the Operator-defined access category definitions are stored together with a PLMN identity of the PLMN that provided them, and is valid in that PLMN or equivalent PLMN.
- 6) the Operator-defined access category definitions can only be used if the SUPI from the USIM matches the SUPI stored in the non-volatile memory of the ME, else the UE shall delete the operator-defined access category definitions.
- 7) the UE maps the kind of request to one or more access identities and one access category and lower layers performs access barring checks for that request based on the determined access identities and access category.
- 8) the UE determines whether or not a particular access attempt is allowed based on uac-BarringInfo broadcast in SIB1 and if the RPLMN is the HPLMN, EHPLMN or visited PLMN of the home country.

### 5.4.11.4 Method of test

#### 5.4.11.4.1 Initial conditions

The values of the 5G-NR UICC as defined in clause 4.5.9 of the present document are used with  $EF_{IMSI}$  as defined in clause 4.6.5 and the following exceptions:

**$EF_{UAC\_AIC}$  and  $EF_{ACC}$**

Access Identity is configured in  $EF_{UAC\_AIC}$  and no Access Classes are configured in  $EF_{ACC}$  as given in Table 5.4.11-1.

**$EF_{UST}$  (USIM Service Table)**

Logically:

Service n°126 UAC Access Identities support available

Coding:

Byte:	B1	B2	B3	B4	B5	B6	B7	B8
Binary:	xxxx xx1x	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxxx xxxx	xxxx xxxx	xxxx xxxx
	<b>B9</b>	<b>B10</b>	<b>B11</b>	...	<b>B16</b>	<b>B17</b>		
	xxxx xxxx	xxxx xxxx	xx11 xxxx	...	xx10 11xx	0000 0xxx		

ME shall be configured with following URSP rules:

Rule Precedence =1

Traffic Descriptor:

DNN=TestGp.rs1

Route Selection Descriptor:

Precedence=1

Network Slice Selection, S-NSSAI: '01 01 01 01' (ST: MBB, SD: 010101)

SSC Mode Selection: SSC Mode 1

Access Type preference: 3GPP access

Rule Precedence = 2

Traffic Descriptor:

DNN=TestGp.rs2

Route Selection Descriptor:

Precedence =1

Network Slice Selection, S-NSSAI: '01 01 01 02' (ST: MBB, SD: 010102)

SSC Mode Selection: SSC Mode 1

The TT (NG-SS) is configured to transmit on the BCCH with the following parameters:

Cell A:

- MCC, MNC: 246/081
- TAC: 000001
- CellIdentity: 000000001

For Table 5.4.11-1:

uac-BarringInfo in SIB1 should be set as in the table:

- Refer to Annex A for the Methods UAC\_BarringInfo\_xxxxxx() in the tables A1-A3.

Cell B:

NOTE: This cell is not required for the sequences in Table 5.4.11-1.

- TAI (MCC/MNC/TAC):MCC, MNC: see Table 5.4.11-1, TAC: 000002.
- CellIdentity: 000000002

For Table 5.4.11-1:

uac-BarringInfo in SIB1 should be set as in the table:

- Refer to Annex A for the Methods UAC\_BarringInfo\_xxxxxx() in the tables A1-A3.

REGISTRATION ACCEPT IEIs.

- Operator-Defined Access Category Definitions IEI is configured as defined in Table 5.4.11-1.
- Refer to Annex A tables A4-A5 for Methods ODAC\_definitions1() and ODAC\_definitions2()

For HPLMN Cells:

- Allowed S-NSSAI IEI is configured to include S-NSSAIs '01 01 01 01', '01 01 01 02' and '01 01 01 03'.

For VPLMN Cells:

- Allowed S-NSSAI IEI is configured to include S-NSSAIs ('01 01 01 01', '01 01 01 01'), ('01 01 01 02', '01 01 01 02'), and ('01 01 01 03', '01 01 01 03').

#### 5.4.11.4.2 Tables related to the test case

**Table 5.4.11-1**

TC Seq#	Access	USIM		Cell 2		SIB 1: uac-BarringInfo (for all the Cells)	Operator-defined access category definitions IEI in	Result	
		EF <sub>UAC_AIC</sub>	EF <sub>ACC</sub> (Byte 1 b8-b4)	Cell Id of	PLMN-identity (MCC/MNC)		1 <sup>st</sup> REGISTRATION ACCEPT, 2 <sup>nd</sup> REGISTRATION ACCEPT	MO Data call 1 successful?	MO Data call 2 successful?
1.1	7,33	0x00 00 00 00	00000	Cell A	246 / 081	Not Present	ODAC_definitions1(0), ODAC_definitions2(1,16)	Yes	Yes
1.2	7,33	0x00 00 00 00	00000	Cell A	246 / 081	UAC_BarringInfo_Common (33,0x0000000'B)	ODAC_definitions1(0), ODAC_definitions2(1,16)	Yes	No
1.3	34,7	0x01 00 00 00	00000	Cell A	246 / 081	UAC_BarringInfo_Common2 (34,0x1000000'B, 50,0x1000000'B)	ODAC_definitions2(18,1), ODAC_definitions1(2)	No	Yes
1.4	7,63	0x01 00 00 00	00000	Cell B	244 / 081	UAC_BarringInfo_Common2 (63,0x0000000'B, 7,0x0100000'B)	ODAC_definitions1(3), ODAC_definitions2(31,18)	No	No
1.5	63,7	0x02 00 00 00	00000	Cell A	246 / 081	UAC_BarringInfo_Common (63,0x0100000'B)	ODAC_definitions1(31), ODAC - Not present	No	Yes
1.6	7,7	0x00 00 00 00	10000	Cell B	246 / 082	UAC_BarringInfo_Common (48,0x0010000'B)	ODAC_definitions1(16), ODAC - Not present	Yes	Yes
1.7	7,7	0x00 00 00 00	00100	Cell B	246 / 082	UAC_BarringInfo_Common2 (32,0x0000100'B, 34,0x0000100'B)	ODAC_definitions2(0,2), ODAC - Empty	Yes	Yes

#### 5.4.11.4.3 Procedure

Procedure/steps to be repeated for all sequences listed in table 5.4.11-1:

Step	Direction	Action	Information	REQ	SA
1	TT	SIB1 of Cell A is transmitted as defined in the initial conditions for tests from table 5.4.11-1	Barring info in SIB1 is set as in table 5.4.11-1  See Annex A for the Methods UAC_BarringInfo_XXXXXX() in the table		
2	USER	Power UE on	The UE performs a SIM initialisation. (includes reading of EF <sub>UAC_AIC</sub> and EF <sub>ACC</sub> )	CR 1	A.2/1 OR A.2/2
3	UE > TT	Send REGISTRATION REQUEST			
4	TT > UE	Send REGISTRATION ACCEPT	1 <sup>st</sup> REGISTRATION ACCEPT with the Operator-Defined Access Category Definitions IEI as defined in the table 5.4.11-1.  For simplicity other signalling is not shown		

If 2 <sup>nd</sup> Cell is Cell A as in table 5.4.11-1:					
5	USER	Disable the UICC profile			
6	USER	Enable the UICC profile			
If 2 <sup>nd</sup> Cell is Cell B as in table 5.4.11-1:					
5	USER	Disable the UICC profile	Deactivate Cell A		
6	USER	Enable the UICC profile	Activate Cell B		
Common test steps					
7	UE > TT	Send REGISTRATION REQUEST	Send to Cell A or B as in the Table 5.4.11-1		
8	USER	Send REGISTRATION ACCEPT	2 <sup>nd</sup> REGISTRATION ACCEPT with the Operator-Defined Access Category Definitions IEI as defined in the table 5.4.11-1.  For simplicity other signalling is not shown		
If 1 <sup>st</sup> MO Data call is not allowed:					
9	UE > TT	Attempt to set up 1 <sup>st</sup> MO Data call	Attempt to set up the MO Data call to DNN TestGp.rs1/S-NSSAI '01 01 01 01' using the MMI or EMMI.	CR 2 to CR 7	
If 1 <sup>st</sup> MO Data call is allowed:					
9	UE > TT	Set up MO Data call (PDU SESSION ESTABLISHMENT)	To set up the MO Data call to DNN TestGp.rs1/S-NSSAI '01 01 01 01' using the MMI or EMMI.	CR 2 to CR 7	
If 2 <sup>nd</sup> MO Data call is not allowed:					
10	UE > TT	Attempt to set up 2 <sup>nd</sup> MO Data call	Attempt to set up the MO Data call to DNN TestGp.rs2/S-NSSAI '01 01 01 02' using the MMI or EMMI	CR 2 to CR 7	
11	USER	End test sequence			
If 2 <sup>nd</sup> MO Data call is allowed:					
10	UE > TT	Set up MO Data call (PDU SESSION ESTABLISHMENT)	To set up the MO Data call to DNN TestGp.rs2/S-NSSAI '01 01 01 02' using the MMI or EMMI.	CR 2 to CR 7	
11	USER	End test sequence			

### 5.4.11.5 Acceptance criteria

For the scenarios in table 5.4.11-1:

CR 1 is explicitly verified at step 2) by analysing the file READ commands for EF<sub>UAC-AIC</sub> and EF<sub>ACC</sub> during the USIM-Terminal initialisation procedure.

CR 2, through CR 7 are verified

- at steps 9) by analysing if the UE shall make a successful or not successful 1<sup>st</sup> MO Data call in accordance with the result indicated in the table if the step is applicable and
- at steps 10) by analysing if the UE shall make a successful or not successful 2<sup>nd</sup> MO Data call in accordance with the result indicated in the table if the step is applicable.

## 5.4.12 Unified Access Control – Operator-Defined Access Categories, SUPI change

### 5.4.12.1 Definition and applicability

The purpose of Unified Access Control procedure is to perform access barring check for a 5GS access attempt associated with a given Access Category and one or more Access Identities upon request from upper layers or the RRC layer.

The 5G network shall be able to broadcast barring control information a list of barring parameters associated with an Access Identity and an Access Category in SIB1. Access category numbers in the 32-63 range are used for operator-defined Access Categories.

The  $EF_{UAC\_AIC}$  in the USIM contains the configuration information pertaining to access identities allocated for high priority services that can be used by the subscriber.

The UE shall be able to determine whether or not a particular new access attempt is allowed based on barring parameters that the UE receives from the broadcast barring control information and the configuration in the USIM.

Operator-defined access category definitions can be signaled to the UE using NAS signaling. Each operator-defined access category definition consists of the parameters a precedence value, an operator-defined access category number, one or more access category criteria type and optionally, a standardized access category.

Operator-defined access category definitions are stored together with a PLMN identity of the PLMN that provided them, and is valid in that PLMN or equivalent PLMN. The operator-defined access category definitions can only be used if the SUPI from the USIM matches the SUPI stored in the non-volatile memory of the ME, else the UE shall delete the operator-defined access category definitions.

In order to determine the access category applicable for the access attempt, the NAS shall check the Access category mapping rules, and use the access category of the lowest rule number for which there is a match for barring check. In the case of operator-defined access categories, the UE shall select the access category from the operator-defined access category definition with the lowest precedence value.

#### 5.4.12.2 Conformance requirement

CR 1 The ME shall read the access control value as part of the USIM initialization procedure, and subsequently adopt this value.

Reference:

- TS 31.102 [19], clause 5.1.1.2.

CR 2 Access Identities are configured at the UE as listed in TS 22.261 [43] Table 6.22.2.2-1. Access Categories are defined by the combination of conditions related to UE and the type of access attempt as listed in TS 22.261 [43] Table 6.22.2.3-1.

Reference:

- TS 22.261 [36], clause 6.22.2

CR 3 Operator may provide one or more PLMN-specific Operator-defined access category definitions to the UE using NAS signalling (Operator-defined access category definitions information element), and the UE handles the Operator-defined access category definitions stored for the Registered PLMN, as specified in TS 24.501.

References:

- TS 23.501 [39], clause 5.2.5
- TS 24.501 [25] clause 9.11.3.38

CR 4 Operator-defined access category definitions are stored together with a PLMN identity of the PLMN that provided them, and is valid in that PLMN or equivalent PLMN. The operator-defined access category definitions can only be used if the SUPI from the USIM matches the SUPI stored in the non-volatile memory of the ME, else the UE shall delete the operator-defined access category definitions.

Reference:

- TS 24.501 [25], Annex C

CR 5 In order to determine the access category applicable for the access attempt, the NAS shall check the rules in TS 24.501 [42] Table 4.5.2.2, and use the access category for which there is a match for barring check. If the access attempt matches more than one rule, the access category of the lowest rule number shall be selected. If the access attempt matches more than one operator-defined access category definition, the UE shall select the access

category from the operator-defined access category definition with the lowest precedence value (see TS 24.501 [42] clause 4.5.3).

Reference:

- TS 24.501 [25], clause 4.5.2

CR 6 If the UE receives Operator-defined access category definitions IE in the REGISTRATION ACCEPT message and the Operator-defined access category definitions IE contains one or more operator-defined access category definitions, the UE shall delete any operator-defined access category definitions stored for the RPLMN and shall store the received operator-defined access category definitions for the RPLMN. If the UE receives the Operator-defined access category definitions IE in the REGISTRATION ACCEPT message and the Operator-defined access category definitions IE contains no operator-defined access category definitions, the UE shall delete any operator-defined access category definitions stored for the RPLMN. If the REGISTRATION ACCEPT message does not contain the Operator-defined access category definitions IE, the UE shall not delete the operator-defined access category definitions stored for the RPLMN.

Reference:

- TS 24.501 [25], clause 5.5.1.2.4

CR 7 The UE shall be able to determine whether or not a particular new access attempt is allowed based on uac-BarringInfo broadcast in SIB1. Access Control check shall be performed as per the information received in uac-BarringInfoSetList.

Reference:

- TS 38.331 [37], clauses 5.3.14

### 5.4.12.3 Test purpose

The purpose of this test is to verify that:

- 1) To verify that the ME reads the access control value from  $EF_{UAC\_AIC}$  and  $EF_{ACC}$  as part of the USIM-Terminal initialisation procedure, and subsequently adopts this value.
- 2) To verify if UE uses operator-defined access categories received within Operator-defined access category definitions information element in the REGISTRATION ACCEPT.
- 3) To verify the UE checks the access category applicable for the access attempt, as per the Access category mapping rules and chooses the matching lowest rule.
- 4) To verify the UE checks operator-defined access category parameters precedence value, operator-defined access category number and access category criteria type associated with the Operator-defined Access Category when determining the Access Category for the access attempt.
- 5) To verify the Operator-defined access category definitions are stored together with a PLMN identity of the PLMN that provided them, and is valid in that PLMN or equivalent PLMN.
- 6) To verify the Operator-defined access category definitions can only be used if the SUPI from the USIM matches the SUPI stored in the non-volatile memory of the ME, else the UE shall delete the operator-defined access category definitions.
- 7) To verify UE maps the kind of request to one or more access identities and one access category and lower layers performs access barring checks for that request based on the determined access identities and access category.
- 8) To verify the UE determines whether or not a particular access attempt is allowed based on uac-BarringInfo broadcast in SIB 1 and if the RPLMN is the HPLMN, EHPLMN or visited PLMN of the home country.

## 5.4.12.4 Method of test

### 5.4.12.4.1 Initial conditions

The values of the 5G-NR UICC as defined in clause 4.5.9 of the present document are used with the following exceptions:

**EF<sub>IMSI</sub>** (International Mobile Subscriber Identity) for UICC 2

Logically:

246081357935799

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9
Hex	08	29	64	80	31	75	39	75	99

**EF<sub>UAC\_AIC</sub>** and **EF<sub>ACC</sub>**

Access Identity is configured in **EF<sub>UAC\_AIC</sub>** and no Access Classes are configured in **EF<sub>ACC</sub>** as given in Table 5.4.12-1.

**EF<sub>UST</sub>** (USIM Service Table)

Logically:

Service n°126      UAC Access Identities support      available

Coding:

Byte:	B1	B2	B3	B4	B5	B6	B7	B8
Binary:	xxxx xx1x	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxxx xxxx	xxxx xxxx	xxxx xxxx
	B9	B10	B11	...	B16	B17		
	xxxx xxxx	xxxx xxxx	xx11 xxxx	...	xx10 11xx	0000 0xxx		

ME shall be configured with following URSP rules.

Rule Precedence =1

Traffic Descriptor:

DNN=TestGp.rs1

Route Selection Descriptor:

Precedence=1

Network Slice Selection, S-NSSAI: '01 01 01 01' (ST: MBB, SD: 010101)

SSC Mode Selection: SSC Mode 1

Access Type preference: 3GPP access

Rule Precedence = 2

Traffic Descriptor:

DNN=TestGp.rs2

Route Selection Descriptor:

Precedence =1

Network Slice Selection, S-NSSAI: '01 01 01 02' (ST: MBB, SD: 010102)

SSC Mode Selection: SSC Mode 1

The TT (NG-SS) is configured to transmit on the BCCH with the following parameters:

Cell A:

- MCC, MNC: 246/081
- TAC: 000001
- CellIdentity: 00000001

For Table 5.4.12-1:

uac-BarringInfo in SIB1 should be set as in the table:

- Refer to Annex A for the Methods UAC\_BarringInfo\_XXXXXX() in the tables A1-A3.

Cell B:

This cell is required for some sequences as in the Table 5.4.12-1.

- TAI (MCC/MNC/TAC):MCC, MNC: see Table 5.4.12-1, TAC: 000002.
- CellIdentity: 00000002

For Table 5.4.12-1:

uac-BarringInfo in SIB1 should be set as in the table:

- Refer to Annex A for the Methods UAC\_BarringInfo\_XXXXXX() in the tables A1-A3.

REGISTRATION ACCEPT IEIs.

- Operator-Defined Access Category Definitions IEI is configured as defined in Table 5.4.12-1.
- Refer to Annex A tables A4-A5 for Methods ODAC\_definitions1() and ODAC\_definitions2().

For HPLMN Cells:

- Allowed S-NSSAI IEI is configured to include S-NSSAIs '01 01 01 01', '01 01 01 02'and '01 01 01 03'.

For VPLMN Cells:

- Allowed S-NSSAI IEI is configured to include S-NSSAIs ('01 01 01 01', '01 01 01 01'), ('01 01 01 02', '01 01 01 02'), and ('01 01 01 03', '01 01 01 03').

5.4.12.4.2 Tables related to the test case

Table 5.4.12-1

TC Seq#	Access Category for Call 1 & 2	USIM		Cell 2		SIB 1: uac-BarringInfo (for all the Cells)	Operator-defined access category definitions IEI in	Result	
		EF <sub>UAC_AIC</sub>	EF <sub>ACC</sub> (Byte 1 b8-b4)	Cell Id of	PLMN-identity (MCC/MNC)		1 <sup>st</sup> REGISTRATION ACCEPT, 2 <sup>nd</sup> REGISTRATION ACCEPT	MO Data call 1 successful?	MO Data call 2 successful?
1.1	7,33	0x00 00 00 00	00000	Cell A	246 / 081	Not Present	ODAC_definitions1(0), ODAC_definitions2(1,16)	Yes	Yes
1.2	7,33	0x00 00 00 00	00000	Cell A	246 / 081	UAC_BarringInfo_Common (33,0x0000000'B)	ODAC_definitions1(0), ODAC_definitions2(1,16)	Yes	No
1.3	34,7	0x01 00 00 00	00000	Cell A	246 / 081	UAC_BarringInfo_Common2 (34,0x1000000'B, 50,0x1000000'B)	ODAC_definitions2(18,1), ODAC_definitions1(2)	No	Yes
1.4	7,63	0x01 00 00 00	00000	Cell B	244 / 081	UAC_BarringInfo_Common2 (63,0x0000000'B, 7,0x0100000'B)	ODAC_definitions1(3), ODAC_definitions2(31,18)	No	No
1.5	7,7	0x02 00 00 00	00000	Cell A	246 / 081	UAC_BarringInfo_Common (63,0x0100000'B)	ODAC_definitions1(31), ODAC - Not present	Yes	Yes
1.6	7,7	0x00 00 00 00	10000	Cell B	246 / 082	UAC_BarringInfo_Common (48,0x0010000'B)	ODAC_definitions1(16), ODAC - Not present	Yes	Yes
1.7	7,7	0x00 00 00 00	00100	Cell B	246 / 082	UAC_BarringInfo_Common2 (32,0x0000100'B, 34,0x0000100'B)	ODAC_definitions2(0,2), ODAC - Empty	Yes	Yes

1.8	7,7	0x00 00 00 00	00100	Cell B	246 / 082	UAC_BarringInfo_Common2 (50,0x0000100'B, 33,0x0000100'B)	ODAC_definitions2(18,1), ODAC - Not present	Yes	Yes
-----	-----	---------------	-------	--------	-----------	--	--	-----	-----

#### 5.4.12.4.3 Procedure

Procedure/steps to be repeated for all sequences listed in table 5.4.12-1:

Step	Direction	Action	Information	REQ	SA
1	TT	SIB1 of Cell A is transmitted as defined in the initial conditions for tests from table 5.4.12-1	Barring info in SIB1 is set as in table 5.4.12-1  See Annex A for the Methods UAC_BarringInfo_XXXXXX() in the table		
2	USER	Power UE on	The UE performs a SIM initialisation. (includes reading of EF <sub>UAC-AIC</sub> and EF <sub>ACC</sub> )	CR 1	A.2/1 OR A.2/2
3	UE > TT	Send REGISTRATION REQUEST			
4	TT > UE	Send REGISTRATION ACCEPT	1 <sup>st</sup> REGISTRATION ACCEPT with the Operator-Defined Access Category Definitions IEI as defined in the table 5.4.12-1.  For simplicity other signalling is not shown		

#### If 2<sup>nd</sup> Cell is Cell A as in table 5.4.12-1:

5	USER	Disable the UICC profile			
6	USER	Enable the UICC profile			

#### If 2<sup>nd</sup> Cell is Cell B as in table 5.4.12-1:

5	USER	Disable the UICC profile	Deactivate Cell A		
6	USER	Enable the UICC profile	Activate Cell B		

#### Common test steps

7	UE > TT	Send REGISTRATION REQUEST	Send to Cell A or B as in the Table 5.4.12-1		
8	USER	Send REGISTRATION ACCEPT	2 <sup>nd</sup> REGISTRATION ACCEPT with the Operator-Defined Access Category Definitions IEI as defined in the table 5.4.12-1.  For simplicity other signalling is not shown		

#### If 1<sup>st</sup> MO Data call is not allowed:

9	UE > TT	Attempt to set up 1 <sup>st</sup> MO Data call	Attempt to set up the MO Data call to DNN TestGp.rs1/S-NSSAI '01 01 01 01' using the MMI or EMMI.	CR 2 to CR 7	
---	---------	--	---	--------------------	--

#### If 1<sup>st</sup> MO Data call is allowed:

9	UE > TT	Set up MO Data call (PDU SESSION ESTABLISHMENT)	To set up the MO Data call to DNN TestGp.rs1/S-NSSAI '01 01 01 01' using the MMI or EMMI.	CR 2 to CR 7	
---	---------	---	---	--------------------	--

#### If 2<sup>nd</sup> MO Data call is not allowed:

10	UE > TT	Attempt to set up 2 <sup>nd</sup> MO Data call	Attempt to set up the MO Data call to DNN TestGp.rs2/S-NSSAI '01 01 01 02' using the MMI or EMMI	CR 2 to CR 7	
11	USER	End test sequence			

#### If 2<sup>nd</sup> MO Data call is allowed:

10	UE > TT	Set up MO Data call (PDU SESSION ESTABLISHMENT)	To set up the MO Data call to DNN TestGp.rs2/S-NSSAI '01 01 01 02' using the MMI or EMMI.	CR 2 to CR 7	
11	USER	End test sequence			

### 5.4.12.5 Acceptance criteria

For the Table 5.4.12-1

CR 1 is explicitly verified at step 2) by analysing the file READ commands for EF<sub>UAC-AIC</sub> and EF<sub>ACC</sub> during the USIM-Terminal initialisation procedure.

CR 2, through CR 7 are verified

- at steps 9) by analysing if the UE shall make a successful or not successful 1<sup>st</sup> MO Data call in accordance with the result indicated in the table if the step is applicable and
- at steps 10) by analysing if the UE shall make a successful or not successful 2<sup>nd</sup> MO Data call in accordance with the result indicated in the table if the step is applicable.

## 5.5 Handling of operator controlled features

### 5.5.1 Display of registered 5G PLMN name from USIM

#### 5.5.1.1 Definition and applicability

If the operator's decision, as indicated by the USIM, is that the ME shall use EF<sub>OPL5G</sub> in association with EF<sub>PNN</sub> or EF<sub>PNNI</sub> to display the Operator 5G PLMN name from USIM, then the ME shall be able to associate the prioritised list of Tracking Area Identity (TAI) identities for NG-RAN in EF<sub>OPL5G</sub> with the operator name contained in EF<sub>PNN</sub>. This prioritized list takes precedence over any network name stored within the ME's internal list and any network name received when registered to the PLMN, as defined by TS 24.501 [25].

#### 5.5.1.2 Conformance requirement

CR 1 EF<sub>OPL5G</sub> association with the EF<sub>PNN</sub> shall be performed by the USIM if service n°129 is available in EF<sub>UST</sub>.

CR 2 The ME shall display the correct Operator network name per 4.4.11.9 in TS 31.102 [19].

Reference:

- TS 31.102 [19], clauses 4.4.11.9.
- TS 24.008 [31], clause 10.5.3.5a

#### 5.5.1.3 Test purpose

The purpose of this test is to verify that the ME displays the 5G Operator PLMN name correctly for the following cases:

- 1) Entire range of TAC for a specific PLMN is configured in EF<sub>OPL5G</sub>;
- 2) Specific range of TAC for a specific PLMN is configured in EF<sub>OPL5G</sub>;
- 3) Specific TAC for a specific PLMN is configured in EF<sub>OPL5G</sub>.

#### 5.5.1.4 Method of tests

##### 5.5.1.4.1 Initial conditions

The values of the 5G-NR UICC as defined in clause 4.5.9 of the present document are used with the following exceptions:

EF<sub>UST</sub> (USIM Service Table)

Logically:

Service n°42:	Operator controlled PLMN selector with Access Technology	available
Service n°45:	PLMN Network Name	available

Service n°129: 5GS Operator PLMN List

available

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Binary:	xxxx xx1x	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxx1 xx1x	xxxx xxxx	xxxx xxxx
	<b>B9</b>	<b>B10</b>	<b>B11</b>	...	<b>B16</b>	<b>B17</b>		
	xxxx xxxx	xxxx xxxx	xx11 xxxx	...	xxx0 11xx	xxxx xxx1		

**EF<sub>OPLMNwACT</sub>** (Operator controlled PLMN selector with Access Technology)

Logically:

1<sup>st</sup> PLMN: 244 010 (MCC MNC), 1<sup>st</sup> ACT: NG-RAN  
 2<sup>nd</sup> PLMN: 244 020 (MCC MNC), 2<sup>nd</sup> ACT: NG-RAN  
 3<sup>rd</sup> PLMN: 244 030 (MCC MNC), 3<sup>rd</sup> ACT: NG-RAN  
 4<sup>th</sup> PLMN: 244 040 (MCC MNC), 4<sup>th</sup> ACT: NG-RAN  
 5<sup>th</sup> PLMN: 244 050 (MCC MNC), 5<sup>th</sup> ACT: NG-RAN  
 6<sup>th</sup> PLMN: 244 060 (MCC MNC), 6<sup>th</sup> ACT: NG-RAN  
 7<sup>th</sup> PLMN: 244 070 (MCC MNC), 7<sup>th</sup> ACT: NG-RAN  
 8<sup>th</sup> PLMN: 244 080 (MCC MNC), 8<sup>th</sup> ACT: NG-RAN

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	42	04	10	08	00	42	04	20
	<b>B9</b>	<b>B10</b>	<b>B11</b>	<b>B12</b>	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>
	08	00	42	04	30	08	00	42
	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	04	40	08	00	42	04	50	08
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>	<b>B31</b>	<b>B32</b>
	00	42	04	60	08	00	42	04
	<b>B33</b>	<b>B34</b>	<b>B35</b>	<b>B36</b>	<b>B37</b>	<b>B38</b>	<b>B39</b>	<b>B40</b>
	70	08	00	42	04	80	08	00

**EF<sub>OPLSG</sub>**

Record 1:

Logically:

MCC: 244,  
 MNC: 010,  
 TAC: Entire range,  
 PNN Record Identifier: 01

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10
Hex	42	04	10	00	00	00	FF	FF	FE	01

Record 2:

Logically:

MCC: 244,  
 MNC: 020,  
 TAC: 000003 - 000006,  
 PNN Record Identifier: 02

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10
Hex	42	04	20	00	00	03	00	00	06	02

Record 3:

Logically:

MCC: 244,  
MNC: 030,  
TAC: 000003,  
PNN Record Identifier: 02

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10
Hex	42	04	30	00	00	03	00	00	03	02

**EF<sub>PNN</sub>**

Record 1:

Logically:

Long name: PLMN 5G

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10
Hex	43	08	87	50	66	D3	09	AA	1D	01
	<b>B11</b>	<b>B12</b>	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>
	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF

Record 2:

Logically:

Long name: ABCD

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10
Hex	43	05	84	41	E1	90	08	FF	FF	FF
	<b>B11</b>	<b>B12</b>	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>
	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF

Record 3:

Logically:

Long name: CCCDDD

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10
Hex	43	07	86	C3	E1	90	48	24	02	FF
	<b>B11</b>	<b>B12</b>	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>
	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF

The NG-SS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/010/000001
- Access control: unrestricted

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and runs an initial activation.

#### 5.5.1.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE > TT	Send REGISTRATION REQUEST	In the registration type IE indicates: - "initial registration" - 5GS mobile identity information element type "SUCI"		
2	TT > UE	Send REGISTRATION ACCEPT	The REGISTRATION ACCEPT is sent with a 5G-GUTI		
3	UE > TT	Send REGISTRATION COMPLETE			
4	User	Wait 30 seconds	"PLMN 5G" is shown as Operator 5G PLMN name	CR 1 CR 2	
5	USER/TT	Power off/deactivate the UE			
6	TT	Stop RF output on the BCCH			
7	TT	Resume the RF output on the BCCH with: - TAI (MCC/MNC/TAC): 244/020/000004 - Access control: unrestricted			
8	UE	Runs activation			
9	UE > TT	Send REGISTRATION REQUEST	In the registration type IE indicates: - "initial registration" - 5GS mobile identity information element type "5G-GUTI"		
10	TT > UE	Send REGISTRATION ACCEPT	The REGISTRATION ACCEPT is sent with a 5G-GUTI		
11	UE > TT	Send REGISTRATION COMPLETE			
12	User	Wait 30 seconds	"ABCD" is shown as Operator 5G PLMN name	CR 1 CR 2	
13	USER/TT	Power off/deactivate the UE			
14	TT	Stop RF output on the BCCH			
15	TT	Resume the RF output on the BCCH with: - TAI (MCC/MNC/TAC): 244/030/000003 - Access control: unrestricted			
16	USER/TT	Run activation of the UE			
17	UE > TT	Send REGISTRATION REQUEST	In the registration type IE indicates: - "initial registration" - 5GS mobile identity information element type "5G-GUTI"		
18	TT > UE	Send REGISTRATION ACCEPT	The REGISTRATION ACCEPT is sent with a 5G-GUTI		
19	UE > TT	Send REGISTRATION COMPLETE			
20	User	Wait 30 seconds	"ABCD" is shown as Operator 5G PLMN name	CR 1 CR 2	
21	USER/TT	Power off/deactivate the UE, then run activation of the UE			

#### 5.5.1.4.3 Acceptance criteria

CR 1 can be implicitly verified. The conformance requirement is met if the expected Operator 5G PLMN name is shown in step 4), step 12) and step 17).

CR 2 shall be verified by checking the UE output for the Operator 5G PLMN name (e.g. on a display). The conformance requirement is met if the appropriate Operator 5G PLMN name is shown:

- "PLMN 5G" in step 4);
- "ABCD" in step 12);
- "ABCD" in step 17).

## 5.5.2 Display of registered 5G PLMN name from ME

### 5.5.2.1 Definition and applicability

If the operator's decision, as indicated by the USIM, is that the ME shall use  $EF_{OPL5G}$  in association with  $EF_{PNN}$  or  $EF_{PNN1}$  to display the Operator 5G PLMN name from ME or other sources, then the displayed network name will be either from the one stored within the ME's internal list or any network name received when registered to the PLMN, as defined by TS 24.501 [25].

### 5.5.2.2 Conformance requirement

CR 1  $EF_{OPL5G}$  ASSOCIATION with the  $EF_{PNN}$  shall be performed by the USIM if service n°129 is available in  $EF_{UST}$ .

CR 2 The ME shall display the correct Operator network name per 4.4.11.9 in TS 31.102 [19].

Reference:

- TS 31.102 [19], clauses 4.4.11.9.
- TS 24.008 [31], clause 10.5.3.5a

### 5.5.2.3 Test purpose

The purpose of this test is to verify that the ME displays the 5G Operator PLMN name correctly for the following cases:

- 1) ME registers to a TAI outside the range referenced in  $EF_{OPL5G}$ ;
- 2) ME registers to a TAI configured in  $EF_{OPL5G}$  and PNN record identified is set as 00.

### 5.5.2.4 Method of tests

#### 5.5.2.4.1 Initial conditions

The values of the 5G-NR UICC as defined in clause 4.5.9 of the present document are used with the following exceptions:

$EF_{UST}$

Logically:

Service n°42:	Operator controlled PLMN selector with Access Technology	available
Service n°45:	PLMN Network Name	available
Service n°129:	5GS Operator PLMN List	available

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Binary:	xxxx xx1x	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxx1 xx1x	xxxx xxxx	xxxx xxxx
	<b>B9</b>	<b>B10</b>	<b>B11</b>	...	<b>B16</b>	<b>B17</b>		
	xxxx xxxx	xxxx xxxx	xx11 xxxx	...	xxx0 11xx	xxxx xxx1		

$EF_{OPLMNwACT}$  (Operator controlled PLMN selector with Access Technology)

Logically:

1 <sup>st</sup> PLMN:	244 010 (MCC MNC),	1 <sup>st</sup> ACT:	NG-RAN
2 <sup>nd</sup> PLMN:	244 020 (MCC MNC),	2 <sup>nd</sup> ACT:	NG-RAN
3 <sup>rd</sup> PLMN:	244 030 (MCC MNC),	3 <sup>rd</sup> ACT:	NG-RAN
4 <sup>th</sup> PLMN:	244 040 (MCC MNC),	4 <sup>th</sup> ACT:	NG-RAN
5 <sup>th</sup> PLMN:	244 050 (MCC MNC),	5 <sup>th</sup> ACT:	NG-RAN
6 <sup>th</sup> PLMN:	244 060 (MCC MNC),	6 <sup>th</sup> ACT:	NG-RAN
7 <sup>th</sup> PLMN:	244 070 (MCC MNC),	7 <sup>th</sup> ACT:	NG-RAN

8<sup>th</sup> PLMN: 244 080 (MCC MNC), 8<sup>th</sup> ACT: NG-RAN

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	42	04	10	08	00	42	04	20
	B9	B10	B11	B12	B13	B14	B15	B16
	08	00	42	04	30	08	00	42
	B17	B18	B19	B20	B21	B22	B23	B24
	04	40	08	00	42	04	50	08
	B25	B26	B27	B28	B29	B30	B31	B32
	00	42	04	60	08	00	42	04
	B33	B34	B35	B36	B37	B38	B39	B40
	70	08	00	42	04	80	08	00

#### EF<sub>OPL5G</sub> (5GS Operator PLMN List)

Record 1:

Logically:

MCC: 244,  
MNC: 010,  
TAC: Entire range,  
PNN Record Identifier: 01

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10
Hex	42	04	10	00	00	00	FF	FF	FE	01

Record 2:

Logically:

MCC: 244,  
MNC: 020,  
TAC: 000003 - 000006,  
PNN Record Identifier: 02

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10
Hex	42	04	20	00	00	03	00	00	06	02

Record 3:

Logically:

MCC: 244,  
MNC: 030,  
TAC: 000005 - 000009,  
PNN Record Identifier: 00

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10
Hex	42	04	30	00	00	05	00	00	09	00

#### EF<sub>PNN</sub> (PLMN Network Name)

Record 1:

Logically:

Long name: PLMN 5G

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10
Hex	43	08	87	50	66	D3	09	AA	1D	01
	<b>B11</b>	<b>B12</b>	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>
	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF

Record 2:

Logically:

Long name: ABCD

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10
Hex	43	05	84	41	E1	90	08	FF	FF	FF
	<b>B11</b>	<b>B12</b>	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>
	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF

Record 3:

Logically:

Long name: CCCDDD

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10
Hex	43	07	86	C3	E1	90	48	24	02	FF
	<b>B11</b>	<b>B12</b>	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>
	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF

The TT (NG-SS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/020/000007
- Access control: unrestricted

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and runs an initial activation.

#### 5.5.2.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE > TT	Send REGISTRATION REQUEST	In the registration type IE indicates: - "initial registration" - 5GS mobile identity information element type "SUCI"		
2	TT > UE	Send REGISTRATION ACCEPT	The REGISTRATION ACCEPT is sent with a 5G-GUTI		
3	UE > TT	Send REGISTRATION COMPLETE			
4	USER	Wait 30 seconds	The ME shows: - MCC: "244" - MNC: "020"	CR 1 CR 2	
5	USER/TT	Power off/deactivate the UE			
6	TT	Stop RF output on the BCCH			
7	TT	Resume the RF output on the BCCH with: - TAI (MCC/MNC/TAC): 244/030/000006 - Access control: unrestricted			
8	USER/TT	Run activation of the UE			
9	UE > TT	Send REGISTRATION REQUEST	In the registration type IE indicates: - "initial registration"		

			- 5GS mobile identity information element type "5G-GUTI"		
10	TT > UE	Send REGISTRATION ACCEPT	The REGISTRATION ACCEPT is sent with a 5G-GUTI		
11	UE > TT	Send REGISTRATION COMPLETE			
12	USER	Wait 30 seconds	The ME shows: - MCC: "244" - MNC: "030"	CR 1 CR 2	
13	USER/TT	Power off/deactivate the UE			

#### 5.5.1.4.3 Acceptance criteria

CR 1 can be implicitly verified. The conformance requirement is met if the expected or a pre-configured Operator 5G PLMN name is shown in step 4) and step 12).

CR 2 shall be verified by checking the UE output for the Operator 5G PLMN name (e.g. on a display). The conformance requirement is met if the appropriate Operator 5G PLMN name is shown:

- MCC: "244", MNC: "020", but not: "PLMN 5G", "ABCD" or "CCCD" in step 4);
- MCC: "244", MNC: "030", but not: "PLMN 5G", "ABCD" or "CCCD" in step 12);

NOTE: MCC/MNC combinations are displayed as formatted by the ME manufacturer. MCC/MNC combinations with correct values are valid, independent from the formatting (e.g. with or without a separator). Different from the MCC/MNC combinations anything else configured by ME as Operator 5G PLMN name may be displayed.

## 5.6 Handling subscription identifier privacy for 5G - SUPI type in NAI format

### 5.6.1 SUCI calculation by ME using null scheme

#### 5.6.1.1 Definition and applicability

If the operator's decision is that ME shall calculate the SUCI, the home network operator shall provision a list of the Protection Scheme Identifiers in the USIM that the operator allows. The list of Protection Scheme Identifiers in the USIM may contain one or more Protection Scheme Identifiers in the order of their priority. The ME shall read the SUCI calculation information from the USIM, including the SUPI, the Home Network Public Key, the Home Network Public Key Identifier, and the list of Protection Scheme Identifiers. The ME shall select the protection scheme from its supported schemes that has the highest priority in the list obtained from the USIM.

The ME shall calculate the SUCI using the null-scheme if the highest priority of the protection schemes listed in the USIM is the null-scheme.

#### 5.6.1.2 Conformance requirement

CR 1 SUCI calculation procedure shall be performed by the ME if Service n°124 is available and Service n°125 is not available in EF<sub>UST</sub>

Reference:

- TS 31.102 [19], clause 5.3.47.

CR 2 SUPI is available in EF<sub>SUPL\_NAI</sub> if Service n°130 is available in EF<sub>UST</sub>

Reference:

- TS 31.102 [19], clauses 4.4.11.10 and 5.3.33.

CR 3 A subscriber identifier is in the form of a SUPI in NAI format

References:

- TS 31.102 [19], clause 4.4.11.10.

CR 4 The SUPI may contain:

- a NSI, used for private networks as defined in TS 22.261 [36] or
- a GLI and an operator identifier of the 5GC operator, used for supporting FN-BRGs, as further described in TS 23.316 [56] or
- a GCI and an operator identifier of the 5GC operator, used for supporting FN-CRGs and 5G-CRG, as further described in TS 23.316 [56].

References:

- TS 22.261 [36], clause 8.5;
- TS 23.316 [56], clause 4.7.3, 4.7.4, 4.7.8 and 4.7.9.

CR 5 As part of the SUCI calculation performed by the ME, the ME performs the reading procedure for  $EF_{SUCI\_Calc\_Info}$ .

Reference:

- TS 31.102 [19], clauses 4.4.11.8 and 5.3.47.

CR 6 The ME shall calculate the SUCI using the null-scheme if highest priority of the protection schemes listed in the USIM is the null-scheme.

Reference:

- TS 31.102 [19], clauses 5.3.47 and 5.3.51;
- TS 33.501 [24], clause Annex C.

### 5.6.1.3 Test purpose

The purpose of this test is to verify that:

- 1) the READ  $EF_{SUCI\_Calc\_Info}$ ,  $EF_{Routing\_Indicator}$  and  $EF_{SUPI\_NAI}$  commands are performed correctly by the ME.
- 2) the ME performs the SUCI calculation procedure using null-scheme.

### 5.6.1.4 Method of test

#### 5.6.1.4.1 Initial conditions

The values of the 5G-NR UICC – non-IMSI SUPI Type as defined in clause 4.5.10 of the present document are used with the following exception:

$EF_{SUCI\_Calc\_Info}$  (Subscription Concealed Identifier Calculation Information EF)

Logically:

Protection Scheme Identifier List data object:

Protection Scheme Identifier 1 – null-scheme

Key Index 1: 0

Protection Scheme Identifier 2 – ECIES scheme profile B

Key Index 2: 1

Protection Scheme Identifier 3 – ECIES scheme profile A

Key Index 3: 2

Home Network Public Key List data object:

Home Network Public Key 1 Identifier:27

Home Network Public Key 1:

04 72 DA 71 97 62 34 CE 83 3A 69 07 42 58 67 B8 2E 07 4D 44 EF 90 7D FB 4B 3E 21 C1 C2 25 6E  
 BC D1 5A 7D ED 52 FC BB 09 7A 4E D2 50 E0 36 C7 B9 C8 C7 00 4C 4E ED C4 F0 68 CD 7B F8 D3  
 F9 00 E3 B4

Home Network Public Key 2 Identifier: 30

Home Network Public Key 2:

5A 8D 38 86 48 20 19 7C 33 94 B9 26 13 B2 0B 91 63 3C BD 89 71 19 27 3B F8 E4 A6 F4 EE C0 A6  
 50

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	A0	06	00	00	02	01	01	02
	<b>B9</b>	<b>B10</b>	<b>B11</b>	<b>B12</b>	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>
	A1	6B	80	01	1B	81	41	04
	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	72	DA	71	97	62	34	CE	83
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>	<b>B31</b>	<b>B32</b>
	3A	69	07	42	58	67	B8	2E
	<b>B33</b>	<b>B34</b>	<b>B35</b>	<b>B36</b>	<b>B37</b>	<b>B38</b>	<b>B39</b>	<b>B40</b>
	07	4D	44	EF	90	7D	FB	4B
	<b>B41</b>	<b>B42</b>	<b>B43</b>	<b>B44</b>	<b>B45</b>	<b>B46</b>	<b>B47</b>	<b>B48</b>
	3E	21	C1	C2	25	6E	BC	D1
	<b>B49</b>	<b>B50</b>	<b>B51</b>	<b>B52</b>	<b>B53</b>	<b>B54</b>	<b>B55</b>	<b>B56</b>
	5A	7D	ED	52	FC	BB	09	7A
	<b>B57</b>	<b>B58</b>	<b>B59</b>	<b>B60</b>	<b>B61</b>	<b>B62</b>	<b>B63</b>	<b>B64</b>
	4E	D2	50	E0	36	C7	B9	C8
	<b>B65</b>	<b>B66</b>	<b>B67</b>	<b>B68</b>	<b>B69</b>	<b>B70</b>	<b>B71</b>	<b>B72</b>
	C7	00	4C	4E	ED	C4	F0	68
	<b>B73</b>	<b>B74</b>	<b>B75</b>	<b>B76</b>	<b>B77</b>	<b>B78</b>	<b>B79</b>	<b>B80</b>
	CD	7B	F8	D3	F9	00	E3	B4
	<b>B81</b>	<b>B82</b>	<b>B83</b>	<b>B84</b>	<b>B85</b>	<b>B86</b>	<b>B87</b>	<b>B88</b>
	80	01	1E	81	20	5A	8D	38
	<b>B89</b>	<b>B90</b>	<b>B91</b>	<b>B92</b>	<b>B93</b>	<b>B94</b>	<b>B95</b>	<b>B96</b>
	86	48	20	19	7C	33	94	B9
	<b>B97</b>	<b>B98</b>	<b>B99</b>	<b>B100</b>	<b>B101</b>	<b>B102</b>	<b>B103</b>	<b>B104</b>
	26	13	B2	0B	91	63	3C	BD
	<b>B105</b>	<b>B106</b>	<b>B107</b>	<b>B108</b>	<b>B109</b>	<b>B110</b>	<b>B111</b>	<b>B112</b>
	89	71	19	27	3B	F8	E4	A6
	<b>B113</b>	<b>B114</b>	<b>B115</b>	<b>B116</b>	<b>B117</b>			
	F4	EE	C0	A6	50			

The TT (NG-SS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/083/000001
- Access control: unrestricted.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and runs an initial activation.

#### 5.6.1.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	READ EF <sub>UST</sub>	(Evaluation of service settings)	(CR 1) (CR 2)	
2	UE	READ EF <sub>SUPI_NAI</sub> , EF <sub>SUCI_Calc_Info</sub> , EF <sub>Routing_indicator</sub>		CR 2 (CR 3) CR 4 CR 5	A.2/1 OR A.2/2
3	ME	Perform SUCI calculation	The ME performs a SUCI calculation using null scheme	(CR 1) (CR 6)	

4	UE > TT	Send REGISTRATION REQUEST	The UE sends a REGISTRATION REQUEST with 5GS registration type IE as "initial registration" and 5GS mobile identity information element type "SUCI"	CR 1 CR 3 CR 6	
5	TT > UE	Send REGISTRATION ACCEPT	The TT sends a REGISTRATION ACCEPT with 5G-GUTI		
6	UE > TT	Send REGISTRATION COMPLETE		CR 4	
<b>Optional step if CR 2, CR 4 and CR 5 verification cannot be performed at step 2)</b>					
7	UE	READ EF <sub>SUPI_NAI</sub> , EF <sub>SUCI_Calc_Info</sub> , EF <sub>Routing_indicator</sub>		CR 2 CR 3 CR 5	A.2/3

### 5.6.1.5 Acceptance criteria

CR 1, CR 3 and CR 6 are implicitly verified in step 4). The conformance requirements are met if the 5GS mobile identity IE in the REGISTRATION REQUEST performed in step 4) includes the following values:

- SUPI format: 2
- NAI format for the SUCI: type3.rid17.schid0.userid00-00-5E-00-53-00@5gc.mnc012.mcc345.3gppnetwork.org
- SUPI Type: 3
- Home Network Identifier: 5gc.mnc012.mcc345.3gppnetwork.org
- Routing indicator: 17
- Protection scheme ID: 00
- Home network public key ID: 0
- Scheme output: 00-00-5E-00-53-00

CR 2, CR 4 and CR 5 can be verified by a method explicitly verifying the correct execution of the READ commands on the listed EFs. The CRs are met if the READ procedure on EF<sub>SUCI\_Calc\_Info</sub>, EF<sub>Routing\_indicator</sub> and EF<sub>SUPI\_NAI</sub> has been executed as defined in [28], clause 14.1.1. This either is done with methods A.2/1 or A.2/2 in step 2) or in the optional step 7) with method A.2/3.

CR 4 is implicitly verified in step 6). The requirement is met if the registration can be completed successfully.

## 5.6.2 UE identification by SUCI during initial registration – SUCI calculation by USIM using profile A

### 5.6.2.1 Definition and applicability

If the operator's decision, indicated by the USIM, is that the USIM shall calculate the SUCI, then the USIM shall not give to the ME any parameter for the calculation of the SUCI including the Home Network Public Key Identifier, the Home Network Public Key, and the Protection Scheme Identifier. If the ME determines that the calculation of the SUCI, indicated by the USIM, shall be performed by the USIM, the ME shall delete any previously received or locally cached parameters for the calculation of the SUCI including the Routing Indicator, the Home Network Public Key Identifier, the Home Network Public Key and the Protection Scheme Identifier.

### 5.6.2.2 Conformance requirement

CR 1 SUCI calculation procedure shall be performed by the USIM if Services n°124 and n°125 are available in EF<sub>UST</sub>

Reference:

- TS 31.102 [19], clause 5.3.47.

CR 2 SUPI is available in EF<sub>SUPI\_NAI</sub> if Service n°130 is available in EF<sub>UST</sub>

Reference:

- TS 31.102 [19], clauses 4.4.11.10 and 5.3.33.

CR 3 A subscriber identifier is in the form of a SUPI in NAI format

References:

- TS 31.102 [19], clause 4.4.11.10.

CR 4 The SUPI may contain:

- a NSI, used for private networks as defined in TS 22.261 [36] or
- a GLI and an operator identifier of the 5GC operator, used for supporting FN-BRGs, as further described in TS 23.316 [56] or
- a GCI and an operator identifier of the 5GC operator, used for supporting FN-CRGs and 5G-CRG, as further described in TS 23.316 [56].

References:

- TS 22.261 [36], clause 8.5;
- TS 23.316 [56], clause 4.7.3, 4.7.4, 4.7.8 and 4.7.9.

CR 5 The ME shall use the GET IDENTITY command in SUCI context to retrieve the SUCI calculated by the USIM.

Reference:

- TS 31.102 [19], clause 5.3.48.

CR 6 This GET IDENTITY command shall be as per 7.5.2 in TS 31.102 [19].

Reference:

- TS 31.102 [19], clause 7.5.2.

CR 7 The USIM shall calculate the SUCI using the ECIES scheme profile A.

Reference:

- TS 31.102 [19], clauses 5.3.48;
- TS 33.501 [24], clause Annex C.

### 5.6.2.3 Test purpose

The purpose of this test is to verify that:

- 1) that the GET IDENTITY command is performed correctly by the ME.
- 2) the ME includes the SUCI received from the USIM within the GET IDENTITY response in the 5GS mobile identity IE.

### 5.6.2.4 Method of test

#### 5.6.2.4.1 Initial conditions

The values of the 5G-NR UICC – non-IMSI SUPI Type as defined in clause 4.5.10 of the present document are used with the following exception:

**EF<sub>UST</sub>** (USIM Service Table)

Services defined in Releases higher than Rel-16 might be available.

Logically:

Service n°125:	SUCI calculation by the USIM	available
----------------	------------------------------	-----------

Coding:

<b>Byte:</b>	<b>B1</b>	<b>B2</b>	<b>B3</b>	<b>B4</b>	<b>B5</b>	<b>B6</b>	<b>B7</b>	<b>B8</b>
Binary:	xx1x xx11	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxxx xxxx	xxxx xxxx	xxxx xxxx
	<b>B9</b>	<b>B10</b>	<b>B11</b>	...	<b>B16</b>	<b>B17</b>		
	xxxx xxxx	xxxx xxxx	xx11 xxxx	...	xxx1 111x	xxxx xxxx		

**EF<sub>SUPI\_NAI</sub>** (SUPI as Network Access Identifier)

Logically: verylongusername1@3gpp.com

SUPI Type: NSI

Username: verylongusername1

Realm: 3gpp.com

Coding:

<b>Byte</b>	<b>B1</b>	<b>B2</b>	<b>B3</b>	<b>B4</b>	<b>B5</b>	<b>B6</b>	<b>B7</b>	<b>B8</b>	<b>B9</b>	<b>B10</b>	<b>B11</b>	<b>B12</b>
Hex	80	1A	76	65	72	79	6C	6F	6E	67	75	73
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	65	72	6E	61	6D	65	31	40	33	67	70	70
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>								
	2E	63	6F	6D								

5G-NR UICC is configured with:

Protection Scheme Identifier: ECIES scheme profile A

Key Index: 1

Home Network Public Key Identifier: 30

Home Network Public Key:

<b>Byte:</b>	<b>B1</b>	<b>B2</b>	<b>B3</b>	<b>B4</b>	<b>B5</b>	<b>B6</b>	<b>B7</b>	<b>B8</b>	<b>B9</b>	<b>B10</b>	<b>B11</b>	<b>B12</b>
Hex	5A	8D	38	86	48	20	19	7C	33	94	B9	26
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	13	B2	0B	91	63	3C	BD	89	71	19	27	3B
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>	<b>B31</b>	<b>B32</b>				
	F8	E4	A6	F4	EE	C0	A6	50				

EF<sub>SUCL\_Calc\_Info</sub> (Subscription Concealed Identifier Calculation Information EF): Not available to the ME.

The TT (NG-SS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/083/000001
- Access control: unrestricted.

The NG-SS shall be configured with Home Network Private Key for profile A:

<b>Byte:</b>	<b>B1</b>	<b>B2</b>	<b>B3</b>	<b>B4</b>	<b>B5</b>	<b>B6</b>	<b>B7</b>	<b>B8</b>	<b>B9</b>	<b>B10</b>	<b>B11</b>	<b>B12</b>
Hex	C5	3C	22	20	8B	61	86	0B	06	C6	2E	54
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	06	A7	B3	30	C2	B5	77	AA	55	58	98	15
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>	<b>B31</b>	<b>B32</b>				
	10	D1	28	24	7D	38	BD	1D				

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and runs an initial activation.

## 5.6.2.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	READ EF <sub>UST</sub> , EF <sub>SUPL_NAI</sub>	(Evaluation of service settings)	(CR 1) (CR 2) (CR 3)	
2	ME > TT	Send GET IDENTITY	The ME sends a GET IDENTITY command with Identity Context in P2 as SUCI (0x01) to the 5G-NR UICC	CR 5 CR 6	A.2/1 OR A.2/2
2a	USIM	Perform SUCI calculation	The USIM shall calculate the SUCI using the ECIES scheme profile A	(CR 7)	
3	UE > TT	Send REGISTRATION REQUEST	The UE sends a REGISTRATION REQUEST with 5GS registration type IE as "initial registration" and 5GS mobile identity information element type "SUCI"	CR 1 CR 2 CR 3 CR 7	
4	TT > UE	Send REGISTRATION ACCEPT	The TT sends a REGISTRATION ACCEPT with 5G-GUTI		
5	UE > TT	Send REGISTRATION COMPLETE		CR 4	

## 5.6.2.5 Acceptance criteria

CR 1, CR 2, CR 3 and CR 7 are implicitly verified in step 3). The conformance requirements are met if the 5GS mobile identity IE in the REGISTRATION REQUEST performed in step 3) includes the following values:

- SUPI format: 1
- NAI format for the SUCI: type1.rid17.schid1.hnkey30.ecckey<ECC ephemeral public key>.cip<encryption of "verylongusername1">.mac<MAC tag value>@3gpp.com
- SUPI Type: 1
- Home Network Identifier: 3gpp.com
- Routing indicator: 17
- Protection scheme ID: 01
- Home network public key ID: 30
- Scheme output: ECC ephemeral public key, encryption of "verylongusername1" and MAC tag value

CR 5 and CR 6 can be verified by a method explicitly verifying the correct execution and contents of the GET IDENTITY command (A.2/1 or A.2/2).

CR 4 is met if the UE sends REGISTRATION COMPLETE message to the TT (NG-SS) in step 5).

CR 1, CR 2, CR 3 may optionally be verified in step 1) using explicit verification (A.2/1, A.2/2).

CR 7 may optionally be verified in step 2a) using explicit verification (A.2/1, A.2/2).

Example with test data from TS 33.501 [43] Annex C:

```
type1.rid17.schid1.hnkey30.ecckey977D8B2FDAA7B64AA700D04227D5B440630EA4EC50F9082273A26BB678C92222.cip8E358A1582ADB15322C10E515141D2039A.mac12E1D7783A97F1AC@3gpp.com
```

## 5.6.3 UE identification by SUCI during initial registration – SUCI calculation by USIM using profile B

## 5.6.3.1 Definition and applicability

If the operator's decision, indicated by the USIM, is that the USIM shall calculate the SUCI, then the USIM shall not give to the ME any parameter for the calculation of the SUCI including the Home Network Public Key Identifier, the Home Network Public Key, and the Protection Scheme Identifier. If the ME determines that the calculation of the SUCI, indicated by the USIM, shall be performed by the USIM, the ME shall delete any previously received or locally cached parameters for the calculation of the SUCI including the Routing Indicator, the Home Network Public Key Identifier, the Home Network Public Key and the Protection Scheme Identifier.

### 5.6.3.2 Conformance requirement

CR 1 SUCI calculation procedure shall be performed by the USIM if Services n°124 and n°125 are available in EF<sub>UST</sub>

Reference:

- TS 31.102 [19], clause 5.3.47.

CR 2 SUPI is available in EF<sub>SUPL\_NAI</sub> if Service n°130 is available in EF<sub>UST</sub>

Reference:

- TS 31.102 [19], clauses 4.4.11.10 and 5.3.33.

CR 3 A subscriber identifier is in the form of a SUPI in NAI format

References:

- TS 31.102 [19], clause 4.4.11.10.

CR 4 The SUPI may contain:

- a NSI, used for private networks as defined in TS 22.261 [36] or
- a GLI and an operator identifier of the 5GC operator, used for supporting FN-BRGs, as further described in TS 23.316 [56] or
- a GCI and an operator identifier of the 5GC operator, used for supporting FN-CRGs and 5G-CRG, as further described in TS 23.316 [56].

References:

- TS 22.261 [36], clause 8.5;
- TS 23.316 [56], clause 4.7.3, 4.7.4, 4.7.8 and 4.7.9.

CR 5 The ME shall use the GET IDENTITY command in SUCI context to retrieve the SUCI calculated by the USIM.

Reference:

- TS 31.102 [19], clause 5.3.48.

CR 6 This GET IDENTITY command shall be as per 7.5.2 in TS 31.102 [19].

Reference:

- TS 31.102 [19], clause 7.5.2.

CR 7 The USIM shall calculate the SUCI using the ECIES scheme profile B.

Reference:

- TS 31.102 [19], clauses 5.3.48;
- TS 33.501 [24], clause Annex C.

### 5.6.3.3 Test purpose

The purpose of this test is to verify that:

- 1) that the GET IDENTITY command is performed correctly by the ME.
- 2) the ME includes the SUCI received from the USIM within the GET IDENTITY response in the 5GS mobile identity IE.

### 5.6.3.4 Method of test

#### 5.6.3.4.1 Initial conditions

The values of the 5G-NR UICC – non-IMSI SUPI Type as defined in clause 4.5.10 of the present document are used with the following exception:

#### EF<sub>UST</sub> (USIM Service Table)

Services defined in Releases higher than Rel-16 might be available.

Logically:

Service n°125: SUCI calculation by the USIM available

Coding:

Byte:	B1	B2	B3	B4	B5	B6	B7	B8
Binary:	xx1x xx11	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxxx xxxx	xxxx xxxx	xxxx xxxx
	B9	B10	B11	...	B16	B17		
	xxxx xxxx	xxxx xxxx	xx11 xxxx	...	xxx1 111x	xxxx xxxx		

#### EF<sub>SUPI\_NAI</sub> (SUPI as Network Access Identifier)

Logically: verylongusername1@3gpp.com

SUPI Type: NSI

Username: verylongusername1

Realm: 3gpp.com

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	80	1A	76	65	72	79	6C	6F	6E	67	75	73
	B13	B14	B15	B16	B17	B18	B19	B20	B21	B22	B23	B24
	65	72	6E	61	6D	65	31	40	33	67	70	70
	B25	B26	B27	B28								
	2E	63	6F	6D								

5G-NR UICC is configured with:

Protection Scheme Identifier: ECIES scheme profile B

Key Index: 1

Home Network Public Key Identifier: 27

Home Network Public Key:

Byte:	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	04	72	DA	71	97	62	34	CE	83	3A	69	07
	B13	B14	B15	B16	B17	B18	B19	B20	B21	B22	B23	B24
	42	58	67	B8	2E	07	4D	44	EF	90	7D	FB
	B25	B26	B27	B28	B29	B30	B31	B32	B33	B34	B35	B36
	4B	3E	21	C1	C2	25	6E	BC	D1	5A	7D	ED
	B37	B38	B39	B40	B41	B42	B43	B44	B45	B46	B47	B48
	52	FC	BB	09	7A	4E	D2	50	E0	36	C7	B9
	B49	B50	B51	B52	B53	B54	B55	B56	B57	B58	B59	B60
	C8	C7	00	4C	4E	ED	C4	F0	68	CD	7B	F8
	B61	B62	B63	B64	B65							
	D3	F9	00	E3	B4							

EF<sub>SUCI\_Calc\_Info</sub> (Subscription Concealed Identifier Calculation Information EF): Not available to the ME.

The TT (NG-SS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/083/000001
- Access control: unrestricted.

The NG-SS shall be configured with Home Network Private Key for profile B:

<b>Byte:</b>	<b>B1</b>	<b>B2</b>	<b>B3</b>	<b>B4</b>	<b>B5</b>	<b>B6</b>	<b>B7</b>	<b>B8</b>	<b>B9</b>	<b>B10</b>	<b>B11</b>	<b>B12</b>
Hex	F1	AB	10	74	47	7E	BC	C7	F5	54	EA	1C
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	5F	C3	68	B1	61	67	30	15	5E	00	41	AC
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>	<b>B31</b>	<b>B32</b>				
	44	7D	63	01	97	5F	EC	DA				

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and runs an initial activation.

#### 5.6.3.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	READ EF <sub>UST</sub> , EF <sub>SUPL_NAI</sub>	(Evaluation of service settings)	(CR 1) (CR 2) (CR 3)	
2	ME > TT	Send GET IDENTITY	The ME sends a GET IDENTITY command with Identity Context in P2 as SUCI (0x01) to the 5G-NR UICC	CR 5 CR 6	A.2/1 OR A.2/2
2a	USIM	Perform SUCI calculation	The USIM shall calculate the SUCI using the ECIES scheme profile B	(CR 7)	
3	UE > TT	Send REGISTRATION REQUEST	The UE sends a REGISTRATION REQUEST with 5GS registration type IE as "initial registration" and 5GS mobile identity information element type "SUCI"	CR 1 CR 2 CR 3 CR 7	
4	TT > UE	Send REGISTRATION ACCEPT	The TT sends a REGISTRATION ACCEPT with 5G-GUTI		
5	UE > TT	Send REGISTRATION COMPLETE		CR 4	

#### 5.6.3.5 Acceptance criteria

CR 1, CR 2, CR 3 and CR 7 are implicitly verified in step 3). The conformance requirements are met if the 5GS mobile identity IE in the REGISTRATION REQUEST performed in step 3) includes the following values:

- SUPI format: 1
- NAI format for the SUCI: type1.rid17.schid2.hnkey27.ecckey<ECC ephemeral public key>.cip<encryption of "verylongusername1">.mac<MAC tag value>@3gpp.com
- SUPI Type: 1
- Home Network Identifier: 3gpp.com
- Routing indicator: 17
- Protection scheme ID: 02
- Home network public key ID: 27
- Scheme output: ECC ephemeral public key, encryption of "verylongusername1" and MAC tag value

CR 5 and CR 6 can be verified by a method explicitly verifying the correct execution and contents of the GET IDENTITY command (A.2/1 or A.2/2).

CR 4 is met if the UE sends REGISTRATION COMPLETE message to the TT (NG-SS) in step 5).

CR 1, CR 2, CR 3 may optionally be verified in step 1) using explicit verification (A.2/1, A.2/2).

CR 7 may optionally be verified in step 2a) using explicit verification (A.2/1, A.2/2).

Example with test data from TS 33.501 [43] Annex C:

```
type1.rid17.schid2.hnkey27.ecckey03759BB22C563D9F4A6B3C1419E543FC2F39D6823F02A9D71162B393
99218B244B.cipBE22D8B9F856A52ED381CD7EAF4CF2D525.mac3CDDC61A0A7882EB@3gpp.com
```

## 5.6.4 UE identification after SUPI is changed

### 5.6.4.1 Definition and applicability

A globally unique temporary user identity for 5GS-based services, the 5G globally unique temporary identity (5G-GUTI), is used for identification within the signalling procedures. A UE supporting N1 mode includes a valid 5G-GUTI, if any is available, in the REGISTRATION REQUEST and DEREGISTRATION REQUEST messages.

### 5.6.4.2 Conformance requirement

CR 1 The following 5GMM parameters shall be stored on the USIM if the corresponding file is present:

- 5G-Globally Unique Temporary Identifier (5G-GUTI);
- Last visited registered Tracking Area Identity in 5GS (TAI);
- 5GS update status;
- 5G NAS security context parameters from a full native 5G NAS security context.

NOTE: The presence and format of corresponding files on the USIM is specified in TS 31.102 [4].

Reference:

- TS 31.102 [19], clauses 4.4.11.2

CR 2 If the corresponding file is not present on the USIM, these 5GMM parameters are stored in a non-volatile memory in the ME together with the SUPI from the USIM ( $EF_{\text{SUPL\_NAI}}$ ). These 5GMM parameters can only be used if the SUPI from the USIM matches the SUPI stored in the non-volatile memory; else the UE shall delete the 5GMM parameters.

Reference:

- TS 24.501 [25], clauses 5.3.3, 5.5.1.2 and Annex C.

CR 3 The ME correctly performs the READ BINARY command on  $EF_{\text{SUPL\_NAI}}$ .

References:

- TS 31 101 [33], clause 11.1.3;
- ETSI TS 102 221 [8], clause 11.1.3 and 14.1.1.

CR 4 The ME shall use the GET IDENTITY command to retrieve the SUCI calculated by the USIM.

Reference:

- TS 31.102 [19], clause 5.3.48.

### 5.6.4.3 Test purpose

The purpose of this test is to verify that:

- 1) the READ  $EF_{\text{SUPL\_NAI}}$  command is performed correctly by the ME.
- 2) the ME deletes the 5GMM parameters from non-volatile memory in case SUPI is changed.
- 3) the GET IDENTITY command is performed correctly by the ME.
- 4) the ME includes the SUCI received from the USIM within GET IDENTITY response in the 5GS mobile identity IE.

## 5.6.4.4 Method of test

### 5.6.4.4.1 Initial conditions

The values of the 5G-NR UICC – non-IMSI SUPI Type as defined in clause 4.5.10 of the present document are used with the following exception:

EF<sub>UST</sub> (USIM Service Table)

Services defined in Releases higher than Rel-16 might be available.

Logically:

Service n°125: SUCI calculation by the USIM available

Coding:

Byte:	B1	B2	B3	B4	B5	B6	B7	B8
Binary:	xx1x xx11	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxxx xxxx	xxxx xxxx	xxxx xxxx
	B9	B10	B11	...	B16	B17		
	xxxx xxxx	xxxx xxxx	xx11 xxxx	...	xxx1 111x	xxxx xxxx		

5G-NR UICC is configured with:

Protection Scheme Identifier: null-scheme  
Key Index: 0

EF<sub>SUCL\_Calc\_Info</sub> (Subscription Concealed Identifier Calculation Information EF): Not available to the ME.

The TT (NG-SS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/083/000001
- Access control: unrestricted.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and runs an initial activation.

### 5.6.4.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	READ EF <sub>UST</sub> , EF <sub>SUPL_NAI</sub>	Evaluation of service settings. Verification of the READ command on EF <sub>SUPL_NAI</sub>	(CR 1) (CR 2) CR 3	A.2/1 OR A.2/2
2	ME > TT	Send GET IDENTITY	The ME sends a GET IDENTITY command with Identity Context in P2 as SUCI (0x01) to the 5G-NR UICC	CR 4	A.2/1 OR A.2/2
3	UE > TT	Send REGISTRATION REQUEST	The UE sends a REGISTRATION REQUEST with 5GS registration type IE as "initial registration"		
4	TT > UE	Send REGISTRATION ACCEPT	The REGISTRATION ACCEPT sent by the TT contains: - 5G-GUTI: "24408300010266436587" - 5GS TAI list with TAI with: - TAI: 244/083/000001	CR 1 CR 2	
5	UE > TT	Send REGISTRATION COMPLETE			
6	USER/TT	Power off/deactivate the UE, then run activation of the UE	Before power on the SUPI value is set to: 00-00-5E-00-53-00@5gc.mnc012.mcc345.3gppnetw.ork.org to 00-00-5E-00-53-01@5gc.mnc012.mcc345.3gppnetw.ork.org		

7	UE	READ EF <sub>SUPI_NAI</sub>	Verification of the READ command on EF <sub>SUPI_NAI</sub>	CR 3	A.2/1 OR A.2/2
8	ME > TT	Send GET IDENTITY	The ME sends a GET IDENTITY command with Identity Context in P2 as SUCI (0x01) to the 5G-NR UICC	CR 4	A.2/1 OR A.2/2
9	UE > TT	Send REGISTRATION REQUEST	The UE sends a REGISTRATION REQUEST with 5GS registration type IE as "initial registration" and 5GS mobile identity information element type "SUCI" with the new SUCI corresponding to the new SUPI value	CR 1 CR 2	

### 5.6.4.5 Acceptance criteria

CR 1 and CR 2 are implicitly verified in step 5). The conformance requirements are met if the REGISTRATION ACCEPT performed in step 4) contains:

- 5G GUTI: 24408300010266436587
- TAI: 244/083/000001

and the REGISTRATION REQUEST performed in step 10) includes the new SUCI:

- SUPI format: 2
- NAI format for the SUCI: type3.rid17.schid0.userid00-00-5E-00-53-01@5gc.mnc012.mcc345.3gppnetwork.org
- SUPI Type: 3
- Home Network Identifier: 5gc.mnc012.mcc345.3gppnetwork.org
- Routing indicator: 17
- Protection scheme ID: 00
- Home network public key ID: 0
- Scheme output: 00-00-5E-00-53-01

CR 3 can be explicitly verified. The requirement is met if the READ command on EF<sub>SUPI\_NAI</sub> is correctly performed in step 1) and step 7) (A.2/1 or A.2/2).

CR 4 can be verified by a method explicitly verifying the correct execution and contents of the GET IDENTITY command in step 2) and step 8) (A.2/1 or A.2/2).

CR 1 and CR 2 may optionally be verified in step 1) using explicit verification (A.2/1, A.2/2).

## 5.6.5 UE identification by SUCI during initial registration – SUCI calculation by ME using profile A

### 5.6.5.1 Definition and applicability

If the operator's decision is that the ME shall calculate the SUCI, the Home Network Operator shall provision a list of the Protection Scheme Identifiers that the operator allows in the USIM. The list of Protection Scheme Identifiers in the USIM may contain one or more Protection Scheme Identifiers in order of their priority. The ME shall read the SUCI calculation information from the USIM, including the SUPI, the Home Network Public Key, the Home Network Public Key Identifier, and the list of Protection Scheme Identifiers. The ME shall select the protection scheme from its supported schemes that has the highest priority in the list obtained from the USIM.

### 5.6.5.2 Conformance requirement

CR 1 SUCI calculation procedure shall be performed by the ME if Service n°124 is available and Service n°125 is not available in EF<sub>UST</sub>

Reference:

- TS 31.102 [19], clause 5.3.47.

CR 2 SUPI is available in EF<sub>SUPI\_NAI</sub> if Service n°130 is available in EF<sub>UST</sub>

Reference:

- TS 31.102 [19], clauses 4.4.11.10, 7.5.2 and Annex N.

CR 3 A subscriber identifier is in the form of a SUPI in NAI format

References:

- TS 31.102 [19], clause 4.4.11.10.

CR 4 The SUPI may contain:

- a NSI, used for private networks as defined in TS 22.261 [36] or
- a GLI and an operator identifier of the 5GC operator, used for supporting FN-BRGs, as further described in TS 23.316 [56] or
- a GCI and an operator identifier of the 5GC operator, used for supporting FN-CRGs and 5G-CRG, as further described in TS 23.316 [56].

References:

- TS 22.261 [36], clause 8.5;
- TS 23.316 [56], clause 4.7.3, 4.7.4, 4.7.8 and 4.7.9.

CR 5 As part of the SUCI calculation performed by the ME, the ME performs the reading procedure for EF<sub>SUCI\_Calc\_Info</sub>.

Reference:

- TS 31.102 [19], clause 4.11.8 and 5.3.47.

CR 6 The ME shall calculate the SUCI using the ECIES scheme profile A if highest priority of the protection schemes listed in the USIM is the ECIES scheme profile A.

Reference:

- TS 31.102 [19], clauses 5.3.47;
- TS 33.501 [24], clause Annex C.

### 5.6.5.3 Test purpose

The purpose of this test is to verify that:

- 1) that the READ EF<sub>SUCI\_Calc\_Info</sub>, EF<sub>Routing\_Indicator</sub> and EF<sub>SUPI\_NAI</sub> commands are performed correctly by the ME;
- 2) the ME performs SUCI calculation procedure using the profile with the highest priority (i.e. ECIES scheme profile A and the Home Network Public Key).

### 5.6.5.4 Method of test

#### 5.6.5.4.1 Initial conditions

The values of the 5G-NR UICC – non-IMSI SUPI Type as defined in clause 4.5.10 of the present document are used with the following exception:

**EF<sub>SUCI\_Calc\_Info</sub>** (Subscription Concealed Identifier Calculation Information EF)

Logically:

Protection Scheme Identifier List data object:

Protection Scheme Identifier 1 – ECIES scheme profile A

Key Index 1: 1  
 Protection Scheme Identifier 2 – ECIES scheme profile B  
 Key Index 2: 2  
 Protection Scheme Identifier 3 – null-scheme  
 Key Index 3: 0

Home Network Public Key List data object

Home Network Public Key 1 Identifier: 30  
 Home Network Public Key 1:  
 - 5A 8D 38 86 48 20 19 7C 33 94 B9 26 13 B2 0B 91 63 3C BD 89 71 19 27 3B F8 E4 A6 F4 EE C0 A6 50  
 Home Network Public Key 2 Identifier: 27  
 Home Network Public Key 2:  
 - 04 72 DA 71 97 62 34 CE 83 3A 69 07 42 58 67 B8 2E 07 4D 44 EF 90 7D FB 4B 3E 21 C1 C2 25 6E BC D1 5A 7D ED 52 FC BB 09 7A 4E D2 50 E0 36 C7 B9 C8 C7 00 4C 4E ED C4 F0 68 CD 7B F8 D3 F9 00 E3 B4

EF<sub>SUPI\_NAI</sub> (SUPI as Network Access Identifier)

Logically: verylongusername1@3gpp.com  
 SUPI Type: NSI  
 Username: verylongusername1  
 Realm: 3gpp.com

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	80	1A	76	65	72	79	6C	6F	6E	67	75	73
	B13	B14	B15	B16	B17	B18	B19	B20	B21	B22	B23	B24
	65	72	6E	61	6D	65	31	40	33	67	70	70
	B25	B26	B27	B28								
	2E	63	6F	6D								

The TT (NG-SS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/083/000001
- Access control: unrestricted.

The NG-SS shall be configured with Home Network Private Key for profile A:

Byte:	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	C5	3C	22	20	8B	61	86	0B	06	C6	2E	54
	B13	B14	B15	B16	B17	B18	B19	B20	B21	B22	B23	B24
	06	A7	B3	30	C2	B5	77	AA	55	58	98	15
	B25	B26	B27	B28	B29	B30	B31	B32				
	10	D1	28	24	7D	38	BD	1D				

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and runs an initial activation.

#### 5.6.5.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	READ EF <sub>UST</sub> , EF <sub>SUPI_NAI</sub> , EF <sub>Routing_Indicator</sub> and EF <sub>SUCI_Calc_Info</sub>	(Evaluation of service settings) Verification of the READ command and the EF contents	(CR 1) (CR 2) CR 5	A.2/1 OR A.2/2
1a	ME	Perform SUCI calculation	The ME shall calculate the SUCI using the ECIES scheme profile A	(CR 6)	

2	UE > TT	Send REGISTRATION REQUEST	The UE sends a REGISTRATION REQUEST with 5GS registration type IE as "initial registration" and 5GS mobile identity information element type "SUCI"	CR 1 CR 2 CR 3 CR 4 CR 6	
3	TT > UE	Send REGISTRATION ACCEPT	The TT sends a REGISTRATION ACCEPT with 5G-GUTI		
4	UE > TT	Send REGISTRATION COMPLETE			

### 5.6.5.5 Acceptance criteria

CR 1, CR 2, CR 3, CR 4 and CR 6 are implicitly verified in step 2). The conformance requirements are met if the 5GS mobile identity IE in the REGISTRATION REQUEST performed in step 2) includes the following values:

- SUPI format: 1
- NAI format for the SUCI: type1.rid17.schid1.hnkey30.ecckey<ECC ephemeral public key>.cip<encryption of "verylongusername1">.mac<MAC tag value>@3gpp.com
- SUPI Type: 1
- Home Network Identifier: 3gpp.com
- Routing indicator: 17
- Protection scheme ID: 01
- Home network public key ID: 30
- Scheme output: ECC ephemeral public key, encryption of "verylongusername1" and MAC tag value

CR 1 and CR 2 may be explicitly verified in step 1) if the READ commands on EF<sub>UST</sub> and EF<sub>SUPL\_NAI</sub> are analysed using either of the methods A.2/1 or A.2/2. CRs for explicit contents verification of EF<sub>Routing\_Indicator</sub> and EF<sub>SUCI\_Calc\_Info</sub> are not defined.

CR 5 is explicitly verified in step 1). The requirement is met if EF<sub>SUCI\_Calc\_Info</sub> is read (A.2/1 or A.2/2).

CR 6 may optionally be explicitly verified in step 1a) by any method tracing the ME behaviour.

Example with test data from TS 33.501 [43] Annex C:

```
type1.rid17.schid1.hnkey30.ecckey977D8B2FDAA7B64AA700D04227D5B440630EA4EC50F9082273A26BB678C92222.cip8E358A1582ADB15322C10E515141D2039A.mac12E1D7783A97F1AC@3gpp.com
```

## 5.6.6 UE identification by SUCI during initial registration – SUCI calculation by ME using profile B

### 5.6.6.1 Definition and applicability

If the operator's decision is that the ME shall calculate the SUCI, the Home Network Operator shall provision a list of the Protection Scheme Identifiers that the operator allows in the USIM. The list of Protection Scheme Identifiers in the USIM may contain one or more Protection Scheme Identifiers in order of their priority. The ME shall read the SUCI calculation information from the USIM, including the SUPI, the Home Network Public Key, the Home Network Public Key Identifier, and the list of Protection Scheme Identifiers. The ME shall select the protection scheme from its supported schemes that has the highest priority in the list obtained from the USIM.

### 5.6.6.2 Conformance requirement

CR 1 SUCI calculation procedure shall be performed by the ME if Service n°124 is available and Service n°125 is not available in EF<sub>UST</sub>

Reference:

- TS 31.102 [19], clause 5.3.47.

CR 2 SUPI is available in EF<sub>SUPL\_NAI</sub> if Service n°130 is available in EF<sub>UST</sub>

Reference:

- TS 31.102 [19], clauses 4.4.11.10, 7.5.2 and Annex N.

CR 3 A subscriber identifier is in the form of a SUPI in NAI format

References:

- TS 31.102 [19], clause 4.4.11.10.

CR 4 The SUPI may contain:

- a NSI, used for private networks as defined in TS 22.261 [36] or
- a GLI and an operator identifier of the 5GC operator, used for supporting FN-BRGs, as further described in TS 23.316 [56] or
- a GCI and an operator identifier of the 5GC operator, used for supporting FN-CRGs and 5G-CRG, as further described in TS 23.316 [56].

References:

- TS 22.261 [36], clause 8.5;
- TS 23.316 [56], clause 4.7.3, 4.7.4, 4.7.8 and 4.7.9.

CR 5 As part of the SUCI calculation performed by the ME, the ME performs the reading procedure for  $EF_{SUCI\_Calc\_Info}$ .

Reference:

- TS 31.102 [19], clause 4.11.8 and 5.3.47.

CR 6 The ME shall calculate the SUCI using the ECIES scheme profile B if highest priority of the protection schemes listed in the USIM is the ECIES scheme profile B.

Reference:

- TS 31.102 [19], clauses 5.3.47;
- TS 33.501 [24], clause Annex C.

### 5.6.6.3 Test purpose

The purpose of this test is to verify that:

- 1) that the READ  $EF_{SUCI\_Calc\_Info}$ ,  $EF_{Routing\_Indicator}$  and  $EF_{SUPI\_NAI}$  commands are performed correctly by the ME;
- 2) the ME performs SUCI calculation procedure using the profile with the highest priority (i.e. ECIES scheme profile B and the Home Network Public Key).

### 5.6.6.4 Method of test

#### 5.6.6.4.1 Initial conditions

The values of the 5G-NR UICC – non-IMSI SUPI Type as defined in clause 4.5.10 of the present document are used with the following exception:

$EF_{SUPI\_NAI}$  (SUPI as Network Access Identifier)

Logically:           verylongusername1@3gpp.com

SUPI Type:       NSI

Username:       verylongusername1

Realm:           3gpp.com

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	80	1A	76	65	72	79	6C	6F	6E	67	75	73
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	65	72	6E	61	6D	65	31	40	33	67	70	70
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>								
	2E	63	6F	6D								

The TT (NG-SS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/083/000001
- Access control: unrestricted.

The NG-SS shall be configured with Home Network Private Key for profile B:

Byte:	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	F1	AB	10	74	47	7E	BC	C7	F5	54	EA	1C
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	5F	C3	68	B1	61	67	30	15	5E	00	41	AC
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>	<b>B31</b>	<b>B32</b>				
	44	7D	63	01	97	5F	EC	DA				

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and runs an initial activation.

#### 5.6.6.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	READ EF <sub>UST</sub> , EF <sub>SUPL_NAI</sub> , EF <sub>Routing_Indicator</sub> and EF <sub>SUCL_Calc_Info</sub>	(Evaluation of service settings) Verification of the READ command and the EF contents	(CR 1) (CR 2) (CR 5)	A.2/1 OR A.2/2
1a	ME	Perform SUCI calculation	The ME shall calculate the SUCI using the ECIES scheme profile B	(CR 6)	
2	UE > TT	Send REGISTRATION REQUEST	The UE sends a REGISTRATION REQUEST with 5GS registration type IE as "initial registration" and 5GS mobile identity information element type "SUCI"	CR 1 CR 2 CR 3 CR 4 CR 6	
3	TT > UE	Send REGISTRATION ACCEPT	The TT sends a REGISTRATION ACCEPT with 5G-GUTI		
4	UE > TT	Send REGISTRATION COMPLETE			

#### 5.6.5.5 Acceptance criteria

CR 1, CR 2, CR 3, CR 4 and CR 6 are implicitly verified in step 2). The conformance requirements are met if the 5GS mobile identity IE in the REGISTRATION REQUEST performed in step 2) includes the following values:

- SUPI format: 1
- NAI format for the SUCI: type1.rid17.schid2.hnkey27.ecckey<ECC ephemeral public key>.cip<encryption of "verylongusername1">.mac<MAC tag value>@3gpp.com
- SUPI Type: 1
- Home Network Identifier: 3gpp.com
- Routing indicator: 17
- Protection scheme ID: 02
- Home network public key ID: 27
- Scheme output: ECC ephemeral public key, encryption of "verylongusername1" and MAC tag value

CR 1 and CR 2 may be explicitly verified in step 1) if the READ commands on EF<sub>UST</sub> and EF<sub>SUPL\_NAI</sub> are analysed using either of the methods A.2/1 or A.2/2. CRs for explicit contents verification of EF<sub>Routing\_Indicator</sub> and EF<sub>SUCL\_Calc\_Info</sub> are not defined.

CR 5 is explicitly verified in step 1). The requirement is met if EF<sub>SUCL\_Calc\_Info</sub> is read (A.2/1 or A.2/2).

CR 6 may optionally be explicitly verified in step 1a) by any method tracing the ME behaviour.

Example with test data from TS 33.501 [43] Annex C:

```
type1.rid17.schid2.hnkey27.ecckey03759BB22C563D9F4A6B3C1419E543FC2F39D6823F02A9D71162B393
99218B244B.cipBE22D8B9F856A52ED381CD7EAF4CF2D525.mac3CDDC61A0A7882EB@3gpp.com
```

## 6 Security related Tests

### 6.1 PIN handling

#### 6.1.1 Entry of PIN

##### 6.1.1.1 Definition and applicability

The PIN is a number used to authenticate the user to the UICC for security. Entry of the correct PIN allows PIN-protected data to be accessed over the UICC-Terminal interface.

##### 6.1.1.2 Conformance requirement

CR 1 Following insertion of the UICC and powering on the UE, the ME shall check the state of the PIN. If the PIN is enabled, the UE asks the user for PIN verification

CR 2 The VERIFY PIN function verifies the PIN presented by the ME to the UICC.

CR 3 Indication of a successful pin verification is presented to user.

Reference:

- ETSI TS 102 221 [8], clauses 9 and 11.1.9;
- TS 31.102 [19], clause 6;
- TS 22.030 [44], clause 6.6.1.

##### 6.1.1.3 Test purpose

The purpose of this test is to verify that:

- 1) the PIN verification procedure is performed by the UE correctly,
- 2) the basic public MMI string is supported.

##### 6.1.1.4 Method of test

###### 6.1.1.4.1 Initial conditions

The values of the Default UICC as defined in clause 4.5.2 of the present document are used.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case with PIN enabled.

###### 6.1.1.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	Run an initial activation			
2	UE > USER	Ask for the PIN to be entered	The ME indicates to the User that a PIN needs to be entered	CR 1	

3	USER > UE	Enter the sequence "0000#"	The UE initiates the VERIFY PIN command on the UICC and gets a confirmation from the UICC.	CR 2	A.2/1 OR A.2/2
4	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR 3	

### 6.1.1.5 Acceptance criteria

CR 1 is met if the ME asks the user for the PIN verification.

CR 2 can be explicitly verified at step 3) via supported options A.2/1 OR A.2/2, ensuring that the VERIFY PIN command is correctly sent via the ME to the UICC, with parameter P2 = "01".

CR 3 is verified on the ME. CR 3 is met if an indication is given to the user showing that this procedure was executed successfully, e.g. by displaying "OK".

## 6.1.2 Change of PIN

### 6.1.2.1 Definition and applicability

The PIN may be changed by the user, by entering the old and new PIN. The length of the PIN is between 4 and 8 digits.

### 6.1.2.2 Conformance requirement

CR1 The ME shall support the change of PIN procedure as defined in ETSI TS 102 221 [8], clause 11.1.10.

CR2 Indication of a successful pin change is presented to the user, and only the new pin shall be accepted for further PIN verification.

Reference:

- ETSI TS 102 221 [8], clauses 9 and 11.1.10;
- TS 31.102 [19], clause 6;
- TS 22.030 [44], clause 6.6.2.

### 6.1.2.3 Test purpose

The purpose of this test is to verify that:

- 1) the PIN substitution procedure is performed correctly by the UE,
- 2) the basic public MMI string is supported,
- 3) the old PIN shall no longer be accepted,
- 4) the new PIN shall be accepted.

### 6.1.2.4 Method of test

#### 6.1.2.4.1 Initial conditions

The values of the Default UICC as defined in clause 4.5.2 of the present document are used.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case with PIN enabled.

#### 6.1.2.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
------	-----------	--------	-------------	-----	----

1	UE	Run an initial activation			
2	USER > UE	Enter the sequence "0000#" when the UE is in the "PIN check" mode			
3	USER > UE	After USIM initialisation is completed, enter "***04*0000*01234567*01234567#" or initiate an equivalent MMI dependent procedure to change the PIN from '0000' to '01234567'	The UE initiates the CHANGE PIN command on the UICC and gets a confirmation from the UICC.	CR 1	A.2/1 OR A.2/2
4	UE > USER	An indication is given to the user showing whether this procedure was successful		CR 2	
5	UE	Deactivate and re-activate			
6	USER > UE	Enter the sequence "0000#" when the UE is in the "PIN check" mode	The UE verifies the entered PIN command on the UICC	CR 1	A.2/1 OR A.2/2
7	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be unsuccessful	CR 2	
8	UE	Deactivate and re-activate			
9	USER > UE	Enter the sequence "1234567#" when the UE is in the "PIN check" mode	The UE verifies the entered PIN command on the UICC and gets a confirmation from the UICC	CR 1	A.2/1 OR A.2/2
10	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR 2	

### 6.1.2.5 Acceptance criteria

CR 1 is explicitly verified at:

- step 3) by analysing the CHANGE PIN command;
- step 6) and step 9) by analysing the VERIFY PIN command;

sent via the ME to the UICC, with parameter P2 = "01" (via any supported option A.2/1 OR A.2/2).

CR 2 is verified at:

- step 4) on the ME by ensuring that an indication of a successful execution of the command and the acceptance of the new PIN is given;
- step 7) on the ME by ensuring that an indication of an unsuccessful execution of the command is given;
- step 10) on the ME by ensuring that an indication of a successful execution of the command is given.

### 6.1.3 Unblock PIN

#### 6.1.3.1 Definition and applicability

After three consecutive wrong entries of the PIN, the PIN shall become blocked. The Unblock PIN command is used to unblock the PIN. This function may be performed whether or not the PIN is blocked.

#### 6.1.3.2 Conformance requirement

CR 1 The UE shall support the Unblock PIN command, as defined in ETSI TS 102 221 [8], clause 11.1.13.

CR 2 Indication of a successful and unsuccessful unblock PIN is presented to user

CR 3 Only the new pin shall be accepted for further PIN verification.

CR 4 Indication of a successful and unsuccessful pin verification is presented to the user and only the new pin shall be accepted for further PIN verification.

Reference:

- ETSI TS 102 221 [8], clause 11.1.13;
- TS 31.102 [19], clause 6;
- TS 22.030 [44], clause 6.6.3.

### 6.1.3.3 Test purpose

The purpose of this test is to verify that:

- 1) the PIN unblocking procedure is performed correctly,
- 2) the basic public MMI string is supported,

### 6.1.3.4 Method of test

#### 6.1.3.4.1 Initial conditions

The values of the Default UICC as defined in clause 4.5.2 of the present document are used.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case with PIN enabled.

#### 6.1.3.4.2 Procedure

#### 6.1.3.4.2 Procedure

Sequence A:

Step	Direction	Action	Information	REQ	SA
1	UE	Run an initial activation			
2	USER > UE	Enter the correct PIN	(If test 6.1.2 has been executed before this probably is "01234567#")		
3	USER > UE	After USIM initialisation is completed, enter "***05*11111111*1234*1234#"	The UE initiates the UNBLOCK PIN command on the UICC and gets a confirmation from the UICC	CR 1	A.2/1 OR A2/2
4	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR 2	
5	UE	Deactivate and re-activate			
6	USER > UE	When the UE is in the "PIN check" mode, enter the new PIN: "1234#"	The UE verifies the entered PIN command on the UICC and gets a confirmation from the UICC	CR 3	A.2/1 OR A2/2
7	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR 4	
8	UE	Deactivate and re-activate the UE			
9	USER > UE	When the UE is in the "PIN check" mode, enter a wrong PIN three times	The UE verifies the entered PIN command on the UICC and gets a confirmation from the UICC	CR 3	A.2/1 OR A2/2
10	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be unsuccessful	CR 4	
11	USER > UE	Enter "***05*11111111*2468*2468#"	The UE verifies the entered UNBLOCK PIN command on the UICC and gets a confirmation from the UICC	CR 1	A.2/1 OR A2/2
12	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR 2	
13	UE	Deactivate and re-activate the UE			
14	USER > UE	When the UE is in the "PIN check" mode, enter the new PIN "2468#"	The UE verifies the entered PIN command on the UICC and gets a confirmation from the UICC	CR 3	A.2/1 OR A2/2

15	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR 4	
----	-----------	--	------------------------------------	------	--

Sequence B:

Step	Direction	Action	Information	REQ	SA
1	UE	Run an initial activation			
2	USER > UE	Enter the wrong PIN three times			
3	USER > UE	The user shall initiate an MMI dependent procedure to unblock the PIN with unblock code '11111111' and a new PIN '2468' ("**05*11111111*1234*1234#")	The UE initiates the UNBLOCK PIN command on the UICC and gets a confirmation from the UICC	CR 1	A.2/1 OR A2/2
4	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR 2	
5	UE	Deactivate and re-activate			
6	USER > UE	When the UE is in the "PIN check" mode, enter the new PIN: "2468#"	The UE verifies the entered PIN command on the UICC and gets a confirmation from the UICC	CR 3	A.2/1 OR A2/2
7	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR 4	

### 6.1.3.5 Acceptance criteria

Sequence A:

CR 1 is explicitly verified at step 3) and step 11) by analysing the UNBLOCK PIN command sent via the ME to the UICC, with parameter P2 = "01" (via any supported options A.2/1 OR A.2/2).

CR 2 is verified at step 4) and step 12) on the UE by ensuring UE shall give an indication following a successful execution of the command and new PIN is accepted.

CR 3 is explicitly verified at step 6), step 9) and step 14) by analysing the status word for both successful and unsuccessful PIN entry.

CR 4 is verified at step 7) and step 15) on the UE by ensuring UE shall give an indication of a successful execution of the command and PIN is accepted, at step 10) on UE by ensuring UE shall give an indication that execution of the command failed.

Sequence B:

CR 1 is explicitly verified at step 3) by analysing the UNBLOCK PIN command sent via the ME to the UICC, with parameter P2 = "01" (via any supported options A.2/1 OR A.2/2) after UE indicates that PIN has been blocked in step 2).

CR 2 is verified at step 4) on the ME by ensuring UE shall give an indication following a successful execution of the command and new PIN is accepted.

CR 3 is explicitly verified at step 6) by analysing the status word for successful PIN entry.

CR 4 is verified at step 7) the requirement is met if the UE gets an indication that the PIN is accepted after the successful entry of the correct PIN value.

## 6.1.4 Entry of PIN2

### 6.1.4.1 Definition and applicability

The PIN2 is a number used to authenticate the user to the UICC for security. Entry of the correct PIN2 allows PIN2-protected data to be accessed over the UICC-Terminal interface.

### 6.1.4.2 Conformance requirement

CR 1 Before allowing the access to PIN2 protected data, the ME shall ask the user for PIN2 verification. Only after presenting the PIN2, the user shall get access to these data.

CR 2 The VERIFY PIN function verifies the PIN2 presented by the ME to the UICC.

CR 3 Indication of a successful PIN2 verification is presented to the user.

Reference:

- ETSI TS 102 221 [8], clauses 9 and 11.1.9;
- TS 31.102 [19], clause 6;
- TS 22.030 [44], clause 6.6.1.

### 6.1.4.3 Test purpose

The purpose of this test is to verify that:

- 1) the PIN2 verification procedure is performed by the UE correctly.
- 2) the basic public MMI string is supported.

### 6.1.4.4 Method of test

#### 6.1.4.4.1 Initial conditions

The values of the Default UICC as defined in clause 4.5.2 of the present document are used.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case with PIN enabled.

NOTE: To perform the UPDATE FDN data (as described in the procedure below), the default FDN UICC may be used.

#### 6.1.4.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	Run an initial activation			
2	USER > UE	When the UE is in the "PIN check" mode, correct PIN shall be entered			
3	USER > UE	The access to a PIN2 protected data field shall be performed (e.g. UPDATE FDN)			
4	USER > UE	Enter the sequence "9999#" in "PIN2 check" mode	When the UE is in the "PIN2 check" mode, the sequence "9999#" shall be entered and the ME is verifying the command	CR 1	A.2/1 OR A2/2
5	UE > USER	An indication is given to the User showing whether this procedure was successful	This procedure shall be successful	CR 2	

### 6.1.4.5 Acceptance criteria

CR 1 is explicitly verified at step 4) via supported options A.2/1 OR A.2/2, ensuring that the VERIFY PIN command is correctly sent via the ME to the UICC, with parameter P2 = "81".

CR 2 is verified on the ME at step 5). CR 2 is met if an indication is given to the user showing that this procedure was executed successfully, e.g. by displaying "OK".

## 6.1.5 Change of PIN2

### 6.1.5.1 Definition and applicability

The PIN2 may be changed by the user, by entering the old and new PIN2. The length of the PIN2 is between 4 and 8 digits.

### 6.1.5.2 Conformance requirement

CR 1 The ME shall support the change of PIN2 procedure as defined in ETSI TS 102 221 [8], clause 11.1.10.

CR 2 Indication of a successful pin change is presented to user, and only the new pin shall be accepted for further PIN verification.

Reference:

- ETSI TS 102 221 [8], clauses 9 and 11.1.10;
- TS 31.102 [19], clause 6;
- TS 22.030 [44], clause 6.6.2.

### 6.1.5.3 Test purpose

The purpose of this test is to verify that:

- 1) the PIN2 substitution procedure is performed correctly by the UE.
- 2) the basic public MMI string is supported.
- 3) the old PIN shall no longer be accepted.
- 4) the new PIN shall be accepted.

### 6.1.5.4 Method of test

#### 6.1.5.4.1 Initial conditions

The values of the Default UICC as defined in clause 4.5.2 of the present document are used.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case with PIN enabled and runs an initial activation with the correct PIN entered.

NOTE: To perform the UPDATE FDN data (as described in the procedure below), the default FDN UICC may be used.

#### 6.1.5.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	USER > UE	After USIM initialisation enter "***042*9999*12345678*12345678#" or initiate an equivalent MMI dependent procedure to change the PIN2 from '9999' to '12345678'	The UE initiates the CHANGE PIN command for PIN 2 on the UICC and gets a confirmation from the UICC.	CR 1	A.2/1 OR A.2/2
2	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR 2	
3	UE	Deactivate and re-activate the UE			
4	USER > UE	Enter the correct PIN			
5	USER > UE	Access a PIN2 protected data field (e.g. perform an UPDATE FDN)			

6	USER > UE	When the UE is in the "PIN2 check" mode, enter "9999#"	An incorrect PIN2 "9999#" is entered and cannot be verified	CR 1	A.2/1 OR A2/2
7	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be unsuccessful	CR 2	
8	UE	Deactivate and re-activate the UE			
9	USER > UE	Enter the correct PIN			
10	USER > UE	Access a PIN2 protected data field (e.g. perform an UPDATE FDN)			
11	USER > UE	When the UE is in the "PIN2 check" mode, enter "12345678#"	The correct PIN2 is entered and shall be verified	CR 1	A.2/1 OR A2/2
12	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR 2	

### 6.1.5.5 Acceptance criteria

CR 1 is explicitly verified at:

- step 1) by analysing the CHANGE PIN command;
- step 6) and step 11) by analysing the VERIFY PIN sent via the ME to the UICC, with parameter P2 = "81" (via any supported options A.2/1 OR A.2/2).

CR 2 is verified (i) at:

- step 2). CR 2 is met if an indication is given to the user showing that this procedure was executed successfully, and new PIN is accepted, e.g. by displaying "OK";
- step 7). CR 2 is met if an indication is given to the user showing that the command failed;
- step 12). CR 2 is met if an indication is given to the user showing that the command was executed successfully.

## 6.1.6 Unblock PIN2

### 6.1.6.1 Definition and applicability

After three consecutive wrong entries of the PIN2, the PIN2 shall become blocked. The Unblock PIN2 command is used to unblock the PIN2. This function may be performed whether or not the PIN2 is blocked.

### 6.1.6.2 Conformance requirement

CR 1 The UE shall support the Unblock PIN2 command, as defined in ETSI TS 102 221 [8], clause 11.1.13.

CR 2 Indication of a successful unblock PIN2 is presented to user.

CR 3 Only the new PIN2 shall be accepted for further PIN2 verification.

CR 4 Indication of a successful and unsuccessful PIN2 verification is presented to user and only the new PIN2 shall be accepted for further PIN2 verification.

Reference:

- ETSI TS 102 221 [8], clauses 9 and 11.1.13;
- TS 31.102 [19], clause 6;
- TS 22.030 [44], clause 6.6.3.

### 6.1.6.3 Test purpose

The purpose of this test is to verify that:

- 1) the PIN2 unblocking procedure is performed correctly.
- 2) the basic public MMI string is supported.

### 6.1.6.4 Method of test

#### 6.1.6.4.1 Initial conditions

The values of the Default UICC as defined in clause 4.5.2 of the present document are used.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case with PIN/PIN2 enabled.

NOTE: To perform the UPDATE FDN data (as described in the procedure below), the default FDN UICC may be used.

#### 6.1.6.4.2 Procedure

Sequence A:

Step	Direction	Action	Information	REQ	SA
1	USER > UE	Run an initial activation of the UE and enter the correct PIN			
2	USER > UE	After USIM initialisation enter ***052*2222222*1234*1234#	The UE sends the UNBLOCK PIN command with parameter P2 = "81" and gets a confirmation from the UICC	CR 1	A.2/1 OR A.2/2
3	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR 2	
4	UE	Deactivate and re-activate the UE			
5	USER > UE	Access a PIN2 protected data field (e.g. UPDATE FDN)			
6	USER > UE	Enter the new PIN2: "1234#"	The correct new PIN2 is entered The UE verifies the entered PIN2 command on the UICC and gets a confirmation from the UICC	CR 3	A.2/1 OR A.2/2
7	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR 2 CR 3 CR 4	
8	UE	Deactivate and re-activate the UE			
9	USER	The access to a PIN2 protected data field shall be performed (e.g. UPDATE FDN)			
10	USER > UE	Enter a wrong PIN2 three times.	The UE verifies the entered PIN command on the UICC and gets a confirmation from the UICC	CR 3	A.2/1 OR A.2/2
11	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be unsuccessful	CR 4	
12	USER > UE	Enter ***052*2222222*3579*3579#.	The UE sends the UNBLOCK PIN command with parameter P2 = "81" to the UICC and gets a confirmation from the UICC	CR 1	A.2/1 OR A.2/2
13	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR 2	
14	UE	The UE is powered off and on and the correct PIN is entered			
15	USER > UE	The access to a PIN2 protected data field shall be performed (e.g. UPDATE FDN)			
16	USER > UE	Enter the new PIN2: "3579#"	The correct new PIN2 is entered The UE verifies the entered PIN2	CR 3	A.2/1 OR A.2/2

			command on the UICC and gets a confirmation from the UICC		
17	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR 4	

Sequence B:

Step	Direction	Action	Information	REQ	SA
1	UE	Run initial activation of the UE and enter the correct PIN			
2	USER > UE	Access a PIN2 protected data field (e.g. UPDATE FDN)			
3	USER > UE	Enter a wrong PIN2 three times.	The UE verifies the entered PIN command on the UICC and gets a confirmation from the UICC		
4	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be unsuccessful	CR 4	
5	USER > UE	The user shall initiate an MMI dependent procedure to unblock the PIN2 with unblock code '22222222' and a new PIN '3579'	The UE sends the UNBLOCK PIN command with correct parameters to the UICC and gets a confirmation from the UICC	CR 1	A.2/1 OR A.2/2
6	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR 2	
7	UE	The UE is powered off and on and the correct PIN is entered.			
8	USER	The access to a PIN2 protected data field shall be performed (e.g. UPDATE FDN)			
9	USER > UE	Enter the new PIN2: "3579#"	The UE sends the VERIFY PIN command with correct parameters to the UICC and gets a confirmation from the UICC	CR 3	A.2/1 OR A.2/2
10	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR 4	

### 6.1.6.5 Acceptance criteria

Sequence A:

CR 1 is explicitly verified at step 2) and step 12) by analysing the UNBLOCK PIN command sent via ME to the UICC, with parameter P2 = "81" (via any supported options A.2/1 OR A.2/2).

CR 2 is verified at step 3), step 7) and step 15) on the UE by ensuring UE shall give an indication of a successful execution of the command and new PIN2 is accepted.

CR 3 is implicitly verified at step 7) if the successful execution is indicated.

CR 3 can be explicitly verified in step 6), step 10) and step 16) for both successful and unsuccessful PIN2 entry.

CR 4 is verified at step 7) and step 17) on the UE by ensuring UE shall give an indication of a successful execution of the command and PIN2 is accepted, at step 11) on UE by ensuring UE shall give an indication that execution of the command failed.

Sequence B:

CR 1 is explicitly verified at step 5) by analysing the UNBLOCK PIN command sent via ME to the UICC, with parameter P2 = "81" (via any supported options A.2/1 OR A.2/2) after UE indicates that PIN has been blocked in step 4).

CR 2 is verified at step 6) on the UE by ensuring UE shall give an indication following a successful execution of the command and new PIN2 is accepted.

CR 3 is explicitly verified at step 8) for a successful PIN2 entry.

CR 4 is verified at step 4) on the UE by ensuring UE shall give an indication following an unsuccessful execution and at step 10) providing an information following a successful execution of the command that PIN2 is accepted.

## 6.1.7 Replacement of PIN

### 6.1.7.1 Definition and applicability

The Universal PIN may be used to replace a PIN used to authenticate the user to the UICC for security. In this case entry of the correct Universal PIN allows PIN-protected data to be accessed over the UICC-Terminal interface. ETSI TS 102 221 [8] defines the range of "01" to "08" as key reference of the PIN on a multi-verification capable UICC.

### 6.1.7.2 Conformance requirement

CR 1 The UE shall support the usage of the Universal PIN as replacement PIN and the replacement procedure as defined in ETSI TS 102 221 [8], clause 11.1.11.

CR 2 The UE shall support the procedure to disable the replacement defined in ETSI TS 102 221 [8], clause 11.1.12.

CR 3 Only the new pin shall be accepted for further PIN verification.

CR 4 Indication of a successful and unsuccessful pin verification is presented to the user and only the new pin shall be accepted for further PIN verification.

Reference:

- ETSI TS 102 221 [8], clauses 9, 11.1.11 and 11.1.12;
- TS 31.102 [19], clause 6.

### 6.1.7.3 Test purpose

The purpose of this test is to verify that:

- 1) the PIN replacement is supported by the UE correctly.
- 2) the PIN replacement procedure is performed by the UE correctly.
- 3) the procedure to disable the PIN replacement is performed by the UE correctly.

### 6.1.7.4 Method of test

#### 6.1.7.4.1 Initial conditions

The values of the Default UICC as defined in clause 4.5.2 of the present document are used.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case with PIN enabled.

#### 6.1.7.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	Run initial activation.			
2	USER > UE	When the UE is in the "PIN check" mode, the sequence "2468#" shall be entered.			
	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful		
3	USER > UE	The user shall initiate an MMI dependent procedure to replace the PIN by the Universal PIN.			
	UE > UICC	DISABLE PIN		CR 1	

	USIM > UE	Check Status word	This is verifiable only if A2/x is supported.		
4	UE > USER	The UE is powered off and on.			
5	USER > UE	When the UE is in the "PIN check" mode, the sequence "2468#" shall be entered.			
	UE > UICC	VERIFY PIN	This is verifiable only if A2/x is supported.	CR 3	A.2/1 OR A2/2
	USIM > UE	Check Status word			
	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be unsuccessful	CR 4	
6		The correct Universal PIN is entered.			
	UE > UICC	VERIFY PIN	This is verifiable only if A2/x is supported.	CR 3	A.2/1 OR A2/2
	USIM > UE	Check Status word			
	UE	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR 4	
7		Initiate an MMI dependent procedure to disable the replacement of the PIN by the Universal PIN			
	UE > UICC	ENABLE PIN	This is verifiable only if A2/x is supported.	CR 2	A.2/1 OR A2/2
	USIM > UE	Check Status word			
8	UE > USER	The UE is powered off and on.			
9	USER > UE	When the UE is in the "PIN check" mode, the sequence "2839#" shall be entered.			
	UE > UICC	VERIFY PIN	This is verifiable only if A2/x is supported.	CR 3	A.2/1 OR A2/2
	USIM > UE	Check Status word			
	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be unsuccessful	CR 4	
10	USER > UE	When the UE is in the "PIN check" mode correct PIN is entered.			
	UE > UICC	VERIFY PIN	This is verifiable only if A2/x is supported.	CR 3	A.2/1 OR A2/2
	USIM > UE	Check Status word			
	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR 4	

### 6.1.7.5 Acceptance criteria

CR 1 is explicitly verified at step 3 by analysing the DISABLE PIN command sent via the ME to the UICC, with parameter P1 = "91" and P2 = "01" (via any supported options A.2/1 OR A2/2).

CR 2 is explicitly verified at step 7) by analysing the ENABLE PIN command sent via the ME to the UICC, with parameter P2 = "01" (via any supported options A.2/1 OR A2/2)

CR 3 is explicitly verified at (i) step 5) by analysing the status word indicating that the PIN has not been accepted for the VERIFY PIN command sent by the ME to the UICC, with parameter P2 = "11", (ii) step 6) by analysing the status word indicating that the PIN has been accepted for the VERIFY PIN command sent by the ME to the UICC, with parameter P2 = "11", (iii) step 9) by analysing the status word indicating that the PIN has not been accepted for the VERIFY PIN command sent by the ME to the UICC, with parameter P2 = "01", (ii) step 10) by analysing the status word indicating that the PIN has been accepted for the VERIFY PIN command sent by the terminal to the UICC, with parameter P2 = "01".

CR 4 is verified (i) at step 5) and 9) on the UE by ensuring UE shall give an indication of an unsuccessful execution of the command and PIN is not accepted, (ii) at step 6) and 10) on the UE by ensuring UE shall give an indication of a successful execution of the command and PIN is accepted.

## 6.1.8 Change of Universal PIN

### 6.1.8.1 Definition and applicability

The Universal PIN may be changed by the user, by entering the old and new Universal PIN. The length of the Universal PIN is between 4 and 8 digits.

### 6.1.8.2 Conformance requirement

CR 1 The UE shall support the change of PIN procedure as defined in ETSI TS 102 221 [8], clause 11.1.10.

CR 2 Only the new pin shall be accepted for further PIN verification.

CR 3 Indication of a successful and unsuccessful pin verification is presented to the user and only the new pin shall be accepted for further PIN verification

Reference:

- ETSI TS 102 221 [8], clauses 9 and 11.1.10;
- TS 31.102 [19], clause 6.

### 6.1.8.3 Test purpose

The purpose of this test is to verify that the PIN substitution procedure is performed correctly by the ME.

### 6.1.8.4 Method of test

#### 6.1.8.4.1 Initial conditions

The values of the Default UICC as defined in clause 4.5.2 of the present document are used with the following exception:

- The Universal PIN is used as a replacement of the PIN.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case with PIN enabled and runs an initial activation with the correct Universal PIN entered.

#### 6.1.8.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	USER > UE	Initiate an MMI dependent procedure to change the Universal PIN to "01234567".	The UE sends the CHANGE PIN command with parameter P2 = "81"		
	UE > UICC	CHANGE PIN	This is verifiable only if A.2/x is supported.	CR 1	A.2/1 OR A.2/2
	USIM > UE	Check Status word			
2	UE	The UE is powered off and on.			
3	USER > UE	When the UE is in the "PIN check" mode, enter the new PIN: "2839#"			
	UE > UICC	VERIFY PIN	This is verifiable only if A.2/x is supported.	CR 2	A.2/1 OR A.2/2
	USIM > UE	Check Status word			
	UE	An indication is given to the user showing whether this procedure was successful	This procedure shall be unsuccessful	CR 3	
4	UE	The UE is powered off and on.			
	USER > UE	When the UE is in the "PIN check" mode, enter the new PIN: "01234567#"			
	UE > UICC	VERIFY PIN	This is verifiable only if A.2/x is supported.	CR 2	A.2/1 OR A.2/2
	USIM > UE	Check Status word			
UE	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR 3		

### 6.1.8.5 Acceptance criteria

CR 1 is explicitly verified at step 1) by analysing both the CHANGE PIN command sent via the ME to the UICC, with parameter P2 = "11" (via any supported options A.2/1 OR A.2/2) and the corresponding status word indicating that the new (Universal) PIN is accepted.

CR 2 is explicitly verified at (i) step 3) by analysing the status word indicating that the entered (Universal) PIN has not been accepted for the VERIFY PIN command sent by the ME to the UICC, and at (ii) step 5) by analysing the status

word indicating that the entered (Universal) PIN has been accepted for the VERIFY PIN command sent by the ME to the UICC.

CR 3 is verified at (i) step 3) on the UE by ensuring UE shall give an indication following an unsuccessful execution of the command and at (ii) step 5) on the UE by ensuring UE shall give an indication following a successful execution of the command.

## 6.1.9 Unblock Universal PIN

### 6.1.9.1 Definition and applicability

After three consecutive wrong entries of the PIN, the PIN shall become blocked. The Unblock PIN command is used to unblock the PIN. This function may be performed whether or not the PIN is blocked.

### 6.1.9.2 Conformance requirement

CR 1 The UE shall support the Unblock PIN command, as defined in ETSI TS 102 221 [8], clause 11.1.13.

CR 2 Only the new pin shall be accepted for further PIN verification.

CR 3 Indication of a successful and unsuccessful pin verification is presented to the user and only the new pin shall be accepted for further PIN verification

Reference:

- ETSI TS 102 221 [8], clause 11.1.13;
- TS 31.102 [19], clause 6.

### 6.1.9.3 Test purpose

To verify that the PIN unblocking procedure is performed correctly.

### 6.1.9.4 Method of test

#### 6.1.9.4.1 Initial conditions

The values of the Default UICC as defined in clause 4.5.2 of the present document are used.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case with PIN enabled.

#### 6.1.9.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	Run initial activation of the UE and enter the correct PIN			
2	USER > UE	The user shall initiate an MMI dependent procedure to unblock the Universal PIN and set the new Universal PIN value to "1234"			
	UE > UICC	UNBLOCK PIN	This is verifiable only if A.2/x is supported.	CR 1	A.2/1 OR A.2/2
	USIM > UE	Check Status word			
3	UE	The UE is powered off and on.			
4	USER > UE	Enter the new PIN: "1234#"			
	UE > UICC	VERIFY PIN	This is verifiable only if A.2/x is supported.	CR 2	A.2/1 OR A.2/2
	USIM > UE	Check Status word			
	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR 3	
5	UE	The UE is powered off and on.			
6	USER > UE	Enter a wrong PIN three times.			
	UE > UICC	VERIFY PIN		CR 2	

	USIM> UE	Check Status word	This is repeated 3 times, and is verifiable only if A.2/x is supported.		A.2/1 OR A.2/2
	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be unsuccessful	CR 3	
7	USER > UE	The user shall initiate an MMI dependent procedure to unblock the Universal PIN and set the new Universal PIN value to "2839".			
	UE > UICC	UNBLOCK PIN	This is verifiable only if A2/x is supported.	CR 1	A.2/1 OR A.2/2
	USIM> UE	Check Status word			
8	UE	The UE is powered off and on.			
9	USER > UE	Enter the new PIN: "2839#"			
	UE > UICC	VERIFY PIN	This is verifiable only if A.2/x is supported.	CR 2	A.2/1 OR A.2/2
	USIM > UE	Check Status word			
	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR 3	

### 6.1.9.5 Acceptance criteria

CR 1 is explicitly verified at step 2) and step 7) by analysing both the UNBLOCK PIN command sent via the ME to the UICC, with parameter P2 = "11" (via any supported options A.2/1 OR A.2/2) and the corresponding status word indicating that the new (Universal) PIN is accepted.

CR 2 is explicitly verified at (i) step 4) and step 9) by analysing the status word indicating that the entered (Universal) PIN has been accepted for the VERIFY PIN command sent by the ME to the UICC, and at (ii) step 6) by analysing each status word(s) indicating that the entered (Universal) PIN has not been accepted for 3 consecutive VERIFY PIN command sent by the ME to the UICC and after the third entry the (Universal) PIN has been blocked.

CR 3 is verified (i) at step 4) on UE by either ensuring UE shall give an indication of a successful execution of the command and new (Universal) PIN is accepted, (ii) at step 6) on UE by ensuring UE shall give an indication that execution of the command failed and (Universal) PIN is blocked, (iii) at step 9) on UE by ensuring UE shall give an indication of a successful execution of the command and new (Universal) PIN is accepted.

### 6.1.10 Entry of PIN on multi-verification capable UICCs

#### 6.1.10.1 Definition and applicability

The PIN is a number used to authenticate the user to the UICC for security. Entry of the correct PIN allows PIN-protected data to be accessed over the UICC-Terminal interface. ETSI TS 102 221 [8] defines the range of "01" to "08" as key reference of the PIN on a multi-verification capable UICC.

#### 6.1.10.2 Conformance requirement

CR 1 Following insertion of the UICC and powering on the UE, the ME shall check the state of the PIN. If the PIN is enabled, the UE asks the user for PIN verification.

CR 2 The VERIFY PIN function verifies the PIN presented by the ME to the UICC.

CR 3 Indication of a successful PIN verification is presented to user.

Reference:

- ETSI TS 102 221 [8], clauses 9 and 11.1.9;
- TS 31.102 [19], clause 6;
- TS 22.030 [44], clause 6.6.1.

#### 6.1.10.3 Test purpose

The purpose of this test is to verify that:

- 1) the PIN verification procedure is performed by the UE correctly.
- 2) the basic public MMI string is supported.
- 3) the UE supports key references in the range of "01" to "08" as PIN.

## 6.1.10.4 Method of test

### 6.1.10.4.1 Initial conditions

The values of the Default UICC as defined in clause 4.5.2 of the present document are used with the following exceptions:

The UICC shall be configured to use "07" as the key reference of the PIN and "87" as key reference of the PIN2 with the following values:

#### PIN

Key reference: 07

Logically:

8642

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	38	36	34	32	FF	FF	FF	FF

#### Unblock PIN

Key reference: 07

Logically:

64534231

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	36	34	35	33	34	32	33	31

#### PIN2

Key reference: 87

Logically:

9753

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	39	37	35	33	FF	FF	FF	FF

#### Unblock PIN2

Key reference: 87

Logically:

57687980

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	35	37	36	38	37	39	38	30

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case with PIN enabled.

#### 6.1.10.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	Run initial activation.			
2	USER > UE	When the UE is in the "PIN check" mode, the sequence "8642#" shall be entered		CR 1	
	UE > UICC	VERIFY PIN	This is verifiable only if A.2/x is supported.	CR 2	A.2/1 OR A.2/2
	USIM > UE	Check Status word			
	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR 3	

#### 6.1.10.5 Acceptance criteria

CR 1 is met if the UE asks the user for the PIN verification.

CR 2 can be explicitly verified at step 2) via supported options A.2/1 OR A.2/2, ensuring that the VERIFY PIN command is correctly sent via the ME to the UICC, with parameter P2 = "07".

CR 3 is verified on the UE. CR 3 is met if an indication is given to the user showing that this procedure was executed successfully, e.g. by displaying: "OK".

### 6.1.11 Change of PIN on multi-verification capable UICCs

#### 6.1.11.1 Definition and applicability

The PIN may be changed by the user, by entering the old and new PIN. The length of the PIN is between 4 and 8 digits. ETSI TS 102 221 [8] defines the range of "01" to "08" as key reference of the PIN on a multi-verification capable UICC.

#### 6.1.11.2 Conformance requirement

CR 1 The UE shall support the change of PIN procedure as defined in ETSI TS 102 221 [8], clause 11.1.10.

CR 2 Indication of a successful pin change is presented to user, and only the new pin shall be accepted for further PIN verification.

Reference:

- ETSI TS 102 221 [8], clauses 9 and 11.1.10;
- TS 31.102 [19], clause 6;
- TS 22.030 [44], clause 6.6.2.

#### 6.1.11.3 Test purpose

The purpose of this test is to verify that:

- 1) the PIN substitution procedure is performed correctly by the UE.
- 2) the basic public MMI string is supported.
- 3) the UE supports key references in the range of "01" to "08" as PIN.

#### 6.1.11.4 Method of test

##### 6.1.11.4.1 Initial conditions

The values of the Default UICC as defined in clause 4.5.2 of the present document are used with the following exceptions:

The UICC shall be configured to use "07" as the reference of the PIN and "87" as reference of the PIN2 with the following values:

**PIN**

Key reference: 07

Logically:

8642

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	38	36	34	32	FF	FF	FF	FF

**Unblock PIN**

Key reference: 07

Logically:

64534231

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	36	34	35	33	34	32	33	31

**PIN2**

Key reference: 87

Logically:

9753

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	39	37	35	33	FF	FF	FF	FF

**Unblock PIN2**

Key reference: 87

Logically:

57687980

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	35	37	36	38	37	39	38	30

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case with PIN enabled and runs an initial activation with the correct PIN entered.

**6.1.11.4.2 Procedure**

Step	Direction	Action	Information	REQ	SA
1	USER > UE	After USIM initialisation is completed, enter "***04*8642*01234567*01234567#" or initiate an equivalent MMI dependent procedure to change the PIN from '8642' to '01234567'			
	UE > UICC	CHANGE PIN	This is verifiable only if A2/x is supported.	CR 1	A.2/1 OR A.2/2
	UICC > UE	Check Status word			

	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure is successful	CR 2	
2	UE	The UE is powered off and on.			
3	USER > UE	When the UE is in the "PIN check" mode, the sequence "8642#" shall be entered.			
	UE > UICC	VERIFY PIN	This is verifiable only if A2/x is supported.	CR 1	A.2/1 OR A.2/2
	USIM > UE	Check Status word			
	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure is unsuccessful	CR 2	
4	UE	The UE is powered off and on.			
5	USER > UE	When the UE is in the "PIN check" mode, the sequence "01234567#" shall be entered.			
	UE > UICC	VERIFY PIN	This is verifiable only if A2/x is supported.	CR 1	A.2/1 OR A.2/2
	USIM > UE	Check Status word			
	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure is successful	CR 2	

### 6.1.11.5 Acceptance criteria

CR 1 is explicitly verified (i) at step 1) by analysing the CHANGE PIN command (ii) at step 3) and step 5) by analysing the VERIFY PIN sent via the ME to the UICC, with parameter P2 = "07" (via any supported options A.2/1 OR A.2/2).

CR 2 is verified (i) at step 1) on UE by either ensuring UE shall give an indication of a successful execution of the command and new PIN is accepted, (ii) at step 3) on UE by ensuring UE shall give an indication that execution of the command failed, (iii) at step 5) on UE by ensuring UE shall give an indication of a successful execution of the command.

## 6.1.12 Unblock PIN on multi-verification capable UICCs

### 6.1.12.1 Definition and applicability

After three consecutive wrong entries of the PIN, the PIN shall become blocked. The Unblock PIN command is used to unblock the PIN. This function may be performed whether or not the PIN is blocked. ETSI TS 102 221 [8] defines the range of "01" to "08" as key reference of the PIN on a multi-verification capable UICC.

### 6.1.12.2 Conformance requirement

CR 1 The UE shall support the Unblock PIN command, as defined in ETSI TS 102 221 [8], clause 11.1.13.

CR 2 Indication of a successful and unsuccessful unblock PIN is presented to user.

CR 3 Only the new pin shall be accepted for further PIN verification.

CR 4 Indication of a successful and unsuccessful pin verification is presented to the user and only the new pin shall be accepted for further PIN verification.

Reference:

- ETSI TS 102 221 [8], clauses 9 and 11.1.13;
- TS 31.102 [19], clause 6;
- TS 22.030 [44], clause 6.6.3.

### 6.1.12.3 Test purpose

The purpose of this test is to verify that:

- 1) the PIN unblocking procedure is performed correctly.
- 2) the basic public MMI string is supported.

3) the ME supports key references in the range of "01" to "08" as PIN.

#### 6.1.12.4 Method of test

##### 6.1.12.4.1 Initial conditions

The values of the Default UICC as defined in clause 4.5.2 of the present document are used with the following exceptions:

The UICC shall be configured to use "07" as the reference of the PIN and "87" as reference of the PIN2 with the following values:

##### **PIN**

Key reference: 07

Logically: 8642

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	38	36	34	32	FF	FF	FF	FF

##### **Unblock PIN**

Key reference: 07

Logically: 64534231

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	36	34	35	33	34	32	33	31

##### **PIN2**

Key reference: 87

Logically: 9753

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	39	37	35	33	FF	FF	FF	FF

##### **Unblock PIN2**

Key reference: 87

Logically: 57687980

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	35	37	36	38	37	39	38	30

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case with PIN enabled.

#### 6.1.12.4.2 Procedure

Sequence A:

Step	Direction	Action	Information	REQ	SA
------	-----------	--------	-------------	-----	----

1	UE	The ME is powered on and the correct PIN is entered.			
2	USER > UE	After USIM initialisation is completed, enter "***05*64534231*1234*1234#" .			
	UE > UICC	UNBLOCK PIN	This is verifiable only if A.2/x is supported.	CR 1	A.2/1 OR A.2/2
	USIM > UE	Check Status word			
	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR 2	
3	UE	The ME is powered off and on.			
4	USER > UE	When the UE is in the "PIN check" mode, enter the new PIN: "1234#" .			
	UE > UICC	VERIFY PIN	This is verifiable only if A.2/x is supported.	CR 3	A.2/1 OR A.2/2
	USIM > UE	Check Status word			
	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR 4	
5	UE	The ME is powered off and on.			
6	USER > UE	Enter a wrong PIN three times.			
	UE > UICC	VERIFY PIN	This is repeated 3x, and is verifiable only if A.2/x is supported.	CR 3	A.2/1 OR A.2/2
	USIM > UE	Check Status word			
	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be unsuccessful	CR 4	
7	USER > UE	Enter "***05*64534231*8642*8642#" .			
	UE > UICC	UNBLOCK PIN	This is verifiable only if A.2/x is supported.	CR 1	A.2/1 OR A.2/2
	USIM > UE	Check Status word			
	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR 2	
8	USER > UE	When the UE is in the "PIN check" mode, enter the new PIN: "8642#" .			
	UE > UICC	VERIFY PIN	This is verifiable only if A.2/x is supported.	CR3	A.2/1 OR A.2/2
	USIM > UE	Check Status word			
	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR4	

## Sequence B:

Step	Direction	Action	Information	REQ	SA
1	UE	The ME is powered on.			
2	USER > UE	Enter a wrong PIN three times.			
3	USER > UE	The user shall initiate a MMI dependent procedure to unblock the PIN with unblock code '64534231' and a new PIN '8642' ("***05*64534231*8642*8642#" ).			
	UE > UICC	UNBLOCK PIN	This is verifiable only if A.2/x is supported.	CR 1	A.2/1 OR A.2/2
	USIM > UE	Check Status word			
	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR 2	
4	UE	The ME is powered off and on.			
5	USER > UE	When the UE is in the "PIN check" mode, enter the new PIN: "8642#" .			
	UE > UICC	VERIFY PIN	This is verifiable only if A.2/x is supported.	CR 3	A.2/1 OR A.2/2
	USIM > UE	Check Status word			
	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR 4	

## 6.1.12.5 Acceptance criteria

## Sequence A:

CR 1 is explicitly verified at step 2) and step 7) by analysing the UNBLOCK PIN command sent via the ME to the UICC, with parameter P2 = "07" (via any supported options A.2/1 OR A.2/2).

CR 2 is verified at step 2) and step 7) on the UE by ensuring UE shall give an indication following a successful execution of the command and new PIN is accepted.

CR 3 is explicitly verified at step 4), step 6) and step 8) by analysing the status word for both successful and unsuccessful PIN entry.

CR 4 is verified at (i) step 4) and step 8) on the UE by ensuring UE shall give an indication of a successful execution of the command and PIN is accepted, (ii) at step) on ME by ensuring UE shall give an indication that execution of the command failed.

Sequence B:

CR 1 is explicitly verified at step 3) by analysing the UNBLOCK PIN command sent via the ME to the UICC, with parameter P2 = "07" (via any supported options A.2/1 OR A.2/2) after UE indicates that PIN has been blocked in step 2).

CR 2 is verified at step 3) on the UE by ensuring UE shall give an indication following a successful execution of the command and new PIN is accepted.

CR 3 is explicitly verified at step 5) by analysing the Status word for successful PIN entry.

CR 4 is verified at step 5) on the UE by ensuring UE shall give an indication following a successful execution of the command when a PIN is accepted.

## 6.1.13 Entry of PIN2 on multi-verification capable UICCs

### 6.1.13.1 Definition and applicability

The PIN2 is a number used to authenticate the user to the UICC for security. Entry of the correct PIN2 allows PIN2-protected data to be accessed over the UICC-Terminal interface. ETSI TS 102 221 [8] defines the range of "81" to "88" as key reference of the PIN2 on a multi-verification capable UICC.

### 6.1.13.2 Conformance requirement

CR 1 Before allowing the access to PIN2 protected data, the UE shall ask the user for PIN2 verification. Only after presenting the PIN2, the user shall get access to these data.

CR 2 The VERIFY PIN function verifies the PIN2 presented by the ME to the UICC.

CR 3 Indication of a successful pin2 verification is presented to the user.

Reference:

- ETSI TS 102 221 [8], clause 9 and clause 11.1.9;
- TS 31.102 [19], clause 6;
- TS 22.030 [44], clause 6.6.1.

### 6.1.13.3 Test purpose

The purpose of this test is to verify that:

- 1) the PIN2 verification procedure is performed by the ME correctly;
- 2) the basic public MMI string is supported;
- 3) the ME supports key references in the range of "81" to "88" as PIN2.

### 6.1.13.4 Method of test

#### 6.1.13.4.1 Initial conditions

The values of the Default UICC as defined in clause 4.5.2 of the present document are used with the following exceptions:

The UICC shall be configured to use "07" as the reference of the PIN and "87" as reference of the PIN2 with the following values:

**PIN**

Key reference: 07

Logically: 8642

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	38	36	34	32	FF	FF	FF	FF

**Unblock PIN**

Key reference: 07

Logically: 64534231

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	36	34	35	33	34	32	33	31

**PIN2**

Key reference: 87

Logically: 9753

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	39	37	35	33	FF	FF	FF	FF

**Unblock PIN2**

Key reference: 87

Logically:

57687980

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	35	37	36	38	37	39	38	30

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case with PIN enabled.

NOTE: To perform the UPDATE FDN data (as described in the procedure below), the default FDN UICC may be used. In this case the exceptions mentioned above shall apply.

#### 6.1.13.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
------	-----------	--------	-------------	-----	----

1	UE	Run initial activation.			
2	USER > UE	When the UE is in the "PIN check" mode, correct PIN shall be entered.			
3		The access to a PIN2 protected data field shall be performed (e.g. UPDATE FDN)			
4		When the UE is in the "PIN2 check" mode, the sequence "9753#" shall be entered.			
	UE	VERIFY PIN	This is verifiable only if A.2/x is supported	CR 1	A.2/1 OR A.2/2
	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR 2	

### 6.1.13.5 Acceptance criteria

CR 1 is explicitly verified at step 4 via supported options A.2/1 OR A.2/2, ensuring that the VERIFY PIN command is correctly sent via the ME to the UICC, with parameter P2 = "87".

CR 2 is verified on the UE. CR 2 is met if an indication is given to the user showing that this procedure was executed successfully, e.g. by displaying "OK".

## 6.1.14 Change of PIN2 on multi-verification capable UICCs

### 6.1.14.1 Definition and applicability

The PIN2 may be changed by the user, by entering the old and new PIN2. The length of the PIN2 is between 4 and 8 digits. ETSI TS 102 221 [8] defines the range of "81" to "88" as key reference of the PIN2 on a multi-verification capable UICC.

### 6.1.14.2 Conformance requirement

CR 1 The UE shall support the change of PIN2 procedure as defined in ETSI TS 102 221 [8], clause 11.1.10.

CR 2 Indication of a successful PIN2 change is presented to user, and only the new pin2 shall be accepted for further PIN verification.

Reference:

- ETSI TS 102 221 [8], clauses 9 and 11.1.10;
- TS 31.102 [19], clause 6;
- TS 22.030 [44], clause 6.6.2.

### 6.1.14.3 Test purpose

The purpose of this test is to verify that:

- 1) the PIN2 substitution procedure is performed correctly by the UE.
- 2) the basic public MMI string is supported.
- 3) the UE supports key references in the range of "81" to "88" as PIN2.

## 6.1.14.4 Method of test

### 6.1.14.4.1 Initial conditions

The values of the Default UICC as defined in clause 4.5.2 of the present document are used with the following exceptions:

The UICC shall be configured to use "07" as the reference of the PIN and "87" as reference of the PIN2 with the following values:

#### **PIN**

Key reference: 07

Logically:

8642

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	38	36	34	32	FF	FF	FF	FF

#### **Unblock PIN**

Key reference: 07

Logically:

64534231

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	36	34	35	33	34	32	33	31

#### **PIN2**

Key reference: 87

Logically:

9753

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	39	37	35	33	FF	FF	FF	FF

#### **Unblock PIN2**

Key reference: 87

Logically:

57687980

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	35	37	36	38	37	39	38	30

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case with PIN enabled and runs an initial activation with the correct PIN entered.

NOTE: To perform the UPDATE FDN data (as described in the procedure below), the default FDN UICC may be used. In this case the above-mentioned exceptions shall apply.

## 6.1.14.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	USER > UE	After USIM initialisation is completed, enter "***042*9753*12345678*12345678#" or initiate an equivalent MMI dependent procedure to change the PIN2 from '9753' to '12345678'			
	UE > UICC	CHANGE PIN	This is verifiable only if A.2/x is supported.	CR 1	A.2/1 OR A.2/2
	USIM > UE	Check Status word			
	UE	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR 2	
2	UE	UE is powered off and on and the correct PIN is entered.			
3		The access to a PIN2 protected data field shall be performed (e.g. UPDATE FDN)			
4	USER > UE	When the UE is in the "PIN2 check" mode, incorrect sequence "9753#" shall be entered.			
	UE > UICC	VERIFY PIN	This is verifiable only if A.2/x is supported.	CR 1	A.2/1 OR A.2/2
	USIM > UE	Check Status word			
	UE	An indication is given to the user showing whether this procedure was successful	This procedure shall be unsuccessful	CR 2	
5	UE	The UE is powered off and on.			
6		The access to a PIN2 protected data field shall be performed (e.g. UPDATE FDN)			
7	USER > UE	When the UE is in the "PIN check" mode, the sequence "12345678#" shall be entered.			
	UE > UICC	VERIFY PIN	This is verifiable only if A.2/x is supported.	CR 1	A.2/1 OR A.2/2
	USIM > UE	Check Status word			
	UE	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR 2	

## 6.1.14.5 Acceptance criteria

CR 1 is explicitly verified (i) at step 1 by analysing the CHANGE PIN command sent from ME to UICC with the parameter P2 set to "87" (ii) at step 4 and step 7 by analysing the VERIFY PIN sent via the ME to the UICC (via any supported options A.2/1 OR A.2/2).

CR 2 is verified (i) at step 1 on UE by ensuring UE shall give an indication of a successful execution of the command and new PIN is accepted, (ii) at step 4 on UE by ensuring UE shall give an indication that execution of the command failed, (iii) at step 7 on UE by ensuring UE shall give an indication of a successful execution of the command.

## 6.1.15 Unblock PIN2 on multi-verification capable UICCs

## 6.1.15.1 Definition and applicability

After three consecutive wrong entries of the PIN2, the PIN2 shall become blocked. The Unblock PIN2 command is used to unblock the PIN2. This function may be performed whether or not the PIN2 is blocked. ETSI TS 102 221 [8] defines the range of "81" to "88" as key reference of the PIN2 on a multi-verification capable UICC.

## 6.1.15.2 Conformance requirement

CR 1 The UE shall support the Unblock PIN2 command, as defined in ETSI TS 102 221 [8], clause 11.1.13.

CR 2 Indication of a successful unblock PIN2 is presented to user.

CR 3 Only the new pin2 shall be accepted for further PIN2 verification.

CR 4 Indication of a successful and unsuccessful pin2 verification is presented to user and only the new pin2 shall be accepted for further PIN2 verification.

Reference:

- ETSI TS 102 221 [8], clauses 9 and 11.1.13;
- TS 31.102 [19], clause 6;
- TS 22.030 [44], clause 6.6.3.

### 6.1.15.3 Test purpose

The purpose of this test is to verify that:

- 1) the PIN2 unblocking procedure is performed correctly.
- 2) the basic public MMI string is supported.
- 3) the UE supports key references in the range of "81" to "88" as PIN2.

### 6.1.15.4 Method of test

#### 6.1.15.4.1 Initial conditions

The values of the Default UICC as defined in clause 4.5.2 of the present document are used with the following exceptions:

The UICC shall be configured to use "07" as the reference of the PIN and "87" as reference of the PIN2 with the following values:

#### **PIN**

Key reference: 07

Logically:

8642

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	38	36	34	32	FF	FF	FF	FF

#### **Unblock PIN**

Key reference: 07

Logically:

64534231

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	36	34	35	33	34	32	33	31

#### **PIN2**

Key reference: 87

Logically:

9753

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	39	37	35	33	FF	FF	FF	FF

## Unblock PIN2

Key reference: 87

Logically:

57687980

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	35	37	36	38	37	39	38	30

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case with PIN enabled.

NOTE: To perform the UPDATE FDN data (as described in the procedure below), the default FDN UICC may be used. In this case the above-mentioned exceptions shall apply.

### 6.1.15.4.2 Procedure

Sequence A:

Step	Direction	Action	Information	REQ	SA
1	UE	Run initial activation of the UE and enter the correct PIN			
2	USER > UE	After USIM initialisation is completed, enter "***052*57687980*1234*1234#" .			
	UE > UICC	UNBLOCK PIN	This is verifiable only if A.2/x is supported.	CR 1	A.2/1 OR A.2/2
	USIM > UE	Check Status word			
	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR 2	
3	UE	The UE is powered off and on and the correct PIN is entered.			
4		The access to a PIN2 protected data field shall be performed (e.g. UPDATE FDN)			
5	USER > UE	Enter the new PIN2: "1234#" .			
	UE > UICC	VERIFY PIN	This is verifiable only if A.2/x is supported.	CR 3	A.2/1 OR A.2/2
	USIM > UE	Check Status word			
	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR 4	
6	UE	The UE is powered off and on and the correct PIN is entered.			
7		The access to a PIN2 protected data field shall be performed (e.g. UPDATE FDN)			
8	USER > UE	Enter a wrong PIN2 three times.			
	UE > UICC	VERIFY PIN	This is repeated 3 times, and is verifiable only if A.2/x is supported.	CR 3	A.2/1 OR A.2/2
	USIM > UE	Check Status word			
	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be unsuccessful	CR 4	
9	USER > UE	Enter "***052*57687980*9753*9753#" .			
	UE > UICC	UNBLOCK PIN	This is verifiable only if A.2/x is supported.	CR 1	A.2/1 OR A.2/2
	USIM > UE	Check Status word			
	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR 2	

10	UE	The UE is powered off and on and the correct PIN is entered.			
11		The access to a PIN2 protected data field shall be performed (e.g. UPDATE FDN)			
12	USER > UE	Enter the new PIN2: "9753#"			
	UE > UICC	VERIFY PIN	This is verifiable only if A.2/x is supported.	CR 3	A.2/1 OR A.2/2
	USIM > UE	Check Status word			
	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR 4	

Sequence B:

Step	Direction	Action	Information	REQ	SA
1	UE	Run initial activation of the UE and enter the correct PIN			
2	USER > UE	Enter a wrong PIN2 three times.			
3	USER > UE	The user shall initiate an MMI dependent procedure to unblock the PIN2 with unblock code '57687980' and a new PIN "9753"			
	UE > UICC	UNBLOCK PIN	This is verifiable only if A.2/x is supported.	CR 1	A.2/1 OR A.2/2
	USIM > UE	Check Status word			
	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR 2	
4	UE	The UE is powered off and on and the correct PIN is entered.			
5		The access to a PIN2 protected data field shall be performed (e.g. UPDATE FDN)			
6	USER > UE	Enter the new PIN2: "9753#"			
	UE > UICC	VERIFY PIN	This is verifiable only if A.2/x is supported.	CR 3	A.2/1 OR A.2/2
	USIM > UE	Check Status word			
	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR 4	

### 6.1.15.5 Acceptance criteria

Sequence A:

CR 1 is explicitly verified at step 2 and step 9 by analysing the UNBLOCK PIN command sent via ME to the UICC, with parameter P2 = "87" (via any supported options A.2/1 OR A.2/2).

CR 2 is verified at step 2 and step 9 on the UE by ensuring UE shall give an indication of a successful execution of the command and new PIN2 is accepted.

CR 3 is explicitly verified at step 5, step 8 and step 12 by analysing the Status word for both successful and unsuccessful PIN2 entry.

CR 4 is verified at (i) step 5 and step 12 on the UE by ensuring UE shall give an indication of a successful execution of the command and PIN2 is accepted, (ii) at step 8 on UE by ensuring UE shall give an indication that execution of the command failed.

Sequence B:

CR 1 is explicitly verified at step 3 by analysing the UNBLOCK PIN command sent via ME to the UICC, with parameter P2 = "87" (via any supported options A.2/1 OR A.2/2) after UE indicates that PIN has been blocked in step 2.

CR 2 is verified at step 3 on the UE by ensuring UE shall give an indication following a successful execution of the command and new PIN2 is accepted.

CR 3 is explicitly verified at step 6 by analysing the Status word for successful PIN2 entry.

CR 4 is verified at step 6 on the UE by ensuring UE shall give an indication following a successful execution of the command that PIN2 is accepted.

## 6.1.16 Replacement of PIN with key reference "07"

### 6.1.16.1 Definition and applicability

The Universal PIN may be used to replace a PIN used to authenticate the user to the UICC for security. In this case entry of the correct Universal PIN allows PIN-protected data to be accessed over the UICC-Terminal interface.

### 6.1.16.2 Conformance requirement

CR 1 The UE shall support the usage of the Universal PIN as replacement PIN and the replacement procedure as defined in ETSI TS 102 221 [8], clause 11.1.11.

CR 2 The UE shall support the procedure to disable the replacement defined in ETSI TS 102 221 [8], clause 11.1.12.

CR 3 Only the new pin shall be accepted for further PIN verification.

CR 4 Indication of a successful and unsuccessful pin verification is presented to the user and only the new pin shall be accepted for further PIN verification.

Reference:

- ETSI TS 102 221 [8], clauses 9, 11.1.11 and 11.1.12;
- TS 31.102 [19], clause 6.

### 6.1.16.3 Test purpose

The purpose of this test is to verify that:

- 1) the PIN replacement is supported by the UE correctly.
- 2) the PIN replacement procedure is performed by the UE correctly.
- 3) the procedure to disable the PIN replacement is performed by the UE correctly.
- 4) the UE supports key references in the range of "01" to "08" as PIN.

### 6.1.16.4 Method of test

#### 6.1.16.4.1 Initial conditions

The values of the Default UICC as defined in clause 4.5.2 of the present document are used with the following exceptions:

The UICC shall be configured to use "07" as the reference of the PIN and "87" as reference of the PIN2 with the following values:

#### **PIN**

Key reference: 07

Logically:

8642

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	38	36	34	32	FF	FF	FF	FF

#### **Unblock PIN**

Key reference: 07

Logically:

64534231

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	36	34	35	33	34	32	33	31

**PIN2**

Key reference: 87

Logically:

9753

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	39	37	35	33	FF	FF	FF	FF

**Unlock PIN2**

Key reference: 87

Logically:

57687980

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	35	37	36	38	37	39	38	30

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case with PIN enabled.

**6.1.16.4.2 Procedure**

Step	Direction	Action	Information	REQ	SA
1	UE	Run initial activation.			
2	USER > UE	When the UE is in the "PIN check" mode, the sequence "8642#" shall be entered.			
	UE > UICC	VERIFY PIN	This is verifiable only if A.2/x is supported.		A.2/1 OR A.2/2
	USIM > UE	Check Status word			
	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful		
3	USER > UE	The user shall initiate an MMI dependent procedure to replace the PIN by the Universal PIN.			
	UE > UICC	DISABLE PIN	This is verifiable only if A.2/x is supported.	CR 1	
	USIM > UE	Check Status word			
4	UE > USER	The UE is powered off and on.			
5	USER > UE	When the UE is in the "PIN check" mode, the sequence "8642#" shall be entered.			
	UE > UICC	VERIFY PIN	This is verifiable only if A.2/x is supported.	CR 3	A.2/1 OR A.2/2
	USIM > UE	Check Status word			
	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be unsuccessful	CR 4	
6		The correct Universal PIN is entered.			
	UE > UICC	VERIFY PIN	This is verifiable only if A.2/x is supported.	CR 3	A.2/1 OR A.2/2
	USIM > UE	Check Status word			

	UE	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR 4	
7		Initiate an MMI dependent procedure to disable the replacement of the PIN by the Universal PIN			
	UE > UICC	ENABLE PIN	This is verifiable only if A.2/x is supported.	CR 2	A.2/1 OR A.2/2
	USIM > UE	Check Status word			
8	UE > USER	The UE is powered off and on.			
9	USER > UE	When the UE is in the "PIN check" mode, the sequence "2839#" shall be entered.			
	UE > UICC	VERIFY PIN	This is verifiable only if A.2/x is supported.	CR 3	A.2/1 OR A.2/2
	USIM > UE	Check Status word			
	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be unsuccessful	CR 4	
10	USER > UE	When the UE is in the "PIN check" mode correct PIN is entered.			
	UE > UICC	VERIFY PIN	This is verifiable only if A.2/x is supported.	CR 3	A.2/1 OR A.2/2
	USIM > UE	Check Status word			
	UE > USER	An indication is given to the user showing whether this procedure was successful	This procedure shall be successful	CR 4	

### 6.1.16.5 Acceptance criteria

CR 1 is explicitly verified at step 3 by analysing the DISABLE PIN command sent via the ME to the UICC, with parameter P1 = "91" and P2 = "07" (via any supported options A.2/1 OR A.2/2).

CR 2 is explicitly verified at step 7 by analysing the ENABLE PIN command sent via the ME to the UICC, with parameter P2 = "07" (via any supported options A.2/1 OR A.2/2)

CR 3 is explicitly verified at (i) step 5 by analysing the status word indicating that the PIN has not been accepted for the VERIFY PIN command sent by the ME to the UICC, with parameter P2 = "11", (ii) step 6 by analysing the status word indicating that the PIN has been accepted for the VERIFY PIN command sent by the ME to the UICC, with parameter P2 = "11", (iii) step 9 by analysing the status word indicating that the PIN has not been accepted for the VERIFY PIN command sent by the ME to the UICC, with parameter P2 = "07", (ii) step 10 by analysing the status word indicating that the PIN has been accepted for the VERIFY PIN command sent by the ME to the UICC, with parameter P2 = "07".

CR 4 is verified (i) at step 5 and 9 by ensuring that the UE gives an indication of an unsuccessful execution of the command and PIN is not accepted, (ii) at step 6 and 10 by ensuring that the UE gives an indication of a successful execution of the command and PIN is accepted.

## 6.2 Fixed Dialling Numbers (FDN) handling

### 6.2.1 ME and USIM with FDN enabled, EF<sub>ADN</sub> readable and updateable

GERAN/UTRAN test - not applicable

### 6.2.2 ME and USIM with FDN disabled

GERAN/UTRAN test - not applicable

### 6.2.3 Enabling, disabling and updating of FDN

GERAN/UTRAN test - not applicable

### 6.2.4 ME and USIM with FDN enabled, EF<sub>ADN</sub> readable and updateable (Rel-4 and onwards)

GERAN/UTRAN test - not applicable

## 6.3 Void

## 6.4 Advice of charge (AoC) handling

### 6.4.1 AoC not supported by USIM

GERAN/UTRAN test - not applicable

### 6.4.2 Maximum frequency of ACM updating

GERAN/UTRAN test - not applicable

### 6.4.3 Call terminated when ACM greater than $ACM_{max}$

GERAN/UTRAN test - not applicable

### 6.4.4 Response codes of increase command of ACM

GERAN/UTRAN test - not applicable

---

## 7 PLMN related tests

### 7.1 FPLMN handling

#### 7.1.1 Adding FPLMN to the Forbidden PLMN list

GERAN/UTRAN test - not applicable

#### 7.1.2 UE updating forbidden PLMNs

GERAN/UTRAN test - not applicable

#### 7.1.3 UE deleting forbidden PLMNs

GERAN/UTRAN test - not applicable

#### 7.1.4 Adding FPLMN to the forbidden PLMN list when accessing E-UTRAN

##### 7.1.4.1 Definition and applicability

A list of forbidden PLMNs stored in the USIM and providing storage for at least 4 entries is managed by the UE. In automatic PLMN selection mode the UE controls registration attempts to appropriate networks with respect to this list of forbidden PLMNs. As a result of a registration reject with the cause "PLMN not allowed" the UE stores the PLMN which rejected the update request in the USIM.

##### 7.1.4.2 Conformance requirement

CR 1 In automatic PLMN selection mode the UE shall only attempt an ATTACH REQUEST during registration on E-UTRAN/EPS if it receives a BCCH containing a PLMN (MCC, MNC) that is not indicated in the  $EF_{FPLMN}$  in the USIM

Reference:

- TS 22.011 [18], clause 2.3;
- TS 31.102 [19], clauses 5.1.1 and 5.2.7.

CR 2 After receipt of an ATTACH REJECT message during registration on E-UTRAN/EPS with the EMM cause "PLMN not allowed" the ME shall update the EF<sub>FPLMN</sub> in the USIM.

Reference:

- TS 22.011 [18], clause 3.2.2 2;
- TS 31.102 [19], clauses 5.1.1 and 5.2.7

CR 3 After receipt of an ATTACH REJECT message during registration on E-UTRAN/EPS with the EMM cause "PLMN not allowed" the ME shall update the EF<sub>EPSLOCI</sub> in the USIM.

Reference:

- TS 24.301 [21], clause 5.5.1.2.5;
- TS 31.102 [19], clauses 5.1.2 and 4.2.9.1.

CR 4 After receipt of an ATTACH REJECT message during registration on E-UTRAN/EPS with the After registration on E-UTRAN/EPS the USIM shall contain the correct GUTI and TAI received by the UE.

Reference:

- TS 31.102 [19], clauses 5.1.2 and 4.2.9.1;
- TS 21.111 [20], clause 10.1.

### 7.1.4.3 Test purpose

The purpose of this test is to verify that:

- 1) in automatic PLMN selection mode the UE does not attempt to access PLMNs stored in EF<sub>FPLMN</sub> on the USIM;
- 2) the EF<sub>FPLMN</sub> is correctly updated by the ME after receipt of an ATTACH REJECT message with cause "PLMN not allowed" during registration;
- 3) the EF<sub>EPSLOCI</sub> has been correctly updated by the ME during registration.

### 7.1.4.4 Method of test

#### 7.1.4.4.1 Initial conditions

The values of the FDN UICC as defined in clause 4.5.3 of the present document are used with EF<sub>IMSI</sub> as defined in clause 4.6.2.

The defined UICC/USIM configuration defined for this test case shall be used and made available on the UE.

Ensure that the automatic PLMN selection mode is set and that the UE has installed and is using the UICC/USIM configuration defined for this test case and runs an initial activation when executing the test procedure.

#### 7.1.4.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	TT	Activate the RF output on the BCCH with: - TAI (MCC/MNC/TAC): 234/002/0001 - Access control: unrestricted	The UE does not send an ATTACH REQUEST message as the PLMN provided by the TT is listed in EF <sub>FPLMN</sub>	CR 1	
2	TT	Stop RF output on the BCCH	The UE starts a reselection procedure		

3	TT	Resume the RF output on the BCCH with: - TAI (MCC/MNC/TAC): 234/003/0001 - Access control: unrestricted	The UE does not send an ATTACH REQUEST message as the PLMN provided by the TT is it is listed in EF <sub>FPLMN</sub>	CR 1	
4	TT	Stop RF output on the BCCH	The UE starts a reselection procedure		
5	TT	Resume the RF output on the BCCH with: - TAI (MCC/MNC/TAC): 234/004/0001 - Access control: unrestricted	The UE does not send an ATTACH REQUEST message as the PLMN provided by the TT is it is listed in EF <sub>FPLMN</sub>	CR 1	
6	TT	Stop RF output on the BCCH	The UE starts a reselection procedure		
7	TT	Resume the RF output on the BCCH with: - TAI (MCC/MNC/TAC): 234/005/0001 - Access control: unrestricted	The UE does not send an ATTACH REQUEST message as the PLMN provided by the TT is it is listed in EF <sub>FPLMN</sub>	CR 1	
8	TT	Stop RF output on the BCCH	The UE starts a reselection procedure		
9	TT	Resume the RF output on the BCCH with: - TAI (MCC/MNC/TAC): 234/007/0001 - Access control: unrestricted	The UE tries to connect to the PLMN provided by the TT	CR 1	
10	UE > TT	Send RRC CONNECTION REQUEST / RRC CONNECTION REQUEST-NB	The TT responds with a RRC CONNECTION SETUP / RRC CONNECTION SETUP-NB		
11	UE > TT	Send RRC CONNECTION SETUP COMPLETE / RRC CONNECTION SETUP COMPLETE-NB			
12	UE > TT	Send ATTACH REQUEST	The TT performs an authentication and starts NAS integrity protection		
13	TT > UE	Send ATTACH REJECT message with cause 'PLMN not allowed'	The UE updates EF <sub>FPLMN</sub> The UE updates EF <sub>EPSLOCI</sub>	CR 2 CR 3	A.2/1 OR A.2/2
14	TT > UE	Send RRC CONNECTION RELEASE / RRC CONNECTION RELEASE-NB			
15	TT	Stop RF output on the BCCH			
16	UE	Disable signalling on RAN			
17	TT	Read out EF <sub>EPSLOCI</sub>	EF <sub>EPSLOCI</sub> content can be verified by the TT	CR 3	A.2/1 OR A.2/2
18	UE	Enable signalling on RAN	The UE starts a reselection procedure		
19	TT	Resume the RF output on the BCCH with: - TAI (MCC/MNC/TAC): 234/008/0001 - Access control: unrestricted	The UE tries to connect to the PLMN provided by the TT	CR 1	
20	UE > TT	Send RRC CONNECTION REQUEST / RRC CONNECTION REQUEST-NB	The TT responds with a RRC CONNECTION SETUP / RRC CONNECTION SETUP-NB		
21	UE > TT	Send RRC CONNECTION SETUP COMPLETE / RRC CONNECTION SETUP COMPLETE-NB			
22	UE > TT	Send ATTACH REQUEST	The TT performs an authentication and starts NAS integrity protection		
23	TT > UE	Send ATTACH ACCEPT message with: - TAI (MCC/MNC/TAC): 234/008/0001 - GUTI (as generated from TT)	The UE responds with an ATTACH COMPLETE message	CR 4	
	UE	Update EF <sub>EPSLOCI</sub>		CR 3	A.2/1 OR A.2/2
24	TT > UE	Send a RRC CONNECTION RELEASE / RRC CONNECTION RELEASE-NB			

#### 7.1.4.4 Acceptance criteria

CR 1 is met if the UE is not sending an ATTACH REQUEST in steps 1), 3), 5) and 7) but in step 9) and 19) as indicated by correctly interpreted EF<sub>FPLMN</sub> content. During test execution the TT shall provide status information related to the ATTACH REQUEST.

CR 2 shall be verified in step 13). Test environments not capable of evaluating the content of EF<sub>FPLMN</sub> while the common test procedure is executed, may verify the correct update of EF<sub>FPLMN</sub> by reading out the file at the end of the test execution. All entries generated during test execution shall be available and comply to the EF listings below, else the conformance requirement is not met.

CR 3 shall be verified in step 17). Test environments not capable of evaluating the content of EF<sub>EPSLOCI</sub> while the common test procedure is executed, may verify the correct update of EF<sub>EPSLOCI</sub> by reading out the file at the end of the test execution. All entries generated during test execution shall be available and comply to the EF listings below, else the conformance requirement is not met.

CR 4 is met if the GUTI derived from EF<sub>EPSLOCI</sub> matches the GUTI generated from the TT in step 13).

**EF<sub>EPSLOCI</sub>** (EPS Location Information)

Logically:

GUTI: as generated from TT in step 13)  
 Last visited registered TAI: 234/007/0001  
 EPS update status: updated

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	0B	F6	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>						
	32	74	00	00	01	00						

The EFs of the USIM read after finishing the common test procedure shall contain the following values:

**EF<sub>FPLMN</sub>** (Forbidden PLMNs)

Logically:

PLMN1: 234 002 (MCC MNC)  
 PLMN2: 234 003  
 PLMN3: 234 004  
 PLMN4: 234 005  
 PLMN5: 234 006  
 PLMN6: 234 007

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	32	24	00	32	34	00	32	44	00	32	54	00
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>						
	32	64	00	32	74	00						

**EF<sub>EPSLOCI</sub>** (EPS Location Information)

Logically:

GUTI: as generated from TT in step 13)  
 Last visited registered TAI: 234/008/0001  
 EPS update status: updated

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	0B	F6	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>						
	32	84	00	00	01	00						

## 7.1.5 UE updating forbidden PLMNs when accessing E-UTRAN

### 7.1.5.1 Definition and applicability

A list of forbidden PLMNs stored in the USIM provides storage for at least 4 entries, and is managed by the UE. In automatic PLMN selection mode the UE controls registration attempts to appropriate networks with respect to this list of forbidden PLMNs. As a result of a registration reject with the cause "PLMN not allowed" the UE stores the PLMN which rejected the update request in the USIM.

### 7.1.5.2 Conformance requirement

CR 1 After receipt of an ATTACH REJECT message during registration with the cause "PLMN not allowed" the ME shall update the EF<sub>FPLMN</sub> in the USIM.

Reference:

- TS 22.011 [18], clause 3.2.2 4;
- TS 31.102 [19], clauses 5.1.1 and 5.2.7

### 7.1.5.3 Test purpose

The purpose of this test is to verify that the UE correctly updates the EF<sub>FPLMN</sub>, i.e. fill up existing gaps in the elementary file before overwriting any existing entries.

### 7.1.5.4 Method of test

#### 7.1.5.4.1 Initial conditions

The values of the E-UTRAN/EPC UICC as defined in clause 4.5.4 of the present document are used with EF<sub>IMSI</sub> as defined in clause 4.6.2.

The defined UICC/USIM configuration defined for this test case shall be used and made available on the UE.

Ensure that the automatic PLMN selection mode is set and that the UE has installed and is using the UICC/USIM configuration defined for this test case in TS 31.121 [2] and runs an initial activation when executing the test procedure.

#### 7.1.5.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE > TT	Send RRC CONNECTION REQUEST / RRC CONNECTION REQUEST-NB	The TT responds with a RRC CONNECTION SETUP / RRC CONNECTION SETUP-NB		
2	UE > TT	Send RRC CONNECTION SETUP COMPLETE / RRC CONNECTION SETUP COMPLETE-NB			
3	UE > TT	Send ATTACH REQUEST	The TT performs an authentication and starts NAS integrity protection		
4	TT > UE	Send ATTACH REJECT message with cause 'PLMN not allowed'	The UE updates EFFPLMN	CR 1	A.2/1 OR A.2/2
5	TT > UE	Send RRC CONNECTION RELEASE / RRC CONNECTION RELEASE-NB			
6	USER > UE	UE is soft powered down			

### 7.1.5.5 Acceptance criteria

CR 1 shall be verified in step 4 after receiving ATTACH REJECT. Test environments not capable of evaluating the content of EF<sub>FPLMN</sub> while the common test procedure is executed, may verify the correct update of EF<sub>FPLMN</sub> by reading

out the file at the end of the test execution. All entries generated during test execution shall be available and comply to the EF listings below, else the conformance requirement is not met.

#### EF<sub>FPLMN</sub> (Forbidden PLMNs)

Logically:

PLMN1: 234 001 (MCC MNC)  
 PLMN2: 234 002  
 PLMN3: 234 003  
 PLMN4: 234 004  
 PLMN5: 234 005  
 PLMN6: 234 006

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	32	14	00	32	24	00	32	34	00	32	44	00
	B13	B14	B15	B16	B17	B18						
	32	54	00	32	64	00						

Or

#### EF<sub>FPLMN</sub> (Forbidden PLMNs)

Logically:

PLMN1: 234 001 (MCC MNC)  
 PLMN2: 234 003  
 PLMN3: 234 004  
 PLMN4: 234 005  
 PLMN5: 234 006  
 PLMN6: 234 002

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	32	14	00	32	34	00	32	44	00	32	54	00
	B13	B14	B15	B16	B17	B18						
	32	64	00	32	24	00						

## 7.1.6 UE deleting forbidden PLMNs when accessing E-UTRAN

### 7.1.6.1 Definition and applicability

In manual PLMN selection mode the UE allows registration attempts to all available PLMNs, including forbidden PLMNs (as indicated by the forbidden PLMN list on the USIM). As a result of a successful registration procedure onto a PLMN which is in the forbidden PLMN list, the forbidden PLMN list is automatically updated by the UE.

### 7.1.6.2 Conformance requirement

CR 1 In manual PLMN selection mode the UE shall be able to perform a ATTACH attempt during registration to a PLMN which is in the forbidden PLMN list.

Reference:

- TS 22.011 [18], clause 3.2.2.2;
- TS 31.102 [19], clauses 5.1.1 and 5.2.7.

CR 2 After receipt of ATTACH ACCEPT message during registration the UE shall delete the forbidden PLMN from the forbidden PLMN list.

Reference:

- TS 22.011 [18], clause 3.2.2.4;

### 7.1.6.3 Test purpose

The purpose of this test is to verify that:

- 1) the UE is able to perform an ATTACH REQUEST during registration on a forbidden PLMN in manual PLMN selection mode.
- 2) the UE after a successful registration attempt deletes the PLMN in the EF<sub>FPLMN</sub> on the USIM.

### 7.1.6.4 Method of test

#### 7.1.6.4.1 Initial conditions

The values of the E-UTRAN/EPC UICC as defined in clause 4.5.4 of the present document are used with EF<sub>IMSI</sub> as defined in clause 4.6.2.

The defined UICC/USIM configuration defined for this test case shall be used and made available on the UE.

The TT (E-USS or NB-SS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 234/005/0001.
- Access control: unrestricted.

Ensure that the manual PLMN selection mode is set and that the UE has installed and is using the UICC/USIM configuration defined for this test case in 31.121 [2] and runs an initial activation when executing the test procedure.

#### 7.1.6.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	USER > UE	PLMN with MCC/MNC 234/005 is manually selected.			
2	UE > TT	RRC CONNECTION REQUEST / RRC CONNECTION REQUEST-NB	The TT responds with a RRC CONNECTION SETUP / RRC CONNECTION SETUP-NB		
3	UE > TT	RRC CONNECTION SETUP COMPLETE / RRC CONNECTION SETUP COMPLETE-NB			
4	UE > TT	ATTACH REQUEST	The TT performs an authentication and starts NAS integrity protection	CR 1	
5	TT > UE	ATTACH ACCEPT message with: - TAI (MCC/MNC/TAC): 234/005/ 0001 - GUTI (as generated from TT)	The UE responds with an ATTACH COMPLETE message		
6	UE > USIM	UPDATE EF <sub>FPLMN</sub> , EF <sub>EPSLOCI</sub>		CR 2	A.2/1 OR A.2/2
7	TT > UE	RRC CONNECTION RELEASE / RRC CONNECTION RELEASE-NB			
8	UE	The UE is soft powered down.			

### 7.1.6.5 Acceptance criteria

CR 1 is met if the UE is sending ATTACH REQUEST in step 4) of Sequence A. TT shall provide status information.

CR 2 shall be explicitly verified in step 6). Test environments not capable of evaluating the content of EF<sub>FPLMN</sub>, EF<sub>EPSLOCI</sub> while the common test procedure is executed, may verify the correct update of EF<sub>FPLMN</sub>, EF<sub>EPSLOCI</sub> by reading

out the file at the end of the test execution. All entries generated during test execution shall be available and comply to the EF listings below, else the conformance requirement is not met.

#### EF<sub>FPLMN</sub> (Forbidden PLMNs)

Logically:

PLMN1: empty  
 PLMN2: empty  
 PLMN3: empty  
 PLMN4: empty  
 PLMN5: empty  
 PLMN6: empty

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
	B13	B14	B15	B16	B17	B18						
	FF	FF	FF	FF	FF	FF						

#### EF<sub>EPSLOCi</sub> (EPS Location Information)

Logically:

GUTI: as generated from TT in step 5)  
 Last visited registered TAI: 234/005/0001  
 EPS update status: updated

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	0B	F6	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx
	B13	B14	B15	B16	B17	B18						
	32	54	00	00	01	00						

### 7.1.7 Updating the Forbidden PLMN list after receiving non-integrity protected reject message – UTRAN

UTRAN test - not applicable

### 7.1.8 Updating the Forbidden PLMN list after receiving non-integrity protected reject message – E-UTRAN

#### 7.1.8.1 Definition and applicability

A list of forbidden PLMNs stored in the USIM and providing storage for at least 4 entries is managed by the UE. In automatic PLMN selection mode the UE controls registration attempts to appropriate networks with respect to this list of forbidden PLMNs. As a result of a registration reject with the cause "PLMN not allowed" the UE stores the PLMN which rejected the update request in the USIM.

#### 7.1.8.2 Conformance requirement

CR 1 After receipt of a not integrity-protected ATTACH REJECT message during registration with the cause "PLMN not allowed" the ME shall update the EF<sub>FPLMN</sub> in the USIM thereafter that VPLMN will not be accessed by the MS in automatic mode:

- if the MS is not configured to use timer T3245, and the MS maintains a list of PLMN-specific attempt counters and the value of the PLMN-specific attempt counter for that VPLMN is equal to the MS implementation specific maximum value or;

- if the MS is not configured to use timer T3245, and the MS is not maintaining a list of PLMN-specific attempt counters

Reference:

- TS 23.122 [41], clause 3.1.
- TS 22.011 [18], clause 3.2.2 2.3;
- TS 31.102 [19], clauses 5.1.1 and 5.2.7.

### 7.1.8.3 Test purpose

The purpose of this test is to verify that:

- 1) in automatic PLMN selection mode and after receipt of ATTACH REJECT message with cause "PLMN not allowed" during registration that the UE correctly updates EF<sub>FPLMN</sub>, in the following cases:
  - if the UE maintains a list of PLMN-specific attempt counters, and the value of the PLMN-specific attempt counter for that VPLMN is equal to the MS implementation specific maximum value;
  - if the UE does not maintain a list of PLMN-specific attempt counters.
- 2) the UE correctly updates the EF<sub>FPLMN</sub>, i.e. fill up existing gaps in the elementary file before overwriting any existing entries.

### 7.1.8.4 Method of test

#### 7.1.8.4.1 Initial conditions

The values of the E-UTRAN/EPC UICC as defined in clause 4.5.4 of the present document are used with EF<sub>IMSI</sub> as defined in clause 4.6.2.

If option A.1/38 is supported by the UE set the implementation specific counter to small value to reduce the test execution time. Use the value set for the number of repetitions as indicated in step 7).

The defined UICC/USIM configuration defined for this test case shall be used and made available on the UE.

The TT (E-USS or NB-SS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC):234/002/0001.
- Access control: unrestricted.

Ensure that the automatic PLMN selection mode is set and that the UE has installed and is using the UICC/USIM configuration defined for this test case in 31.121 [2] and runs an initial activation when executing the test procedure.

#### 7.1.8.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE > TT	Send RRC CONNECTION REQUEST / RRC CONNECTION REQUEST-NB	TT responds with RRC CONNECTION SETUP / RRC CONNECTION SETUP-NB		
2	UE > TT	Send RRC CONNECTION SETUP COMPLETE / RRC CONNECTION SETUP COMPLETE-NB			
3	UE > TT	ATTACH REQUEST			
4	TT > UE	ATTACH REJECT (Cause: PLMN Not Allowed)	Not integrity protected		
5	TT > UE	Send RRC CONNECTION RELEASE / RRC CONNECTION RELEASE-NB			
6	If the UE supports A.1/38, perform step 7) after the expiry of timer T3247, otherwise perform step 8).				
7	Using the settings declared for the implementation specific counter, repeat step 1) – 6) until the PLMN-specific attempt counters has reached the maximum value for that VPLMN				

8	UE > USIM	Update EF <sub>FPLMN</sub>		CR 1	A.2/1 OR A.2/2
9	UE	The UE is soft powered down.			

### 7.1.8.5 Acceptance criteria

CR 1 shall be verified in step 8). Test environments not capable of evaluating the content of EF<sub>FPLMN</sub> while the common test procedure is executed, may verify the correct update of EF<sub>FPLMN</sub> by reading out the file at the end of the test execution. All entries generated during test execution shall be available and comply to the EF listings below, else the conformance requirement is not met.

#### EF<sub>FPLMN</sub> (Forbidden PLMNs)

Logically:

PLMN1: 234 001 (MCC MNC)

PLMN2: 234 002

PLMN3: 234 003

PLMN4: 234 004

PLMN5: 234 005

PLMN6: 234 006

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	32	14	00	32	24	00	32	34	00	32	44	00
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>						
	32	54	00	32	64	00						

Or

#### EF<sub>FPLMN</sub> (Forbidden PLMNs)

Logically:

PLMN1: 234 001 (MCC MNC)

PLMN2: 234 003

PLMN3: 234 004

PLMN4: 234 005

PLMN5: 234 006

PLMN6: 234 002

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	32	14	00	32	34	00	32	44	00	32	54	00
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>						
	32	64	00	32	24	00						

## 7.2 User controlled PLMN selector handling

### 7.2.1 UE updating the User controlled PLMN selector list

#### 7.2.1.1 Definition and applicability

The User controlled PLMN selector list gives in priority order the preferred UPLMNs on which the UE shall register. The Radio Access Technology identifier defines the Radio network in which the UE shall register. The list is stored on the USIM in the EF<sub>PLMNWACT</sub>. Update and deletion of PLMNs may be performed by the subscriber.

### 7.2.1.2 Conformance requirement

CR 1 The UE shall correctly replace the selected UPLMN in the User controlled PLMN selector list.

Reference:

- TS 31.102 [19], clause 5.3.6.

### 7.2.1.3 Test purpose

The purpose of this test is to verify that the UE correctly updates the EF<sub>PLMNwACT</sub>.

### 7.2.1.4 Method of test

#### 7.2.1.4.1 Initial conditions

The values of the Default UICC as defined in clause 4.5.2 of the present document are used.

The defined UICC/USIM configuration defined for this test case shall be used and made available on the UE.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and runs an initial activation.

#### 7.2.1.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	USER > UE	Initiate an MMI dependent procedure to change the UPLMN	Change the second UPLMN in the User controlled PLMN selector list to MCC/MNC of 567/02, the ACT identifier shall set to UTRAN only.		
2	UE > USIM	Update EF <sub>PLMNwACT</sub>		CR 1	A.2/1 OR A.2/2
3	UE	The UE is soft powered down			
<b>Optional step if CR 1 verification cannot be performed at step 2)</b>					
4	UE	READ EF <sub>PLMNwACT</sub> PLMNwACT		CR 1	A.2/3

### 7.2.1.5 Acceptance criteria

After step b) the USIM shall contain the following values:

EF<sub>PLMNwACT</sub> (UPLMN Selector)

Logically:

1<sup>st</sup> PLMN: 244 081 (MCC MNC)  
 1<sup>st</sup> ACT: UTRAN  
 2<sup>nd</sup> PLMN: 567 02  
 2<sup>nd</sup> ACT: UTRAN  
 3<sup>rd</sup> PLMN: 244 082  
 3<sup>rd</sup> ACT: UTRAN  
 4<sup>th</sup> PLMN: 244 082  
 4<sup>th</sup> ACT: GSM  
 5<sup>th</sup> PLMN: 244 003  
 5<sup>th</sup> ACT: UTRAN  
 6<sup>th</sup> PLMN: 244 004  
 6<sup>th</sup> ACT: UTRAN  
 7<sup>th</sup> PLMN: 244 005  
 7<sup>th</sup> ACT: UTRAN  
 8<sup>th</sup> PLMN: 244 006  
 8<sup>th</sup> ACT: UTRAN  
 9<sup>th</sup> PLMN: 244 007

9<sup>th</sup> ACT UTRAN  
 10<sup>th</sup> PLMN: 244 008  
 10<sup>th</sup> ACT UTRAN  
 11<sup>th</sup> PLMN: 244 009  
 11<sup>th</sup> ACT UTRAN  
 12<sup>th</sup> PLMN: 244 010  
 12<sup>th</sup> ACT UTRAN

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	42	14	80	80	00	65	F7	20	80	00	42	24
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	80	80	00	32	24	00	00	80	42	34	00	80
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>	<b>B31</b>	<b>B32</b>	<b>B33</b>	<b>B34</b>	<b>B35</b>	<b>B36</b>
	00	42	44	00	80	00	42	54	00	80	00	42
	<b>B37</b>	<b>B38</b>	<b>B39</b>	<b>B40</b>	<b>B41</b>	<b>B42</b>	<b>B43</b>	<b>B44</b>	<b>B45</b>	<b>B46</b>	<b>B47</b>	<b>B48</b>
	64	00	80	00	42	74	00	80	00	42	84	00
	<b>B49</b>	<b>B50</b>	<b>B51</b>	<b>B52</b>	<b>B53</b>	<b>B54</b>	<b>B55</b>	<b>B56</b>	<b>B57</b>	<b>B58</b>	<b>B59</b>	<b>B60</b>
	80	00	42	94	00	80	00	42	04	10	80	00

## 7.2.2 UE recognizing the priority order of the User controlled PLMN selector list with the same access Technology

GERAN/UTRAN test - not applicable

## 7.2.3 UE recognizing the priority order of the User controlled PLMN selector list using an ACT Preference

GERAN/UTRAN test - not applicable

## 7.2.4 Void

## 7.2.5 UE updating the User controlled PLMN selector list for E-UTRAN

### 7.2.5.1 Definition and applicability

The User controlled PLMN selector list gives in priority order the preferred UPLMNs on which the UE shall register. The Radio Access Technology identifier defines the Radio network in which the UE shall register. The list is stored on the USIM in the EF<sub>PLMNwACT</sub>. Update and deletion of PLMNs may be performed by the subscriber.

### 7.2.5.2 Conformance requirement

CR 1 The UE shall correctly replace the selected UPLMN in the User controlled PLMN selector list.

Reference:

- TS 31.102 [19], clause 5.3.6 and 4.2.5.

### 7.2.5.3 Test purpose

The purpose of this test is to verify that the UE correctly updates the EF<sub>PLMNwACT</sub>.

## 7.2.5.4 Method of test

### 7.2.5.4.1 Initial conditions

The values of the E-UTRAN/EPC UICC as defined in clause 4.5.4 of the present document are used.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and runs an initial activation.

### 7.2.5.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	USER > UE	Initiate an MMI dependent procedure to change the UPLMN	Change the second UPLMN in the User controlled PLMN selector list to MCC/MNC of 567/04, the ACT identifier shall set to E-UTRAN only.		
2	UE > USIM	Update EF <sub>PLMNwACT</sub>		CR 1	A.2/1 OR A.2/2
3	UE	The UE is soft powered down			
<b>Optional step if CR 1 verification cannot be performed at step 2)</b>					
4	UE	READ EF <sub>PLMNwACT</sub> PLMNwACT		CR 1	A.2/3

## 7.2.5.5 Acceptance criteria

After step b) the USIM shall contain the following values:

EF<sub>PLMNwACT</sub> (UPLMN Selector)

Logically:

1<sup>st</sup> PLMN: 244 081 (MCC MNC)  
 1<sup>st</sup> ACT: E-UTRAN  
 2<sup>nd</sup> PLMN: 567 04  
 2<sup>nd</sup> ACT: E-UTRAN  
 3<sup>rd</sup> PLMN: 244 083  
 3<sup>rd</sup> ACT: E-UTRAN  
 4<sup>th</sup> PLMN: 244 082  
 4<sup>th</sup> ACT: GSM  
 5<sup>th</sup> PLMN: 244 003  
 5<sup>th</sup> ACT: E-UTRAN  
 6<sup>th</sup> PLMN: 244 004  
 6<sup>th</sup> ACT: UTRAN  
 7<sup>th</sup> PLMN: 244 005  
 7<sup>th</sup> ACT: UTRAN  
 8<sup>th</sup> PLMN: 244 081  
 8<sup>th</sup> ACT: UTRAN  
 9<sup>th</sup> PLMN: 244 007  
 9<sup>th</sup> ACT: UTRAN  
 10<sup>th</sup> PLMN: 244 008  
 10<sup>th</sup> ACT: E-UTRAN  
 11<sup>th</sup> PLMN: 244 009  
 11<sup>th</sup> ACT: UTRAN  
 12<sup>th</sup> PLMN: 244 010  
 12<sup>th</sup> ACT: E-UTRAN

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	42	14	80	40	00	65	F7	40	40	00	42	34
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	80	40	00	42	24	80	00	80	42	34	00	40
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>	<b>B31</b>	<b>B32</b>	<b>B33</b>	<b>B34</b>	<b>B35</b>	<b>B36</b>
	00	42	44	00	80	00	42	54	00	80	00	42
	<b>B37</b>	<b>B38</b>	<b>B39</b>	<b>B40</b>	<b>B41</b>	<b>B42</b>	<b>B43</b>	<b>B44</b>	<b>B45</b>	<b>B46</b>	<b>B47</b>	<b>B48</b>
	14	80	80	00	42	74	00	80	00	42	84	00
	<b>B49</b>	<b>B50</b>	<b>B51</b>	<b>B52</b>	<b>B53</b>	<b>B54</b>	<b>B55</b>	<b>B56</b>	<b>B57</b>	<b>B58</b>	<b>B59</b>	<b>B60</b>
	40	00	42	94	00	80	00	42	04	10	40	00

## 7.2.6 UE recognizing the priority order of the User controlled PLMN selector list using an ACT preference - UTRAN/E-UTRAN

Not applicable as UTRAN testing is involved.

## 7.2.7 UE recognizing the priority order of the User controlled PLMN selector list using an ACT preference - GSM/E-UTRAN

Not applicable as GERAN testing is involved.

## 7.2.8 UE recognising the priority order of the User controlled PLMN selector list with the same access technology – E-UTRAN in NB-S1 mode

### 7.2.8.1 Definition and applicability

The User controlled PLMN selector list gives in priority order the preferred PLMNs of the User on which the UE shall register. The Radio Access Technology identifier defines the Radio network in which the UE shall register. The list is stored on the USIM in the EF<sub>PLMNwACT</sub>. Update and deletion of User controlled PLMNs may be performed by the subscriber by the use of the PIN.

### 7.2.8.2 Conformance requirement

CR 1 When registering onto a VPLMN the UE shall consider the priority of the ACT identifier in the preferred list on the USIM.

Reference:

- TS 22.011 [18], clause 3.2.2;
- TS 31.102 [19], clauses 4.2.5 and 5.1.1.2.

CR 2 The modified value of EF<sub>EPSLOC1</sub> shall be available on the USIM when ending the test case.

### 7.2.8.3 Test purpose

The purpose of this test is to verify that ACT with the higher priority (defined by its position in EF<sub>PLMNwACT</sub>) takes precedence over the UPLMN with the lower priority when the UE performs a network selection. Hereby the new coding for E-UTRAN in NB-S1 mode has to be handled correctly by the UE.

### 7.2.8.4 Method of test

#### 7.2.8.4.1 Initial conditions

The values of the E-UTRAN/EPC ISIM UICC as defined in clause 4.5.5 of the present document are used with the following exception:

**EF<sub>PLMNwACT</sub>** (User Controlled PLMN Selector with Access Technology)

Logically:

1<sup>st</sup> PLMN: 244 083 (MCC MNC)  
 1<sup>st</sup> ACT: E-UTRAN in NB-S1 mode  
 2<sup>nd</sup> PLMN: 244 081  
 2<sup>nd</sup> ACT: E-UTRAN in NB-S1 mode  
 3<sup>rd</sup> PLMN: 244 083  
 3<sup>rd</sup> ACT: E-UTRAN  
 4<sup>th</sup> PLMN: 244 082  
 4<sup>th</sup> ACT: GSM  
 5<sup>th</sup> PLMN: 244 003  
 5<sup>th</sup> ACT: E-UTRAN  
 6<sup>th</sup> PLMN: 244 004  
 6<sup>th</sup> ACT: UTRAN  
 7<sup>th</sup> PLMN: 244 005  
 7<sup>th</sup> ACT: UTRAN  
 8<sup>th</sup> PLMN: 244 081  
 8<sup>th</sup> ACT: UTRAN  
 9<sup>th</sup> PLMN: 244 007  
 9<sup>th</sup> ACT: UTRAN  
 10<sup>th</sup> PLMN: 244 008  
 10<sup>th</sup> ACT: E-UTRAN  
 11<sup>th</sup> PLMN: 244 009  
 11<sup>th</sup> ACT: UTRAN  
 12<sup>th</sup> PLMN: 244 010  
 12<sup>th</sup> ACT: E-UTRAN

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	42	34	80	50	00	42	14	80	50	00	42	34
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	80	40	00	42	24	80	00	80	42	34	00	40
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>	<b>B31</b>	<b>B32</b>	<b>B33</b>	<b>B34</b>	<b>B35</b>	<b>B36</b>
	00	42	44	00	80	00	42	54	00	80	00	42
	<b>B37</b>	<b>B38</b>	<b>B39</b>	<b>B40</b>	<b>B41</b>	<b>B42</b>	<b>B43</b>	<b>B44</b>	<b>B45</b>	<b>B46</b>	<b>B47</b>	<b>B48</b>
	14	80	80	00	42	74	00	80	00	42	84	00
	<b>B49</b>	<b>B50</b>	<b>B51</b>	<b>B52</b>	<b>B53</b>	<b>B54</b>	<b>B55</b>	<b>B56</b>	<b>B57</b>	<b>B58</b>	<b>B59</b>	<b>B60</b>
	40	00	42	94	00	80	00	42	04	10	40	00

The defined UICC/USIM configuration defined for this test case shall be used and made available on the UE. The UE is set to automatic PLMN selection mode.

The TT (NB-SS) transmits on the BCCH, with the following network parameters:

Cell A:

- TAI (MCC/MNC/TAC):244/081/0001.
- Access control: unrestricted.

Cell B:

- TAI (MCC/MNC/TAC):244/083/0001.
- Access control: unrestricted.

## 7.2.8.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	Run initial activation.			

2	UE > TT	Send RRC CONNECTION REQUEST-NB	The RRC CONNECTION REQUEST-NB sent to the BCCH transmitting MCC/MNC 244/083 gets a RRC CONNECTION SETUP-NB as response from the TT	CR 1	
3	UE > TT	Send RRC CONNECTION SETUP COMPLETE-NB			
4	UE > TT	Send ATTACH REQUEST	During registration the TT performs an authentication and starts integrity by using the security procedure.		
5	TT > UE	Send ATTACH ACCEPT	The ATTACH ACCPT is sent with: - TAI (MCC/MNC/TAC): 244/083/ 0001 - GUTI: "24408300010266436587"	(CR 1)	
6	UE > TT	Send ATTACH COMPLETE	The TT sends RRC CONNECTION RELEASE-NB		
7	USER > UE	UE is soft powered down			
8	TT	Verify the contents of EF <sub>EPSLOCI</sub>	Reading EF <sub>EPSLOCI</sub> may also be performed before step 7)	CR 2	A.2/3

### 7.2.8.5 Acceptance criteria

CR 1 is verified in step 2). The requirement is met if in step 2) the UE sends a RRC CONNECTION REQUEST-NB to the BCCH transmitting MCC/MNC 244/083 to the NB-SS

If the request is sent correctly can also be verified in the ATTACH ACCEPT send by the NB-SS if it is containing:

- TAI (MCC/MNC/TAC):244/083/ 0001
- GUTI: "24408300010266436587"

CR 2 is verified by reading the contents of EF<sub>EPSLOCI</sub> in step 8). CR 2 is met if the file contains the following data:

EF<sub>EPSLOCI</sub> (EPS Information)

Logically:

GUTI: 24408300010266436587  
Last visited registered TAI: 244/083/0001  
EPS update status: updated

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	0B	F6	42	34	80	00	01	02	66	43	65	87
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>						
	42	34	80	00	01	00						

## 7.2.9 UE recognising the priority order of the User controlled PLMN selector list using the ACT preference – E-UTRAN in WB-S1/E-UTRAN in NB-S1

### 7.2.9.1 Definition and applicability

The User controlled PLMN selector list gives in priority order the preferred PLMNs of the User on which the UE shall register. The Radio Access Technology identifier defines the Radio network in which the UE shall register. The list is stored on the USIM in the EF<sub>PLMNwACT</sub>. Update and deletion of User controlled PLMNs may be performed by the subscriber by the use of the PIN.

### 7.2.9.2 Conformance requirement

CR 1 When registering onto a VPLMN the UE shall consider the priority of the ACT identifier in the preferred list on the USIM.

Reference:

- TS 22.011 [18], clause 3.2.2;
- TS 31.102 [19], clauses 4.2.5 and 5.1.1.2.

CR 2 The modified value of  $EF_{EPSLOC1}$  shall be available on the USIM when ending the test case.

### 7.2.9.3 Test purpose

The purpose of this test is to verify that ACT with the higher priority (defined by its position in  $EF_{PLMNwACT}$ ) takes precedence over the UPLMN with the lower priority when the UE performs a network selection. Hereby the new coding for RAT E-UTRAN in WB-S1 mode and E-UTRAN in NB-S1 mode has to be handled correctly by the UE.

### 7.2.9.4 Method of test

#### 7.2.9.4.1 Initial conditions

The values of the E-UTRAN/EPC UICC as defined in clause 4.5.4 of the present document are used with the following exception:

$EF_{PLMNwACT}$  (User Controlled PLMN Selector with Access Technology)

Logically:

1 <sup>st</sup> PLMN:	244 081 (MCC MNC)
1 <sup>st</sup> ACT:	E-UTRAN
2 <sup>nd</sup> PLMN:	244 081
2 <sup>nd</sup> ACT:	GSM
3 <sup>rd</sup> PLMN:	244 083
3 <sup>rd</sup> ACT:	E-UTRAN in NB-S1 mode
4 <sup>th</sup> PLMN:	244 083
4 <sup>th</sup> ACT:	E-UTRAN in WB-S1 mode
5 <sup>th</sup> PLMN:	244 003
5 <sup>th</sup> ACT:	E-UTRAN
6 <sup>th</sup> PLMN:	244 004
6 <sup>th</sup> ACT:	UTRAN
7 <sup>th</sup> PLMN:	244 005
7 <sup>th</sup> ACT:	UTRAN
8 <sup>th</sup> PLMN:	244 081
8 <sup>th</sup> ACT:	UTRAN
9 <sup>th</sup> PLMN:	244 007
9 <sup>th</sup> ACT:	UTRAN
10 <sup>th</sup> PLMN:	244 008
10 <sup>th</sup> ACT:	E-UTRAN
11 <sup>th</sup> PLMN:	244 009
11 <sup>th</sup> ACT:	UTRAN
12 <sup>th</sup> PLMN:	244 010
12 <sup>th</sup> ACT:	E-UTRAN

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	42	14	80	40	00	42	14	80	00	80	42	34
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	80	50	00	42	34	80	60	00	42	34	00	40
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>	<b>B31</b>	<b>B32</b>	<b>B33</b>	<b>B34</b>	<b>B35</b>	<b>B36</b>
	00	42	44	00	80	00	42	54	00	80	00	42
	<b>B37</b>	<b>B38</b>	<b>B39</b>	<b>B40</b>	<b>B41</b>	<b>B42</b>	<b>B43</b>	<b>B44</b>	<b>B45</b>	<b>B46</b>	<b>B47</b>	<b>B48</b>
	14	80	80	00	42	74	00	80	00	42	84	00
	<b>B49</b>	<b>B50</b>	<b>B51</b>	<b>B52</b>	<b>B53</b>	<b>B54</b>	<b>B55</b>	<b>B56</b>	<b>B57</b>	<b>B58</b>	<b>B59</b>	<b>B60</b>
	40	00	42	94	00	80	00	42	04	10	40	00

The defined UICC/USIM configuration defined for this test case shall be used and made available on the UE. The UE is set to automatic PLMN selection mode.

The TT (E-USS and NB-SS) transmits on the BCCH, with the following network parameters on both cells:

- TAI (MCC/MNC/TAC):244/083/0001.
- Access control: unrestricted.

#### 7.2.9.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	Run initial activation.			
2	UE > TT	Send RRC CONNECTION REQUEST-NB	The RRC CONNECTION REQUEST-NB sent to the BCCH transmitting MCC/MNC 244/083 gets a RRC CONNECTION SETUP-NB as response from the TT	CR 1	
3	UE > TT	Send RRC CONNECTION SETUP COMPLETE-NB			
4	UE > TT	Send ATTACH REQUEST	During registration the TT performs an authentication and starts integrity by using the security procedure.		
5	TT > UE	Send ATTACH ACCEPT	The ATTACH ACCPT is sent with: - TAI (MCC/MNC/TAC): 244/083/ 0001 - GUTI: "24408300010266436587"	(CR 1)	
6	UE > TT	Send ATTACH COMPLETE	The TT sends RRC CONNECTION RELEASE-NB		
7	USER > UE	UE is soft powered down			
8	TT	Verify the contents of EF <sub>EPSLOCI</sub>	Reading EF <sub>EPSLOCI</sub> may also be performed before step 7)	CR 2	A.2/3

#### 7.2.9.5 Acceptance criteria

CR 1 is verified in step 2). The requirement is met if in step 2) the UE sends a RRC CONNECTION REQUEST-NB to the BCCH transmitting MCC/MNC 244/083 to the NB-SS

If the request is sent correctly can also be verified in the ATTACH ACCEPT send by the NB-SS if it is containing:

- TAI (MCC/MNC/TAC):244/083/ 0001
- GUTI: "24408300010266436587"

CR 2 is verified by reading the contents of EF<sub>EPSLOCI</sub> in step 8). CR 2 is met if the file contains the following data:

EF<sub>EPSLOCI</sub> (EPS Information)

Logically:

GUTI: 24408300010266436587  
Last visited registered TAI: 244/083/0001  
EPS update status: updated

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	0B	F6	42	34	80	00	01	02	66	43	65	87
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>						
	42	34	80	00	01	00						

## 7.3 Operator controlled PLMN selector handling

### 7.3.1 UE recognizing the priority order of the Operator controlled PLMN selector list

GERAN/UTRAN test - not applicable

### 7.3.2 UE recognizing the priority order of the User controlled PLMN selector over the Operator controlled PLMN selector list

GERAN/UTRAN test - not applicable

### 7.3.3 UE recognizing the priority order of the Operator controlled PLMN selector list when accessing E-UTRAN

#### 7.3.3.1 Definition and applicability

The Operator controlled PLMN selector list gives in priority order the preferred OPLMNs on which the UE shall register if no network of the User controlled PLMN selector list is available. The Radio Access Technology identifier defines the Radio network in which the UE shall register. The list is stored on the USIM in the EF<sub>OPLMNwACT</sub>. Update and deletion of OPLMNs shall not be possible by the subscriber by the use of the PIN.

#### 7.3.3.2 Conformance requirement

CR 1 When registering onto a VPLMN the UE shall consider the priority of OPLMNs in the preferred list on the USIM.

Reference:

- TS 22.011 [18], clause 3.2.2;
- TS 31.102 [19], clause 4.2.53, 4.2.5 and 5.1.1.2.

CR 2 The modified value of EF<sub>EPSLOC1</sub> shall be available on the USIM when ending the test case.

#### 7.3.3.3 Test purpose

The purpose of this test is to verify that the OPLMN with the higher priority (defined by its position in EF<sub>OPLMNwACT</sub>) takes precedence over the OPLMN with the lower priority when the UE performs a network selection. Hereby the new coding for RAT E-UTRAN/NB-IoT has to be handled correctly by the UE.

#### 7.3.3.4 Method of test

##### 7.3.3.4.1 Initial conditions

The values of the E-UTRAN/EPC UICC as defined in clause 4.5.4 of the present document are used with the following exception:

EF<sub>UST</sub> (USIM Service Table)

Logically:

Service n°42:	Operator controlled PLMN selector with Access Technology	available
Service n°86:	Allowed CSG Lists and corresponding indications	not available

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Binary	xx1x xx11	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxxx xx1x	xxxx xxxx	xxxx xxxx
	B9	B10	B11	B12	B13	B14	B15	
	xxxx xxxx	xxxx xxxx	xx01 xxxx	xxxx xxxx	xxxx xxxx	xxxx xxxx	xxxx xxxx	

The coding of EF<sub>UST</sub> shall conform with the capabilities of the USIM used.

EF<sub>OPLMNwACT</sub> (OPLMN Selector)

Logically:

1 <sup>st</sup> PLMN:	254 012 (MCC MNC)
1 <sup>st</sup> ACT	E-UTRAN
2 <sup>nd</sup> PLMN:	254 011
2 <sup>nd</sup> ACT	E-UTRAN
3 <sup>rd</sup> PLMN:	254 002
3 <sup>rd</sup> ACT:	E-UTRAN
4 <sup>th</sup> PLMN:	254 012
4 <sup>th</sup> ACT:	GSM
5 <sup>th</sup> PLMN:	254 011
5 <sup>th</sup> ACT:	GSM
6 <sup>th</sup> PLMN:	254 005
6 <sup>th</sup> ACT:	UTRAN
7 <sup>th</sup> PLMN:	254 006
7 <sup>th</sup> ACT:	UTRAN
8 <sup>th</sup> PLMN:	254 007
8 <sup>th</sup> ACT:	UTRAN

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	52	24	10	40	00	52	14	10	40	00	52	24
	B13	B14	B15	B16	B17	B18	B19	B20	B21	B22	B23	B24
	00	40	00	52	24	10	00	80	52	14	10	00
	B25	B26	B27	B28	B29	B30	B31	B32	B33	B34	B35	B36
	80	52	54	00	80	00	52	64	00	80	00	52
	B37	B38	B39	B40								
	74	00	80	00								

The defined UICC/USIM configuration defined for this test case shall be used and made available on the UE. The UE is set to automatic PLMN selection mode.

The TT (E-USS or NB-SS) transmits on the BCCH, with the following network parameters:

Cell A:

- TAI (MCC/MNC/TAC):254/011/0001.
- Access control: unrestricted.

Cell B:

- TAI (MCC/MNC/TAC):254/012/0001.
- Access control: unrestricted.

## 7.3.3.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	Run initial activation.			
2	UE > TT	Send RRC CONNECTION REQUEST / RRC CONNECTION REQUEST-NB	The RRC CONNECTION REQUEST / RRC CONNECTION REQUEST-NB sent to the BCCH transmitting MCC/MNC 254/012 gets a RRC CONNECTION SETUP / RRC CONNECTION SETUP-NB as response from the TT	CR 1	
3	UE > TT	Send RRC CONNECTION SETUP COMPLETE / RRC CONNECTION SETUP COMPLETE-NB			
4	UE > TT	Send ATTACH REQUEST	During registration the TT performs an authentication and starts integrity by using the security procedure.		
5	TT > UE	Send ATTACH ACCEPT	The ATTACH ACCPT is sent with: - TAI (MCC/MNC/TAC): 254/012/0001 - GUTI: "25401200010266436587"	(CR 1)	
6	UE > TT	Send ATTACH COMPLETE	The TT sends RRC CONNECTION RELEASE / RRC CONNECTION RELEASE-NB		
7	USER > UE	UE is soft powered down			
8	TT	Verify the contents of EF <sub>EPSLOC1</sub>	Reading EF <sub>EPSLOC1</sub> may also be performed before step 7)	CR 2	A.2/3

## 7.3.3.5 Acceptance criteria

CR 1 is verified in step 2). The requirement is met if in step 2) the UE sends a RRC CONNECTION REQUEST/ RRC CONNECTION REQUEST-NB to the BCCH transmitting MCC/MNC 254/012 to the E-USS/NB-SS

If the request is sent correctly can also be verified in the ATTACH ACCEPT send by the E-USS/NB-SS if it is containing:

- TAI (MCC/MNC/TAC):254/012/0001
- GUTI: "25401200010266436587"

CR 2 is verified by reading the contents of EF<sub>EPSLOC1</sub> in step 8). CR 2 is met if the file contains the following data:

EF<sub>EPSLOC1</sub> (EPS Information)

Logically:

GUTI: 25401200010266436587  
Last visited registered TAI: 254/012/0001  
EPS update status: updated

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	0B	F6	52	24	10	00	01	02	66	43	65	87
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>						
	52	24	10	00	01	00						

## 7.3.4 UE recognizing the priority order of the User controlled PLMN selector over the Operator controlled PLMN selector list – E-UTRAN

### 7.3.4.1 Definition and applicability

The User controlled PLMN selector list has a higher priority as the OPLMN selector list on which the UE shall register. The Radio Access Technology identifier defines the Radio network in which the UE shall register. The list is stored on the USIM in the EF<sub>PLMNwACT</sub>.

### 7.3.4.2 Conformance requirement

CR 1 When registering onto a VPLMN the UE shall consider the priority of UPLMNs first before the OPLMNs in the preferred list on the USIM.

Reference:

- TS 22.011 [18], clause 3.2.2;
- TS 31.102 [19], clause 4.2.53, 4.2.5 and 5.1.1.2.

CR 2 The modified value of EF<sub>EPSLOC1</sub> shall be available on the USIM when ending the test case.

### 7.3.4.3 Test purpose

The purpose of this test is to verify that the User controlled PLMN with a lower priority (defined by its position in EF<sub>PLMNwACT</sub>) takes precedence over the OPLMN with a higher priority when the UE performs a network selection. Hereby the new coding for RAT E-UTRAN/NB-IoT has to be handled correctly by the UE.

### 7.3.4.4 Method of test

#### 7.3.4.4.1 Initial conditions

The values of the E-UTRAN/EPC UICC as defined in clause 4.5.4 of the present document are used with the following exception:

EF<sub>UST</sub> (USIM Service Table)

Logically:

Service n°1:	Local Phone Book	available
Service n°2:	Fixed Dialling Numbers (FDN)	available
Service n°6:	Barred Dialling Numbers (BDN)	available
Service n°17:	Group Identifier Level 1	not available
Service n°18:	Group Identifier Level 2	not available
Service n°20:	User controlled PLMN selector with Access Technology	available
Service n°27:	GSM Access	available
Service n°33:	shall be set to 'I'	available
Service n°34:	Enabled Services Table	available
Service n°42:	Operator controlled PLMN selector with Access Technology	available
Service n°85:	EPS Mobility Management Information	available
Service n°86:	Allowed CSG Lists and corresponding indications	not available

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Binary	xx1x xx11	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxxx xx1x	xxxx xxxx	xxxx xxxx
	B9	B10	B11	B12	B13	B14	B15	
	xxxx xxxx	xxxx xxxx	xx01 xxxx	xxxx xxxx	xxxx xxxx	xxxx xxxx	xxxx xxxx	

The coding of EF<sub>UST</sub> shall conform with the capabilities of the USIM used.

The defined UICC/USIM configuration defined for this test case shall be used and made available on the UE. The UE is set to automatic PLMN selection mode.

The TT (E-USS or NB-SS) transmits on the BCCH, with the following network parameters:

Cell A:

- TAI (MCC/MNC/TAC):254/011/0001.
- Access control: unrestricted.

Cell B:

- TAI (MCC/MNC/TAC):244/010/0001.
- Access control: unrestricted.

#### 7.3.4.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	Run initial activation.			
2	UE > TT	Send RRC CONNECTION REQUEST / RRC CONNECTION REQUEST-NB	The RRC CONNECTION REQUEST / RRC CONNECTION REQUEST-NB sent to the BCCH transmitting MCC/MNC 244/010 gets a RRC CONNECTION SETUP / RRC CONNECTION SETUP-NB as response from the TT	CR 1	
3	UE > TT	Send RRC CONNECTION SETUP COMPLETE / RRC CONNECTION SETUP COMPLETE-NB			
4	UE > TT	Send ATTACH REQUEST	During registration the TT performs an authentication and starts integrity by using the security procedure.		
5	TT > UE	Send ATTACH ACCEPT	The ATTACH ACCPT is sent with: - TAI (MCC/MNC/TAC): 244/010/0001 - GUTI: "24401000010266436587"	(CR 1)	
6	UE > TT	Send ATTACH COMPLETE	The TT sends RRC CONNECTION RELEASE / RRC CONNECTION RELEASE-NB		
7	USER > UE	UE is soft powered down			
8	TT	Verify the contents of EF <sub>EPSLOCI</sub>	Reading EF <sub>EPSLOCI</sub> may also be performed before step 7)	CR 2	A.2/3

#### 7.3.4.5 Acceptance criteria

CR 1 is verified in step 2). The requirement is met if in step 2) the UE sends a RRC CONNECTION REQUEST/ RRC CONNECTION REQUEST-NB to the BCCH transmitting MCC/MNC 244/010 to the E-USS/NB-SS

If the request is sent correctly can also be verified in the ATTACH ACCEPT send by the E-USS/NB-SS if it is containing:

- TAI (MCC/MNC/TAC):244/010/0001
- GUTI: "24401000010266436587"

CR 2 is verified by reading the contents of EF<sub>EPSLOCI</sub> in step 8). CR 2 is met if the file contains the following data:

EF<sub>EPSLOCI</sub> (EPS Information)

Logically:

GUTI: 24401000010266436587  
Last visited registered TAI: 244/010/0001

EPS update status: updated

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	0B	F6	42	04	10	00	01	02	66	43	65	87
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>						
	42	04	10	00	01	00						

## 7.3.5 UE recognising the priority order of the Operator controlled PLMN selector list when accessing E-UTRAN in NB-S1 mode

### 7.3.5.1 Definition and applicability

The Operator controlled PLMN selector list gives in priority order the preferred OPLMNs on which the UE shall register if no network of the User controlled PLMN selector list is available. The Radio Access Technology identifier defines the Radio network in which the UE shall register. The list is stored on the USIM in the EF<sub>OPLMNwACT</sub>. Update and deletion of OPLMNs shall not be possible by the subscriber by the use of the PIN.

### 7.3.5.2 Conformance requirement

CR 1 When registering onto a VPLMN the UE shall consider the priority of OPLMNs in the preferred list on the USIM.

Reference:

- TS 22.011 [18], clause 3.2.2;
- TS 31.102 [19], clause 4.2.53, 4.2.5 and 5.1.1.2.

CR 2 The modified value of EF<sub>EPSLOC1</sub> shall be available on the USIM when ending the test case.

### 7.3.5.3 Test purpose

The purpose of this test is to verify that the OPLMN with the higher priority (defined by its position in EF<sub>OPLMNwACT</sub>) takes precedence over the OPLMN with the lower priority when the UE performs a network selection. Hereby the new coding for RAT E-UTRAN in NB-IoT mode has to be handled correctly by the UE.

### 7.3.5.4 Method of test

#### 7.3.5.4.1 Initial conditions

The values of the E-UTRAN/EPC UICC as defined in clause 4.5.4 of the present document are used with the following exception:

EF<sub>UST</sub> (USIM Service Table)

Logically:

Service n°42:	Operator controlled PLMN selector with Access Technology	available
Service n°86:	Allowed CSG Lists and corresponding indications	not available

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Binary	xx1x xx11	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxxx xx1x	xxxx xxxx	xxxx xxxx
	<b>B9</b>	<b>B10</b>	<b>B11</b>	<b>B12</b>	<b>B13</b>	<b>B14</b>	<b>B15</b>	
	xxxx xxxx	xxxx xxxx	xx01 xxxx	xxxx xxxx	xxxx xxxx	xxxx xxxx	xxxx xxxx	

The coding of EF<sub>UST</sub> shall conform with the capabilities of the USIM used.

**EF<sub>OPLMNwACT</sub>** (OPLMN Selector)

Logically:

- 1<sup>st</sup> PLMN: 254 012 (MCC MNC)
- 1<sup>st</sup> ACT: E-UTRAN in NB-S1 mode
- 2<sup>nd</sup> PLMN: 254 011
- 2<sup>nd</sup> ACT: E-UTRAN in NB-S1 mode
- 3<sup>rd</sup> PLMN: 254 002
- 3<sup>rd</sup> ACT: E-UTRAN
- 4<sup>th</sup> PLMN: 254 012
- 4<sup>th</sup> ACT: GSM
- 5<sup>th</sup> PLMN: 254 011
- 5<sup>th</sup> ACT: GSM
- 6<sup>th</sup> PLMN: 254 005
- 6<sup>th</sup> ACT: UTRAN
- 7<sup>th</sup> PLMN: 254 006
- 7<sup>th</sup> ACT: UTRAN
- 8<sup>th</sup> PLMN: 254 007
- 8<sup>th</sup> ACT: UTRAN

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	52	24	10	50	00	52	14	10	50	00	52	24
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	00	40	00	52	24	10	00	80	52	14	10	00
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>	<b>B31</b>	<b>B32</b>	<b>B33</b>	<b>B34</b>	<b>B35</b>	<b>B36</b>
	80	52	54	00	80	00	52	64	00	80	00	52
	<b>B37</b>	<b>B38</b>	<b>B39</b>	<b>B40</b>								
	74	00	80	00								

The defined UICC/USIM configuration defined for this test case shall be used and made available on the UE. The UE is set to automatic PLMN selection mode.

The TT (NB-SS) transmits on the BCCH, with the following network parameters:

Cell A:

- TAI (MCC/MNC/TAC):254/011/0001.
- Access control: unrestricted.

Cell B:

- TAI (MCC/MNC/TAC):254/012/0001.
- Access control: unrestricted.

7.3.5.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	Run initial activation			
2	UE > TT	Send RRC CONNECTION REQUEST-NB	The RRC CONNECTION REQUEST-NB sent to the BCCH transmitting MCC/MNC 254/012 gets a RRC CONNECTION SETUP-NB as response from the TT	CR 1	
3	UE > TT	Send RRC CONNECTION SETUP COMPLETE-NB			

4	UE > TT	Send ATTACH REQUEST	During registration the TT performs an authentication and starts integrity by using the security procedure.		
5	TT > UE	Send ATTACH ACCEPT	The ATTACH ACCPT is sent with: - TAI (MCC/MNC/TAC): 254/012/0001 - GUTI: "25401200010266436587"	(CR 1)	
6	UE > TT	Send ATTACH COMPLETE	The TT sends RRC CONNECTION RELEASE-NB		
7	USER > UE	UE is soft powered down			
8	TT	Verify the contents of EF <sub>EPSLOCI</sub>	Reading EF <sub>EPSLOCI</sub> may also be performed before step 7)	CR 2	A.2/3

### 7.3.5.5 Acceptance criteria

CR 1 is verified in step 2). The requirement is met if in step 2) the UE sends a RRC CONNECTION REQUEST-NB to the BCCH transmitting MCC/MNC 254/012 to the TT (NB-SS).

If the request is sent correctly can also be verified in the ATTACH ACCEPT send by the NB-SS if it is containing:

- TAI (MCC/MNC/TAC):254/012/0001
- GUTI: "25401200010266436587"

CR 2 is verified by reading the contents of EF<sub>EPSLOCI</sub> in step 8). CR 2 is met if the file contains the following data:

#### EF<sub>EPSLOCI</sub> (EPS Information)

Logically:

GUTI: 25401200010266436587  
Last visited registered TAI: 254/012/0001  
EPS update status: updated

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	0B	F6	52	24	10	00	01	02	66	43	65	87
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>						
	52	24	10	00	01	00						

## 7.3.6 UE recognising the priority order of the User controlled PLMN selector over the Operator controlled PLMN selector list – E-UTRAN in NB-S1 mode

### 7.3.6.1 Definition and applicability

The User controlled PLMN selector list has a higher priority as the OPLMN selector list on which the UE shall register. The Radio Access Technology identifier defines the Radio network in which the UE shall register. The list is stored on the USIM in the EF<sub>PLMNwACT</sub>.

### 7.3.6.2 Conformance requirement

CR 1 When registering onto a VPLMN the UE shall consider the priority of UPLMNs first before the OPLMNs in the preferred list on the USIM.

Reference:

- TS 22.011 [18], clause 3.2.2.2;
- TS 31.102 [19], clause 4.2.53, 4.2.5 and 5.1.1.2.

CR 2 The modified value of  $EF_{EPSLOC}$  shall be available on the USIM when ending the test case.

### 7.3.6.3 Test purpose

The purpose of this test is to verify that the User controlled PLMN with a lower priority (defined by its position in  $EF_{PLMNwACT}$ ) takes precedence over the OPLMN with a higher priority when the UE performs a network selection. Hereby the new coding for RAT E-UTRAN in NB-IoT mode has to be handled correctly by the UE.

### 7.3.6.4 Method of test

#### 7.3.6.4.1 Initial conditions

The values of the E-UTRAN/EPC UICC as defined in clause 4.5.4 of the present document are used with the following exception:

#### $EF_{UST}$ (USIM Service Table)

Logically:

Service n°42:	Operator controlled PLMN selector with Access Technology	available
Service n°86:	Allowed CSG Lists and corresponding indications	not available

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Binary	xx1x xx11	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxxx xx1x	xxxx xxxx	xxxx xxxx
	<b>B9</b>	<b>B10</b>	<b>B11</b>	<b>B12</b>	<b>B13</b>	<b>B14</b>	<b>B15</b>	
	xxxx xxxx	xxxx xxxx	xx01 xxxx	xxxx xxxx	xxxx xxxx	xxxx xxxx	xxxx xxxx	

The coding of  $EF_{UST}$  shall conform with the capabilities of the USIM used.

#### $EF_{PLMNwACT}$ (User Controlled PLMN Selector with Access Technology)

Logically:

1 <sup>st</sup> PLMN:	244 081 (MCC MNC)
1 <sup>st</sup> ACT:	E-UTRAN
2 <sup>nd</sup> PLMN:	244 081
2 <sup>nd</sup> ACT:	GSM
3 <sup>rd</sup> PLMN:	244 083
3 <sup>rd</sup> ACT:	E-UTRAN
4 <sup>th</sup> PLMN:	244 082
4 <sup>th</sup> ACT:	GSM
5 <sup>th</sup> PLMN:	244 003
5 <sup>th</sup> ACT:	E-UTRAN
6 <sup>th</sup> PLMN:	244 004
6 <sup>th</sup> ACT:	UTRAN
7 <sup>th</sup> PLMN:	244 005
7 <sup>th</sup> ACT:	UTRAN
8 <sup>th</sup> PLMN:	244 081
8 <sup>th</sup> ACT:	UTRAN
9 <sup>th</sup> PLMN:	244 007
9 <sup>th</sup> ACT:	UTRAN
10 <sup>th</sup> PLMN:	244 008
10 <sup>th</sup> ACT:	E-UTRAN
11 <sup>th</sup> PLMN:	244 009
11 <sup>th</sup> ACT:	UTRAN
12 <sup>th</sup> PLMN:	244 010
12 <sup>th</sup> ACT:	E-UTRAN in NB-S1 mode

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	42	14	80	40	00	42	14	80	00	80	42	34
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	80	40	00	42	24	80	00	80	42	34	00	40
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>	<b>B31</b>	<b>B32</b>	<b>B33</b>	<b>B34</b>	<b>B35</b>	<b>B36</b>
	00	42	44	00	80	00	42	54	00	80	00	42
	<b>B37</b>	<b>B38</b>	<b>B39</b>	<b>B40</b>	<b>B41</b>	<b>B42</b>	<b>B43</b>	<b>B44</b>	<b>B45</b>	<b>B46</b>	<b>B47</b>	<b>B48</b>
	14	80	80	00	42	74	00	80	00	42	84	00
	<b>B49</b>	<b>B50</b>	<b>B51</b>	<b>B52</b>	<b>B53</b>	<b>B54</b>	<b>B55</b>	<b>B56</b>	<b>B57</b>	<b>B58</b>	<b>B59</b>	<b>B60</b>
	40	00	42	94	00	80	00	42	04	10	50	00

**EF<sub>OPLMNwACT</sub>** (OPLMN Selector)

Logically:

1<sup>st</sup> PLMN: 254 001 (MCC MNC)  
 1<sup>st</sup> ACT: E-UTRAN in NB-S1 mode  
 2<sup>nd</sup> PLMN: 254 001  
 2<sup>nd</sup> ACT: GSM  
 3<sup>rd</sup> PLMN: 254 002  
 3<sup>rd</sup> ACT: E-UTRAN  
 4<sup>th</sup> PLMN: 254 003  
 4<sup>th</sup> ACT: E-UTRAN  
 5<sup>th</sup> PLMN: 254 004  
 5<sup>th</sup> ACT: UTRAN  
 6<sup>th</sup> PLMN: 254 005  
 6<sup>th</sup> ACT: UTRAN  
 7<sup>th</sup> PLMN: 254 006  
 7<sup>th</sup> ACT: UTRAN  
 8<sup>th</sup> PLMN: 254 007  
 8<sup>th</sup> ACT: UTRAN

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	52	14	00	50	00	52	14	00	00	80	52	24
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	00	40	00	52	34	00	40	00	52	44	00	80
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>	<b>B31</b>	<b>B32</b>	<b>B33</b>	<b>B34</b>	<b>B35</b>	<b>B36</b>
	00	52	54	00	80	00	52	64	00	80	00	52
	<b>B37</b>	<b>B38</b>	<b>B39</b>	<b>B40</b>								
	74	00	80	00								

The defined UICC/USIM configuration defined for this test case shall be used and made available on the UE. The UE is set to automatic PLMN selection mode.

The TT (NB-SS) transmits on the BCCH, with the following network parameters:

Cell A:

- TAI (MCC/MNC/TAC):254/001/0001.
- Access control: unrestricted.

Cell B:

- TAI (MCC/MNC/TAC):244/010/0001.
- Access control: unrestricted.

## 7.3.6.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	Run initial activation			
2	UE > TT	Send RRC CONNECTION REQUEST-NB	The RRC CONNECTION REQUEST-NB sent to the BCCH transmitting MCC/MNC 244/010 gets a RRC CONNECTION SETUP-NB as response from the TT	CR 1	
3	UE > TT	Send RRC CONNECTION SETUP COMPLETE-NB			
4	UE > TT	Send ATTACH REQUEST	During registration the TT performs an authentication and starts integrity by using the security procedure.		
5	TT > UE	Send ATTACH ACCEPT	The ATTACH ACCPT is sent with: - TAI (MCC/MNC/TAC): 244/010/0001 - GUTI: "24401000010266436587"	(CR 1)	
6	UE > TT	Send ATTACH COMPLETE	The TT sends RRC CONNECTION RELEASE-NB		
7	USER > UE	UE is soft powered down			
8	TT	Verify the contents of EF <sub>EPSLOCI</sub>	Reading EF <sub>EPSLOCI</sub> may also be performed before step 7)	CR 2	A.2/3

## 7.3.6.5 Acceptance criteria

CR 1 is verified in step 2). The requirement is met if in step 2) the UE sends a RRC CONNECTION REQUEST-NB to the BCCH transmitting MCC/MNC 244/010 to the TT (NB-SS).

If the request is sent correctly can also be verified in the ATTACH ACCEPT send by the NB-SS if it is containing:

- TAI (MCC/MNC/TAC):244/010/0001
- GUTI: "24401000010266436587"

CR 2 is verified by reading the contents of EF<sub>EPSLOCI</sub> in step 8). CR 2 is met if the file contains the following data:

EF<sub>EPSLOCI</sub> (EPS Information)

Logically:

GUTI: 24401000010266436587  
Last visited registered TAI: 244/010/0001  
EPS update status: updated

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	0B	F6	42	04	10	00	01	02	66	43	65	87
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>						
	42	04	10	00	01	00						

### 7.3.7 UE recognising the priority order of the Operator controlled PLMN selector list using the ACT preference – E-UTRAN in NB-S1/ E-UTRAN in WB-S1 mode

#### 7.3.7.1 Definition and applicability

The Operator controlled PLMN selector list gives in priority order the preferred OPLMNs on which the UE shall register if no network of the User controlled PLMN selector list is available. The Radio Access Technology identifier

defines the Radio network in which the UE shall register. The list is stored on the USIM in the  $EF_{OPLMNwACT}$ . Update and deletion of OPLMNs shall not be possible by the subscriber by the use of the PIN.

### 7.3.7.2 Conformance requirement

CR 1 When registering onto a VPLMN the UE shall consider the priority of of OPLMNs in the preferred list on the USIM.

Reference:

- TS 22.011 [18], clause 3.2.2;
- TS 31.102 [19], clause 4.2.53, 4.2.5 and 5.1.1.2.

CR 2 The modified value of  $EF_{EPSLOC1}$  shall be available on the USIM when ending the test case.

### 7.3.7.3 Test purpose

The purpose of this test is to verify that the OPLMN with the higher priority (defined by its position in  $EF_{OPLMNwACT}$ ) takes precedence over the OPLMN with the lower priority when the UE performs a network selection. Hereby the new coding for RAT E-UTRAN in NB-IoT mode and E-UTRAN in WB-S1 mode has to be handled correctly by the UE.

### 7.3.7.4 Method of test

#### 7.3.7.4.1 Initial conditions

The values of the E-UTRAN/EPC UICC as defined in clause 4.5.4 of the present document are used with the following exception:

$EF_{UST}$  (USIM Service Table)

Logically:

Service n°42:	Operator controlled PLMN selector with Access Technology	available
Service n°86:	Allowed CSG Lists and corresponding indications	not available

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Binary	xx1x xx11	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxxx xx1x	xxxx xxxx	xxxx xxxx
	<b>B9</b>	<b>B10</b>	<b>B11</b>	<b>B12</b>	<b>B13</b>	<b>B14</b>	<b>B15</b>	
	xxxx xxxx	xxxx xxxx	xx01 xxxx	xxxx xxxx	xxxx xxxx	xxxx xxxx	xxxx xxxx	

The coding of  $EF_{UST}$  shall conform with the capabilities of the USIM used.

$EF_{OPLMNwACT}$  (OPLMN Selector)

Logically:

1 <sup>st</sup> PLMN:	254 012 (MCC MNC)
1 <sup>st</sup> ACT	E-UTRAN in NB-S1 mode
2 <sup>nd</sup> PLMN:	254 012
2 <sup>nd</sup> ACT	E-UTRAN in WB-S1 mode
3 <sup>rd</sup> PLMN:	254 002
3 <sup>rd</sup> ACT:	E-UTRAN
4 <sup>th</sup> PLMN:	254 012
4 <sup>th</sup> ACT:	GSM
5 <sup>th</sup> PLMN:	254 011
5 <sup>th</sup> ACT:	GSM
6 <sup>th</sup> PLMN:	254 005
6 <sup>th</sup> ACT:	UTRAN

7<sup>th</sup> PLMN: 254 006  
 7<sup>th</sup> ACT: UTRAN  
 8<sup>th</sup> PLMN: 254 007  
 8<sup>th</sup> ACT: UTRAN

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	52	24	10	50	00	52	24	10	60	00	52	24
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	00	40	00	52	24	10	00	80	52	14	10	00
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>	<b>B31</b>	<b>B32</b>	<b>B33</b>	<b>B34</b>	<b>B35</b>	<b>B36</b>
	80	52	54	00	80	00	52	64	00	80	00	52
	<b>B37</b>	<b>B38</b>	<b>B39</b>	<b>B40</b>								
	74	00	80	00								

The defined UICC/USIM configuration defined for this test case shall be used and made available on the UE. The UE is set to automatic PLMN selection mode.

The TT (NB-SS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC):254/012/0001.
- Access control: unrestricted.

#### 7.3.7.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	Run initial activation			
2	UE > TT	Send RRC CONNECTION REQUEST-NB	The RRC CONNECTION REQUEST-NB sent to the BCCH transmitting MCC/MNC 254/012 gets a RRC CONNECTION SETUP-NB as response from the TT	CR 1	
3	UE > TT	Send RRC CONNECTION SETUP COMPLETE-NB			
4	UE > TT	Send ATTACH REQUEST	During registration the TT performs an authentication and starts integrity by using the security procedure.		
5	TT > UE	Send ATTACH ACCEPT	The ATTACH ACCPT is sent with: - TAI (MCC/MNC/TAC): 254/012/0001 - GUTI: "25401200010266436587"	(CR 1)	
6	UE > TT	Send ATTACH COMPLETE	The TT sends RRC CONNECTION RELEASE-NB		
7	USER > UE	UE is soft powered down			
8	TT	Verify the contents of EF <sub>EPSLOCI</sub>	Reading EF <sub>EPSLOCI</sub> may also be performed before step 7)	CR 2	A.2/3

#### 7.3.7.5 Acceptance criteria

CR 1 is verified in step 2). The requirement is met if in step 2) the UE sends a RRC CONNECTION REQUEST-NB to the BCCH transmitting MCC/MNC 254/012 to the TT (NB-SS).

If the request is sent correctly can also be verified in the ATTACH ACCEPT send by the NB-SS if it is containing:

- TAI (MCC/MNC/TAC):254/012/0001
- GUTI: "25401200010266436587"

CR 2 is verified by reading the contents of EF<sub>EPSLOCI</sub> in step 8). CR 2 is met if the file contains the following data:

EF<sub>EPSLOCI</sub> (EPS Information)

Logically:

GUTI: 25401200010266436587  
 Last visited registered TAI: 254/012/0001  
 EPS update status: updated

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	0B	F6	52	24	10	00	01	02	66	43	65	87
	B13	B14	B15	B16	B17	B18						
	52	24	10	00	01	00						

### 7.3.8 UE recognising the priority order of the Operator controlled PLMN selector list using the ACT preference – E-UTRAN in NB-S1 mode/GSM

Not applicable as GERAN testing is involved.

### 7.3.9 UE recognising the priority order of the Operator controlled PLMN selector list using the ACT preference – E-UTRAN in WB-S1 mode/GSM

Not applicable as GERAN testing is involved.

## 7.4 Higher priority PLMN search handling

### 7.4.1 UE recognizing the search period of the Higher priority PLMN

GERAN/UTRAN test - not applicable

### 7.4.2 GSM/UMTS dual mode UEs recognizing the search period of the Higher priority PLMN

GERAN/UTRAN test - not applicable

### 7.4.3 UE recognizing the search period of the Higher priority PLMN – E-UTRAN

#### 7.4.3.1 Definition and applicability

The Higher priority PLMN list gives in priority order the Higher priority PLMN on which the UE shall register first. The Higher priority PLMN search period gives the time interval in which the UE shall search for a possible Higher priority PLMN registration.

#### 7.3.7.2 Conformance requirement

CR 1 After registered onto a VPLMN the UE shall consider the Higher priority PLMN search period timer and the priority order of the Higher priority PLMNs in the preferred lists on the USIM.

Reference:

- TS 22.011 [18], clause 3.2.2 and 3.2.2.5;
- TS 24.301 [21], clause 5.5.3.2
- TS 31.102 [19], clause 4.2.6.

CR 2 The modified value of  $EF_{EPSLOC1}$  shall be available on the USIM when ending the test case.

### 7.4.3.3 Test purpose

The purpose of this test is to verify that:

- 1) the Higher priority PLMN timer is read
- 2) the Higher priority PLMN takes precedence over the VPLMN in which the UE is currently registered in. Hereby the new coding for RAT E-UTRAN/NB-IoT has to be handled correctly by the UE.

### 7.4.3.4 Method of test

#### 7.4.3.4.1 Initial conditions

The values of the E-UTRAN/EPC UICC as defined in clause 4.5.4 of the present document are used with the following exception:

$EF_{HPPLMN}$  (Higher Priority PLMN Search period)

Logically:

Time interval between two searches: n minutes/n hours (2 hours)

Coding:

Byte	B1
Hex	01

NOTE; UEs only supporting any of the following or a combination of: NB-S1 mode or GERAN EC-GSM-IoT or Category M1 of E-UTRAN enhanced-MTC mode, T is 2 hours. Otherwise T is 6 minutes.

The defined UICC/USIM configuration defined for this test case shall be used and made available on the UE. The UE is set to automatic PLMN selection mode.

The TT (E-USS/NB-SS) transmits on the BCCH, with the following network parameters:

Cell A:

- TAI (MCC/MNC/TAC):244/008/0001.
- Access control: unrestricted.

Cell B, after the registration of UE:

- TAI (MCC/MNC/TAC):244/083/0001.
- Access control: unrestricted.

#### 7.4.3.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	Run initial activation			
2	UE > TT	Send RRC CONNECTION REQUEST / RRC CONNECTION REQUEST-NB	The RRC CONNECTION REQUEST / RRC CONNECTION REQUEST-NB sent to the BCCH transmitting MCC/MNC 244/008 gets a RRC CONNECTION SETUP / RRC CONNECTION SETUP-NB as response from the TT		
3	UE > TT	Send RRC CONNECTION SETUP COMPLETE / RRC CONNECTION SETUP COMPLETE-NB			

4	UE > TT	Send ATTACH REQUEST	During registration the TT performs an authentication and starts integrity by using the security procedure.		
5	TT > UE	Send ATTACH ACCEPT	The ATTACH ACCPT is sent with: - TAI (MCC/MNC/TAC): 244/008/0001 - GUTI: "24400800010266436587"		
6	UE > TT	Send ATTACH COMPLETE	The TT sends RRC CONNECTION RELEASE / RRC CONNECTION RELEASE-NB		
7	TT	Start transmitting on Cell B	The E-USS/NB-SS starts to send on the second BCCH with the MCC/MNC 244/083. An internal timer shall start to run.		
8	UE > TT	Send RRC CONNECTION REQUEST / RRC CONNECTION REQUEST-NB	The RRC CONNECTION REQUEST / RRC CONNECTION REQUEST-NB sent to the BCCH transmitting MCC/MNC 244/083 gets a RRC CONNECTION SETUP / RRC CONNECTION SETUP-NB as response from the TT	CR 1	
9	UE > TT	Send RRC CONNECTION SETUP COMPLETE / RRC CONNECTION SETUP COMPLETE-NB			
10	UE > TT	Send TRACKING AREA UPDATE REQUEST	During registration the TT performs an authentication and starts integrity by using the security procedure.		
11	TT > UE	Send TRACKING AREA UPDATE ACCEPT	The TRACKING AREA UPDATE ACCPT is sent with: - TAI (MCC/MNC/TAC): 244/083/0001 - GUTI: "24408300010266436587"	(CR 1)	
12	UE > TT	Send TRACKING AREA UPDATE COMPLETE	The TT sends RRC CONNECTION RELEASE / RRC CONNECTION RELEASE-NB		
13	USER > UE	UE is soft powered down			
14	TT	Verify the contents of EF <sub>EPSLOCI</sub>	Reading EF <sub>EPSLOCI</sub> may also be performed before step 7)		A.2/3

### 7.4.3.5 Acceptance criteria

CR 1 is verified in step 8). The requirement is met if in step 8) the UE sends a RRC CONNECTION REQUEST / RRC CONNECTION REQUEST-NB to the BCCH transmitting MCC/MNC 244/083 to the TT (E-USS or NB-SS).

If the request is sent correctly can also be verified in the TRACKING AREA UPDATE ACCEPT send by the TT (E-USS or NB-SS) if it is containing:

- TAI (MCC/MNC/TAC):244/083/0001
- GUTI: "24408300010266436587"

CR 2 is verified by reading the contents of EF<sub>EPSLOCI</sub> in step 14). CR 2 is met if the file contains the following data:

**EF<sub>EPSLOCI</sub>** (EPS Information)

Logically:

GUTI: 24408300010266436587  
Last visited registered TAI: 244/083/0001  
EPS update status: updated

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	0B	F6	42	34	80	00	01	02	66	43	65	87
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>						
	42	34	80	00	01	00						

#### 7.4.4 E-UTRAN/EPC capable UEs recognizing the search period of the Higher priority PLMN – GSM/E-UTRAN

Not applicable as GERAN testing is involved.

#### 7.4.5 E-UTRAN/EPC capable UEs recognizing the search period of the Higher priority PLMN – UTRAN/E-UTRAN

Not applicable as UTRAN testing is involved.

#### 7.4.6 UE recognising the search period of the higher priority PLMN – Satellite NG-RAN

FFS

#### 7.4.7 UE recognising the search period of the higher priority PLMN – NG-RAN

##### 7.4.7.1 Definition and applicability

The higher priority PLMN list gives in priority order the higher priority PLMN on which the UE shall register first. The higher priority PLMN search period gives the time interval in which the UE shall search for a possible higher priority PLMN registration.

##### 7.4.7.2 Conformance requirement

CR 1 After registered onto a VPLMN the UE shall consider the higher priority PLMN search period timer and the priority order of the higher priority PLMNs in the preferred lists on the USIM.

Reference:

- TS 22.011 [18], clauses 3.2.2 and 3.2.2.5;
- TS 24.501 [25], clause 5.5.1.2.4;
- TS 31.102 [19], clause 4.2.6.

CR 2 The UE shall start the search for a higher priority PLMN right after expiration of the search period timer.

Reference:

- TS 23.122 [41], clause 4.4.3.3.1.1;
- TS 31.102 [19], clause 4.2.6.

CR 3 The UE shall update EF<sub>5GS3GPPLOC1</sub>

Reference:

- TS 24.501 [25], 9.11.3;
- TS 31.102 [19], clause 4.4.11.2.

### 7.4.7.3 Test purpose

To verify that the higher priority PLMN timer is read and the higher priority PLMN takes precedence over the VPLMN in which the UE is currently registered in. Hereby the new coding for NG-RAN has to be handled correctly by the UE.

### 7.4.7.4 Method of test

#### 7.4.7.4.1 Initial conditions

The values of the 5G-NR UICC as defined in clause 4.5.9 of the present document are used with the following exceptions:

#### EF<sub>HPLMNwACT</sub> (HPLMN selector with Access Technology)

Logically:

1<sup>st</sup> PLMN: 244 083 (MCC MNC)  
1<sup>st</sup> ACT: NG-RAN

Coding:

Byte	B1	B2	B3	B4	B5
Hex	42	34	80	08	00

#### EF<sub>HPLMN</sub> (Higher Priority HPLMN Search period)

Logically:

Time interval: '01' - 6 minutes

Coding:

Byte	B1
Hex	01

#### EF<sub>UST</sub> (USIM Service Table)

Logically:

Service n°43: HPLMN selector with access technology available  
Service n°127: Control plane-based steering of UE in VPLMN not available

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Binary:	xxxx xx1x	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxxx x1xx	xxxx xxxx	xxxx xxxx
	<b>B9</b>	<b>B10</b>	<b>B11</b>	...	<b>B16</b>			
	xxxx xxxx	xxxx xxxx	xxxx xx11	...	x0x0 111x			

#### EF<sub>PLMNwACT</sub> (User controlled PLMN Selector with Access Technology)

Logically:

1<sup>st</sup> PLMN: 244 081 (MCC MNC)  
1<sup>st</sup> ACT: E-UTRAN  
2<sup>nd</sup> PLMN: 244 081  
2<sup>nd</sup> ACT: GSM  
3<sup>rd</sup> PLMN: 244 083  
3<sup>rd</sup> ACT: NG-RAN  
4<sup>th</sup> PLMN: 244 082  
4<sup>th</sup> ACT: GSM  
5<sup>th</sup> PLMN: 244 003

5<sup>th</sup> ACT: satellite NG-RAN  
 6<sup>th</sup> PLMN: 244 004  
 6<sup>th</sup> ACT: UTRAN  
 7<sup>th</sup> PLMN: 244 005  
 7<sup>th</sup> ACT: NG-RAN  
 8<sup>th</sup> PLMN: 244 081  
 8<sup>th</sup> ACT: UTRAN  
 9<sup>th</sup> PLMN: 244 007  
 9<sup>th</sup> ACT: UTRAN  
 10<sup>th</sup> PLMN: 244 008  
 10<sup>th</sup> ACT: E-UTRAN  
 11<sup>th</sup> PLMN: 244 009  
 11<sup>th</sup> ACT: UTRAN  
 12<sup>th</sup> PLMN: 244 010  
 12<sup>th</sup> ACT: E-UTRAN

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12	B13	B14	B15	B16
Hex	42	14	80	40	00	42	14	80	00	80	42	34	80	08	00	42
	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>	<b>B31</b>	<b>B32</b>
	24	80	00	80	42	34	00	04	00	42	44	00	80	00	42	54
	<b>B33</b>	<b>B34</b>	<b>B35</b>	<b>B36</b>	<b>B37</b>	<b>B38</b>	<b>B39</b>	<b>B40</b>	<b>B41</b>	<b>B42</b>	<b>B43</b>	<b>B44</b>	<b>B45</b>	<b>B46</b>	<b>B47</b>	<b>B48</b>
	00	08	00	42	14	80	80	00	42	74	00	80	00	42	84	00
	<b>B49</b>	<b>B50</b>	<b>B51</b>	<b>B52</b>	<b>B53</b>	<b>B54</b>	<b>B55</b>	<b>B56</b>	<b>B57</b>	<b>B58</b>	<b>B59</b>	<b>B60</b>				
	40	00	42	94	00	80	00	42	04	10	40	00				

The UICC/USIM configuration defined for this test case shall be used and made available on the UE. The UE is set to automatic PLMN selection mode.

The TT (NG-SS) is configured to transmit on the BCCH with the following network parameters:

Cell A:

- TAI (MCC/MNC/TAC): 244/008/000001;
- Access control: unrestricted.

Cell B:

- TAI (MCC/MNC/TAC): 244/083/000001;
- Access control: unrestricted.

The TT is transmitting on Cell A.

#### 7.4.7.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	Run initial activation			
2	UE > TT	Send <i>RRCRequest</i>	The UE sends a <i>RRCRequest</i> to the BCCH transmitting MCC/MNC 244/008.		
3	TT > UE	Send <i>RRCSetup</i>	<i>RRCSetup</i> is sent from Cell A		
4	UE > TT	Send <i>RRCSetupComplete</i>			
5	UE > TT	Send REGISTRATION REQUEST	The TT initiates the authentication and starts integrity by using the security procedure.		
6	TT > UE	Send REGISTRATION ACCEPT	The REGISTRATION ACCEPT is sent with: - TAI (MCC/MNC/TAC): 244/008/000001 - 5G-GUTI: "24400800010266436587"		
7	UE > TT	Send REGISTRATION COMPLETE			
8	TT > UE	Send <i>RRCRelease</i>			

9	TT > UE	Start transmitting on Cell B	The TT (NG-SS) starts to send on the BCCH with the MCC/MNC 244/083. An internal timer shall start to run.		
10	UE > TT	Send <i>RRCRequest</i>	The UE sends a <i>RRCRequest</i> to the BCCH transmitting MCC/MNC 244/083. The internal timer shall be stopped.	CR 2	
11	TT > UE	Send <i>RRCSetup</i>	<i>RRCSetup</i> is sent from Cell B		
12	UE > TT	Send <i>RRCSetupComplete</i>			
13	UE > TT	Send REGISTRATION REQUEST	The TT initiates the authentication and starts integrity by using the security procedure.		
14	TT > UE	Send REGISTRATION ACCEPT	The REGISTRATION ACCEPT is sent with: - TAI (MCC/MNC/TAC): 244/083/000001 - 5G-GUTI: "24408300010266436587"		
15	UE > TT	Send REGISTRATION COMPLETE		CR 1	
16	UE	Power off/deactivate the UE			
17	TT	Verify the contents of EF <sub>5GS3GPPLOC1</sub>	Reading EF <sub>5GS3GPPLOC1</sub> may also be performed before step 16)	CR 3	A.2/3

#### 7.4.7.5 Acceptance criteria

CR 1 is implicitly verified in step 15). The REGISTRATION COMPLETE on Cell B proves that the UE correctly handles the HPLMNwACT list.

CR 2 is verified in step 10), the UE shall send the *RRCRequest* to the higher priority PLMN after the given time interval is elapsed (+10%).

CR 3 is verified by reading the contents of EF<sub>5GS3GPPLOC1</sub> in step 17)

#### EF<sub>5GS3GPPLOC1</sub> (5GS 3GPP location information)

Logically:

5G-GUTI:

MCC: 244

MNC: 083

AMF Region ID: 0

AMF Set ID: 4

AMF Pointer: 2

5G-TMSI: 66 43 65 87

Last visited registered TAI in 5GS for 3GPP access: 244 083 000001

5GS update status for 3GPP access: 5U1 UPDATED

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	00	0B	F2	42	34	80	00	01	02	66	43	65
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>				
	87	42	34	80	00	00	01	00				

## 7.5 Void

---

# 8 Subscription independent tests

## 8.1 Phone book procedures

### 8.1.1 Recognition of a previously changed phonebook

GERAN test - not applicable

### 8.1.2 Update of the Phonebook Synchronization Counter (PSC)

#### 8.1.2.1 Definition and applicability

The phonebook synchronisation counter is used to unambiguously identify the status of the phonebook. Every time the phonebook is reset/deleted or the UID and/or the CC has run out of range, the PSC shall be regenerated.

The PSC is a part of the phonebook identifier.

#### 8.1.2.2 Conformance requirement

CR 1 Every time either the UID or the CC is incremented by the ME, the value of the content of the appropriate EF shall be tested.

Reference:

- TS 31.102 [4], clause 4.4.2.12.2.

CR 2 If either UID or CC has reached "FF FF", the related EF shall be set to "00 01" and the PSC is incremented.

Reference:

- TS 31.102 [4], clause 4.4.2.12.2.

#### 8.1.2.3 Test purpose

The purpose of this test is to verify that:

- 1) the ME has recognised that the values of UID and CC has changed;
- 2) the ME resets the value of  $EF_{UID}$  and  $E_{FCC}$ ;
- 3) the ME updates  $EF_{PSC}$ .

#### 8.1.2.4 Method of test

##### 8.1.2.4.1 Initial conditions

The values of the Default UICC as defined in clause 4.5.2 of the present document are used with the following exceptions:

$EF_{UID}$  (Unique Identifier)

Logically:

one record is set to 'FF FF'

Coding:

Byte	B1	B2
Hex	FF	FF

**EF<sub>PUID</sub>** (Previous Unique Identifier)

Logically:

record is set to 'FF FF'

Coding:

Byte	B1	B2
Hex	FF	FF

**EF<sub>CC</sub>** (Change Counter)

Logically:

record is set to 'FF FF'

Coding:

Byte	B1	B2
Hex	FF	FF

**EF<sub>PSC</sub>** (Phonebook Synchronisation Counter)

Logically:

record is set to '00 00 FF FF'

Coding:

Byte	B1	B2	B3	B4
Hex	00	00	FF	FF

At least one phonebook entry shall be empty and available for creating a new entry (e.g. an appropriate ADN record).

The TT does not need to transmit on any BCCH.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and runs an initial activation.

## 8.1.2.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	USER	Create a new phonebook entry	This may be done by storing a new telephone number in an empty ADN record		
2	UE	Perform the regeneration of the UID records	It is assumed that the UE will indicate the time it needs to perform the regeneration by displaying a busy signal to the user.	(CR 1)	
3	TT	READ EF <sub>UID</sub> , EF <sub>PSC</sub> and EF <sub>CC</sub>	Read and verify the content of the listed EFs	CR 1 CR 2	A.2/1 OR A.2/2 OR A.2/3

### 8.1.2.5 Acceptance criteria

CR 1 and CR 2 are explicitly verified in (or after) step 3) by any verification method listed in Table A.2. The requirements are met if:

- 1) the EF<sub>UID</sub> (Unique Identifier) has been regenerated with UID values starting with "00 01".

NOTE: The UID values may be stored in any order, but shall be unique. The entry in EF<sub>UID</sub> with value FF FF (the maximum value) shall have been replaced by an appropriate value which shall be distinguishable to the maximum value.

- 2) EF<sub>PUID</sub> contains a UID value (other than FFFF) that is present in EF<sub>UID</sub>.
- 3) EF<sub>CC</sub> contains the following value:

**EF<sub>CC</sub>** (Change Counter)

Logically:

record is set to "00 01"

Coding:

Byte	B1	B2
Hex	00	01

- 4) EF<sub>PSC</sub> contains the following value:

**EF<sub>PSC</sub>** (Phonebook Synchronisation Counter)

Logically:

record is set to "00 01 00 00"

Coding:

Byte	B1	B2	B3	B4
Hex	00	01	00	00

## 8.1.3 Handling of BCD number/ SSC content extension

### 8.1.3.1 Definition and applicability

The length of BCD number/SSC contents in EF<sub>ADN</sub> byte gives the number of bytes of the following two data items containing actual BCD number/SSC information. This means that the maximum value is 11, even when the actual ADN/SSC information length is greater than 11. When an ADN/SSC has extension, it is indicated by the extension1 identifier being unequal to 'FF'. The remainder is stored in the EF<sub>EXT1</sub> with the remaining length of the additional data being coded in the appropriate additional record itself.

### 8.1.3.2 Conformance requirement

CR 1 The ME shall support the BCD number/SSC extension for EF<sub>ADN</sub>.

Reference:

- TS 31.102 [4], clauses 4.4.2.3 and 4.4.2.4.

### 8.1.3.3 Test purpose

The purpose of this test is to verify that the ME is able to read and update BCD numbers/ SSC content with and without extension correctly in EF<sub>ADN</sub> and EF<sub>EXT1</sub>.

### 8.1.3.4 Method of test

#### 8.1.3.4.1 Initial conditions

The values of the Default UICC as defined in clause 4.5.2 of the present document are used with the following exceptions:

Only the global phonebook is present, containing an **EF<sub>PBR</sub>** (Phonebook Reference File) were only **EF<sub>ADN</sub>** and **EF<sub>EXT1</sub>** are present.

#### **EF<sub>ADN</sub>** (Abbreviated dialling numbers)

Logically:

10 records, each record non-empty and unique. Unless otherwise stated, the ADN records shall not use extended BCD numbers/SSC strings

Record 1:

Length of alpha identifier: 32 characters;  
 Alpha identifier: "Contact001";  
 Length of BCD number: 11 bytes;  
 TON and NPI: Telephony and International;  
 Dialed number: 00112233445566778899;  
 CCI: 'FF';  
 Ext1: '01'.

Coding for record 1:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	...
Hex	43	6F	6E	74	61	63	74	30	30	31	FF	...
	<b>B32</b>	<b>B33</b>	<b>B34</b>	<b>B35</b>	<b>B36</b>	<b>B37</b>	<b>B38</b>	<b>B39</b>	<b>B40</b>	<b>B41</b>	<b>B42</b>	<b>B43</b>
	FF	0B	91	00	11	22	33	44	55	66	77	88
	<b>B44</b>	<b>B45</b>	<b>B46</b>									
	99	FF	01									

Record 2:

Length of alpha identifier: 32 characters;  
 Alpha identifier: "Contact002";  
 Length of BCD number: 11 bytes;  
 TON and NPI: Telephony and International;  
 Dialed number: 01234567890123456789;  
 CCI: 'FF';  
 Ext1: 'FF'.

Coding for record 2:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	...
Hex	43	6F	6E	74	61	63	74	30	30	32	FF	...
	<b>B32</b>	<b>B33</b>	<b>B34</b>	<b>B35</b>	<b>B36</b>	<b>B37</b>	<b>B38</b>	<b>B39</b>	<b>B40</b>	<b>B41</b>	<b>B42</b>	<b>B43</b>
	FF	0B	91	10	32	54	76	98	10	32	54	76
	<b>B44</b>	<b>B45</b>	<b>B46</b>									
	98	FF	FF									

Record 3:

Length of alpha identifier: 32 characters;  
 Alpha identifier: "Contact003";  
 Length of BCD number: 11 bytes;  
 TON and NPI: Telephony and International;  
 Dialed number: 99887766554433221100;  
 CCI: 'FF';  
 Ext1: '02'.

Coding for record 3:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	...
Hex	43	6F	6E	74	61	63	74	30	30	33	FF	...
	<b>B32</b>	<b>B33</b>	<b>B34</b>	<b>B35</b>	<b>B36</b>	<b>B37</b>	<b>B38</b>	<b>B39</b>	<b>B40</b>	<b>B41</b>	<b>B42</b>	<b>B43</b>
	FF	0B	91	99	88	77	66	55	44	33	22	11
	<b>B44</b>	<b>B45</b>	<b>B46</b>									
	00	FF	02									

Record 4:

Length of alpha identifier: 32 characters;  
 Alpha identifier: "Contact004";  
 Length of BCD number: 9 bytes;  
 TON and NPI: Telephony and International;  
 Dialed number: 1212121212121212;  
 CCI: 'FF';  
 Ext1: 'FF'.

Coding for record 4:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	...
Hex	43	6F	6E	74	61	63	74	30	30	34	FF	...
	<b>B32</b>	<b>B33</b>	<b>B34</b>	<b>B35</b>	<b>B36</b>	<b>B37</b>	<b>B38</b>	<b>B39</b>	<b>B40</b>	<b>B41</b>	<b>B42</b>	<b>B43</b>
	FF	09	91	21	21	21	21	21	21	21	21	FF
	<b>B44</b>	<b>B45</b>	<b>B46</b>									
	FF	FF	02									

Record 7:

Length of alpha identifier: 32 characters;  
 Alpha identifier: "Contact007";  
 Length of BCD number: 3 bytes;  
 TON and NPI: Telephony and International;  
 Dialed number: 678;  
 CCI: 'FF';  
 Ext1: 'FF'.

Coding for record 7:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	...
Hex	43	6F	6E	74	61	63	74	30	30	37	FF	...
	<b>B32</b>	<b>B33</b>	<b>B34</b>	<b>B35</b>	<b>B36</b>	<b>B37</b>	<b>B38</b>	<b>B39</b>	<b>B40</b>	<b>B41</b>	<b>B42</b>	<b>B43</b>
	FF	03	91	76	F8	FF	FF	FF	FF	FF	FF	FF
	<b>B44</b>	<b>B45</b>	<b>B46</b>									
	FF	FF	FF									

#### EF<sub>EXT1</sub> (Extension 1)

Logically:

4 records

Record 1:

Record type: '02';  
 Extension data: "01234567890123456789";  
 Identifier: 'FF'.

Coding for record 1:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	02	0A	10	32	54	76	98	10	32	54	76	98
	<b>B13</b>											
	FF											

Record 2:

Record type: '02';  
 Extension data: "11p12345";  
 Identifier: 'FF'.

Coding for record 2:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	02	0A	99	88	77	66	55	44	33	22	11	00
	<b>B13</b>											
	03											

Record 3:

Record type: '02';  
 Extension data: "11p12345";  
 Identifier: 'FF'.

Coding for record 3:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	02	04	11	1C	32	54	FF	FF	FF	FF	FF	FF
	<b>B13</b>											
	FF											

Record 4:

Record type: '00';  
 Extension data: empty;  
 Identifier: 'FF'.

Coding for record 4:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	00	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF
	<b>B13</b>											
	FF											

The TT does not need to transmit on any BCCH.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and runs an initial activation.

#### 8.1.3.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	USER	Select the global phonebook	The user shall use an MMI dependent procedure to select the global phonebook.		
2	TT	READ EF <sub>PBR</sub>		CR 1	A.2/1 OR A.2/2
3	USER	Change BCD number of the entry "Contact002" from EF <sub>ADN</sub>	The user shall change the BCD number of the entry "Contact002" to 22446622446622446600777888999.		

			If the maximum number of BCD digits supported for the global phonebook update is less than in the requested input BCD number string, then the user shall enter the BCD number string as requested, but only up to the maximum number of BCD digits which are supported for updating.		
4	TT	READ EF <sub>ADN</sub> and EF <sub>EXT1</sub>		CR 1	A.2/1 OR A.2/2 (OR A.2/3)
5	USER	Extend the BCD number of the entry "Contact007" from EF <sub>ADN</sub>	The user shall extend the BCD number of the entry "Contact007" to "01234567890123456789777888999". If the maximum number of BCD digits supported for the global phonebook update is less than in the requested input BCD number string, then the user shall enter the BCD number string as requested, but only up to the maximum number of BCD digits which are supported for updating.		
6	TT	READ EF <sub>ADN</sub> and EF <sub>EXT1</sub>		CR 1	A.2/1 OR A.2/2 (OR A.2/3)
7	USER	Delete the entry "Contact001" from EF <sub>ADN</sub>			
8	TT	READ EF <sub>ADN</sub> and EF <sub>EXT1</sub>		CR 1	A.2/1 OR A.2/2 (OR A.2/3)
9	USER	Change BCD number of the entry "Contact002" from EF <sub>ADN</sub>	The user shall change the BCD number of the entry "Contact002" to "22446622446600".		
10	TT	READ EF <sub>ADN</sub> and EF <sub>EXT1</sub>		CR 1	A.2/1 OR A.2/2 (OR A.2/3)
11	USER	Create a new entry in EF <sub>ADN</sub>	The user shall create the new phonebook entry "NewContact" with the BCD number "1234567890123456789012345678901234567890123456789012". If the maximum number of BCD digits supported for the global phonebook update is less than in the requested input BCD number string, then the user shall enter the BCD number string as requested, but only up to the maximum number of BCD digits which are supported for updating.		
12	TT	READ EF <sub>ADN</sub> and EF <sub>EXT1</sub>		CR 1	A.2/1 OR A.2/2 (OR A.2/3)
13	USER	Delete the entry "Contact003" from EF <sub>ADN</sub>			
14	TT	READ EF <sub>ADN</sub> and EF <sub>EXT1</sub>		CR 1	A.2/1 OR A.2/2

					(OR A.2/3)
--	--	--	--	--	---------------

### 8.1.3.5 Acceptance criteria

CR 1 is explicitly verified in step 2) by using the methods A.2/1 or A.2/2 CR 1 the requirement is met if the ME has selected the global phonebook and has read EF<sub>PBR</sub>.

CR 1 is explicitly verified in (or after, when using method A.2/3) steps 4), 6), 8), 10), 12) and 14), by any verification method listed in Table A.2. The requirement is met if:

in step 4), the global phonebook contains a record with "22446622446622446600" as BCD number and "04" as extension record identifier. EF<sub>EXT1</sub> shall contain a record with "Additional data" as record type, the BCD number extension "777888999" and "FF" as identifier to indicate the end of the chain.

NOTE: If the maximum number of BCD digits supported for global phonebook updating is less than in the requested input BCD number, then EF<sub>ADN</sub> and EF<sub>EXT1</sub> shall contain the BCD number as entered on the MMI. has selected selected the global phonebook and shall have read EF<sub>PBR</sub> in the global phonebook.

in step 6), the ME acted to prevent storage of the extended BCD number, e.g. by giving an indication to the user or not allowing to enter the extended number. EF<sub>EXT1</sub> has not been updated and the extension record identifier of the entry "Contact007" remains as "FF".

in step 8), the records of EF<sub>ADN</sub> and EF<sub>EXT1</sub> for the phonebook entry "Contact001" are empty, i.e. the EF<sub>ADN</sub> record shall be "FF... FF" and the EF<sub>EXT1</sub> record shall be "00FF... FF".

in step 10), the record of EF<sub>EXT1</sub> which was used to store the BCD number extension "777888999" is empty and the record of EF<sub>ADN</sub> used for storing the entry with the alpha identifier "Contact002" contains the BCD number "22446622446600" and the extension record identifier "FF".

in step 12), a record of EF<sub>ADN</sub> contains "NewContact" as alpha identifier, "12345678901234567890" as BCD number and uses an extension record identifier unequal to "FF".

NOTE: The EF<sub>EXT1</sub> record which was indicated in the EF<sub>ADN</sub> record used in this case shall contain "Additional data" as record type, "12345678901234567890" as BCD number and an extension record identifier unequal to "FF", while the EF<sub>EXT1</sub> record used to continue the chain inside EF<sub>EXT1</sub> shall contain "Additional data" as record type, "123456789012" as BCD number and "FF" as extension record identifier.

If the maximum number of BCD digits supported for global phonebook updating is less than the requested input BCD number, then EF<sub>ADN</sub> and EF<sub>EXT1</sub> shall contain the BCD number as entered on the MMI.

in step 14), the EF<sub>ADN</sub> record, which was used to store the data for "Contact003" and the related records of EF<sub>EXT1</sub> are empty.

If A.2/3 is the only method used, the reading of EF<sub>PBR</sub> in step 2) can be handled as implicitly verified if all the following phonebook actions can be executed successfully.

## 8.1.4 Phonebook selection

### 8.1.4.1 Definition and applicability

The UICC may contain a global phonebook, or application specific phonebooks, or both in parallel. When both phonebook types co-exist, they are independent and no data is shared. In this case, it shall be possible for the user to select which phonebook the user would like to access.

### 8.1.4.2 Conformance requirement

CR 1 The ME shall support the global and the application specific phonebooks.

Reference:

- TS 31.102 [4], clauses 4.4.2.

### 8.1.4.3 Test purpose

The purpose of this test is to verify that:

- 1) the ME offers a possibility to select which phonebook the user would like to use. If both, the global and the local phonebook, co-exist;
- 2) the data contained in the local phonebook can be read and updated correctly;
- 3) the data contained in the global phonebook can be read and updated correctly.

### 8.1.4.4 Method of test

#### 8.1.4.4.1 Initial conditions

The values of the Default UICC as defined in clause 4.5.2 of the present document are used with the following exceptions:

The local and the global phonebook are both present.

The local phonebook shall contain an:

**EF<sub>PBR</sub>** (Phonebook Reference File) were only **EF<sub>ADN</sub>** and **EF<sub>EXT1</sub>** are present:

**EF<sub>ADN</sub>** (Abbreviated dialling numbers)

Logically:

10 records, each record non-empty and unique.

Record 4:

Length of alpha identifier: 32 characters;  
 Alpha identifier: "Contact004";  
 Length of BCD number: 3 bytes;  
 TON and NPI: Telephony and International;  
 Dialed number: 004;  
 CCI: 'FF';  
 Ext1: 'FF'.

Coding for record 4:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	...
Hex	43	6F	6E	74	61	63	74	30	30	34	FF	...
	<b>B32</b>	<b>B33</b>	<b>B34</b>	<b>B35</b>	<b>B36</b>	<b>B37</b>	<b>B38</b>	<b>B39</b>	<b>B40</b>	<b>B41</b>	<b>B42</b>	<b>B43</b>
	FF	03	91	00	F4	FF	FF	FF	FF	FF	FF	FF
	<b>B44</b>	<b>B45</b>	<b>B46</b>									
	FF	FF	FF									

Record 5:

Length of alpha identifier: 32 characters;  
 Alpha identifier: "Contact005";  
 Length of BCD number: 3 bytes;  
 TON and NPI: Telephony and International;  
 Dialed number: 1234;  
 CCI: 'FF';  
 Ext1: None.

Coding for record 5:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	...
Hex	43	6F	6E	74	61	63	74	30	30	35	FF	...
	<b>B32</b>	<b>B33</b>	<b>B34</b>	<b>B35</b>	<b>B36</b>	<b>B37</b>	<b>B38</b>	<b>B39</b>	<b>B40</b>	<b>B41</b>	<b>B42</b>	<b>B43</b>
	FF	03	91	21	43	FF	FF	FF	FF	FF	FF	FF
	<b>B44</b>	<b>B45</b>	<b>B46</b>									
	FF	FF	FF									

The global phonebook shall contain an:

$EF_{PBR}$  (Phonebook Reference File) were only  $EF_{ADN}$  is present:

$EF_{ADN}$  (Abbreviated dialling numbers)

Logically:

8 records, record 3 and record 6 are empty, each record non-empty is unique.

Record 1:

Length of alpha identifier: 32 characters;  
 Alpha identifier: "Contact001";  
 Length of BCD number: 3 bytes;  
 TON and NPI: Telephony and International;  
 Dialed number: 001;  
 CCI: 'FF';  
 Ext1: 'FF'.

Coding for record 1:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	...
Hex	43	6F	6E	74	61	63	74	30	30	31	FF	...
	<b>B32</b>	<b>B33</b>	<b>B34</b>	<b>B35</b>	<b>B36</b>	<b>B37</b>	<b>B38</b>	<b>B39</b>	<b>B40</b>	<b>B41</b>	<b>B42</b>	<b>B43</b>
	FF	03	91	00	F1	FF	FF	FF	FF	FF	FF	FF
	<b>B44</b>	<b>B45</b>	<b>B46</b>									
	FF	FF	FF									

Record 2:

Length of alpha identifier: 32 characters;  
 Alpha identifier: "Contact002";  
 Length of BCD number: 3 bytes;  
 TON and NPI: Telephony and International;  
 Dialed number: 002;  
 CCI: 'FF';  
 Ext1: 'FF'.

Coding for record 2:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	...
Hex	43	6F	6E	74	61	63	74	30	30	32	FF	...
	<b>B32</b>	<b>B33</b>	<b>B34</b>	<b>B35</b>	<b>B36</b>	<b>B37</b>	<b>B38</b>	<b>B39</b>	<b>B40</b>	<b>B41</b>	<b>B42</b>	<b>B43</b>
	FF	03	91	00	F2	FF	FF	FF	FF	FF	FF	FF
	<b>B44</b>	<b>B45</b>	<b>B46</b>									
	FF	FF	FF									

Record 4:

Length of alpha identifier: 32 characters;  
 Alpha identifier: "Contact004";  
 Length of BCD number: 3 bytes;  
 TON and NPI: Telephony and International;  
 Dialed number: 0041;  
 CCI: 'FF';  
 Ext1: 'FF'.

Coding for record 4:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	...
Hex	43	6F	6E	74	61	63	74	30	30	34	FF	...
	<b>B32</b>	<b>B33</b>	<b>B34</b>	<b>B35</b>	<b>B36</b>	<b>B37</b>	<b>B38</b>	<b>B39</b>	<b>B40</b>	<b>B41</b>	<b>B42</b>	<b>B43</b>
	FF	03	91	00	14	FF	FF	FF	FF	FF	FF	FF
	<b>B44</b>	<b>B45</b>	<b>B46</b>									
	FF	FF	FF									

Record 5:

Length of alpha identifier: 32 characters;  
 Alpha identifier: "Contact005";  
 Length of BCD number: 3 bytes;  
 TON and NPI: Telephony and International;  
 Dialed number: 1234;  
 CCI: 'FF';  
 Ext1: 'FF'.

Coding for record 5:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	...
Hex	43	6F	6E	74	61	63	74	30	30	35	FF	...
	<b>B32</b>	<b>B33</b>	<b>B34</b>	<b>B35</b>	<b>B36</b>	<b>B37</b>	<b>B38</b>	<b>B39</b>	<b>B40</b>	<b>B41</b>	<b>B42</b>	<b>B43</b>
	FF	03	91	21	43	FF	FF	FF	FF	FF	FF	FF
	<b>B44</b>	<b>B45</b>	<b>B46</b>									
	FF	FF	FF									

Record 7:

Length of alpha identifier: 32 characters;  
 Alpha identifier: "Contact007";  
 Length of BCD number: 3 bytes;  
 TON and NPI: Telephony and International;  
 Dialed number: 007;  
 CCI: 'FF';  
 Ext1: 'FF'.

Coding for record 7:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	...
Hex	43	6F	6E	74	61	63	74	30	30	37	FF	...
	<b>B32</b>	<b>B33</b>	<b>B34</b>	<b>B35</b>	<b>B36</b>	<b>B37</b>	<b>B38</b>	<b>B39</b>	<b>B40</b>	<b>B41</b>	<b>B42</b>	<b>B43</b>
	FF	03	91	00	F7	FF	FF	FF	FF	FF	FF	FF
	<b>B44</b>	<b>B45</b>	<b>B46</b>									
	FF	FF	FF									

Record 8:

Length of alpha identifier: 32 characters;  
 Alpha identifier: "Contact008";  
 Length of BCD number: 3 bytes;  
 TON and NPI: Telephony and International;  
 Dialed number: 008;  
 CCI: 'FF';  
 Ext1: 'FF'.

Coding for record 7:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	...
Hex	43	6F	6E	74	61	63	74	30	30	38	FF	...
	<b>B32</b>	<b>B33</b>	<b>B34</b>	<b>B35</b>	<b>B36</b>	<b>B37</b>	<b>B38</b>	<b>B39</b>	<b>B40</b>	<b>B41</b>	<b>B42</b>	<b>B43</b>
	FF	03	91	00	F8	FF	FF	FF	FF	FF	FF	FF
	<b>B44</b>	<b>B45</b>	<b>B46</b>									
	FF	FF	FF									

The TT does not need to transmit on any BCCH.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and runs an initial activation.

#### 8.1.4.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	ME	READ EF <sub>UST</sub>	The ME shall have read the status of the local phonebook in EF <sub>UST</sub>	CR 1	A.2/1 OR A.2/2
2	USER	Select the global phonebook	The user shall use an MMI dependent procedure to select the global phonebook		
3	TT	READ EF <sub>PBR</sub>	The ME shall have read EF <sub>PBR</sub> of the global phonebook.	CR 1	A.2/1 OR A.2/2
4	USER	Read "Contact005"	The global phonebook record with the alpha identifier "Contact005" and the dialling number "+1234" shall be presented to the user	CR 1	
5	USER	Change "Contact005"	The dialling number of the global phonebook record with the alpha identifier "Contact005" shall be set to "+1122330"		
6	TT	READ EF <sub>ADN</sub>	The ME shall have given an indication to the user that the phonebook update has been performed successfully	CR 1	A.2/1 OR A.2/2 (OR A.2/3)
7	USER	Add an entry "Contact006"	The new entry with alpha identifier "Contact006" and "+9876543210" as associated dialling number shall be added to the global phonebook		
8	TT	READ EF <sub>ADN</sub>		CR 1	A.2/1 OR A.2/2 (OR A.2/3)
9	USER	Select the local phonebook	The user shall use an MMI dependent procedure to select the local phonebook		
10	TT	READ EF <sub>PBR</sub>	The ME shall have read EF <sub>PBR</sub> of the local phonebook.	CR 1	A.2/1 OR A.2/2
11	USER	Read "Contact005"	The local phonebook record with the alpha identifier "Contact005" and the dialling number "+1234" shall be presented to the user	CR 1	
12	USER	Change BCD number of the entry "Contact005" from EF <sub>ADN</sub>	The user shall change the BCD number of the entry "Contact005" to "+11223345".		
13	TT	READ EF <sub>ADN</sub>	The ME shall have given an indication to the user that the phonebook update has been performed successfully	CR 1	A.2/1 OR A.2/2 (OR A.2/3)
14	USER	Create a new entry in EF <sub>ADN</sub>	The user shall try to add a new entry with the values "Contact007" as alpha		

			identifier and "+007" as associated dialling number to the local phonebook		
15	TT	READ EF <sub>ADN</sub>	The ME shall have given an indication to the user that the phonebook update cannot be performed	CR 1	A.2/1 OR A.2/2 (OR A.2/3)
16	USER	Delete the entry "Contact004" from EF <sub>ADN</sub>			
17	TT	READ EF <sub>ADN</sub>	The ME shall have given an indication to the user that the deletion in the phonebook has been performed successfully	CR 1	A.2/1 OR A.2/2 (OR A.2/3)
18	USER	Create a new entry in EF <sub>ADN</sub>	The user shall try to add a new entry with the values "Contact007" as alpha identifier and "+007" as associated dialling number to the local phonebook		
19	TT	READ EF <sub>ADN</sub>		CR 1	A.2/1 OR A.2/2 (OR A.2/3)
20	USER	Select the global phonebook	The user shall use an MMI dependent procedure to select the global phonebook		
21	TT	READ EF <sub>PBR</sub>	The ME shall have read EF <sub>PBR</sub> of the global phonebook.	CR 1	A.2/1 OR A.2/2
22	USER	Delete the entry "Contact007" from EF <sub>ADN</sub>			
23	TT	READ EF <sub>ADN</sub>	The ME shall have given an indication to the user that the deletion in the phonebook has been performed successfully	CR 1	A.2/1 OR A.2/2 (OR A.2/3)

### 8.1.4.5 Acceptance criteria

In step 4), step 11) and step 15) CR 1 is verified via the MMI. The requirement is met if:

- in steps 4) and 11), the correct phonebook entry is presented to the user;
- in step 15) an appropriate error message is presented to the user.

CR 1 is explicitly verified in (or after, when using method A.2/3) steps 6), 8), 13), 17), 19) and 23), by any verification method listed in Table A.2. The requirement is met if:

- in step 6), the user gets the indication that global phonebook update has been performed successfully, and if the global phonebook contains an ADN record with the alpha identifier "Contact005" and a dialling number set to "+1122330".
- in step 8), the global phonebook contains an ADN record with the alpha identifier "Contact006" and a dialling number set to "+9876543210".
- in step 13), the user gets the indication that the update of the local phonebook has been performed successfully, and if the local phonebook contains an ADN record with the alpha identifier "Contact005" and a dialling number set to "+11223345".
- in step 17), the user gets the indication that the deletion from the local phonebook has been performed successfully, and if the record which was used to store the entry "Contact004" is empty.
- in step 19), the local phonebook contains an ADN record with the alpha identifier "Contact007" and a dialling number set to "+007".

in step 23), the user gets the indication that the deletion from the global phonebook has been performed successfully, and if the record which was used to store the entry "Contact007" is empty.

If A.2/3 is the only method used, the reading of EF<sub>UST</sub> in step 1) and of EF<sub>PBR</sub> in steps 3), 10) and 21) can be handled as implicitly verified if all the following phonebook actions can be executed successfully.

## 8.1.5 Local Phonebook handling

### 8.1.5.1 Definition and applicability

The UICC may contain a global phonebook, or application specific phonebooks, or both in parallel.

### 8.1.5.2 Conformance requirement

CR 1 The ME shall support the the local phonebook.

Reference:

- TS 31.102 [4], clauses 4.4.2.

### 8.1.5.3 Test purpose

The purpose of this test is to verify that:

- 1) the ME supports the local phonebook without existence of the global phonebook;
- 2) the data contained in the local phonebook can be read and updated correctly;

### 8.1.5.4 Method of test

#### 8.1.5.4.1 Initial conditions

The values of the Default UICC as defined in clause 4.5.2 of the present document are used with the following exceptions:

Only the local phonebook is present, containing an EF<sub>PBR</sub> (Phonebook Reference File) were only EF<sub>ADN</sub> and EF<sub>EXT1</sub> are present.

EF<sub>ADN</sub> (Abbreviated dialling numbers)

Logically:

10 records, each record non-empty and unique.

Record 4:

Length of alpha identifier: 32 characters;  
 Alpha identifier: "Contact004";  
 Length of BCD number: 3 bytes;  
 TON and NPI: Telephony and International;  
 Dialed number: 004;  
 CCI: 'FF';  
 Ext1: 'FF'.

Coding for record 4:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	...
Hex	43	6F	6E	74	61	63	74	30	30	34	FF	...
	<b>B32</b>	<b>B33</b>	<b>B34</b>	<b>B35</b>	<b>B36</b>	<b>B37</b>	<b>B38</b>	<b>B39</b>	<b>B40</b>	<b>B41</b>	<b>B42</b>	<b>B43</b>
	FF	03	91	00	F4	FF	FF	FF	FF	FF	FF	FF
	<b>B44</b>	<b>B45</b>	<b>B46</b>									
	FF	FF	FF									

Record 5:

Length of alpha identifier: 32 characters;  
 Alpha identifier: "Contact005";  
 Length of BCD number: 3 bytes;  
 TON and NPI: Telephony and International;  
 Dialed number: 1234;  
 CCI: 'FF';  
 Ext1: None.

Coding for record 5:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	...
Hex	43	6F	6E	74	61	63	74	30	30	35	FF	...
	<b>B32</b>	<b>B33</b>	<b>B34</b>	<b>B35</b>	<b>B36</b>	<b>B37</b>	<b>B38</b>	<b>B39</b>	<b>B40</b>	<b>B41</b>	<b>B42</b>	<b>B43</b>
	FF	03	91	21	43	FF	FF	FF	FF	FF	FF	FF
	<b>B44</b>	<b>B45</b>	<b>B46</b>									
	FF	FF	FF									

The TT does not need to transmit on any BCCH.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and run an initial activation before step 1).

#### 8.1.5.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	USER	Select the global phonebook	The user shall use an MMI dependent procedure to select the global phonebook.		
2	TT	READ EF <sub>PBR</sub>		CR 1	A.2/1 OR A.2/2
3	USER	Change BCD number of the entry "Contact002" from EF <sub>ADN</sub>	The user shall change the BCD number of the entry "Contact002" to 22446622446622446600777888999. If the maximum number of BCD digits supported for the global phonebook update is less than in the requested input BCD number string, then the user shall enter the BCD number string as requested, but only up to the maximum number of BCD digits which are supported for updating.		
4	TT	READ EF <sub>ADN</sub> and EF <sub>EXT1</sub>		CR 1	A.2/1 OR A.2/2 (OR A.2/3)
5	USER	Extend the BCD number of the entry "Contact007" from EF <sub>ADN</sub>	The user shall extend the BCD number of the entry "Contact007" to "01234567890123456789777888999". If the maximum number of BCD digits supported for the global phonebook update is less than in the requested input BCD number string, then the user shall enter the BCD number string as requested, but only up to the maximum number of BCD digits which are supported for updating.		
6	TT	READ EF <sub>ADN</sub> and EF <sub>EXT1</sub>		CR 1	A.2/1 OR A.2/2

					(OR A.2/3)
7	USER	Delete the entry "Contact001" from EF <sub>ADN</sub>			
8	TT	READ EF <sub>ADN</sub> and EF <sub>EXT1</sub>		CR 1	A.2/1 OR A.2/2 (OR A.2/3)
9	USER	Change BCD number of the entry "Contact002" from EF <sub>ADN</sub>	The user shall change the BCD number of the entry "Contact002" to "22446622446600".		
10	TT	READ EF <sub>ADN</sub> and EF <sub>EXT1</sub>		CR 1	A.2/1 OR A.2/2 (OR A.2/3)
11	USER	Create a new entry in EF <sub>ADN</sub>	The user shall create the new phonebook entry "NewContact" with the BCD number "1234567890123456789012345678901234567890123456789012". If the maximum number of BCD digits supported for the global phonebook update is less than in the requested input BCD number string, then the user shall enter the BCD number string as requested, but only up to the maximum number of BCD digits which are supported for updating.		
12	TT	READ EF <sub>ADN</sub> and EF <sub>EXT1</sub>		CR 1	A.2/1 OR A.2/2 (OR A.2/3)
13	USER	Delete the entry "Contact003" from EF <sub>ADN</sub>			
14	TT	READ EF <sub>ADN</sub> and EF <sub>EXT1</sub>		CR 1	A.2/1 OR A.2/2 (OR A.2/3)

### 8.1.5.5 Acceptance criteria

CR 1 is explicitly verified in step 2) by using the methods A.2/1 or A.2/2 CR 1 the requirement is met if the ME has selected the global phonebook and has read EF<sub>PBR</sub>.

CR 1 is explicitly verified in (or after, when using method A.2/3) steps 4), 6), 8), 10), 12) and 14), by any verification method listed in Table A.2. The requirement is met if:

in step 4), the global phonebook contains a record with "22446622446622446600" as BCD number and "04" as extension record identifier. EF<sub>EXT1</sub> shall contain a record with "Additional data" as record type, the BCD number extension "777888999" and "FF" as identifier to indicate the end of the chain.

**NOTE:** If the maximum number of BCD digits supported for global phonebook updating is less than in the requested input BCD number, then EF<sub>ADN</sub> and EF<sub>EXT1</sub> shall contain the BCD number as entered on the MMI. has selected selected the global phonebook and shall have read EF<sub>PBR</sub> in the global phonebook.

in step 6), the ME acted to prevent storage of the extended BCD number, e.g. by giving an indication to the user or not allowing to enter the extended number. EF<sub>EXT1</sub> has not been updated and the extension record identifier of the entry "Contact007" remains as "FF".

in step 8), the records of EF<sub>ADN</sub> and EF<sub>EXT1</sub> for the phonebook entry "Contact001" are empty, i.e. the EF<sub>ADN</sub> record shall be "FF... FF" and the EF<sub>EXT1</sub> record shall be "00FF... FF."

in step 10), the record of EF<sub>EXT1</sub> which was used to store the BCD number extension "777888999" is empty and the record of EF<sub>ADN</sub> used for storing the entry with the alpha identifier "Contact002" contains the BCD number "22446622446600" and the extension record identifier "FF".

in step 12), a record of EF<sub>ADN</sub> contains "NewContact" as alpha identifier, "12345678901234567890" as BCD number and uses an extension record identifier unequal to "FF".

NOTE: The EF<sub>EXT1</sub> record which was indicated in the EF<sub>ADN</sub> record used in this case shall contain "Additional data" as record type, "12345678901234567890" as BCD number and an extension record identifier unequal to "FF", while the EF<sub>EXT1</sub> record used to continue the chain inside EF<sub>EXT1</sub> shall contain "Additional data" as record type, "123456789012" as BCD number and "FF" as extension record identifier.

If the maximum number of BCD digits supported for global phonebook updating is less than the requested input BCD number, then EF<sub>ADN</sub> and EF<sub>EXT1</sub> shall contain the BCD number as entered on the MMI.

in step 14), the EF<sub>ADN</sub> record, which was used to store the data for "Contact003" and the related records of EF<sub>EXT1</sub> are empty.

If A.2/3 is the only method used, the reading of EF<sub>PBR</sub> in step 2) can be handled as implicitly verified if all the following phonebook actions can be executed successfully.

## 8.2 Short message handling report

### 8.2.1 Correct storage of a SM on the USIM

GERAN/UTRAN test - not applicable

### 8.2.2 Correct reading of a SM on the USIM

GERAN/UTRAN test - not applicable

### 8.2.3 SM memory capacity exceeded handling

GERAN/UTRAN test - not applicable

### 8.2.4A Correct storage of an SM on the UICC

GERAN/UTRAN test - not applicable

### 8.2.4B Correct storage of an SM on the UICC

FFS

### 8.2.5 Correct reading of a SM on the USIM if USIM and ISIM are present

FFS

### 8.2.6 Correct reading of a SM on the ISIM if USIM and ISIM are present

FFS

### 8.2.7 Correct storage of an SM on the UICC

FFS

## 8.3 MMS related tests

### 8.3.0 General condition

Currently MMS related test cases defined in TS 31.121 [2] are not used for device certification by any of the certification organisations. As long as there is no demand the tests from this clause will not be defined and set to FFS.

#### 8.3.1 UE recognizing the priority order of MMS Issuer Connectivity Parameters

FFS

#### 8.3.2 UE recognizing the priority order of MMS User Connectivity Parameters

FFS

#### 8.3.3 UE recognizing the priority order of MMS Issuer Connectivity Parameters over the MMS User Connectivity Parameters

FFS

#### 8.3.4 Usage of MMS notification

FFS

## 8.4 UICC presence detection

Not applicable for UEs with nrUSIMs.

## 8.5 UICC presence detection when connected to E-UTRAN/EPC

Not applicable for UEs with nrUSIMs.

---

## 9 USIM service handling

### 9.1 Access Point Name Control List handling

#### 9.1.1 Access Point Name Control List handling for UEs supporting ACL

GERAN/UTRAN test - not applicable

#### 9.1.2 Network provided APN handling for UEs supporting ACL

GERAN/UTRAN test - not applicable

### 9.1.3 Access Point Name Control List handling for UEs not supporting ACL

GERAN/UTRAN test - not applicable

### 9.1.4 Access Point Name Control List handling for UEs supporting ACL connected to E-UTRAN/EPC

#### 9.1.4.1 Definition and applicability

This EF<sub>ACL</sub> contains the list of allowed APNs (Access Point Names). If the APN Control List service is enabled and the ME is to provide an APN as part of attach for PDN connectivity, then the ME shall verify that the APN value is present in the EF<sub>ACL</sub> and if it is not the ME shall not proceed with the attach procedure. If the APN Control List service is enabled and the ME does not intend to provide an APN as part of the attach for PDN connectivity and use a network provided APN, the ME shall not check if "network provided APN" is contained within EF<sub>ACL</sub>.

There is 1:1 mapping between one PDP context and one EPS Bearer.

Some MEs might not support the enablement or the disablement of the APN Control List service or the modification of the APN Control List. In these cases, the test sequence below provides separate branches.

#### 9.1.4.2 Conformance requirement

CR 1 The terminal shall support the APN Control List service as defined in TS 31.102 [19], clauses 5.1.1.2 and 5.3.14.

Reference:

- TS 31.102 [19], clauses 4.2.8, 4.2.48, 5.1.1.2 and 5.3.14;
- TS 23.060 [55], clause 9.2, 9.2.1A.

#### 9.1.4.3 Test purpose

The purpose of this test is to verify that:

- 1) the ME considers the status of the APN Control List service as indicated in EF<sub>UST</sub> and EF<sub>EST</sub>.
- 2) The ME checks that the entire APN of any EPS Bearer is listed in EF<sub>ACL</sub> before requesting this EPS Bearer activation from the network if the ACL service is enabled.
- 3) the ME does not request the corresponding EPS Bearer activation from the network if the ACL service is enabled and the APN is not present in EF<sub>ACL</sub>.
- 4) the ME does not check that the network provided APN is present in EF<sub>ACL</sub> during the initial attach procedure.

#### 9.1.4.4 Method of test

##### 9.1.4.4.1 Initial conditions

The values of the E-UTRAN/EPC UICC as defined in clause 4.5.4 of the present document are used with the following exceptions:

**EF<sub>UST</sub>** (USIM Service Table)

Logically:

Service n°86:	Allowed CSG Lists and corresponding indications	not available
---------------	---	---------------

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Binary	xx1x xx11	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx x111	xxxx xxxx	xxxx xxxx	xxxx xxxx
	<b>B9</b>	<b>B10</b>	<b>B11</b>	<b>B12</b>	<b>B13</b>	<b>B14</b>	<b>B15</b>	
	xxxx xxxx	xxxx xxxx	xx01 xxxx	xxxx xxxx	xxxx xxxx	xxxx xxxx	xxxx xxxx	

### EFACL (Access Point Control List)

Logically:

Number of available bytes: 64  
 Number of APNs: 3  
 1<sup>st</sup> APN: test.test  
 2<sup>nd</sup> APN: 3gpp.test  
 3<sup>rd</sup> APN: 2gpp.test

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	03	DD	0A	04	74	65	73	74	04	74	65	73
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	74	DD	0A	04	33	67	70	70	04	74	65	73
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>	<b>B31</b>	<b>B32</b>	<b>B33</b>	<b>B34</b>	<b>B35</b>	<b>B36</b>
	74	DD	0A	04	32	67	70	70	04	74	65	73
	<b>B37</b>	<b>B38</b>	...	<b>B64</b>								
	74	FF	...	FF								

The ME is configured to use the network provided APN for the initial attach procedure.

The TT (E-USS) transmits on the BCCH, with valid network parameters

#### 9.1.4.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	Run initial activation			
2	UE > TT	Attach to E-UTRAN	The ME shall have read the status of the ACL service in EF <sub>UST</sub> and EF <sub>EST</sub> . The ME shall be in updated idle mode on the E-USS.		
3	USER > UE	Request PDN connectivity to "1gpp.test"	The ME shall not request PDN connectivity.	CR 1	
4	USER > UE	Request PDN connectivity to "3gpp.test"	PDN connectivity shall be activated.	CR 1	
5	USER > UE	Deactivate the PDN connectivity to "3gpp.test"	PDN connectivity shall be deactivated.	CR 1	

Steps to be executed if the user interface supports disabling the APN Control List service					
6	USER > UE	Disable the APN Control List service	When prompted to enter PIN2, the user shall present the correct PIN2 value (most probably 9999#). The APN Control List service shall have been set to disabled in EF <sub>EST</sub> .	CR 1	A.2/3
7	USER > UE	Request PDN connectivity to "1gpp.test"	PDN connectivity shall be activated.	CR 1	
8	USER > UE	Deactivate the PDN connectivity to "1gpp.test"	PDN connectivity shall be deactivated.	CR 1	
9	UE	The UE is powered off and then on			
10	USER > UE	Enable the APN Control List service	When prompted to enter PIN2, the user shall present the correct PIN2 value (most probably 9999#). The APN Control List service shall have been set to enabled in EF <sub>EST</sub> .	CR 1	A.2/3
11	USER > UE	Request PDN connectivity to "1ppp.test"	The ME shall not request PDN connectivity.	CR 1	
12	UE	The UE is powered off and then on			
13	USER > UE	Add the APN "1ppp.net" to the APN Control List	When prompted to enter PIN2, the user shall present the correct PIN2 value (most probably 9999#).	CR 1	A.2/3

			APN "1ppp.net" shall have been added to the APN Control List in EF <sub>ACL</sub> .		
14	USER > UE	Request PDN connectivity to "1ppp.test"	PDN connectivity shall be activated.	CR 1	
15	USER > UE	Deactivate the PDN connectivity	PDN connectivity shall be deactivated.	CR 1	
<b>Common test steps for all UEs</b>					
16	USER > UE	UE is soft powered down			

### 9.1.4.5 Acceptance criteria

For devices not supporting a user interface supports to disable the APN Control List service CR 1 is implicitly verified at steps 3), 4) and 5). The requirement is met if the UE is not requesting PDN connectivity in step 3), activating PDN connectivity in step 4) and deactivating PDN connectivity in step 5).

For devices supporting a user interface supports to disable the APN Control List service further aspects of CR 1 are verified in steps 6), 7), 8), 10), 11), 13), 14) and 15).

The requirements are met if the implicit verification in steps 7), 8), 11), 14) and 15) returns the expected results.

Additional verification is possible by exploring the contents of EF<sub>EST</sub> via method A.2/3 in steps 6), 10) and 13).

## 9.2 Service Dialling Numbers handling

### 9.2.1 Service Dialling Numbers handling

GERAN/UTRAN test - not applicable

---

## 10 CSG list handling

### 10.1 CSG list handling for E-UTRA

#### 10.1.1 Automatic CSG selection in E-UTRA with CSG list on USIM, success

##### 10.1.1.1 Definition and applicability

A Closed Subscriber Group identifies subscribers of an operator who are permitted to access one or more cells of the PLMN but which have restricted access (CSG cells). A CSG cell is part of the PLMN, broadcasting a CSG indication that is set to TRUE and a specific CSG identity. A CSG cell is accessible by the members of the closed subscriber group for that CSG identity. For a CSG cell, the UE shall check the broadcast CSG ID against the Allowed CSG list provided by NAS to check whether a CSG cell is suitable for the UE.

##### 10.1.1.2 Conformance requirement

CR 1 The ME shall read the allowed CSG IDs from EF<sub>ACSGL</sub> in order to perform HNB selection procedures. The lists in EF<sub>ACSGL</sub> shall take precedence over the list stored in the ME non-volatile memory. If the MS supports CSG and if the list is available in the USIM, it is provisioned with a list of allowed CSG identities and associated PLMN identities from the USIM.

Reference:

- TS 31.102 [19], clauses 4.4.6.2 and 5.8.1;
- TS 23.122 [41], clause 3.1A.

CR 2 When a UE in idle mode detects the presence of a permissible CSG cell (a CSG cell whose CSG identity is in the UE's permitted CSG list), the UE shall select the CSG cell.

Reference:

- TS 22.011 [18], clause 8.2.2.1.

### 10.1.1.3 Test purpose

The purpose of this test is to verify that the ME only selects a CSG cell if the CSG IDs of the cell is found in the allowed CSG IDs from EF<sub>ACSGL</sub>.

### 10.1.1.4 Method of test

#### 10.1.1.4.1 Initial conditions

The values of the Default UICC as defined in clause 4.5.2 of the present document are used with EF<sub>IMSI</sub> as defined in clause 4.6.2.

The TT (E-USS) transmits on the BCCH, with the following network parameters:

Cell A:

- TAI (MCC/MNC/TAC): 246/081/0001.
- Access control: unrestricted.
- csg-Indication: TRUE
- csg-Identity: 05

Cell B:

- TAI (MCC/MNC/TAC): 246/081/0002.
- Access control: unrestricted.
- csg-Indication: TRUE
- csg-Identity: 04

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and set the UE to automatic PLMN selection mode.

#### 10.1.1.4.2 Procedure

Step	Direction	Action	Comment	REQ	SA
1	UE	Run initial activation			
2	UE	READ EF <sub>ACSGL</sub>		CR 1	A.2/1 OR A.2/2
3	UE	The UE shall not attempt an Attach procedure, this is checked for 2 mins.		CR 2	
4	TT	TT stops all RF output for the first cell.			
5	TT	The network parameters in BCCH of Cell A is reconfigured to indicate the following: - csg-Identity:03 TT resumes RF output on the BCCH.			
6	UE > TT	Send RRC CONNECTION REQUEST on first Cell (TAI 246/081/0001)	The TT responds with RRC CONNECTION SETUP		
7	UE > TT	Send RRC CONNECTION SETUP COMPLETE		CR 2	
8	UE > TT	Send ATTACH REQUEST	The TT initiates authentication, starts integrity by using the security procedure.		
9	TT > UE	Send ATTACH ACCEPT with: - TAI (MCC/MNC/TAC): 246/081/ 0001	UE sends ATTACH COMPLETE, and further TT sends RRC CONNECTION RELEASE		

		- GUTI: "24608100010266436587"			
10	TT > UE	UE is soft powered down.			

### 10.1.1.5 Acceptance criteria

CR 1 shall be explicitly verified in step 2) by ensuring that UE has successfully read EF<sub>ACSG</sub>L

CR 2 shall be verified by ensuring that:

- 1) UE has not attempted registration in step 3),
- 2) UE has successfully registered to the permissible CSG cell that was pre-configured in EF<sub>ACSG</sub>L at step 9). This may also be explicitly verified at step 9) by ensuring EF<sub>EPSLOC</sub>I contains the following data using any of the methods identified in clause 3.7.2 of the present document.

#### EF<sub>EPSLOC</sub>I (EPS Location Information)

Logically:

GUTI: 24608100010266436587  
 Last visited registered TAI: 246/081/0001  
 EPS update status: updated

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	0B	F6	42	16	80	00	01	02	66	34	56	78
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>						
	42	16	80	00	01	00						

## 10.1.2 Automatic CSG selection in E-UTRA with CSG list on USIM, removal of CSG ID from the USIM

### 10.1.2.1 Definition and applicability

A Closed Subscriber Group identifies subscribers of an operator who are permitted to access one or more cells of the PLMN but which have restricted access (CSG cells). A CSG cell is part of the PLMN, broadcasting a CSG indication that is set to TRUE and a specific CSG identity. A CSG cell is accessible by the members of the closed subscriber group for that CSG identity. For a CSG cell, the UE shall check the broadcast CSG ID against the Allowed CSG list provided by NAS to check whether a CSG cell is suitable for the UE.

### 10.1.2.2 Conformance requirement

CR 1 If the UE receives ATTACH REJECT with cause #25 (Not authorized for this CSG) with integrity protection, the UE shall remove the CSG ID of the cell where the UE has sent the ATTACH REQUEST message from the Allowed CSG list.

Reference:

- TS 22.011 [18], clause 8.2.2.1;
- TS 31.102 [19], clauses 4.4.6.2 and 5.8.1;
- TS 23.122 [41], clause 3.1A.
- TS 24.301 [21], clause 5.5.1.2.5

### 10.1.2.3 Test purpose

The purpose of this test is to verify that the ME removes the CSG ID from the Allowed CSG list in EF<sub>ACSGL</sub> in case this CSG ID belongs to the cell where the ME has sent the ATTACH REQUEST message which was rejected with cause #25 by the E-USS.

### 10.1.2.4 Method of test

#### 10.1.2.4.1 Initial conditions

The values of the Default UICC as defined in clause 4.5.2 of the present document are used with EF<sub>IMSI</sub> as defined in clause 4.6.2.

The TT (E-USS) transmits on the BCCH, with the following network parameters:

Cell A:

- TAI (MCC/MNC/TAC): 246/081/0001.
- Access control: unrestricted.
- csg-Indication: TRUE
- csg-Identity: 03

Cell B:

- TAI (MCC/MNC/TAC): 246/081/0002.
- Access control: unrestricted.
- csg-Indication: TRUE
- csg-Identity: 04

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and set the UE to automatic PLMN selection mode.

#### 10.1.2.4.2 Procedure

Step	Direction	Action	Comment	REQ	SA
1	UE	Run initial activation			
2	UE > TT	Send RRC CONNECTION REQUEST on Cell A (TAI 246/081/0001)	The TT responds with RRC CONNECTION SETUP		
3	UE > TT	Send RRC CONNECTION SETUP COMPLETE			
4	UE > TT	Send ATTACH REQUEST	The TT initiates authentication, starts integrity by using the security procedure.		
5	TT > UE	Send ATTACH REJECT with cause #25 (Not authorized for this CSG) with integrity protection.	TT sends RRC CONNECTION RELEASE		
6	UE > USIM	UPDATE EF <sub>ACSGL</sub>	This may be alternatively verified at step 8).	CR 1	A.2/2
7	TT > UE	UE is soft powered down.			

Optional step if CR 1 verification cannot be performed at step 6)					
8	UE	READ EF <sub>ACSGL</sub> , EF <sub>EPSLOC</sub>		CR 1	A.2/3

### 10.1.2.5 Acceptance criteria

CR 1 shall be explicitly verified either in step 6) by analysing the UPDATE command used to update EF<sub>ACSGL</sub> (A.2/1 or A.2/2) or at step 8) by reading the EF<sub>ACSGL</sub>, EF<sub>EPSLOC</sub> and verifying that it contains the following:

EF<sub>EPSLOC</sub> (EPS Information)

Logically:

GUTI: not checked  
 Last visited registered TAI: 246/081/0001  
 EPS update status: ROAMING NOT ALLOWED

Coding:

Byte:	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx	xx
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>						
	42	16	80	00	01	02						

**EF<sub>ACSGL</sub>** (Allowed CSG Lists)

Logically:

1<sup>st</sup> CSG list

PLMN: 246 081 (MCC MNC)  
 1<sup>st</sup> CSG list 1<sup>st</sup> CSG Type indication 02  
 1<sup>st</sup> CSG list 1<sup>st</sup> CSG HNB Name indication 02  
 1<sup>st</sup> CSG list 1<sup>st</sup> CSG CSG ID: 02 (27bit)

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	A0	0D	80	03	42	16	80	81	06	02	02	00
	<b>B13</b>	<b>B14</b>	<b>B15</b>									
	00	00	5F									

2<sup>nd</sup> CSG list

PLMN: 244 081 (MCC MNC)  
 2<sup>nd</sup> CSG list 1<sup>st</sup> CSG Type indication 08  
 2<sup>nd</sup> CSG list 1<sup>st</sup> CSG HNB Name indication 08  
 2<sup>nd</sup> CSG list 1<sup>st</sup> CSG CSG ID: 08 (27bit)

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	A0	0D	80	03	42	14	80	81	06	08	08	00
	<b>B13</b>	<b>B14</b>	<b>B15</b>									
	00	01	1F									

NOTE: the 1<sup>st</sup> and 2<sup>nd</sup> CSG list may be stored together or separately in any record in arbitrary order.

## 10.1.3 Manual CSG selection in E-UTRA with CSG list on USIM, success

### 10.1.3.1 Definition and applicability

A Closed Subscriber Group identifies subscribers of an operator who are permitted to access one or more cells of the PLMN but which have restricted access (CSG cells). A CSG cell is part of the PLMN, broadcasting a CSG indication that is set to TRUE and a specific CSG identity. A CSG cell is accessible by the members of the closed subscriber group for that CSG identity. For a CSG cell, the UE shall check the broadcast CSG ID against the Allowed CSG list provided by NAS to check whether a CSG cell is suitable for the UE.

A UE supporting CSG selection selects CSG cell either automatically based on the list of allowed CSG identities or manually based on user selection of CSG on indication of list of available CSGs.

### 10.1.3.2 Conformance requirement

CR 1 In manual CSG selection mode, the ME indicates to the user the list of available CSGs in the currently selected PLMN. The list of CSGs presented to the user is not restricted by the allowed CSG list.

If the MS supports CSG, it is provisioned with a list of allowed CSG identities and associated PLMN identities from the USIM if the list is available in the USIM.

Reference:

- TS 31.102 [19], clauses 4.4.6.2 and 5.8.1;
- TS 23.122 [41], clause 3.1A.

CR 2 If the UE supporting CSG selection has attempted manual CSG selection, the UE, when receiving the TRACKING AREA UPDATE ACCEPT message, shall check if the CSG ID of the cell where the UE has sent the TRACKING AREA UPDATE REQUEST message is contained in the Allowed CSG list. If not, the UE shall add that CSG ID to the allowed CSG list.

Reference:

- TS 24.301 [21], clause 5.5.3.2.4

### 10.1.3.3 Test purpose

The purpose of this test is to verify that the ME adds the CSG ID to the Allowed CSG list in EF<sub>ACSGL</sub> in case this CSG ID belongs to the cell where the ME has sent the TRACKING AREA UPDATE REQUEST message which was accepted by the E-USS.

### 10.1.3.4 Method of test

#### 10.1.3.4.1 Initial conditions

The values of the Default UICC as defined in clause 4.5.2 of the present document are used with EF<sub>IMSI</sub> as defined in clause 4.6.2.

The TT (E-USS) transmits on the BCCH, with the following network parameters:

Cell A:

- TAI (MCC/MNC/TAC): 246/081/0001.
- Access control: unrestricted.
- csg-Indication: FALSE
- csg-Identity: not present

Cell B:

- TAI (MCC/MNC/TAC): 246/081/0002.
- Access control: unrestricted.
- csg-Indication: TRUE
- csg-Identity: 04

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and set the UE to automatic PLMN selection mode.

#### 10.1.3.4.2 Procedure

Step	Direction	Action	Comment	REQ	SA
1	UE	Run initial activation			
2	UE > TT	Send RRC CONNECTION REQUEST on Cell A (TAI 246/081/0001)	The TT responds with RRC CONNECTION SETUP		
3	UE > TT	Send RRC CONNECTION SETUP COMPLETE			
4	UE > TT	Send ATTACH REQUEST	The TT initiates authentication, starts integrity by using the security procedure.		
5	TT > UE	Send ATTACH ACCEPT with: - TAI (MCC/MNC/TAC): 246/081/0001	UE sends ATTACH COMPLETE, and further TT sends RRC CONNECTION RELEASE		

		- GUTI: "24608100010266345678"			
6	TT > UE	Use the MMI of the UE to perform manual CSG selection.	The UE shall indicate the availability of a cell with csg-Identity 04 for PLMN 246/081. The user shall select this cell by using the MMI.	CR 1	
7	UE > TT	Send RRC CONNECTION REQUEST on Cell A (TAI 246/081/0002)	The TT responds with RRC CONNECTION SETUP		
8	UE > TT	Send RRC CONNECTION SETUP COMPLETE			
9	UE > TT	Send TRACKING AREA UPDATE REQUEST	The TT initiates authentication, starts integrity by using the security procedure.		
10	TT > UE	Send TRACKING AREA UPDATE ACCEPT with: - TAI (MCC/MNC/TAC): 246/081/ 0002 - GUTI: "24608100010266436599"	UE sends TRACKING AREA UPDATE COMPLETE, and further TT sends RRC CONNECTION RELEASE		
11	UE > USIM	UPDATE EF <sub>ACSGL</sub>	This may be alternatively verified at step 13).	CR 2	A.2/2
12	TT > UE	UE is soft powered down.			
<b>Optional step if CR 2 verification cannot be performed at step 11)</b>					
13	UE	READ EF <sub>ACSGL</sub>		CR 2	A.2/3

### 10.1.3.5 Acceptance criteria

CR 1 is verified at step 6) by ensuring that during the manual CSG selection, the UE shall provide the information for a cell with csg-Identity 04 for PLMN 246/081 to the user.

CR 2 is verified explicitly at step 11) by ensuring that UE has successfully updated EF<sub>ACSGL</sub> with CSG ID: 04 or at step 8) or step 13) by analysing the EF<sub>ACSGL</sub> and verifying that it contains the following CSG lists:

#### EF<sub>EPSLOC1</sub> (EPS Information)

Logically:

GUTI: 24608100010266436599  
 Last visited registered TAI: 246/081/0002  
 EPS update status: updated

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	0B	F6	42	16	80	00	01	02	66	43	65	99
	B13	B14	B15	B16	B17	B18						
	42	16	80	00	02	00						

#### EF<sub>ACSGL</sub> (Allowed CSG Lists)

Logically:

1<sup>st</sup> CSG list

PLMN: 246 081 (MCC MNC)  
 1<sup>st</sup> CSG list 1<sup>st</sup> CSG Type indication 02  
 1<sup>st</sup> CSG list 1<sup>st</sup> CSG HNB Name indication 02  
 1<sup>st</sup> CSG list 1<sup>st</sup> CSG CSG ID: 02 (27bit)  
 1<sup>st</sup> CSG list 2<sup>nd</sup> CSG Type indication 03  
 1<sup>st</sup> CSG list 2<sup>nd</sup> CSG HNB Name indication 03  
 1<sup>st</sup> CSG list 2<sup>nd</sup> CSG CSG ID: 03 (27bit)  
 1<sup>st</sup> CSG list 3<sup>rd</sup> CSG Type indication 'xx' (not checked)  
 1<sup>st</sup> CSG list 3<sup>rd</sup> CSG HNB Name indication 'xx' (not checked)  
 1<sup>st</sup> CSG list 3<sup>rd</sup> CSG CSG ID: 04 (27bit)

Coding:

Byte:	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Coding:	A0	1D	80	03	42	16	80	81	06	02	02	00
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	00	00	5F	81	06	03	03	00	00	00	7F	81
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>	<b>B31</b>					
	06	xx	xx	00	00	00	9F					

2nd CSG list

PLMN: 244 081 (MCC MNC)  
 2<sup>nd</sup> CSG list 1<sup>st</sup> CSG Type indication 08  
 2<sup>nd</sup> CSG list 1<sup>st</sup> CSG HNB Name indication 08  
 2<sup>nd</sup> CSG list 1<sup>st</sup> CSG CSG ID: 08 (27bit)

Coding:

Byte:	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Coding:	A0	0D	80	03	42	14	80	81	06	08	08	00
	<b>B13</b>	<b>B14</b>	<b>B15</b>									
	00	01	1F									

NOTE: The 1<sup>st</sup> and 2<sup>nd</sup> CSG list may be stored together or separately in any record in arbitrary order.  
 The CSG entries within each of the CSG lists are not sorted and may occur in arbitrary order.

## 10.1.4 Manual CSG selection in E-UTRA with CSG list on USIM, rejected

### 10.1.4.1 Definition and applicability

A Closed Subscriber Group identifies subscribers of an operator who are permitted to access one or more cells of the PLMN but which have restricted access (CSG cells). A CSG cell is part of the PLMN, broadcasting a CSG indication that is set to TRUE and a specific CSG identity. A CSG cell is accessible by the members of the closed subscriber group for that CSG identity. For a CSG cell, the UE shall check the broadcast CSG ID against the Allowed CSG list provided by NAS to check whether a CSG cell is suitable for the UE.

A UE supporting CSG selection selects CSG cell either automatically based on the list of allowed CSG identities or manually based on user selection of CSG on indication of list of available CSGs.

### 10.1.4.2 Conformance requirement

CR 1 If the UE supporting CSG selection has attempted manual CSG selection, the UE, when receiving the TRACKING AREA UPDATE REJECT message with cause #25 (Not authorized for this CSG) with integrity protection, shall not add the CSG ID of the cell where the UE has sent the TRACKING AREA UPDATE REQUEST message if the CSG ID is contained in the Allowed CSG list.

Reference:

- TS 31.102 [4], clauses 4.4.6.2 and 5.8.1;
- TS 23.122 [31], clause 3.1A.
- TS 24.301 [26], clause 5.5.3.2.5

### 10.1.4.3 Test purpose

The purpose of this test is to verify that the ME does not add the CSG ID to the Allowed CSG list in EF<sub>ACSGL</sub> in case this CSG ID belongs to the cell where the ME has sent the TRACKING AREA UPDATE REQUEST message which was rejected by the E-USS.

#### 10.1.4.4 Method of test

##### 10.1.4.4.1 Initial conditions

The values of the Default UICC as defined in clause 4.5.2 of the present document are used with EF<sub>IMSI</sub> as defined in clause 4.6.2.

The TT (E-USS) transmits on the BCCH, with the following network parameters:

Cell A:

- TAI (MCC/MNC/TAC): 246/081/0001.
- Access control: unrestricted.
- csg-Indication: FALSE
- csg-Identity: not present

Cell B:

- TAI (MCC/MNC/TAC): 246/081/0002.
- Access control: unrestricted.
- csg-Indication: TRUE
- csg-Identity: 04

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and set the UE to automatic PLMN selection mode.

##### 10.1.4.4.2 Procedure

Step	Direction	Action	Comment	REQ	SA
1	UE	Run initial activation			
2	UE > TT	Send RRC CONNECTION REQUEST on Cell A (TAI 246/081/0001)	The TT responds with RRC CONNECTION SETUP		
3	UE > TT	Send RRC CONNECTION SETUP COMPLETE			
4	UE > TT	Send ATTACH REQUEST	The TT initiates authentication, starts integrity by using the security procedure.		
5	TT > UE	Send ATTACH ACCEPT with: - TAI (MCC/MNC/TAC): 246/081/ 0001 - GUTI: "24608100010266345678"	UE sends ATTACH COMPLETE, and further TT sends RRC CONNECTION RELEASE		
6	TT > UE	Use the MMI of the UE to perform manual CSG selection	The UE shall indicate the availability of a cell with csg-Identity 04 for PLMN 246/081. The user shall select this cell by using the MMI.		
7	UE > TT	Send RRC CONNECTION REQUEST on Cell A (TAI 246/081/0002)	The TT responds with RRC CONNECTION SETUP		
8	UE > TT	Send RRC CONNECTION SETUP COMPLETE			
9	UE > TT	Send TRACKING AREA UPDATE REQUEST	The TT initiates authentication, starts integrity by using the security procedure.		
10	TT > UE	Send TRACKING AREA UPDATE REJECT with cause #25 (Not authorized for this CSG) with integrity protection.	TT sends RRC CONNECTION RELEASE		
11	UE > USIM	Update EF <sub>ACSGL</sub>	This step shall not occur.	CR 1	A.2/2
12	TT > UE	UE is soft powered down.			
13	UE	Read EF <sub>ACSGL</sub>		CR 1	A.2/3

##### 10.1.4.5 Acceptance criteria

CR 1 shall be explicitly verified either at step 11) by ensuring that UE shall not update EF<sub>ACSGL</sub> (A.2/1 or A.2/2) or alternatively at step 13) by analysing the EF<sub>ACSGL</sub>, EF<sub>EPSLOC1</sub> and verifying that values shall be as follows:

**EF<sub>EPSLOC1</sub>** (EPS Information)

Logically:

GUTI: not checked  
 Last visited registered TAI: 246/081/0001  
 EPS update status: ROAMING NOT ALLOWED

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX	XX
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>						
	42	16	80	00	01	02						

**EF<sub>ACSGL</sub>** (Allowed CSG Lists)

Content not changed, shall be the same as defined in clause 4.5.4 of the present document.

## 10.1.5 CSG selection in E-UTRA with no CSG list on USIM, no IMSI change

### 10.1.5.1 Definition and applicability

A Closed Subscriber Group identifies subscribers of an operator who are permitted to access one or more cells of the PLMN but which have restricted access (CSG cells). A CSG cell is part of the PLMN, broadcasting a CSG indication that is set to TRUE and a specific CSG identity. A CSG cell is accessible by the members of the closed subscriber group for that CSG identity. For a CSG cell, the UE shall check the broadcast CSG ID against the Allowed CSG list provided by NAS to check whether a CSG cell is suitable for the UE.

A UE supporting CSG selection selects CSG cell either automatically based on the list of allowed CSG identities or manually based on user selection of CSG on indication of list of available CSGs.

### 10.1.5.2 Conformance requirement

CR 1 If the corresponding file is not present on the USIM, then the UE that supports CSG selection stores the allowed CSG list in a non-volatile memory in the ME together with the IMSI from the USIM. These EMM parameters can only be used if the IMSI from the USIM matches the IMSI stored in the non-volatile memory; else the UE shall delete the EMM parameters.

Reference:

- TS 31.102 [19], clauses 4.4.6.2 and 5.8.1;
- TS 24.301 [21], clause 5.5.3.2.4 and Annex C.

CR 2 To verify that the ME still has this CSG ID stored in the Allowed CSG list (in the non-volatile memory) available together with the IMSI after powered down and up in case the IMSI of the USIM has not changed.

Reference:

- TS 31.102 [19], clauses 4.4.6.2 and 5.8.1;
- TS 24.301 [21], clause 5.5.3.2.4 and Annex C.

CR 3 To verify that the ME removes the CSG ID from the Allowed CSG list inside the ME's (non-volatile memory) in case this CSG ID belongs to the cell where the ME has sent the ATTACH REQUEST message which was rejected with cause #25 by the E-USS.

Reference:

- TS 23.122 [41], clause 3.1A.

### 10.1.5.3 Test purpose

The purpose of this test is to verify that:

- 1) the ME adds the CSG ID to the Allowed CSG list in a non-volatile memory in the ME together with the IMSI from the USIM in case this CSG ID belongs to the cell where the ME has sent the TRACKING AREA UPDATE REQUEST message which was accepted by the E-USS as the corresponding file is not present on the simulated USIM.
- 2) the ME still has this CSG ID stored in the Allowed CSG list available together with the IMSI after powered down and up in case the IMSI of the USIM has not changed.
- 3) the ME removes the CSG ID from the Allowed CSG list inside the UE in case this CSG ID belongs to the cell where the ME has sent the ATTACH REQUEST message which was rejected with cause #25 by the EUSS.

### 10.1.5.4 Method of test

#### 10.1.5.4.1 Initial conditions

The values of the Default UICC as defined in clause 4.5.2 of the present document are used with EF<sub>IMSI</sub> as defined in clause 4.6.2 and the following exceptions:

EF<sub>UST</sub> (USIM Service Table)

Logically:

Service n°86: Allowed CSG Lists and corresponding indications not available

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Binary	xx1x xx11	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxxx xxxx	xxxx xxxx	xxxx xxxx
	<b>B9</b>	<b>B10</b>	<b>B11</b>	<b>B12</b>				
	xxxx xxxx	xxxx xxxx	xx01 xxxx	0000 0xxx				

The ME shall neither have stored csg-ID = 04 nor csg-ID=06 in the allowed CSG list in a non-volatile memory.

The TT (E-USS) transmits on the BCCH, with the following network parameters:

Cell A:

- TAI (MCC/MNC/TAC): 246/081/0001.
- Access control: unrestricted.
- csg-Indication: FALSE
- csg-Identity: not present

Cell B:

- TAI (MCC/MNC/TAC): 246/081/0002.
- Access control: unrestricted.
- csg-Indication: TRUE
- csg-Identity: 04

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and set the UE to automatic PLMN selection mode.

#### 10.1.5.4.2 Procedure

Step	Direction	Action	Comment	REQ	SA
1	UE	Run initial activation			

2	UE > TT	Send RRC CONNECTION REQUEST on Cell A (TAI 246/081/0001)	The TT responds with RRC CONNECTION SETUP		
3	UE > TT	Send RRC CONNECTION SETUP COMPLETE			
4	UE > TT	Send ATTACH REQUEST	The TT initiates authentication, starts integrity by using the security procedure.		
5	TT > UE	Send ATTACH ACCEPT with: - TAI (MCC/MNC/TAC): 246/081/ 0001 - GUTI: "24608100010266345678"	UE sends ATTACH COMPLETE, and further TT sends RRC CONNECTION RELEASE		
6	TT > UE	Use the MMI of the UE to perform manual CSG selection	The UE shall indicate the availability of a cell with csg-Identity 04 for PLMN 246/081. The user shall select this cell by using the MMI.		
7	UE > TT	Send RRC CONNECTION REQUEST on csg cell (Cell B) (TAI 246/081/0002)	The TT responds with RRC CONNECTION SETUP		
8	UE > TT	Send RRC CONNECTION SETUP COMPLETE			
9	UE > TT	Send TRACKING AREA UPDATE REQUEST	The TT initiates authentication, starts integrity by using the security procedure.		
10	TT > UE	Send TRACKING AREA UPDATE ACCEPT with the following parameters with integrity protection: - TAI (MCC/MNC/TAC): 246/081/0002 - GUTI: "24608100010266345699"	UE sends TRACKING AREA UPDATE COMPLETE, and further TT sends RRC CONNECTION RELEASE.		
11	UE > USIM	UE is powered off and performs DETACH procedure			
12	TT	The network parameters in BCCH of Cell A (246/081/0001) is reconfigured to indicate the following: - csg-Indication: TRUE - csg-Identity: 06 TT resumes RF output on the BCCH.			
13	UE > USIM	UE is powered on	(with same default E-UTRAN UICC as defined in initial conditions)		
14	UE > TT	Send RRC CONNECTION REQUEST on csg cell (Cell B) (TAI 246/081/0002)	The TT responds with RRC CONNECTION SETUP	CR 1	CR 2
15	UE > TT	Send RRC CONNECTION SETUP COMPLETE			
16	UE > TT	Send ATTACH REQUEST	The TT initiates authentication, starts integrity by using the security procedure.		
17	TT > UE	Send ATTACH REJECT with cause #25 (Not authorized for this CSG) with integrity protection.	TT sends RRC CONNECTION RELEASE		
18	UE > USIM	UE is soft powered down			
19	UE > USIM	UE is powered on (with same default E-UTRAN UICC as defined in initial conditions)			
20	USER > UE	After 2 min, UE is powered down		CR 3	

### 10.1.5.5 Acceptance criteria

CR 1 and CR 2 are verified at step 14) by ensuring that UE shall send TRACKING AREA UPDATE REQUEST and complete the registration to the csg cell (TAI 246/081/0002 with csg identity: 02) successfully.

CR 3 is verified at step 20) by ensuring that the UE shall not attempt to register to the CSG cell (CSG ID: 04) where it previously (at step 17) received an ATTACH REJECT with cause #25.

## 10.1.6 CSG selection in E-UTRA with no CSG list on USIM, with IMSI change

### 10.1.6.1 Definition and applicability

A Closed Subscriber Group identifies subscribers of an operator who are permitted to access one or more cells of the PLMN but which have restricted access (CSG cells). A CSG cell is part of the PLMN, broadcasting a CSG indication that is set to TRUE and a specific CSG identity. A CSG cell is accessible by the members of the closed subscriber group for that CSG identity. For a CSG cell, the UE shall check the broadcast CSG ID against the Allowed CSG list provided by NAS to check whether a CSG cell is suitable for the UE.

A UE supporting CSG selection selects CSG cell either automatically based on the list of allowed CSG identities or manually based on user selection of CSG on indication of list of available CSGs.

### 10.1.6.2 Conformance requirement

CR 1 In manual CSG selection mode, the ME indicates to the user the list of available CSGs in the currently selected PLMN. The list of CSGs presented to the user is not restricted by the allowed CSG list. If the MS supports CSG, it is provisioned with a list of allowed CSG identities and associated PLMN identities from the USIM if the list is available in the USIM. If the UE supporting CSG selection has attempted manual CSG selection, the UE, when receiving the TRACKING AREA UPDATE ACCEPT message, shall check if the CSG ID of the cell where the UE has sent the TRACKING AREA UPDATE REQUEST message is contained in the Allowed CSG list. If not, the UE shall add that CSG ID to the Allowed CSG list.

Reference:

- TS 31.102 [19], clauses 4.4.6.2 and 5.8.1;
- TS 23.122 [41], clause 3.1A.
- TS 24.301 [21], clause 5.5.3.2.4 and Annex C.

CR 2 If the corresponding file is not present on the USIM, these EMM parameters except allowed CSG list are stored in a non-volatile memory in the ME together with the IMSI from the USIM. The allowed CSG list is stored in a non-volatile memory in the ME if the UE supports CSG selection. These EMM parameters can only be used if the IMSI from the USIM matches the IMSI stored in the non-volatile memory; else the UE shall delete the EMM parameters.

Reference:

- TS 23.122 [41], clause 3.1A.
- TS 24.301 [21], clause 5.5.3.2.4 and Annex C.

### 10.1.6.3 Test purpose

The purpose of this test is to verify that:

- 1) the ME adds the CSG ID to the Allowed CSG list in a non-volatile memory in the ME together with the IMSI from the USIM in case this CSG ID belongs to the cell where the ME has sent the TRACKING AREA UPDATE REQUEST message which was accepted by the E-USS as the corresponding file is not present on the configured USIM.
- 2) the ME removes this CSG ID stored in the Allowed CSG list available together with the IMSI after powered down and up in case the IMSI of the USIM has changed.

### 10.1.6.4 Method of test

#### 10.1.6.4.1 Initial conditions

The values of the Default UICC as defined in clause 4.5.2 of the present document are used with EF<sub>IMSI</sub> as defined in clause 4.6.2 and the following exceptions:

**EF<sub>UST</sub>** (USIM Service Table)

Logically:

Service n°86: Allowed CSG Lists and corresponding indications not available

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Binary	xx1x xx11	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxxx xxxx	xxxx xxxx	xxxx xxxx
	<b>B9</b>	<b>B10</b>	<b>B11</b>	<b>B12</b>				
	xxxx xxxx	xxxx xxxx	xx01 xxxx	0000 0xxx				

The ME shall neither have stored csg-ID = 04 nor csg-ID=06 in the allowed CSG list in a non-volatile memory.

The TT (E-USS) transmits on the BCCH, with the following network parameters:

Cell A:

- TAI (MCC/MNC/TAC): 246/081/0001.
- Access control: unrestricted.
- csg-Indication: FALSE
- csg-Identity: not present

Cell B:

- TAI (MCC/MNC/TAC): 246/081/0002.
- Access control: unrestricted.
- csg-Indication: TRUE
- csg-Identity: 04

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and set the UE to automatic PLMN selection mode.

## 10.1.6.4.2 Procedure

Step	Direction	Action	Comment	REQ	SA
1	UE	Run initial activation			
2	UE > TT	Send RRC CONNECTION REQUEST on the Cell A (TAI 246/081/0001)	The TT responds with RRC CONNECTION SETUP		
3	UE > TT	Send RRC CONNECTION SETUP COMPLETE			
4	UE > TT	Send ATTACH REQUEST	The TT initiates authentication, starts integrity by using the security procedure.		
5	TT > UE	Send ATTACH ACCEPT with: - TAI (MCC/MNC/TAC): 246/081/ 0001 - GUTI: "24608100010266345678"	UE sends ATTACH COMPLETE, and further TT sends RRC CONNECTION RELEASE		
6	TT > UE	Use the MMI of the UE to perform manual CSG selection	The UE shall indicate the availability of a cell with csg-Identity 04 for PLMN 246/081. The user shall select this cell by using the MMI.	CR 1	
7	UE > TT	Send RRC CONNECTION REQUEST on csg cell (Cell B) (TAI 246/081/0002)	The TT responds with RRC CONNECTION SETUP		
8	UE > TT	Send RRC CONNECTION SETUP COMPLETE			
9	UE > TT	Send TRACKING AREA UPDATE REQUEST	The TT initiates authentication, starts integrity by using the security procedure.		

10	TT > UE	Send TRACKING AREA UPDATE ACCEPT with the following parameters with integrity protection: - TAI (MCC/MNC/TAC): 246/081/0002 - GUTI: "24608100010266345699"	UE sends TRACKING AREA UPDATE COMPLETE, and further TT sends RRC CONNECTION RELEASE.		
11	UE > USIM	UE is powered off and performs DETACH procedure			
12	UE > USIM	UE is powered on (with default UICC, with the following exception. The IMSI is set to "246081222233333".)			
13	TT	The network parameters in BCCH of Cell A (246/081/0001) is reconfigured to indicate the following: - csg-Indication: TRUE - csg-Identity: 06 TT resumes RF output on the BCCH.			
14	TT	Check if UE tries to register to the cell.	UE shall not try to register to Cell A.	CR 2	
15	USER > UE	After 2 min, UE is soft powered down			

### 10.1.6.5 Acceptance criteria

CR 1 is verified at step 6) by ensuring that MMI of the UE shall indicate to the user the list of available CSGs in the currently selected PLMN, and user is able to select the CSG cell (CSG ID: 04)

CR 2 is verified at step 20) by ensuring that the UE shall not attempt to register to the CSG cell (CSG ID: 06).

## 10.1.7 Manual CSG selection without display restrictions in E-UTRA with ACSG list and OCSG list on USIM

### 10.1.7.1 Definition and applicability

A Closed Subscriber Group identifies subscribers of an operator who are permitted to access one or more cells of the PLMN but which have restricted access (CSG cells). A CSG cell is part of the PLMN, broadcasting a CSG indication that is set to TRUE and a specific CSG identity. A CSG cell is accessible by the members of the closed subscriber group for that CSG identity. For a CSG cell, the UE shall check the broadcast CSG ID against the Allowed CSG list provided by NAS to check whether a CSG cell is suitable for the UE.

A UE supporting CSG selection selects a CSG cell either automatically based on the list of allowed CSG identities or manually based on user selection of CSG on indication of list of available CSGs.

*Editor's note: it is still being investigated whether the testing of Automatic CSG selection should be performed using a separate test case or an enhanced version of the Manual CSG selection test case.*

### 10.1.7.2 Conformance requirement

CR 1 The ME shall read the allowed CSG IDs from EF<sub>ACSGL</sub> and EF<sub>OCSGL</sub> in order to perform HNB selection procedures. The lists in EF<sub>ACSGL</sub> and EF<sub>OCSGL</sub> shall take precedence over the list stored in the ME non-volatile memory.  
If the MS supports CSG, it is provisioned with a list of allowed CSG identities and associated PLMN identities from the USIM if the list is available in the USIM.

Reference:

- TS 31.102 [19], clauses 4.2.18, 4.4.6.2, 4.4.6.5 and 5.8.1;
- TS 24.301 [21], clause 5.5.3.2.4
- TS 22.220 [52], clause 5.3.2 and 5.5.4

CR 2 If the UE supporting CSG selection has attempted manual CSG selection, the UE, when receiving the TRACKING AREA UPDATE ACCEPT message, shall check if the CSG ID of the cell where the UE has sent the TRACKING AREA UPDATE REQUEST message is contained in the Allowed CSG list. If not, the UE shall add that CSG ID to the Allowed CSG list EF<sub>ACSGL</sub>.

Reference:

- TS 24.301 [21], clause 5.5.3.2.4

CR 3 By default, the UE shall display all available CSGs for any PLMN, unless the UE has been configured by the HPLMN, for a specific PLMN, to display only CSGs in the Operator CSG List that are available.

Reference:

- TS 22.220 [52], clause 5.5.4

### 10.1.7.3 Test purpose

The purpose of this test is to verify that:

- 1) the ME adds the CSG ID to the Allowed CSG list in  $EF_{ACSGL}$  in case this CSG ID belongs to the cell where the ME has sent the TRACKING AREA UPDATE REQUEST message which was accepted by the E-USS.
- 2) during the manual CSG selection all available CSG ID shall be displayed without restrictions.

### 10.1.7.4 Method of test

#### 10.1.7.4.1 Initial conditions

The values of the ACSGL/OCSGL UICC as defined in clause 4.5.6 of the present document are used with  $EF_{IMSI}$  as defined in clause 4.6.2.

The TT (E-USS) transmits on the BCCH, with the following network parameters:

Cell A:

- TAI (MCC/MNC/TAC):246/081/0001.
- Access control: unrestricted.
- csg-Indication: FALSE
- csg-Identity: not present

Cell B:

- TAI (MCC/MNC/TAC):246/081/0002.
- Access control: unrestricted.
- csg-Indication: TRUE
- csg-Identity: 04

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and set the UE to automatic PLMN selection mode.

#### 10.1.7.4.2 Procedure

Step	Direction	Action	Comment	REQ	SA
1	UE	Run initial activation			
2	UE > USIM	READ $EF_{ACSGL}$ , $EF_{OCSGL}$		CR 1	A.2/1 OR A.2/2
3	UE > TT	Send RRC CONNECTION REQUEST on Cell A (TAI 246/081/0001)	The TT responds with RRC CONNECTION SETUP		
4	UE > TT	Send RRC CONNECTION SETUP COMPLETE			
5	UE > TT	Send ATTACH REQUEST	The TT initiates authentication, starts integrity by using the security procedure.		
6	TT > UE	Send ATTACH ACCEPT with: - TAI (MCC/MNC/TAC): 246/081/ 0001 - GUTI: "24608100010266345678"	UE sends ATTACH COMPLETE, and further TT sends RRC CONNECTION RELEASE		

7	TT > UE	Use the MMI of the UE to perform manual CSG selection.	The UE shall indicate the availability of a cell with csg-Identity 04 for PLMN 246/081 (Cell B). The user shall select this cell by using the MMI.	CR 3	
8	UE > TT	Send RRC CONNECTION REQUEST on csg cell (Cell B) (TAI 246/081/0002)	The TT responds with RRC CONNECTION SETUP		
9	UE > TT	Send RRC CONNECTION SETUP COMPLETE			
10	UE > TT	Send TRACKING AREA UPDATE REQUEST	The TT initiates authentication, starts integrity by using the security procedure.		
11	TT > UE	Send TRACKING AREA UPDATE ACCEPT with the following parameters with integrity protection: - TAI (MCC/MNC/TAC): 246/081/0002 - GUTI: "24608100010266345699"	UE sends TRACKING AREA UPDATE COMPLETE, and further TT sends RRC CONNECTION RELEASE.		
12	UE > USIM	Update EF <sub>ACSGL</sub>	In case the verification of the contents of EF <sub>ACSGL</sub> is not done during the UPDATE command step 14) needs to be executed.	CR 2	A.2/1 OR A.2/2
13	UE > USIM	UE is soft powered down.			
14	User > UE	READ EF <sub>EPSLOC1</sub> , EF <sub>ACSGL</sub> , EF <sub>OCSGL</sub>			A.2/3

10.1.7.5 Acceptance criteria

CR 1 shall be explicitly verified in step 2) by ensuring that UE has successfully read EF<sub>ACSGL</sub> and EF<sub>OCSGL</sub>.

CR 3 is verified at step 7) by ensuring that MMI of the UE shall indicate to the user the list of available CSGs in the currently selected PLMN, and user is able to select the CSG cell (CSG ID: 04)

CR 2 shall be explicitly verified either in step 12) by analysing the UPDATE command used to update EF<sub>ACSGL</sub> (A.2/1 or A.2/2) or at step 14) by reading the EF<sub>EPSLOC1</sub>, EF<sub>ACSGL</sub>, EF<sub>OCSGL</sub> and verifying that it contains the following:

EF<sub>EPSLOC1</sub> (EPS Information)

Logically:

GUTI: 24608100010266436599  
 Last visited registered TAI: 246/081/0002  
 EPS update status: updated

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	0B	F6	42	16	80	00	01	02	66	43	65	99
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>						
	42	16	80	00	02	00						

EF<sub>ACSGL</sub> (Allowed CSG Lists)

Logically:

1<sup>st</sup> CSG list

PLMN: 246 081 (MCC MNC)  
 1<sup>st</sup> CSG list 1<sup>st</sup> CSG Type indication 02  
 1<sup>st</sup> CSG list 1<sup>st</sup> CSG HNB Name indication 02  
 1<sup>st</sup> CSG list 1<sup>st</sup> CSG CSG ID: 02 (27bit)  
 1<sup>st</sup> CSG list 2<sup>nd</sup> CSG Type indication 03  
 1<sup>st</sup> CSG list 2<sup>nd</sup> CSG HNB Name indication 03  
 1<sup>st</sup> CSG list 2<sup>nd</sup> CSG CSG ID: 03 (27bit)  
 1<sup>st</sup> CSG list 3<sup>rd</sup> CSG Type indication 'xx' (not checked)  
 1<sup>st</sup> CSG list 3<sup>rd</sup> CSG HNB Name indication 'xx' (not checked)  
 1<sup>st</sup> CSG list 3<sup>rd</sup> CSG CSG ID: 04 (27bit)

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	A0	1D	80	03	42	16	80	81	06	02	02	00
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	00	00	5F	81	06	03	03	00	00	00	7F	81
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B30</b>	<b>B31</b>	<b>B32</b>					
	06	xx	xx	00	00	00	9F					

2<sup>nd</sup> CSG list

PLMN: 244 081 (MCC MNC)  
 2<sup>nd</sup> CSG list 1<sup>st</sup> CSG Type indication 08  
 2<sup>nd</sup> CSG list 1<sup>st</sup> CSG HNB Name indication 08  
 2<sup>nd</sup> CSG list 1<sup>st</sup> CSG CSG ID: 08 (27bit)

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	A0	0D	80	03	42	14	80	81	06	08	08	00
	<b>B13</b>	<b>B14</b>	<b>B15</b>									
	00	01	1F									

NOTE: The 1<sup>st</sup> and 2<sup>nd</sup> CSG list may be stored together or separately in any record in arbitrary order.

**EF<sub>OCSGL</sub>** (Operator CSG Lists)

Unchanged, values as defined in clause 4.5.6 of the present document.

## 10.1.8 Manual CSG selection with display restrictions in E-UTRA with ACSG list and OCSG list on USIM

### 10.1.8.1 Definition and applicability

A Closed Subscriber Group identifies subscribers of an operator who are permitted to access one or more cells of the PLMN but which have restricted access (CSG cells). A CSG cell is part of the PLMN, broadcasting a CSG indication that is set to TRUE and a specific CSG identity. A CSG cell is accessible by the members of the closed subscriber group for that CSG identity. For a CSG cell, the UE shall check the broadcast CSG ID against the Allowed CSG list provided by NAS to check whether a CSG cell is suitable for the UE.

A UE supporting CSG selection selects a CSG cell either automatically based on the list of allowed CSG identities or manually based on user selection of CSG on indication of list of available CSGs.

### 10.1.8.2 Conformance requirement

CR 1 The ME shall read the allowed CSG IDs from EF<sub>ACSGL</sub> and EF<sub>OCSGL</sub> in order to perform HNB selection procedures. The lists in EF<sub>ACSGL</sub> and EF<sub>OCSGL</sub> shall take precedence over the list stored in the ME non-volatile memory.

If the MS supports CSG, it is provisioned with a list of allowed CSG identities and associated PLMN identities from the USIM if the list is available in the USIM.

Reference:

- TS 31.102 [19], clauses 4.2.18, 4.4.6.2, 4.4.6.5 and 5.8.1;
- TS 24.301 [21], clause 5.5.3.2.4

CR 2 If the UE supporting CSG selection has attempted manual CSG selection, the UE, when receiving the TRACKING AREA UPDATE ACCEPT message, shall check if the CSG ID of the cell where the UE has sent the TRACKING AREA UPDATE REQUEST message is contained in the Allowed CSG list. If not, the UE shall add that CSG ID to the Allowed CSG list EF<sub>ACSGL</sub>.

Reference:

- TS 24.301 [21], clause 5.5.3.2.4

CR 3 By default, the UE shall display all available CSGs for any PLMN, unless the UE has been configured by the HPLMN, for a specific PLMN, to display only CSGs in the Operator CSG List that are available.

Reference:

- TS 22.220 [52], clause 5.3.2 and 5.5.4

### 10.1.8.3 Test purpose

The purpose of this test is to verify that:

- 1) the ME adds the CSG ID to the Allowed CSG list in EF<sub>ACSGL</sub> in case this CSG ID belongs to the cell where the ME has sent the TRACKING AREA UPDATE REQUEST message which was accepted by the TT (E-USS).
- 2) during the manual CSG selection all available CSG ID shall be displayed with restrictions.

### 10.1.8.4 Method of test

#### 10.1.8.4.1 Initial conditions

The values of the ACSGL/OCSGL UICC as defined in clause 4.5.6 of the present document are used with EF<sub>IMSI</sub> as defined in clause 4.6.2 and the following exceptions:

EF<sub>AD</sub> (Administrative Data)

Logically:

- UE operation mode: Normal operation + specific facilities
- Additional information: Ciphering indicator feature disabled
- MNC: 3 digit
- For every PLMN not included in EF<sub>OCSGL</sub> or any PLMN for which a CSG display indicator tag is not present, only the available CSGs found in the Operator CSG list shall be displayed (B3)

Coding:

Byte	B1	B2	B3	B4
Hex	01	00	02	03

The TT (E-USS) transmits on the BCCH, with the following network parameters:

Cell A:

- TAI (MCC/MNC/TAC): 246/081/0001.
- Access control: unrestricted.
- csg-Indication: FALSE
- csg-Identity: not present

Cell B:

- TAI (MCC/MNC/TAC): 246/080/0002.
- Access control: unrestricted.
- csg-Indication: TRUE
- csg-Identity: 04

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and set the UE to automatic PLMN selection mode.

#### 10.1.8.4.2 Procedure

Step	Direction	Action	Comment	REQ	SA
1	UE	Run initial activation			

2	UE > USIM	READ EF <sub>ACSGL</sub> , EF <sub>OCSGL</sub>		CR 1	A.2/1 or A.2/2
3	UE > TT	Send RRC CONNECTION REQUEST on Cell A (TAI 246/081/0001)	The TT responds with RRC CONNECTION SETUP		
4	UE > TT	Send RRC CONNECTION SETUP COMPLETE			
5	UE > TT	Send ATTACH REQUEST	The TT initiates authentication, starts integrity by using the security procedure.		
6	TT > UE	Send ATTACH ACCEPT with: - TAI (MCC/MNC/TAC): 246/081/ 0001 - GUTI: "24608100010266345678"	UE sends ATTACH COMPLETE, and further TT sends RRC CONNECTION RELEASE		
7	TT > UE	Use the MMI of the UE to perform manual CSG selection.	The UE shall not indicate the availability of a cell with csg-Identity 04 for PLMN 246/080, this shall be verified for 2 minutes.	CR 3	
8	TT	The network stops all RF output for Cell A (TAI 246/081/0001)	The BCCH of Cell A is reconfigured to indicate the following: - TAI (MCC/MNC/TAC): 246/081/0002 - csg-Indication: TRUE - csg-Identity: 04 TT resumes RF output on the BCCH.		
9	TT > UE	Use the MMI of the UE to perform manual CSG selection.	The UE shall indicate the availability of a cell with csg-Identity 04 for PLMN 246/081 (Cell A). The user shall select this cell by using the MMI.	CR 3	
10	UE > TT	Send RRC CONNECTION REQUEST on csg cell (Cell A) (TAI 246/081/0002)	The TT responds with RRC CONNECTION SETUP		
11	UE > TT	Send RRC CONNECTION SETUP COMPLETE			
12	UE > TT	Send TRACKING AREA UPDATE REQUEST	The TT initiates authentication, starts integrity by using the security procedure.		
13	TT > UE	Send TRACKING AREA UPDATE ACCEPT with the following parameters with integrity protection: - TAI (MCC/MNC/TAC): 246/081/ 0002 - GUTI: "24608100010266345699"	UE sends TRACKING AREA UPDATE COMPLETE, and further TT sends RRC CONNECTION RELEASE.		
14	UE > USIM	UPDATE EF <sub>ACSGL</sub>	In case the verification of the contents of EF <sub>ACSGL</sub> is not done during the UPDATE command step 14) needs to be executed.	CR 2	A.2/1 OR A.2/2
15	UE > USIM	UE is soft powered down.			
16	USER > UE	READ EF <sub>EPSLOCI</sub> , EF <sub>ACSGL</sub> , EF <sub>OCSGL</sub>			A.2/3

### 10.1.8.5 Acceptance criteria

CR 1 shall be explicitly verified in step 2) by ensuring that UE has successfully read EF<sub>ACSGL</sub> and EF<sub>OCSGL</sub>,

CR 3 shall be verified:

- 1- At step 7) by ensuring that MMI of the UE shall not indicate to the user CSG cell (CSG ID: 04) for PLMN 246/080 and also
- 2- At step 9) by ensuring that MMI of the UE shall indicate to the user CSG cell (CSG ID: 04) for PLMN 246/081

CR 2 shall be explicitly verified either in step 14) by analysing the UPDATE command used to update EF<sub>ACSGL</sub> (A.2/1 or A.2/2) or at step 16) by reading the EF<sub>EPSLOCI</sub>, EF<sub>ACSGL</sub>, EF<sub>OCSGL</sub> and verifying that it contains the following.

**EF<sub>EPSLOCI</sub>** (EPS Information)

Logically:

GUTI: 24608100010266345699

Last visited registered TAI: 246/081/0002

EPS update status: updated

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	0B	F6	42	16	80	00	01	02	66	43	65	99
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>						
	42	16	80	00	02	00						

#### EF<sub>AC</sub>CSGL (Allowed CSG Lists)

Logically:

1<sup>st</sup> CSG list

PLMN: 246 081 (MCC MNC)  
 1<sup>st</sup> CSG list 1<sup>st</sup> CSG Type indication 02  
 1<sup>st</sup> CSG list 1<sup>st</sup> CSG HNB Name indication 02  
 1<sup>st</sup> CSG list 1<sup>st</sup> CSG CSG ID: 02 (27bit)  
 1<sup>st</sup> CSG list 2<sup>nd</sup> CSG Type indication 03  
 1<sup>st</sup> CSG list 2<sup>nd</sup> CSG HNB Name indication 03  
 1<sup>st</sup> CSG list 2<sup>nd</sup> CSG CSG ID: 03 (27bit)  
 1<sup>st</sup> CSG list 3<sup>rd</sup> CSG Type indication 'xx' (not checked)  
 1<sup>st</sup> CSG list 3<sup>rd</sup> CSG HNB Name indication 'xx' (not checked)  
 1<sup>st</sup> CSG list 3<sup>rd</sup> CSG CSG ID: 04 (27bit)

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	A0	1D	80	03	42	16	80	81	06	02	02	00
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	00	00	5F	81	06	03	03	00	00	00	7F	81
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>	<b>B31</b>					
	06	xx	xx	00	00	00	9F					

2<sup>nd</sup> CSG list

PLMN: 244 081 (MCC MNC)  
 2<sup>nd</sup> CSG list 1<sup>st</sup> CSG Type indication 08  
 2<sup>nd</sup> CSG list 1<sup>st</sup> CSG HNB Name indication 08  
 2<sup>nd</sup> CSG list 1<sup>st</sup> CSG CSG ID: 08 (27bit)

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	A0	0D	80	03	42	14	80	81	06	08	08	00
	<b>B13</b>	<b>B14</b>	<b>B15</b>									
	00	01	1F									

NOTE: The 1<sup>st</sup> and 2<sup>nd</sup> CSG list may be stored together or separately in any record in arbitrary order.

#### EF<sub>OC</sub>CSGL (Operator CSG Lists)

Unchanged values as defined in 4.5.6.

## 10.2 CSG list handling for UTRA

### 10.2.1 Manual CSG selection without display restrictions in UTRA with ACSG list and OCSG list on USIM

UTRAN test - not applicable

## 10.2.2 Manual CSG selection with display restrictions in UTRA with ACSG list and OCSG list on USIM

UTRAN test - not applicable

## 10.2.3 Manual CSG selection in UTRA with CSG list on USIM, success

UTRAN test - not applicable

---

# 11 NAS security context parameter handling

## 11.1 NAS security context parameter handling when service "EMM Information" is available

### 11.1.1 Definition and applicability

The security parameters for authentication, integrity protection and ciphering are tied together in an EPS security context and identified by a key set identifier for E-UTRAN (eKSI). The relationship between the security parameters is defined in TS 33.401 [50].

The EPS security context parameters shall be stored on the USIM if the corresponding file is present. If the corresponding file is not present on the USIM, these EMM parameters except allowed CSG list are stored in a non-volatile memory in the ME together with the IMSI from the USIM.

The EF<sub>EPSNSC</sub> contains the EPS NAS Security context as defined in TS 33.401 [50]. This file shall contain only one record and shall be updated only when the requirements defined in TS 33.401 [50] are met.

### 11.1.2 Conformance requirement

CR 1 The EPS security context parameters shall be stored on the USIM and mark the native EPS security context on the USIM as valid if the corresponding file is present, and shall be updated only when the requirements defined in TS 33.401 [50] are met.

CR 2 The EPS NAS security context parameters shall be stored when the UE transitions to EMM-DEREGISTERED state from EMM-REGISTERED state, as defined in TS 33.401 [50].

Reference:

- TS 24.301 [21], clause 4.4.2.1 and Annex C;
- TS 31.102 [19], clause 4.2.92;
- TS 33.401 [50], clause 6.1.1, 7.2.5.1 and 7.2.5.2.1.

### 11.1.3 Test purpose

The purpose of this test is to verify that the ME generates the EPS security context identified by a key set identifier for E-UTRAN (eKSI) and stores all inside EF<sub>EPSNSC</sub> if this EF is available and when the requirements defined in TS 33.401 [50], clauses 7.2.5.1 and 7.2.5.2.1 are met.

### 11.1.4 Method of test

#### 11.1.4.1 Initial conditions

The values of the E-UTRAN/EPC-UICC as defined in clause 4.5.4 of the present document are used with EF<sub>IMSI</sub> as defined in clause 4.6.2.

The TT (E-USS OR NB-SS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC):246/081/0001.
- Access control: unrestricted.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case.

#### 11.1.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	USER	Run initial activation.			
2	UE > USIM	Read EF <sub>UST</sub> , Read record 1 EF <sub>EPSNSC</sub>		CR 1	A.2/1 OR A.2/2
3	UE > TT	RRC CONNECTION REQUEST / RRC CONNECTION REQUEST-NB	TT responds with a RRC CONNECTION SETUP / RRC CONNECTION SETUP-NB		
4	UE > TT	RRC CONNECTION SETUP COMPLETE / RRC CONNECTION SETUP COMPLETE-NB			
5	UE > TT	ATTACH REQUEST	eKSI: '07'	CR 1	
6	TT > UE	AUTHENTICATION REQUEST	For EPS authentication and AKA procedure TT uses eKSI: '00'		
7	UE > TT	AUTHENTICATION RESPONSE			
8	UE > TT	SecurityModeCommand	UE responds with a SECURITY MODE COMPLETE		
9	TT > UE	ATTACH ACCEPT - TAI (MCC/MNC/TAC): 246/081/ 0001 - GUTI "24608100010266345678"			
10	UE > TT	ATTACH COMPLETE			
11	TT > UE	Send a RRC CONNECTION RELEASE / RRC CONNECTION RELEASE-NB			
12	UE > USIM	READ RECORD 1 of EF <sub>EPSNSC</sub>		CR 2	A.2/1 OR A.2/2
13	UE > TT	The UE is soft powered down, and initiates DETACH procedure.			
14	UE > USIM	UPDATE EF <sub>EPSNSC</sub>		CR 1 CR 2	A.2/1 OR A.2/2 OR A.2/3

#### 11.1.4.5 Acceptance criteria

CR1 is explicitly verified at step 2) before UE attempts registration by ensuring that UE shall read EF<sub>UST</sub> and EF<sub>EPSNSC</sub>, and also at Step 14) after detach is performed by ensuring that UE shall update the EF<sub>EPSNSC</sub>.

At step 2), EF<sub>EPSNSC</sub> shall contain:

**EF<sub>EPSNSC</sub>** (EPS NAS Security Context)

Logically:

Key Set Identifier KSI<sub>ASME</sub>: '07'  
ASME Key (KSI<sub>ASME</sub>): 32 byte key, value not checked  
Uplink NAS count: any value  
Downlink NAS count: any value  
Identifiers of selected NAS integrity and encryption algorithm any value

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	A0	xx	80	01	07	81	xx	xx
	...	<b>Bxx</b>						
	...	xx						

At step 14), EF<sub>EPSNSC</sub> shall contain:

EF<sub>EPSNSC</sub> (EPS NAS Security Context)

Logically:

Key Set Identifier KSI<sub>ASME</sub>: '00'  
 ASME Key (KSI<sub>ASME</sub>): 32 byte key, value not checked  
 Uplink NAS count: any value  
 Downlink NAS count: any value  
 Identifiers of selected NAS integrity and encryption algorithm: any value

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Hex	A0	xx	80	01	00	81	xx	xx
	...	<b>Bxx</b>						
	...	xx						

CR 1 is also verified at step 5) by analysing the ATTACH REQUEST and UE indicated that no key is available.

CR 2 is explicitly verified at step 12) and ensure that EF<sub>EPSNSC</sub> remains unchanged from initial value.

## 11.2 NAS security context parameter handling when service "EMM Information" is not available, no IMSI change

### 11.2.1 Definition and applicability

The security parameters for authentication, integrity protection and ciphering are tied together in an EPS security context and identified by a key set identifier for E-UTRAN (eKSI). The relationship between the security parameters is defined in TS 33.401 [50].

The EPS security context parameters shall be stored on the USIM if the corresponding file is present. If the corresponding file is not present on the USIM, these EMM parameters except allowed CSG list are stored in a non-volatile memory in the ME together with the IMSI from the USIM.

The EF<sub>EPSNSC</sub> contains the EPS NAS Security context as defined in TS 33.401 [50]. This file shall contain only one record.

### 11.2.2 Conformance requirement

CR 1 The EPS security context parameters shall be stored on the non-volatile memory in the ME together with the IMSI from the USIM if the corresponding file to store EPS security context parameters is not present on the USIM.

Reference:

- TS 24.301 [21], clause 4.4.2.1 and Annex C;
- TS 31.102 [19], clause 4.2.92;
- TS 33.401 [50], clause 6.1.1.

CR 2 These EMM parameters can only be used if the IMSI from the USIM matches the IMSI stored in the non-volatile memory; else the UE shall delete the EMM parameters.

Reference:

- TS 24.301 [21], clause 4.4.2.1 and Annex C;
- TS 33.401 [50], clause 6.1.1.

### 11.2.3 Test purpose

The purpose of this test is to verify that the ME generates the EPS security context identified by a key set identifier for E-UTRAN (eKSI) and stores all inside a non-volatile memory in the ME as EMM information is not available on the USIM. During the test the IMSI on the USIM remains unchanged.

### 11.2.4 Method of test

#### 11.2.4.1 Initial conditions

The values of the Default UICC as defined in clause 4.5.2 of the present document are used with the following exception:

**EF<sub>UST</sub>** (USIM Service Table)

Logically:

Service n°85:            EPS Mobility Management Information            not available

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8
Binary	xx1x xx11	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxxx xxxx	xxxx xxxx	xxxx xxxx
	<b>B9</b>	<b>B10</b>	<b>B11</b>	<b>B12</b>				
	xxxx xxxx	xxxx xxxx	xx10 xxxx	0000 0xxx				

The TT (E-USS OR NB-SS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC):246/081/0001.
- Access control:            unrestricted.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case.

#### 11.2.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	USER	Run initial activation.			
2	UE > USIM	READ EF <sub>UST</sub>		CR 1	A.2/1 OR A.2/2
3	UE > TT	RRC CONNECTION REQUEST / RRC CONNECTION REQUEST-NB	TT responds with a RRC CONNECTION SETUP / RRC CONNECTION SETUP-NB		
4	UE > TT	RRC CONNECTION SETUP COMPLETE / RRC CONNECTION SETUP COMPLETE-NB			
5	UE > TT	ATTACH REQUEST	eKSI: '07'		
6	TT > UE	AUTHENTICATION REQUEST	For EPS authentication and AKA procedure TT uses eKSI: '00'		
7	UE > TT	AUTHENTICATION RESPONSE			
8	UE > TT	SecurityModeCommand	TT responds with a SECURITY MODE COMPLETE		
9	TT > UE	ATTACH ACCEPT - TAI (MCC/MNC/TAC): 246/081/ 0001 - GUTI: "24608100010266345678"			

10	UE > TT	ATTACH COMPLETE			
11	TT > UE	RRC CONNECTION RELEASE / RRC CONNECTION RELEASE-NB			
12	UE > TT	The UE is powered off, and initiates Detach procedure.			
13	USER	Run initial activation			
14	UE > TT	RRC CONNECTION REQUEST / RRC CONNECTION REQUEST-NB	TT responds with a RRC CONNECTION SETUP / RRC CONNECTION SETUP-NB		
15	UE > TT	RRC CONNECTION SETUP COMPLETE / RRC CONNECTION SETUP COMPLETE-NB			
16	UE > TT	ATTACH REQUEST	eKSI: '00'	CR 2	
17	TT > UE	SecurityModeCommand (TT uses the last known K <sub>ASME</sub> )	UE responds with a SECURITY MODE COMPLETE	CR 2	
18	TT > UE	ATTACH ACCEPT - TAI (MCC/MNC/TAC): 246/081/0001 - GUTI: "24608100010266345619"			
19	UE > TT	ATTACH COMPLETE			
20	TT > UE	RRC CONNECTION RELEASE / RRC CONNECTION RELEASE-NB			
21	USER	The UE is powered down			

## 11.2.5 Acceptance criteria

CR1 is explicitly verified at step 2) by verifying that UE read EF<sub>UST</sub>

CR 2 can be verified at step 16) by ensuring that the UE has indicated in ATTACH REQUEST eKSI as '00' and NAS security mode procedure is successful at step 17).

## 11.3 NAS security context parameter handling when service "EMM Information" is not available, IMSI Changed

### 11.3.1 Definition and applicability

The security parameters for authentication, integrity protection and ciphering are tied together in an EPS security context and identified by a key set identifier for E-UTRAN (eKSI). The relationship between the security parameters is defined in TS 33.401 [50].

The EPS security context parameters shall be stored on the USIM if the corresponding file is present. If the corresponding file is not present on the USIM, these EMM parameters except allowed CSG list are stored in a non-volatile memory in the ME together with the IMSI from the USIM.

The EF<sub>EPSNSC</sub> contains the EPS NAS Security context as defined in TS 33.401 [50]. This file shall contain only one record.

### 11.3.2 Conformance requirement

CR 1 The EPS security context parameters shall be stored on the non-volatile memory in the ME together with the IMSI from the USIM if the corresponding file to store EPS security context parameters is not present on the USIM.

Reference:

- TS 24.301 [21], clause 4.4.2.1 and Annex C;
- TS 31.102 [19], clause 4.2.92;
- TS 33.401 [50], clause 6.1.1.



7	UE > TT	AUTHENTICATION RESPONSE			
8	UE > TT	SecurityModeCommand	TT responds with a SECURITY MODE COMPLETE		
9	TT > UE	ATTACH ACCEPT - TAI (MCC/MNC/TAC): 246/081/ 0001 - GUTI: "24608100010266345678"			
10	UE > TT	ATTACH COMPLETE			
11	TT > UE	RRC CONNECTION RELEASE / RRC CONNECTION RELEASE-NB			
12	UE > TT	The UE is powered off, and initiates DETACH procedure.			
13	UE	Run initial activation with IMSI set to "246081222233333".			
14	UE > TT	RRC CONNECTION REQUEST / RRC CONNECTION REQUEST-NB	TT responds with a RRC CONNECTION SETUP / RRC CONNECTION SETUP-NB		
15	UE > TT	RRC CONNECTION SETUP COMPLETE / RRC CONNECTION SETUP COMPLETE-NB			
16	UE > TT	ATTACH REQUEST	eKSI: '07'	CR 2	
17	TT > UE	SecurityModeCommand (TT uses the last known K <sub>ASME</sub> )	UE responds with a SECURITY MODE REJECT	CR 2	
20	TT > UE	RRC CONNECTION RELEASE / RRC CONNECTION RELEASE-NB			
21	USER	The UE is powered down			

### 11.3.5 Acceptance criteria

CR1 is explicitly verified at step 2) by verifying that UE read EF<sub>UST</sub>

CR 2 can be verified at step 16) by ensuring that the UE has indicated in ATTACH REQUEST eKSI as '07' and NAS security mode procedure is rejected by ME at step 17).

## 11.4 EPS NAS Security Context Storage

### 11.4.1 Definition and applicability

The security parameters for authentication, integrity protection and ciphering are tied together in an EPS security context and identified by a key set identifier for E-UTRAN (eKSI). The relationship between the security parameters is defined in TS 33.401 [27].

The EPS security context parameters shall be stored on the USIM if the corresponding file is present. If the corresponding file is not present on the USIM, these EMM parameters except allowed CSG list are stored in a non-volatile memory in the ME together with the IMSI from the USIM.

The EF<sub>EPSNSC</sub> contains the EPS NAS Security context as defined in TS 33.401 [27]. This file shall contain only one record and shall be updated only when the requirements defined in TS 33.401 [27] are met.

### 11.4.2 Conformance requirement

CR 1 The EPS security context parameters shall be stored on the USIM and mark the native EPS security context on the USIM as valid if the corresponding file is present, and shall be updated only when the requirements defined in TS 33.401 [27] are met.

Reference:

- TS 24.301 [21], clause 4.4.2.1 and Annex C;
- TS 31.102 [19], clause 4.2.92 and 5.2.28;
- TS 33.401 [50], clause 6.1.1, 7.2.5.2, 7.2.6.1 and 7.2.6.3.

CR 2 The initial NAS message shall be integrity protected by the current EPS NAS security context if such exists. If no current EPS NAS security context exists the ME shall signal “no key available” in the initial NAS message, as defined in TS 33.401 [27].

Reference:

- TS 24.301 [21], clause 4.4.2.1 and Annex C;
- TS 31.102 [19], clause 4.2.92 and 5.2.28;
- TS 33.401 [50], clause 6.1.1, 7.2.5.2, 7.2.6.1 and 7.2.6.3.

CR 3 ME shall handle the EPS NAS security context in accordance with the rules and procedures as specified in TS 33.401 [27] during ECM state transition.

Reference:

- TS 33.401 [50], clause 6.1.1, 7.2.5.2, 7.2.6.1 and 7.2.6.3.

### 11.4.3 Test purpose

The purpose of this test is to verify that the update of EPS NAS security context shall be according to the rules and procedures specified in TS 33.401 [50], clauses 6.1.1, 7.2.5.2, 7.2.6.1 and 7.2.6.3.

### 11.4.4 Method of test

#### 11.4.4.1 Initial conditions

The values of the Default UICC as defined in clause 4.5.4 of the present document are used

The TT (E-USS OR NB-SS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC):246/081/0001.
- Access control: unrestricted.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case.

#### 11.4.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	USER	Run initial activation.			
2	UE > USIM	READ EF <sub>UST</sub> and EF <sub>EPSNSC</sub>		CR 1	A.2/1 OR A.2/2
3	UE > TT	RRC CONNECTION REQUEST / RRC CONNECTION REQUEST-NB	TT responds with a RRC CONNECTION SETUP / RRC CONNECTION SETUP-NB		
4	UE > TT	RRC CONNECTION SETUP COMPLETE / RRC CONNECTION SETUP COMPLETE-NB			
5	UE > TT	ATTACH REQUEST	eKSI: '07'	CR 2	
6	TT > UE	AUTHENTICATION REQUEST	For EPS authentication and AKA procedure TT uses eKSI: '00'	CR 3	A.2/1 OR A.2/2
7	UE > TT	AUTHENTICATION RESPONSE		CR 3	A.2/1 OR A.2/2
8	UE > TT	SecurityModeCommand	TT responds with a SECURITY MODE COMPLETE	CR 3	A.2/1 OR A.2/2
9	TT > UE	ATTACH ACCEPT with: - TAI (MCC/MNC/TAC): 246/081/ 0001 - GUTI: "24608100010266345678"		CR 3	A.2/1 OR A.2/2

10	UE > TT	ATTACH COMPLETE		CR 3	A.2/1 OR A.2/2
11	TT > UE	RRC CONNECTION RELEASE / RRC CONNECTION RELEASE-NB		CR 3	A.2/1 OR A.2/2
12	UE > TT	PAGING / PAGING-NB using the S-TMSI	CN domain indicator set to "PS".	CR 3	A.2/1 OR A.2/2
14	UE > TT	RRC CONNECTION REQUEST / RRC CONNECTION REQUEST-NB	TT responds with a RRC CONNECTION SETUP / RRC CONNECTION SETUP- NB	CR 3	A.2/1 OR A.2/2
15	UE > TT	RRC CONNECTION SETUP COMPLETE / RRC CONNECTION SETUP COMPLETE-NB		CR 3	(A.2/1 OR A.2/2)
16	UE > TT	EMM SERVICE REQUEST (for WB-S1) CONTROL PLANE SERVICE REQUEST (for NB-IOT)	For WB-S1: TT Activates AS security by the E-USS and the Dedicated EPS bearer is established. For NB-IOT: TT responds with SERVICE ACCEPT and default bearer is established.	CR 3	A.2/1 OR A.2/2
17		Wait 5 seconds			
18	TT > UE	RRC CONNECTION RELEASE / RRC CONNECTION RELEASE-NB		CR 3	A.2/1 OR A.2/2

### 11.4.5 Acceptance criteria

CR 1 is explicitly verified at step 2) by verifying that UE reads  $EF_{UST}$  and  $EF_{EPSNSC}$

CR 2 can be verified at step 5) by ensuring that the UE has indicated in ATTACH REQUEST eKSI as '07' and at step 18) by ensuring NAS security mode procedure is rejected by ME.

CR 3 is explicitly verified at steps 6) to 16) by verifying that UE shall not update  $EF_{EPSNSC}$ . This can be alternatively verified by explicitly reading and analysing the value of  $EF_{EPSNSC}$  at step 15).

---

## 12 Non Access Stratum (NAS) Configuration parameter handling

### 12.1 $EF_{NASCONFIG}$ - NAS signalling priority handling

The test case is covered in TS 34.123-1 [43] clauses 9.4.3.7, 9.4.5.5, 11.1.1.3, 11.1.1.4, 11.1.3.4, 11.2.2.3, 12.4.1.1e and 12.4.3.2a. See CP-170166, CR #0229 to TS 31.121 [2] for details

### 12.2 $EF_{NASCONFIG}$ - NMO I Network Mode of Operation I handling

The test case is covered in TS 34.123-1 [43] clause 12.2.2.3a. See CP-170166, CR #0230 to TS 31.121 [2] for details.

### 12.3 $EF_{NASCONFIG}$ - Attach with IMSI handling

The test case is covered in TS 34.123-1 [43] clause 12.2.1.1a. See CP-170166, CR #0224 to TS 31.121 [2] for details.

### 12.4 $EF_{NASCONFIG}$ - Verifying Minimum Periodic Search Timer

The test case is covered in TS 34.123-1 [43] clauses 9.4.5.4 and 9.4.5.4.7. See CP-170166, CR #0228 to TS 31.121 [2] for details.

## 12.5 EF<sub>NASCONFIG</sub> - Extended access barring handling

The test case is covered in TS 34.123-1 [43] clauses 8.1.1.20, 9.4.11, 12.2.1.16 and 12.4.1.9. See CP-170166, CR #0226 to TS 31.121 [2] for details.

## 12.6 EF<sub>NASCONFIG</sub> - Verifying Timer T3245 Behaviour

UTRAN test - not applicable

## 12.7 EF<sub>NASCONFIG</sub> - Override NAS signalling low priority

UTRAN test - not applicable

## 12.8 EF<sub>NASCONFIG</sub> - Override Extended access barring

UTRAN test - not applicable

## 12.9 EF<sub>NASCONFIG</sub> - Fast First Higher Priority PLMN Search

UTRAN test - not applicable

## 12.10 EF<sub>NASCONFIG</sub> - E-UTRA Disabling Allowed for EMM cause #15

Test using UTRAN – not applicable

## 12.11 EF<sub>NASCONFIG</sub> - SM\_RetryWaitTime

UTRAN test - not applicable

## 12.12 EF<sub>NASCONFIG</sub> - SM\_RetryAtRATChange

FFS

---

# 13 UICC interface during PSM

## 13.1 UICC interface in PSM handling for E-UTRAN – No UICC deactivation in PSM

### 13.1.1 Definition and applicability

PSM is intended for UEs that are expecting only infrequent mobile originating and terminating services and that can accept a corresponding latency in the mobile terminating communication. In order to reduce power consumption while in PSM, and only in case the PIN of the USIM is disabled, the ME may optionally deactivate the UICC after entering the PSM.

## 13.1.2 Conformance requirement

CR 1 In order to reduce power consumption while the ME is in PSM, and only in case the PIN of the USIM is disabled, the ME may optionally deactivate the UICC (as specified in clause 6A.1 of TS 31.101 [33]) after entering the PSM.

Reference:

- TS 31.102 [19], clause 5.1.10;
- TS 24.301 [21], clauses 5.3.5 and 5.3.11.
- TS 31.101 [33], clause 6A.1.

## 13.1.3 Test purpose

To verify that UE does not deactivate the UICC in case the PIN for the USIM is enabled and verified.

## 13.1.4 Method of test

### 13.1.4.1 Initial conditions

The values of the E-UTRAN/EPC UICC as defined in clause 4.5.4 of the present document are used with the following exceptions:

The PIN of the USIM is enabled.

$EF_{UMPC}$

Logically:

UICC maximum power consumption: 60 mA  
 Operator defined time out (T\_OP): 5 seconds  
 Additional information: UICC does not require increased idle current  
 UICC does not support the UICC suspension procedure  
 Byte 4 and byte 5: RFU

Coding:

Byte	B1	B2	B3	B4	B5
Hex	3C	05	00	00	00

The UE is configured to use Power Saving Mode.

The UE is configured to use the timer T3324 set to T3324\_V.

The TT (E-USS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.
- Access control: unrestricted.

The TT (NB-SS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.
- Access control: unrestricted.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case.

### 13.1.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
------	-----------	--------	-------------	-----	----

1	UE	Run initial activation.			
2	USER > UE	Enter PIN when in PIN check mode	The PIN 0000 is used		
3	UE > TT	Send RRC CONNECTION REQUEST / RRC CONNECTION REQUEST-NB	TT responds with RRC CONNECTION SETUP / RRC CONNECTION SETUP-NB		
3	UE > TT	The UE transmits an ATTACH REQUEST message including T3324 set to T3324_V	The TT sends the ATTACH ACCEPT message contains T3324 set to T3324_V and T3412 set to T3412_V. The ATTACH ACCEPT message shall not contain the eDRX parameters		
4	UE > TT	The UE transmits the ATTACH COMPLETE during registration from the UE	The TT sends RRC CONNECTION RELEASE / RRC CONNECTION RELEASE-NB.	CR 1	
5	UE	The UE is waiting for the T3412 timer expiration		CR 1	
6	UE	The UE sends TRACKING AREA UPDATE REQUEST	The TT sends TRACKING AREA UPDATE ACCEPT	CR 1	
7	UE	The UE is powered off.			

### 13.1.5 Acceptance criteria

CR 1 is met if the UE does not deactivate the UICC or send SUSPEND UICC command after step 4).

## 13.2 UICC interface in PSM handling for E-UTRAN – PSM not accepted by E-USS/NB-SS

### 13.2.1 Definition and applicability

PSM is intended for UEs that are expecting only infrequent mobile originating and terminating services and that can accept a corresponding latency in the mobile terminating communication. In order to reduce power consumption while in PSM, and only in case the PIN of the USIM is disabled, the ME may optionally deactivate the UICC after entering the PSM.

### 13.2.2 Conformance requirement

CR 1 In order to reduce power consumption while the ME is in PSM, and only in case the PIN of the USIM is disabled, the ME may optionally deactivate the UICC (as specified in clause 6A.1 of TS 31.101 [33]) after entering the PSM.

Reference:

- TS 31.102 [19], clause 5.1.10;
- TS 24.301 [21], clauses 5.3.5 and 5.3.11.
- TS 31.101 [33] in clause 6A.1.

### 13.2.3 Test purpose

The purpose of this test is to verify that the UE does not deactivate the UICC in case the network is not supporting/accepting PSM.

### 13.2.4 Method of test

#### 13.2.4.1 Initial conditions

The UE is configured to use Power Saving Mode.

The UE is configured to use the timer T3324 set to T3324\_V.

The E-USS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.
- Access control: unrestricted.

The NB-SS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.
- Access control: unrestricted.

The default E-UTRAN UICC is installed into the Terminal.

The PIN of the USIM is disabled.

### 13.2.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	Run initial activation.			
2	UE > TT	The UE requests RRC Connection	The TT responds with RRC Connection setup		
3	UE > TT	The UE transmits an ATTACH REQUEST message including T3324 set to T3324_V.			
4	TT > UE	The TT sends the ATTACH ACCEPT message contains T3324 set to "deactivated".	The ATTACH ACCEPT message shall not contain the eDRX parameters	CR1	
5	UE > TT	The UE transmits the ATTACH COMPLETE during registration from the UE	The TT sends RRC CONNECTION RELEASE/RRC CONNECTION RELEASE-NB.	CR1	
6	TT	The TT is waiting for the T3324_V time period to pass		CR1	
7	TT > UE	The TT transmits PAGING / PAGING-NB using the S-TMSI.		CR1	
8	UE > TT	Send RRC CONNECTION REQUEST / RRC CONNECTION REQUEST-NB	The TT responds with a RRC CONNECTION SETUP / RRC CONNECTION SETUP-NB	CR1	
9	UE > TT	Send RRC CONNECTION SETUP COMPLETE / RRC CONNECTION SETUP COMPLETE-NB		CR1	
10	UE > TT	The UE sends SERVICE REQUEST	The TT sends SERVICE ACCEPT followed by RRC CONNECTION RELEASE/RRC CONNECTION RELEASE-NB	CR1	
11	UE	The UE is powered off.			

### 13.2.5 Acceptance criteria

CR 1 is met if the UE does not deactivate the UICC or send SUSPEND UICC command after step 4).

NOTE: The execution of the SUSPEND UICC command is no subject to be tested in this sequence.

## 13.3 UICC interface in PSM handling for E-UTRAN – UICC deactivation in PSM

A reliable verification of the activation/deactivation of the UICC in PSM can be done with a physical connection to supply contacts only. Unless a suitable and sufficient environment is introduced the definition of this test is FFS.

## 13.4 UICC interface in PSM for E-UTRAN – SUSPEND UICC

### 13.4.1 Definition and applicability

PSM is intended for UEs that are expecting only infrequent mobile originating and terminating services and that can accept a corresponding latency in the mobile terminating communication. If the UICC supports the UICC suspension mechanism (SUSPEND UICC command), the ME may suspend the UICC after entering the PSM. In this case, the ME shall successfully resume the UICC before it can leave the PSM.

### 13.4.2 Conformance requirement

CR 1 If the UICC supports the UICC suspension mechanism (SUSPEND UICC command), the ME may suspend the UICC after entering the PSM. In this case, the ME shall successfully resume the UICC before it can leave the PSM.

Reference:

- TS 31.102 [19], clause 5.1.10;
- TS 24.301 [21], clauses 5.3.5, 5.3.11 and 5.5.1.2.2.
- TS 31.101 [33], clause 11.1.22.

### 13.4.3 Test purpose

- 1) To verify that after reading  $EF_{UMPC}$  and entering the PSM the ME sends a SUSPEND UICC command to the UICC in case the UICC indicates the support of the SUSPEND UICC command.
- 2) To verify that the ME resumes the UICC before it can leave the PSM.

### 13.4.4 Method of test

#### 13.4.4.1 Initial conditions

The UE is configured to use Power Saving Mode.

The UE is configured to use the timer T3324 set to T3324\_V.

The E-USS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.
- Access control: unrestricted.

The NB-SS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.
- Access control: unrestricted.

The default E-UTRAN UICC is used with the following exceptions:

$EF_{UMPC}$  (UICC Maximum Power Consumption)

Logically:

UICC maximum power consumption:	60 mA
Operator defined time out (T_OP):	5 seconds
Additional information:	UICC does not require increased idle current
	UICC supports the UICC suspension procedure
Byte 4 and byte 5:	RFU

Coding:

Byte	B1	B2	B3	B4	B5
Hex	3C	05	00	00	00

The PIN of the USIM is enabled and verified.

### 13.4.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	Run initial activation.			
2	UE > TT	The UE requests RRC Connection	The TT responds with RRC Connection setup		
3	UE > TT	The UE transmits an ATTACH REQUEST message including T3324 set to T3324_V.			
4	TT > UE	The TT sends the ATTACH ACCEPT message contains T3324 set to T3324_V and T3412 set to T3412_V.	The ATTACH ACCEPT message shall not contain the eDRX parameters	CR1	
5	UE > TT	The UE transmits the ATTACH COMPLETE during registration from the UE	The TT sends RRC CONNECTION RELEASE/RRC CONNECTION RELEASE-NB.	CR1	
6	ME > UICC	The ME sends <i>SUSPEND UICC</i> command to the UICC indicating "Minimum duration of the suspension proposed by the terminal" and the "Maximum duration of the suspension proposed by the terminal"	The UICC returns a maximum suspension duration in the range proposed by the ME, Resume token and SW 9000.		
7	UE	The UE is waiting for the T3412 timer expiration		CR1	
8	UE	The UE sends TRACKING AREA UPDATE REQUEST	The TT sends TRACKING AREA UPDATE ACCEPT	CR1	
9	UE	The UE is powered off.			

NOTE: For testing purposes, and to not extend the test execution time the maximum suspension duration returned by the UICC shall be equal to the minimum duration of the suspension proposed by the terminal.

### 13.4.5 Acceptance criteria

CR 1 is met if the ME:

- 1) reads EF<sub>UMPC</sub> after step 1) to verify that the SUSPEND UICC command is supported.

Note: RFU – agreed method to verify contents of EF<sub>UMPC</sub>

- 2) deactivates the UICC after Step (6) as specified in TS 31.101 [39].
- 3) leaves the PSM and resumes the UICC after Step (8).

---

## 14 UICC interface during eDRX

### 14.1 UICC interface during eDRX for E-UTRAN – eDRX is not supported by the UICC

#### 14.1.1 Definition and applicability

In order to reduce power consumption when the UE uses extended idle mode DRX cycle, the UE may optionally deactivate the UICC during the extended idle mode DRX cycle.



2	UE > TT	The UE requests RRC Connection	The TT responds with RRC Connection setup		
3	UE > TT	The UE transmits an ATTACH REQUEST message including the eDRX parameters			
4	TT > UE	The TT sends the ATTACH ACCEPT message containing the eDRX parameters.	If ATTACH REQUEST in step 3) above also contains T3324, the ATTACH ACCEPT message shall contain T3324 set to "deactivated". If ATTACH REQUEST in step 3) does not contain T3324, the ATTACH ACCEPT message shall not contain T3324.		
5	UE > TT	The UE transmits the ATTACH COMPLETE during registration from the UE	The TT sends RRC CONNECTION RELEASE / RRC CONNECTION RELEASE-NB.	CR1	
6	TT > UE	The TT transmits PAGING / PAGING-NB using the S-TMSI in a valid paging occasion within the PTW of the paging Hyperframes as per Idle eDRX.		CR1	
7	UE > TT	Send RRC CONNECTION REQUEST / RRC CONNECTION REQUEST-NB	The TT responds with a RRC CONNECTION SETUP / RRC CONNECTION SETUP-NB	CR1	
8	UE > TT	Send RRC CONNECTION SETUP COMPLETE / RRC CONNECTION SETUP COMPLETE-NB		CR1	
9	UE > TT	The UE sends ServiceRequest	The TT sends ServiceAccept followed by RRC CONNECTION RELEASE / RRC CONNECTION RELEASE-NB	CR1	
10	UE	The UE is powered off.			

### 14.1.5 Acceptance criteria

CR 1 is met if the UE does not deactivate the UICC or send SUSPEND UICC command after step 5).

## 14.2 UICC interface during eDRX for E-UTRAN – eDRX is not accepted by E-USS/NB-SS

### 14.2.1 Definition and applicability

In order to reduce power consumption when the UE uses extended idle mode DRX cycle, the UE may optionally deactivate the UICC during the extended idle mode DRX cycle.

### 14.2.2 Conformance requirement

CR 1 In case the UICC does not support the UICC suspension mechanism, the PIN of the USIM is disabled and deactivation of UICC is authorized in EF<sub>AD</sub>, the UE may optionally deactivate the UICC (as specified in clause 6A.1 of TS 31.101 [33]) during the extended idle mode DRX cycle.

Reference:

- TS 31.102 [19], clause 5.1.11;
- TS 24.301 [21], clauses 5.3.12;
- TS 23.401 [42], clause 5.13a;
- TS 31.101 [33], clause 6A.1.

### 14.2.3 Test purpose

- 1) To verify that UE does not deactivate the UICC in case extended DRX cycle is not supported by the network

### 14.2.4 Method of test

#### 14.2.4.1 Initial conditions

The UE is configured to request the use of eDRX (in the ATTACH REQUEST and *TrackingAreaUpdate* messages).

The E-USS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.
- Access control: unrestricted.

The NB-SS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 246/081/0001.
- Access control: unrestricted.

The default E-UTRAN UICC is used with the following exceptions:

EF<sub>AD</sub> (Administrative Data)

- Logically:
- Normal operation + specific facilities;
  - Ciphering indicator feature disabled;
  - CSG Display Control: for every PLMN not included in EF\_OCSGL, or for which a CSG display indicator tag is not present, all available CSGs can be displayed without any restriction;
  - ProSe services for Public Safety: the ME is not authorized for ProSe services for Public Safety usage without contacting the ProSe Function;
  - Extended DRX cycle: the ME is authorized to modify the polling interval and/or disable the UICC interface during extended DRX cycle;
  - Length of MNC in the IMSI: 3.

Coding:

Byte	B1	B2	B3	B4
Hex	01	00	08	03

The PIN of the USIM is disabled.

#### 14.2.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	Run initial activation.			
2	UE > TT	The UE requests RRC Connection	The TT responds with RCC Connection setup		
3	UE > TT	The UE transmits an ATTACH REQUEST message including the eDRX parameters			
4	TT > UE	The TT sends the ATTACH ACCEPT message containing the eDRX parameters.	If ATTACH REQUEST in step 3) above also contains T3324, the ATTACH ACCEPT message shall contain T3324 set to "deactivated". If ATTACH REQUEST in step 3) does not contain T3324, the ATTACH ACCEPT message shall not contain T3324.		

5	UE > TT	The UE transmits the ATTACH COMPLETE during registration from the UE	The TT sends RRC CONNECTION RELEASE/RRC CONNECTION RELEASE-NB.	CR1	
6	TT > UE	The TT transmits PAGING / PAGING-NB in a valid paging occasion as per normal DRX.		CR1	
7	UE > TT	Send RRC CONNECTION REQUEST / RRC CONNECTION REQUEST-NB	The TT responds with a RRC CONNECTION SETUP / RRC CONNECTION SETUP-NB	CR1	
8	UE > TT	Send RRC CONNECTION SETUP COMPLETE / RRC CONNECTION SETUP COMPLETE-NB		CR1	
9	UE > TT	The UE sends ServiceRequest	The TT sends ServiceAccept followed by RRC CONNECTION RELEASE/RRC CONNECTION RELEASE-NB	CR1	
10	UE	The UE is powered off.			

### 14.2.5 Acceptance criteria

CR 1 is met if the UE does not deactivate the UICC or send SUSPEND UICC command after step 5).

## 14.3 UICC interface during eDRX for E-UTRAN – UICC deactivation during eDRX

FFS

## 14.4 UICC interface during eDRX for E-UTRAN– SUSPEND UICC

FFS

---

# 15 Authentication procedure and NAS security context handling for 5G

## 15.1 Authentication procedure for EAP-AKA'

### 15.1.1 Authentication procedure for EAP-AKA' - Authentication is successful

#### 15.1.1.1 Definition and applicability

The purpose of the primary authentication and key agreement procedure is to enable mutual authentication between the UE and the network and to provide keying material that can be used between the UE and network in subsequent security procedures. The UE and the AMF shall support the EAP based primary authentication and key agreement procedure.

In order to initiate the EAP based primary authentication and key agreement procedure using EAP-AKA', the AUSF shall send an EAP message IE with EAP-request/AKA'-challenge message in the AUTHENTICATION REQUEST message.

The 5G NAS security context parameters from a full native 5G NAS security context shall be stored on the USIM if the corresponding file is present on the USIM as specified in TS 31.102 [19]. If the corresponding file is not present on the USIM, this 5GMM parameters is stored in a non-volatile memory in the ME together with the SUPI from the USIM.

The EF<sub>5GS3GPPNSC</sub> contains the 5GS 3GPP access NAS security context as defined in TS 24.501 [25], consisting of K<sub>AMF</sub> with the associated key set identifier, the UE security capabilities, and the uplink and downlink NAS COUNT values. This file shall contain one record.

The EF<sub>5GAUTHKEYS</sub> contains K<sub>AUSF</sub> and K<sub>SEAF</sub> that are generated on the ME using CK and IK as part of AKA procedures as described in TS 33.501 [24].

### 15.1.1.2 Conformance requirement

- CR 1 The UE shall support the EAP based primary authentication and key agreement procedure.
- CR 2 The ME shall forward the RAND and AUTN received in EAP message IE with EAP-Request/AKA'-Challenge within the AUTHENTICATION REQUEST message to the USIM.
- CR 3 The ME shall return the EAP message IE with EAP-response/AKA'-challenge in AUTHENTICATION RESPONSE message.
- CR 4 As a result of successful authentication procedure and upon receipt of the EAP-Success message, the 5G NAS security context parameters shall be stored on the USIM if the corresponding file is present on the USIM when entering state 5GMM-DEREGISTERED.
- CR 5 If service n°122 is available, the ME shall store K<sub>AMF</sub> with the associated key set identifier, the UE security capabilities, and the uplink and downlink NAS COUNT values in EF<sub>5GS3GPPNSC</sub> on the USIM.
- CR 6 If service n°123 is available, the ME shall store the K<sub>AUSF</sub> and K<sub>SEAF</sub> in EF<sub>5GAUTHKEYS</sub> on the USIM.
- CR 7 The UE can successfully register to the network.

Reference:

- TS 31.102 [19], clauses 4.4.11.3, 4.4.11.4 and 4.4.11.6;
- TS 33.501 [24], clause 6.1.3.1;
- TS 24.501 [25], clause 5.4.1.2 and Annex C.

### 15.1.1.3 Test purpose

The purpose of this test is to verify that:

- 1) the primary authentication and key agreement procedure enables mutual authentication between the UE and the network and provides keying material that can be used between the UE and network in subsequent security procedures.
- 2) the UE and the AMF support the EAP based primary authentication and key agreement procedure.
- 3) the EAP based primary authentication and key agreement procedure using EAP-AKA' is performed if the AUSF has initiated an EAP message IE with EAP-request/AKA'-challenge message in the AUTHENTICATION REQUEST message.
- 4) if the corresponding file is present on the USIM the 5G NAS security context parameters from a full native 5G NAS security context are stored on the USIM
- 5) EF<sub>5GS3GPPNSC</sub> contains one record with the 5GS 3GPP access NAS security context as defined in TS 24.501 [42], consisting of K<sub>AMF</sub> with the associated key set identifier, the UE security capabilities, and the uplink and downlink NAS COUNT values.
- 6) EF<sub>5GAUTHKEYS</sub> contains K<sub>AUSF</sub> and K<sub>SEAF</sub> that are generated on the ME using CK and IK as part of AKA procedures as described in TS 33.501 [41].
- 7) the UE can successfully register to the network.

### 15.1.1.4 Method of test

#### 15.1.1.4.1 Initial conditions

The values of the 5G-NR UICC as defined in clause 4.5.9 of the present document are used.

The TT (NG-SS) is configured to transmit on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/083/000001
- Access control: unrestricted.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case.

#### 15.1.1.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	TT	Activate NG-SS cell	The NG-SS cell on the TT is activated with SIB1 as defined in the initial conditions		
2	UE	Run initial activation			
3	UE <> TT	Establish RRC connection	UE camps on NG-SS cell and establishes RRC connection		
4	UE > TT	Send REGISTRATION REQUEST			
5	TT > UE	Send AUTHENTICATION REQUEST	The TT sends an AUTHENTICATION REQUEST message with EAP message IE with EAP request/AKA' challenge message with: - ngKSI: - NAS key set identifier: '000' - TSC: '0' - EAP message: - EAP-request/AKA'-challenge The NG-SS on the TT generates K <sub>AMF</sub> , K <sub>AUSF</sub> and K <sub>SEAF</sub> values, and initiates the EAP-AKA' authentication procedure		
6	ME > USIM	Pass RAND and AUTN values to the USIM	The ME provides the EAP request/AKA' challenge data received in the AUTHENTICATION REQUEST to the USIM	CR 1 CR 2	A.2/1 OR A.2/2
7	UE > TT	Send AUTHENTICATION RESPONSE	The UE sends an AUTHENTICATION RESPONSE message with EAP message IE with EAP response/AKA' challenge message: - Authentication response parameter: 4 – 16 octets RES value calculated according to TS 24.501 [25] The UE shall return RES equal to the XRES calculated at the NG-SS with the parameters provided/indicated in the AUTHENTICATION REQUEST at step 4	CR 3	
8	TT > UE	Sends SECURITY MODE COMMAND message with EAP-success	The NG-SS sends a SECURITY MODE COMMAND message with EAP-success		
9	UE > TT	Send SECURITY MODE COMPLETE	UE updates EF <sub>5GAUTHKEYS</sub> in parallel or after the NAS message	CR6	A.2/1 OR A.2/2
10	TT > UE	Send REGISTRATION ACCEPT	NG-SS sends a REGISTRATION ACCEPT message with: - 5G-GUTI: 24408300010266436587 - TAI: 244/83/000001		
11	UE > TT	UE sends REGISTRATION COMPLETE		CR7	
12	UE	The UE is powered off and/or deactivated, performs the DEREGISTRATION procedure.	UE enters the 5GMM-DEREGISTERED state and updates EF <sub>5GS3GPPNSC</sub>	CR4	A.2/1 OR A.2/2

**Optional step if CR 4, CR 5 and CR 6 verification cannot be performed at step 9) and 12)**

13	TT	READ EF <sub>5GS3GPPNSC</sub> and EF <sub>5GAUTHKEYS</sub>	The TT or the test operator shall perform whatever action is needed to get read access to EF <sub>5GS3GPPNSC</sub> and EF <sub>5GAUTHKEYS</sub>	CR 4 CR 5 CR 6	A.2/3
----	----	--	---	----------------------	-------

### 15.1.1.5 Acceptance criteria

CR 1 is verified if CR 2 is met, and the ME forwards the RAND and AUTN received in EAP-Request/AKA'-Challenge message to the USIM.

CR 3 requirements are met if the NG-SS receives an EAP message IE with EAP-response/AKA'-challenge in the AUTHENTICATION RESPONSE message sent in response to the AUTHENTICATION REQUEST in step 6).

CR 4 can be verified in step 12) or 13) after the state 5GMM-DEREGISTERED is entered and if an appropriate method to monitor the APDU for EF update or read the EF content is provided by the UE manufacturer.

CR 5 can be verified in step 12) or 13) if an appropriate method to monitor the APDU for EF update or read the EF content is provided by the UE manufacturer.

CR 6 can be verified in step 9) or 13) if an appropriate method to monitor the APDU for EF update or read the EF content is provided by the UE manufacturer.

CR 7 is verified if the UE is capable to register to the NG-SS at step 11).

The EF contents to be verified at step 9), 12) and/or 13) for CR 5 and 6 are listed as below:

**EF<sub>5GAUTHKEYS</sub>** (5G authentication keys)

Logically:

K<sub>AUSF</sub>: 32 bytes, value not checked

K<sub>SEAF</sub>: 32 bytes, value not checked

Coding:

Byte	B1	B2	B3	Bx	Bx+1	Bx+2	Bx+3	...	Bxx
Hex	80	L1	Xx	..	81	L2	xx	...	xx

**EF<sub>5GS3GPPNSC</sub>** (5GS 3GPP Access NAS Security Context)

Logically:

5GS NAS Security Context:

ngKSI: 00

K<sub>AMF</sub>: 32 bytes, value not checked

Uplink NAS count: any value

Downlink NAS count: any value

Identifiers of selected NAS integrity  
and encryption algorithms: any value

Identifiers of selected EPS NAS  
integrity and encryption algorithms  
for use after mobility to EPS: any value

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	Bx
Hex	A0	XX	80	01	00	81	xx	xx	...	xx

### 15.1.1.5 Acceptance criteria

CR 1 is verified if CR 2 is met, and the ME forwards the RAND and AUTN received in EAP-Request/AKA'-Challenge message to the USIM.

CR 3 requirements are met if the NG-SS receives an EAP message IE with EAP-response/AKA'-challenge in the AUTHENTICATION RESPONSE message sent in response to the AUTHENTICATION REQUEST in step 6).

CR 4 can be verified in step 12) after the state 5GMM-DEREGISTERED is entered and if an appropriate method to read the EF content is provided by the UE manufacturer.

CR 5 and CR 6 can be verified in step 13) if an appropriate method to read the EF content is provided by the UE manufacturer.

CR 7 is verified if the UE is capable to register to the NG-SS at step 11).

## 15.1A.1 Authentication procedure for EAP-AKA' - Authentication is successful

### 15.1A.1.1 Definition and applicability

The purpose of the primary authentication and key agreement procedure is to enable mutual authentication between the UE and the network and to provide keying material that can be used between the UE and network in subsequent security procedures. The UE and the AMF shall support the EAP based primary authentication and key agreement procedure.

In order to initiate the EAP based primary authentication and key agreement procedure using EAP-AKA', the AUSF shall send an EAP message IE with EAP-request/AKA'-challenge message in the AUTHENTICATION REQUEST message.

The 5G NAS security context parameters from a full native 5G NAS security context shall be stored on the USIM if the corresponding file is present on the USIM as specified in TS 31.102 [19]. If the corresponding file is not present on the USIM, this 5GMM parameters is stored in a non-volatile memory in the ME together with the SUPI from the USIM.

The EF<sub>5GS3GPPNSC</sub> contains the 5GS 3GPP access NAS security context as defined in TS 24.501 [25], consisting of K<sub>AMF</sub> with the associated key set identifier, the UE security capabilities, and the uplink and downlink NAS COUNT values. This file shall contain one record.

The EF<sub>5GSAUTHKEYS</sub> contains K<sub>AUSF</sub> and K<sub>SEAF</sub> that are generated on the ME using CK and IK as part of AKA procedures as described in TS 33.501 [24]. If service n°133 is "available" in EF<sub>UST</sub>, the EF<sub>5GSAUTHKEYS</sub> also contains SOR counter and UE parameter update counter associated with the key K<sub>AUSF</sub> as described in TS 33.501 [24] and TS 31.102 [19].

### 15.1A.1.2 Conformance requirement

CR 1 The UE shall support the EAP based primary authentication and key agreement procedure.

CR 2 The ME shall forward the RAND and AUTN received in EAP message IE with EAP-request/AKA'-challenge within the AUTHENTICATION REQUEST message to the USIM.

CR 3 The ME shall return the EAP message IE with EAP-response/AKA'-challenge in AUTHENTICATION RESPONSE message.

CR 4 As a result of successful authentication procedure and upon receipt of the EAP-Success message, the 5G NAS security context parameters shall be stored on the USIM if the corresponding file is present on the USIM when entering state 5GMM-DEREGISTERED.

CR 5 If service n°122 is available, the ME shall store K<sub>AMF</sub> with the associated key set identifier, the UE security capabilities, and the uplink and downlink NAS COUNT values in EF<sub>5GS3GPPNSC</sub> on the USIM.

CR 6 If service n°123 is available, and service n°133 is available the ME shall store the K<sub>AUSF</sub>, K<sub>SEAF</sub>, SOR counter and UE parameter update counter in the EF<sub>5GSAUTHKEYS</sub> on the USIM.

CR 7 The UE can successfully register to the network.

Reference:

- TS 31.102 [19], clauses 4.4.11.3, 4.4.11.4 and 4.4.11.6;
- TS 33.501 [24], clause 6.1.3.1;
- TS 24.501 [25], clause 5.4.1.2 and Annex C.

### 15.1A.1.3 Test purpose

The purpose of this test is to verify that:

- 1) the ME forwards the RAND and AUTN received in EAP-request/AKA'-challenge within EAP message IE to the USIM.
- 2) the ME returns the EAP message IE with EAP-response/AKA'-challenge in AUTHENTICATION RESPONSE message indicating the response calculated in the USIM (RES).
- 3) the ME stores 5G NAS security context parameters, consisting of  $K_{AMF}$  with the associated key set identifier in  $EF_{5GS3GPPNSC}$  on the USIM if service n°122 is "available".
- 4) the ME stores the  $K_{AUSF}$ ,  $K_{SEAF}$ , SOR counter and UE parameter update in the  $EF_{5GAUTHKEYS}$  on the USIM if services n°123 and n°133 are available.
- 5) the UE can successfully register to the network.

### 15.1A.1.4 Method of test

#### 15.1A.1.4.1 Initial conditions

The values of the 5G-NR UICC – support of Rel-16 features as defined in clause 4.5.11 of the present document are used.

The TT (NG-SS) is configured to transmit on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/083/000001
- Access control: unrestricted.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case.

#### 15.1A.1.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	TT	Activate NG-SS cell	The NG-SS cell on the TT is activated with SIB1 as defined in the initial conditions		
2	UE	Run initial activation			
3	UE <> TT	Establish RRC connection	UE camps on NG-SS cell and establishes RRC connection		
4	UE > TT	Send REGISTRATION REQUEST			
5	TT > UE	Send AUTHENTICATION REQUEST	The TT sends an AUTHENTICATION REQUEST message with EAP message IE with EAP request/AKA' challenge message with: <ul style="list-style-type: none"> <li>- ngKSI: <ul style="list-style-type: none"> <li>- NAS key set identifier: '000'</li> <li>- TSC: '0'</li> </ul> </li> <li>- EAP message: <ul style="list-style-type: none"> <li>- EAP-request/AKA'-challenge</li> </ul> </li> </ul> The NG-SS on the TT generates $K_{AMF}$ , $K_{AUSF}$ and $K_{SEAF}$ values, and initiates the EAP-AKA' authentication procedure		

6	ME > USIM	Pass RAND and AUTN values to the USIM	The ME provides the EAP request/AKA' challenge data received in the AUTHENTICATION REQUEST to the USIM	CR 1 CR 2	A.2/1 OR A.2/2
7	UE > TT	Send AUTHENTICATION RESPONSE	The UE sends an AUTHENTICATION RESPONSE message with EAP message IE with EAP response/AKA' challenge message: - Authentication response parameter: message identity: '0101 0111' 4 – 16 octets RES value calculated according to TS 24.501 [25] The UE shall return RES equal to the XRES calculated at the NG-SS with the parameters provided/indicated in the AUTHENTICATION REQUEST at step 4	CR 3	
8	TT > UE	Sends SECURITY MODE COMMAND message with EAP-success	The NG-SS sends a SECURITY MODE COMMAND message with EAP-success		
9	UE > TT	Send SECURITY MODE COMPLETE	UE updates EF <sub>5GAUTHKEYS</sub> in parallel or after the NAS message	CR 6	A.2/1 OR A.2/2
10	TT > UE	Send REGISTRATION ACCEPT	NG-SS sends a REGISTRATION ACCEPT message with: - 5G-GUTI: 24408300010266436587 - TAI: 244/83/000001		
11	UE > TT	UE sends REGISTRATION COMPLETE		CR 7	
12	UE	The UE is powered off and/or deactivated, performs the DEREGISTRATION procedure.	UE enters the 5GMM-DEREGISTERED state and updates EF <sub>5GS3GPPNSC</sub>	CR 4	A.2/1 OR A.2/2
<b>Optional step if CR 4, CR 5 and CR 6 verification cannot be performed at step 9) and 12)</b>					
13	TT	READ EF <sub>5GS3GPPNSC</sub> and EF <sub>5GAUTHKEYS</sub>	The TT or the test operator shall perform whatever action is needed to get read access to EF <sub>5GS3GPPNSC</sub> and EF <sub>5GAUTHKEYS</sub>	CR 4 CR 5 CR 6	A.2/3

### 15.1A.1.5 Acceptance criteria

CR 1 is verified if CR 2 is met, and the ME forwards the RAND and AUTN received in EAP-Request/AKA'-Challenge message to the USIM.

CR 3 requirements are met if the NG-SS receives an EAP message IE with EAP-response/AKA'-challenge in the AUTHENTICATION RESPONSE message sent in response to the AUTHENTICATION REQUEST in step 6).

CR 4 can be verified in step 12) or 13) after the state 5GMM-DEREGISTERED is entered and if an appropriate method to monitor the APDU for EF update or read the EF content is provided by the UE manufacturer.

CR 5 can be verified in step 12) or 13) if an appropriate method to monitor the APDU for EF update or read the EF content is provided by the UE manufacturer.

CR 6 can be verified in step 9) or 13) if an appropriate method to monitor the APDU for EF update or read the EF content is provided by the UE manufacturer.

CR 7 is verified if the UE is capable to register to the NG-SS at step 11).

The EF contents to be verified at step 9), 12) and/or 13) for CR 5 and 6 are listed as below:

**EF<sub>5GAUTHKEYS</sub>** (5G authentication keys)

Logically:

K<sub>AUSF</sub>: 32 bytes, value not checked

K<sub>SEAF</sub>: 32 bytes, value not checked

K<sub>SEAF</sub> for non-3GPP access: 32 bytes, length and value not checked

SOR counter: 2 bytes, value not checked

UE parameter update counter: 2 bytes, value not checked

Coding:

Byte	B1	B2	B3	Bx	Bx+1	Bx+2	Bx+3	...	By
Hex	80	L1	xx	..	81	L2	xx	...	xx
	<b>By+1</b>	<b>By+2</b>	<b>By+3</b>	<b>Bz</b>	<b>Bz+1</b>	<b>Bz+2</b>	<b>Bz+3</b>	..	<b>Bi+1</b>
	82	L3	xx	..	83	L4	xx	..	84
	<b>Bi+2</b>	<b>Bi+3</b>	<b>Bj</b>	<b>Bxx</b>					
	L5	xx	..	xx					

**EF**<sub>5GS3GPPNSC</sub> (5GS 3GPP Access NAS Security Context)

Logically:

5GS NAS Security Context:

ngKSI: 00

$K_{AMF}$ : 32 bytes, value not checked

Uplink NAS count: any value

Downlink NAS count: any value

Identifiers of selected NAS integrity  
and encryption algorithms: any value

Identifiers of selected EPS NAS  
integrity and encryption algorithms  
for use after mobility to EPS: any value

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	Bx
Hex	A0	xx	80	01	00	81	xx	xx	...	xx

## 15.1.2 Authentication procedure for EAP-AKA' – Authentication is successful - GSM UICC

### 15.1.2.1 Definition and applicability

The purpose of the primary authentication and key agreement procedure is to enable mutual authentication between the UE and the network and to provide keying material that can be used between the UE and network in subsequent security procedures. The UE and the AMF shall support the EAP based primary authentication and key agreement procedure.

The 5G NAS security context parameters from a full native 5G NAS security context shall be stored on the USIM if the corresponding file is present on the USIM as specified in TS 31.102 [19]. If the corresponding file is not present on the USIM, this 5GMM parameters is stored in a non-volatile memory in the ME together with the SUPI from the USIM.

During the authentication procedure if the USIM computes a  $K_c$  (i.e. GPRS  $K_c$ ) from CK and IK using conversion function c3 as described in TS 33.102 [53], and sends it to the ME, then the ME shall ignore such GPRS  $K_c$  and not store the GPRS  $K_c$  on USIM or in ME.

### 15.1.2.2 Conformance requirement

- CR 1 The ME shall ignore the GPRS  $K_c$  and not store the GPRS  $K_c$  on USIM if the USIM computes a  $K_c$  (i.e. GPRS  $K_c$ ) from CK and IK using conversion function c3 as described in TS 33.102 [53].
- CR 2 The ME shall ignore the GPRS  $K_c$  and not store the GPRS  $K_c$  in ME if the USIM computes a  $K_c$  (i.e. GPRS  $K_c$ ) from CK and IK using conversion function c3 as described in TS 33.102 [53].

CR 3 If Service n°122 and Service n°123 are not available on the USIM, the 5GS 3GPP access NAS security context parameters and the 5G authentication keys shall be stored in the non-volatile memory of the ME.

Reference:

- TS 33.501 [24], clause 6.1.3.1;
- TS 24.501 [25], clause 5.4.1.2 and Annex C.

### 15.1.2.3 Test purpose

The purpose of this test is to verify that:

- 1) the ME will ignore the GPRS Kc and will not store the GPRS Kc on USIM or in ME when the USIM computes a Kc (i.e. GPRS Kc) from CK and IK.
- 2) the ME stores the 5GS 3GPP access NAS security context parameters and the 5G authentication keys inside the ME non-volatile memory when Service n°122 and Service n°123 are not available on the USIM.

### 15.1.2.4 Method of test

#### 15.1.2.4.1 Initial conditions

The values of the 5G-NR UICC as defined in clause 4.5.9 of the present document are used.

The TT (NG-SS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC):244/083/000001.
- Access control: unrestricted.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case.

#### 15.1.2.4.2 Procedure

Step	Direction	Action	Comment	REQ	SA
1	TT UE	NG-SS Cell is powered up Run initial activation	The NG-SS on the TT is activated		
2	UE<>TT	UE camps on NG-SS Cell and establishes RRC connection			
3	UE > TT	UE sends REGISTRATION REQUEST			
4	TT > UE	NG-SS sends REGISTRATION REJECT (cause: #13 Roaming not allowed in this tracking area) and release RRC connection	UE shall delete 5G-GUTI, last visited registered TAI, TAI list and ngKSI.		
5	UE	The UE is powered off and then on again			
6	UE<>TT	UE camps on NG-SS Cell and establishes RRC connection			
7	UE > TT	UE sends REGISTRATION REQUEST message with: - ngKSI: - NAS key set identifier: '111'	UE shall indicate in the REGISTRATION REQUEST that no key is available for the NAS key set identifier		
8	TT > UE	NG-SS sends AUTHENTICATION REQUEST with EAP message IE with EAP request/AKA' challenge message with: - ngKSI: - NAS key set identifier: '000' - TSC: '0' - EAP message: - EAP-request/AKA'-challenge	The NG-SS on the TT generates K <sub>AMF</sub> , K <sub>AUSF</sub> and K <sub>SEAF</sub> values, and initiates the EAP-AKA' authentication procedure		
9	UE	ME passes the RAND and AUTN values to the USIM	The ME provides the EAP request/AKA' challenge data received in the AUTHENTICATION REQUEST to the USIM; the USIM calculates the response		

			parameter K <sub>c</sub> (i.e. GPRS K <sub>c</sub> ) from CK and IK using conversion function c3		
10	UE > TT	UE sends AUTHENTICATION RESPONSE message with EAP message IE with EAP response/AKA' challenge message: - Authentication response parameter: 16 octets RES value calculated according to TS 24.501 [25]	ME does not store GPRS K <sub>c</sub> on the USIM through step 10 to 15	CR 1	
11	TT > UE	NG-SS sends SECURITY MODE COMMAND message with EAP-success			
12	UE > TT	UE send SECURITY MODE COMPLETE			
13	TT > UE	NG-SS sends REGISTRATION ACCEPT message with: - 5G-GUTI: 24408300010266436587 - TAI: 42 34 80 00 00 01			
14	UE > TT	UE sends REGISTRATION COMPLETE			
15	UE	The UE is powered off and/or deactivated, performs the DEREGISTRATION procedure			
16	UE	Run initial activation and/or activated			
17	UE<>TT	UE camps on NG-SS Cell and establishes RRC connection			
18	UE > TT	UE sends REGISTRATION REQUEST message that is Security protected (indicated by Security header) with - ngKSI: - NAS key set identifier: '000' - TSC: '0' - 5GS mobile identity: 5G-GUTI type with value 24408300010266436587		CR 1 CR 2 CR 3	
19	TT > UE	NG-SS sends REGISTRATION ACCEPT			
20	UE > TT	UE sends REGISTRATION COMPLETE			

### 15.1.2.5 Acceptance criteria

CR 1, CR 2 and CR 3 can be implicitly verified in step 18 when UE sends REGISTRATION REQUEST message that is Security protected and includes ngKSI and 5G-GUTI type 5GS mobile identity as specified in the test procedure.

Optionally, CR1 can be explicitly verified with methods A.2/1 or A.2/2 that ME does not store GPRS K<sub>c</sub> on the USIM through steps 10 to 15.

## 15.1.3 Authentication procedure for EAP-AKA' – AUTN fails on the USIM

### 15.1.3.1 Definition and applicability

The purpose of the primary authentication and key agreement procedure is to enable mutual authentication between the UE and the network and to provide keying material that can be used between the UE and network in subsequent security procedures. The UE and the AMF shall support the EAP based primary authentication and key agreement procedure.

At receipt of the RAND and AUTN, the USIM shall verify the freshness of the AV' by checking whether AUTN can be accepted as described in TS 33.102 [53]. If so, the USIM computes a response RES. The USIM shall return RES, CK, IK to the ME. The ME shall derive CK' and IK'. If the verification of the AUTN fails on the USIM, then the USIM and ME shall proceed as described in clause 6.1.3.3 in TS 33.501 [24].

When 5G AKA is used or when EAP-AKA' is used, at the receipt of the RAND and AUTN, if the verification of the AUTN fails, then the USIM indicates to the ME the reason for failure and in the case of a synchronisation failure passes the AUTS parameter (see TS 33.102 [53]) to the ME.

If EAP-AKA' is used: The ME shall send the EAP-Response/AKA-Synchronization-Failure include the AT\_AUTS attribute (RFC 4187 [54]).

### 15.1.3.2 Conformance requirement

CR 1 The ME shall forward the RAND and AUTN received in the EAP message IE with EAP-request/AKA'-challenge in the AUTHENTICATION REQUEST message to the USIM.

CR 2 If the verification of the AUTN fails on the USIM, then ME shall send AUTHENTICATION FAILURE indicates EAP-Response/AKA-Synchronization-Failure and includes the AUTS from USIM.

CR 3 If the verification of the AUTN success, the UE shall send AUTHENTICATION RESPONSE message contains the response calculated in the USIM (RES)

Reference:

- TS 33.501 [24], clause 6.1.3.1 and 6.1.3.3;
- TS 24.501 [25], clauses 5.4.1.2.2.1.
- RFC 4187 [54], clause 9.6.

### 15.1.3.3 Test purpose

1) To verify that the ME forwards the RAND and AUTN received in EAP-request/AKA'-challenge message to the USIM.

2) To verify that the ME returns the EAP-Response/AKA-Synchronization-Failure if the verification of AUTN failed on the USIM due to a synchronisation failure.

### 15.1.3.4 Method of test

#### 15.1.3.4.1 Initial conditions

The NG-SS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC):244/083/000001.
- Access control: unrestricted.

The default 5G-NR UICC is used and installed into the ME and the UE runs an initial activation.

#### 15.1.3.4.2 Procedure

Step	Direction	Action	Comment	REQ	SA
1	TT	NG-SS Cell is powered up	The NG-SS on the TT is activated		
2	UE<>TT	UE camps on NG-SS Cell and establishes RRC connection			
3	UE > TT	UE sends REGISTRATION REQUEST			
4	TT > UE	NG-SS sends AUTHENTICATION REQUEST with EAP message IE with EAP request/AKA' challenge message with: - ngKSI: - NAS key set identifier: '000' - TSC: '0' - Authentication parameter AUTN: '1111 1111 1111 1111' - EAP message: - EAP-request/AKA'-challenge	AUTHENTICATION REQUEST with the AMF field in the IE "Authentication parameter AUTN" set to "AMF <sub>RESYNCH</sub> " value to trigger SQN re-synchronisation procedure in the USIM (see TS 34.108 [5], 8.1.2.2)		
5	UE	ME passes the RAND and AUTN values to the USIM	The ME provides the EAP request/AKA' challenge data received in the AUTHENTICATION REQUEST at step 4 to the USIM	CR1	A.2/1 OR A.2/2
6	UE	The UICC returns AUTS parameter to the ME indicating that the verification of AUTN failed due to a synchronisation failure			

7	UE > TT	UE sends AUTHENTICATION FAILURE message with: - 5GMM cause: '0001 0101' - Authentication failure parameter: AUTS value calculated according to TS 34.108, 8.1.2.2 [5]	AUTHENTICATION RESPONSE message including the EAP-response/AKA'-synchronization-failure message, with AUTS from USIM	CR2	
8	TT > UE	NG-SS sends AUTHENTICATION REQUEST with EAP message IE with EAP request/AKA' challenge message with: - ngKSI: - NAS key set identifier: '000' - TSC: '0' - EAP message: - EAP-request/AKA'-challenge			
9	UE	ME passes the RAND and AUTN values to the USIM	The ME provides the EAP request/AKA' challenge data received in the AUTHENTICATION REQUEST at step 8 to the USIM	CR1	A.2/1 OR A.2/2
10	UE > TT	UE sends AUTHENTICATION RESPONSE message with EAP message IE with EAP response/AKA' challenge message: - Authentication response parameter: 4 - 16 octets RES value calculated according to TS 24.501 [25]	The UE shall return RES equal to the XRES calculated at the NG-SS with the parameters provided/indicated in the AUTHENTICATION REQUEST at step 8	CR3	
11	TT > UE	NG-SS sends SECURITY MODE COMMAND message with EAP-success			
12	UE > TT	UE send SECURITY MODE COMPLETE			
13	TT > UE	NG-SS sends REGISTRATION ACCEPT message with: - 5G-GUTI: 24408300010266436587 - TAI: 42 34 80 00 00 01			
14	UE > TT	UE sends REGISTRATION COMPLETE			

### 15.1.3.5 Acceptance criteria

CR 1 can be verified at step 5 and 9.

CR 2 can be verified at step 7 with AUTS value verified according to TS 34.108, 8.1.2.2.

CR 3 can be verified at step 10.

## 15.1.4 Authentication procedure for EAP-AKA' - after SUPI is changed

### 15.1.4.1 Definition and applicability

The purpose of the primary authentication and key agreement procedure is to enable mutual authentication between the UE and the network and to provide keying material that can be used between the UE and network in subsequent security procedures. The UE and the AMF shall support the EAP based primary authentication and key agreement procedure.

The 5G NAS security context parameters from a full native 5G NAS security context shall be stored on the USIM if the corresponding file is present on the USIM as specified in TS 31.102 [19]. If the corresponding file is not present on the USIM, this 5GMM parameters is stored in a non-volatile memory in the ME together with the SUPI from the USIM. These 5GMM parameters can only be used if the SUPI from the USIM matches the SUPI stored in the non-volatile memory; else the UE shall delete the 5GMM parameters.

### 15.1.4.2 Conformance requirement

CR 1 The UE shall support the EAP based primary authentication and key agreement procedure.

CR 2 The 5G NAS security context parameters shall be stored on the USIM or in a non-volatile memory in the ME together with the SUPI from the USIM.

CR 3 The UE shall delete the 5GMM parameters if the SUPI from the USIM does not match the SUPI stored in the non-volatile memory.

Reference:

- TS 33.501 [24], clause 6.1.3.1;
- TS 24.501 [25], clauses 5.4.1.2 and Annex C.

### 15.1.4.3 Test purpose

- 1) To verify that the UE generates the 5G NAS security context parameters and stores them inside the non-volatile memory in the ME together with the SUPI from the USIM.
- 2) To verify that the UE rejects the SECURITY MODE COMMAND with the existing 5G NAS security context parameters if the SUPI is changed.

### 15.1.4.4 Method of test

#### 15.1.4.4.1 Initial conditions

The values of the 5G-NR UICC as defined in clause 4.5.9 of the present document are used with the following exception:

**EF<sub>UST</sub>** (USIM Service Table)

Services defined in Releases higher than Rel-15 might be available.

Logically:

Service n°122:	5GS Mobility Management Information	not available
Service n°123:	5G Security Parameters	not available

Coding:

Byte:	B1	B2	B3	B4	B5	B6	B7	B8
Binary:	xxxx xx1x	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxx1 xx1x	xxxx xxxx	xxxx xxxx
	<b>B9</b>	<b>B10</b>	<b>B11</b>	...	<b>B16</b>	<b>B17</b>		
	xxxx xxxx	xxxx xxxx	xx11 xxxx	...	xxx0 100x	xxxx xxxx		

The TT (NG-SS) transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/083/000001.
- Access control: unrestricted.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case.

#### 15.1.4.4.2 Procedure

Step	Direction	Action	Comment	REQ	SA
1	TT	NG-SS Cell is powered up	The NG-SS on the TT is activated		
	UE	Run initial activation with IMSI set as 246081685533963			
2	UE<>TT	UE camps on NG-SS Cell and establishes RRC connection			
3	UE > TT	UE sends REGISTRATION REQUEST			
4	TT > UE	NG-SS sends REGISTRATION REJECT (cause: #13 Roaming not allowed in this	UE shall delete 5G-GUTI, last visited registered TAI, TAI list and ngKSI.		

		tracking area) and release RRC connection			
5	UE TT	The UE is powered off NG-SS Cell is powered off			
6	UE TT	Run an UE activation with default IMSI NG-SS Cell is powered on			
7	UE<>TT	UE camps on NG-SS Cell and establishes RRC connection			
8	UE > TT	UE sends REGISTRATION REQUEST message with: - ngKSI: - NAS key set identifier: '111' - 5GS mobile identity: SUCI of the UE	UE shall indicate in the REGISTRATION REQUEST that no key is available for the NAS key set identifier		
9	TT > UE	NG-SS sends AUTHENTICATION REQUEST with EAP message IE with EAP request/AKA' challenge message with: - ngKSI: - NAS key set identifier: '000' - TSC: '0' - EAP message: - EAP-request/AKA'-challenge	The NG-SS on the TT generates $K_{AMF}$ , $K_{AUSF}$ and $K_{SEAF}$ values, and initiates the EAP-AKA' authentication procedure		
10	UE > TT	UE sends AUTHENTICATION RESPONSE message with EAP message IE with EAP response/AKA' challenge message: - Authentication response parameter: 16 octets RES value calculated according to TS 24.501 [25]	The UE shall return RES equal to the XRES calculated at the NG-SS with the parameters provided/indicated in the AUTHENTICATION REQUEST at step 9		
11	TT > UE	NG-SS sends SECURITY MODE COMMAND message with EAP-success			
12	UE > TT	UE send SECURITY MODE COMPLETE			
13	TT > UE	NG-SS sends REGISTRATION ACCEPT message with: - 5G-GUTI: 24408300010266436587 - TAI: 42 34 80 00 00 01			
14	UE > TT	UE sends REGISTRATION COMPLETE		CR 1	
15	UE <> TT	The UE is powered off and, performs the DEREGISTRATION procedure			
16	TT	NG-SS Cell is powered off			
17	UE TT	Run initial activation, with IMSI set as 246081685533963 NG-SS Cell is powered on			
18	UE<>TT	UE camps on NG-SS Cell and establishes RRC connection			
19	UE > TT	UE sends REGISTRATION REQUEST message with: - ngKSI: - NAS key set identifier: '111' - 5GS mobile identity: SUCI of the UE	UE shall indicate within the REGISTRATION REQUEST for the NAS key set identifier that no key is available, and use SUCI as 5GS mobile identity IE	CR 3	
20	TT > UE	NG-SS sends AUTHENTICATION REQUEST with EAP message IE with EAP request/AKA' challenge message with: - ngKSI: - NAS key set identifier: '000' - TSC: '0' - EAP message: - EAP-request/AKA'-challenge			
21	UE > TT	UE sends AUTHENTICATION RESPONSE message with EAP message IE with EAP response/AKA' challenge message: - Authentication response parameter: 16 octets RES value calculated according to TS 24.501 [25]	The UE shall return RES equal to the XRES calculated at the NG-SS with the parameters provided/indicated in the AUTHENTICATION REQUEST at step 20		

22	TT > UE	NG-SS sends SECURITY MODE COMMAND with: - ngKSI: The ngKSI of the partial native 5G security context assigned in the SECURITY MODE COMMAND message sent in step 11			
23	UE > TT	UE send SECURITY MODE REJECT with - 5GMM cause: '0001 1000'	Cause #24 - Security mode rejected, unspecified	CR 2	
24	UE	The UE is powered off			

#### 15.1.4.5 Acceptance criteria

CR 1 can be verified at step 14.

CR 3 can be implicitly verified at step 19 where REGISTRATION REQUEST includes NAS key set identifier that no key is available and use SUCI as 5GS mobile identity IE.

CR 2 can be verified at step 24.

## 15.2 Authentication procedure for 5G AKA

### 15.2.1 Authentication procedure for 5G AKA - Authentication is successful

#### 15.2.1.1 Definition and applicability

The purpose of the 5G AKA based primary authentication and key agreement procedure is to provide mutual authentication between the UE and the network and to agree on the keys  $K_{AUSF}$ ,  $K_{SEAF}$  and  $K_{AMF}$ . The UE and the AMF shall support the 5G AKA based primary authentication and key agreement procedure.

The 5G NAS security context parameters from a full native 5G NAS security context shall be stored on the USIM if the corresponding file is present on the USIM as specified in TS 31.102 [19]. If the corresponding file is not present on the USIM, this 5GMM parameters is stored in a non-volatile memory in the ME together with the SUPI from the USIM.

The  $EF_{5GS3GPPNSC}$  contains the 5GS 3GPP access NAS security context as defined in TS 24.501 [25], consisting of  $K_{AMF}$  with the associated key set identifier, the UE security capabilities, and the uplink and downlink NAS COUNT values. This file shall contain one record.

The  $EF_{5GAUTHKEYS}$  contains  $K_{AUSF}$  and  $K_{SEAF}$  that are generated on the ME using CK and IK as part of AKA procedures as described in TS 33.501[24]

#### 15.2.1.2 Conformance requirement

CR 1 The UE shall support the 5G AKA based primary authentication and key agreement procedure.

CR 2 The ME shall forward the RAND and AUTN received in AUTHENTICATION REQUEST message to the USIM.

CR 3 The ME shall compute RES\* from RES according to Annex A.4 TS 33.501[24] and return it in AUTHENTICATION RESPONSE message.

CR 4 If service n°122 is "available", when entering state 5GMM-DEREGISTERED, the ME shall store the  $K_{AMF}$  with the associated key set identifier, the UE security capabilities, and the uplink and downlink NAS COUNT values in  $EF_{5GS3GPPNSC}$  on the USIM.

CR 5 If service n°123 is "available", the ME shall store the  $K_{AUSF}$  and  $K_{SEAF}$  in  $EF_{5GAUTHKEYS}$  on the USIM.

CR 6 The UE can successfully register to the network.

Reference:

- TS 31.102 [19], clauses 4.4.11.3, 4.4.11.4 and 4.4.11.6;
- TS 33.501 [24], clause 6.1.3.2;
- TS 24.501 [25], clause 5.4.1.3 and Annex C.

### 15.2.1.3 Test purpose

The purpose of this test is to verify that: 1) the ME forwards the RAND and AUTN received in 5G authentication challenge data within AUTHENTICATION REQUEST message to the USIM.

- 2) the ME sends AUTHENTICATION RESPONSE message contains the calculated RES\* in response to AUTHENTICATION REQUEST message.
- 3) the ME stores 5G NAS security context parameters when entering state 5GMM-DEREGISTERED, consisting of K<sub>AMF</sub> with the associated key set identifier in EF<sub>5GS3GPPNSC</sub> on the USIM if service n°122 is "available".
- 4) the ME stores the K<sub>AUSF</sub> and K<sub>SEAF</sub> in EF<sub>5GAUTHKEYS</sub> on the USIM if service n°123 is "available".

### 15.2.1.4 Method of test

#### 15.2.1.4.1 Initial conditions

The NG-SS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC):244/083/000001.
- Access control: unrestricted.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case.

#### 15.2.1.4.2 Procedure

Step	Direction	Action	Comment	REQ	SA
1	TT	NG-SS Cell is powered up with SIB1 as defined in the initial conditions	The NG-SS on the TT is activated		
	UE	Run initial activation			
2	UE<>TT	UE camps on NG-SS Cell and establishes RRC connection			
3	UE > TT	UE sends REGISTRATION REQUEST			
4	TT > UE	NG-SS sends AUTHENTICATION REQUEST with 5G AKA-Challenge message: - ngKSI: - NAS key set identifier: '000' - TSC: '0' - Authentication parameter RAND (5G authentication challenge): 128 bits value - Authentication parameter AUTN (5G Authentication challenge). 128 bits value	The NG-SS on the TT generates K <sub>AMF</sub> , K <sub>AUSF</sub> and K <sub>SEAF</sub> values, and initiates the 5G AKA authentication procedure		
5	UE	ME passes the RAND and AUTN values to the USIM	The ME provides the authentication challenge data received in the AUTHENTICATION REQUEST to the USIM	CR 1 CR 2	A.2/1 OR A.2/2
6	UE > TT	UE sends AUTHENTICATION RESPONSE message with: - Authentication response parameter: 16 octets RES* value calculated according to TS 24.501 [25]	The UE shall return RES* equal to the XRES* calculated at the NG-SS with the parameters provided/indicated in the AUTHENTICATION REQUEST	CR 3	
7	TT > UE	NG-SS sends SECURITY MODE COMMAND message including the ngKSI of the new 5G NAS security context (as provided in step 4)			

8	UE > TT	UE send SECURITY MODE COMPLETE integrity protected and ciphered with the new 5G NAS security context identified by the ngKSI received in the SECURITY MODE COMMAND message in step 7	UE updates EF <sub>5GAUTHKEYS</sub> in parallel or after the NAS message	CR 5	A.2/1 OR A.2/2 OR A.2/3
9	TT > UE	NG-SS sends REGISTRATION ACCEPT message with: - 5G-GUTI: 24408300010266436587 - TAI: 42 34 80 00 00 01			
10	UE > TT	UE sends REGISTRATION COMPLETE		CR 6	
11	UE <> TT	The UE is powered off and/or deactivated, performs the DEREGISTRATION procedure	UE enters the 5GMM-DEREGISTERED during this step, and updates EF <sub>5GS3GPPNSC</sub>	CR 4	A.2/1 OR A.2/2 OR A.2/3
12	TT	Read EF <sub>5GS3GPPNSC</sub> and EF <sub>5GAUTHKEYS</sub>	Optional step if CR4 and CR5 verification cannot be performed at step 8 and 11: The TT or the test operator perform whatever action is needed to get read access to EF <sub>5GS3GPPNSC</sub> and EF <sub>5GAUTHKEYS</sub>	CR 4 CR 5	A.2/3

15.2.1.5 Acceptance criteria

CR 1 is verified if CR 2 is met, and the ME forwards the RAND and AUTN received in received in the AUTHENTICATION REQUEST to the USIM.

CR 3 requirements are met if the NG-SS receives RES\* in the AUTHENTICATION RESPONSE message sent in response to the AUTHENTICATION REQUEST in step 6.

CR 4 can be verified in step 11 or 12 if an appropriate method to monitor the APDU for EF update or read the EF content is provided by the UE manufacturer.

CR 5 can be verified in step 8) or 12) if an appropriate method to monitor the APDU for EF update or read the EF content is provided by the UE manufacturer.

CR 6 is verified if the UE is capable to register to the NG-SS at step 13).

The EF contents to be verified at step 8), 11) and/or 12) for CR 4 and CR 5 are listed as below:

**EF<sub>5GAUTHKEYS</sub>** (5G authentication keys)

Logically:

K<sub>AUSF</sub>: value not checked

K<sub>SEAF</sub>: value not checked

Coding:

Byte	B1	B2	B3	Bx	Bx+1	Bx+2	Bx+3	..	Bxx
Hex	80	L1	xx	..	81	L2	xx	..	xx

7) After step 11) the ME updates EF<sub>5GS3GPPNSC</sub> as shown below.

**EF<sub>5GS3GPPNSC</sub>** (5GS 3GPP Access NAS Security Context)

Logically:

5GS NAS Security Context:

ngKSI: 00

K<sub>AMF</sub>: value not checked

Uplink NAS count: any value

Downlink NAS count: any value

Identifiers of selected NAS integrity  
and encryption algorithms: any value

Identifiers of selected EPS NAS  
integrity and encryption algorithms  
for use after mobility to EPS: any value

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	Bx
Hex	A0	xx	80	01	00	81	xx	xx	...	xx

## 15.2A.1 Authentication procedure for 5G AKA - Authentication is successful

### 15.2A.1.1 Definition and applicability

The purpose of the 5G AKA based primary authentication and key agreement procedure is to provide mutual authentication between the UE and the network and to agree on the keys  $K_{AUSF}$ ,  $K_{SEAF}$  and  $K_{AMF}$ . The UE and the AMF shall support the 5G AKA based primary authentication and key agreement procedure.

The 5G NAS security context parameters from a full native 5G NAS security context shall be stored on the USIM if the corresponding file is present on the USIM as specified in TS 31.102 [19]. If the corresponding file is not present on the USIM, this 5GMM parameters is stored in a non-volatile memory in the ME together with the SUPI from the USIM.

The  $EF_{5GS3GPPNSC}$  contains the 5GS 3GPP access NAS security context as defined in TS 24.501 [25], consisting of  $K_{AMF}$  with the associated key set identifier, the UE security capabilities, and the uplink and downlink NAS COUNT values. This file shall contain one record.

The  $EF_{5GAUTHKEYS}$  contains  $K_{AUSF}$  and  $K_{SEAF}$  that are generated on the ME using CK and IK as part of AKA procedures as described in TS 33.501[24]

### 15.2A.1.2 Conformance requirement

CR 1 The UE shall support the 5G AKA based primary authentication and key agreement procedure.

CR 2 The ME shall forward the RAND and AUTN received in AUTHENTICATION REQUEST message to the USIM.

CR 3 The ME shall compute RES\* from RES according to Annex A.4 TS 33.501[24] and return it in AUTHENTICATION RESPONSE message.

CR 4 If service n°122 is "available", when entering state 5GMM-DEREGISTERED, the ME shall store the  $K_{AMF}$  with the associated key set identifier, the UE security capabilities, and the uplink and downlink NAS COUNT values in  $EF_{5GS3GPPNSC}$  on the USIM.

CR 5 If services n°123 and n°133 are available, the ME shall store the  $K_{AUSF}$ ,  $K_{SEAF}$ , SOR counter and UE parameter update counter in  $EF_{5GAUTHKEYS}$  on the USIM.

CR 6 The UE can successfully register to the network.

Reference:

- TS 31.102 [19], clauses 4.4.11.3, 4.4.11.4 and 4.4.11.6;
- TS 33.501 [24], clause 6.1.3.2;
- TS 24.501 [25], clause 5.4.1.3 and Annex C.

### 15.2A.1.3 Test purpose

- The purpose of this test is to verify that: 1) the ME forwards the RAND and AUTN received in 5G authentication challenge data within AUTHENTICATION REQUEST message to the USIM.
- 2) the ME sends AUTHENTICATION RESPONSE message contains the calculated RES\* in response to AUTHENTICATION REQUEST message.
  - 3) the ME stores 5G NAS security context parameters when entering state 5GMM-DEREGISTERED, consisting of  $K_{AMF}$  with the associated key set identifier in  $EF_{5GS3GPPNSC}$  on the USIM if service n°122 is "available".
  - 4) the ME stores the  $K_{AUSF}$ ,  $K_{SEAF}$ , SOR counter and UE parameter update counter in  $EF_{5GAUTHKEYS}$  on the USIM if services n°123 and n°133 are available.

### 15.2A.1.4 Method of test

#### 15.2A.1.4.1 Initial conditions

The values of the 5G-NR UICC – support of Rel-16 features as defined in clause 4.5.11 of the present document are used.

The TT (NG-SS) is configured to transmit on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC): 244/083/000001
- Access control: unrestricted.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case.

#### 15.2A.1.4.2 Procedure

Step	Direction	Action	Comment	REQ	SA
1	TT	NG-SS Cell is powered up with SIB1 as defined in the initial conditions	The NG-SS on the TT is activated		
2	UE	Run initial activation			
3	UE<>TT	UE camps on NG-SS Cell and establishes RRC connection			
4	UE > TT	UE sends REGISTRATION REQUEST			
5	TT > UE	NG-SS sends AUTHENTICATION REQUEST with 5G AKA-Challenge message: - ngKSI: - NAS key set identifier: '000' - TSC: '0' - Authentication parameter RAND (5G authentication challenge): 128 bits value - Authentication parameter AUTN (5G Authentication challenge). 128 bits value	The NG-SS on the TT generates $K_{AMF}$ , $K_{AUSF}$ and $K_{SEAF}$ values, and initiates the 5G AKA authentication procedure		
6	UE	ME passes the RAND and AUTN values to the USIM	The ME provides the authentication challenge data received in the AUTHENTICATION REQUEST to the USIM	CR 1 CR 2	A.2/1 OR A.2/2
7	UE > TT	UE sends AUTHENTICATION RESPONSE message with: - Authentication response parameter: 16 octets RES* value calculated according to TS 24.501 [25]	The UE shall return RES* equal to the XRES* calculated at the NG-SS with the parameters provided/indicated in the AUTHENTICATION REQUEST	CR 3	
8	TT > UE	NG-SS sends SECURITY MODE COMMAND message including the ngKSI of the new 5G NAS security context (as provided in step 4)			

9	UE > TT	UE send SECURITY MODE COMPLETE integrity protected and ciphered with the new 5G NAS security context identified by the ngKSI received in the SECURITY MODE COMMAND message in step 7	UE updates EF <sub>5GAUTHKEYS</sub> in parallel or after the NAS message	CR 5	A.2/1 OR A.2/2
10	TT > UE	NG-SS sends REGISTRATION ACCEPT message with: - 5G-GUTI: 24408300010266436587 - TAI: 42 34 80 00 00 01			
11	UE > TT	UE sends REGISTRATION COMPLETE		CR 6	
12	UE <> TT	The UE is powered off and/or deactivated, performs the DEREGISTRATION procedure	UE enters the 5GMM-DEREGISTERED during this step, and updates EF <sub>5GS3GPPNSC</sub>	CR 4	A.2/1 OR A.2/2
<b>Optional step if CR 4, and CR 5 verification cannot be performed at step 9) and 12)</b>					
13	TT	READ EF <sub>5GS3GPPNSC</sub> and EF <sub>5GAUTHKEYS</sub>	The TT or the test operator shall perform whatever action is needed to get read access to EF <sub>5GS3GPPNSC</sub> and EF <sub>5GAUTHKEYS</sub>	CR 4 CR 5	A.2/3

### 15.2A.1.5 Acceptance criteria

CR 1 is verified if CR 2 is met, and the ME forwards the RAND and AUTN received in received in the AUTHENTICATION REQUEST to the USIM.

CR 3 requirements are met if the NG-SS receives RES\* in the AUTHENTICATION RESPONSE message sent in response to the AUTHENTICATION REQUEST in step 6).

CR 4 can be verified in step 12) or 13) if an appropriate method to monitor the APDU for EF update or read the EF content is provided by the UE manufacturer.

CR 5 can be verified in step 9) or 13) if an appropriate method to monitor the APDU for EF update or read the EF content is provided by the UE manufacturer.

CR 6 is verified if the UE is capable to register to the NG-SS at step 11).

The EF contents to be verified at step 9), 12) and/or 13) for CR 4 and CR 5 are listed as below:

**EF<sub>5GAUTHKEYS</sub>** (5G authentication keys)

Logically:

K<sub>AUSF</sub>: 32 bytes, value not checked

K<sub>SEAF</sub>: 32 bytes, value not checked

K<sub>SEAF</sub> for non-3GPP access: 32 bytes, length and value not checked

SOR counter: 2 bytes, value not checked

UE parameter update counter: 2 bytes, value not checked

Coding:

Byte	B1	B2	B3	Bx	Bx+1	Bx+2	Bx+3	...	By
Hex	80	L1	xx	..	81	L2	xx	...	xx
	<b>By+1</b>	<b>By+2</b>	<b>By+3</b>	<b>Bz</b>	<b>Bz+1</b>	<b>Bz+2</b>	<b>Bz+3</b>	..	<b>Bi+1</b>
	82	L3	xx	..	83	L4	xx	..	84
	<b>Bi+2</b>	<b>Bi+3</b>	<b>Bj</b>	<b>Bxx</b>					
	L5	xx	..	xx					

**EF<sub>5GS3GPPNSC</sub>** (5GS 3GPP Access NAS Security Context)

Logically:

5GS NAS Security Context:

ngKSI: 00

K<sub>AMF</sub>: 32 bytes, value not checked

Uplink NAS count: any value

Downlink NAS count: any value

Identifiers of selected NAS integrity  
and encryption algorithms: any value

Identifiers of selected EPS NAS  
integrity and encryption algorithms  
for use after mobility to EPS: any value

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	Bx
Hex	A0	xx	80	01	00	81	xx	xx	...	xx

## 15.2.2 Authentication procedure for 5G AKA – Authentication is successful - GSM UICC

### 15.2.2.1 Definition and applicability

The purpose of the 5G AKA based primary authentication and key agreement procedure is to provide mutual authentication between the UE and the network and to agree on the keys  $K_{AUSF}$ ,  $K_{SEAF}$  and  $K_{AMF}$ . The UE and the AMF shall support the 5G AKA based primary authentication and key agreement procedure.

The 5G NAS security context parameters from a full native 5G NAS security context shall be stored on the USIM if the corresponding file is present on the USIM as specified in TS 31.102 [19]. If the corresponding file is not present on the USIM, this 5GMM parameters is stored in a non-volatile memory in the ME together with the SUPI from the USIM.

During the authentication procedure if the USIM computes a Kc (i.e. GPRS Kc) from CK and IK using conversion function c3 as described in TS 33.102 [53], and sends it to the ME, then the ME shall ignore such GPRS Kc and not store the GPRS Kc on USIM or in ME.

### 15.2.2.2 Conformance requirement

- CR 1 The ME shall ignore the GPRS Kc and not store the GPRS Kc on USIM if the USIM computes a Kc (i.e. GPRS Kc) from CK and IK using conversion function c3 as described in TS 33.102 [53].
- CR 2 The ME shall ignore the GPRS Kc and not store the GPRS Kc in ME if the USIM computes a Kc (i.e. GPRS Kc) from CK and IK using conversion function c3 as described in TS 33.102 [53].
- CR 3 If Service n°122 and Service n°123 are not available on the USIM, the 5GS 3GPP access NAS security context parameters and the 5G authentication keys shall be stored in the non-volatile memory of the ME.

Reference:

- TS 33.501 [24], clause 6.1.3.1;
- TS 24.501 [25], clause 5.4.1.2 and Annex C.

### 15.2.2.3 Test purpose

- 1) To verify that the ME will ignore the GPRS Kc and will not store the GPRS Kc on USIM or in ME when the USIM computes a Kc (i.e. GPRS Kc) from CK and IK.
- 2) To verify that the ME stores the 5GS 3GPP access NAS security context parameters and the 5G authentication keys inside the ME non-volatile memory when Service n°122 and Service n°123 are not available on the USIM.

## 15.2.2.4 Method of test

### 15.2.2.4.1 Initial conditions

The values of the default UICC as defined in clause 4.5.2 of the present document are used.

The NR-SS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC):244/083/000001.
- Access control: unrestricted.

The default UICC is used and installed into the ME.

### 15.2.2.4.2 Procedure

Step	Direction	Action	Comment	REQ	SA
1	TT	NG-SS Cell is powered up	The NG-SS on the TT is activated		
2	UE	Run initial activation			
3	UE<>TT	UE camps on NG-SS Cell and establishes RRC connection			
4	UE > TT	UE sends REGISTRATION REQUEST			
5	TT > UE	NG-SS sends REGISTRATION REJECT (cause: #13 Roaming not allowed in this tracking area) and release RRC connection	UE shall delete 5G-GUTI, last visited registered TAI, TAI list and ngKSI.		
6	UE	The UE is powered off and then on again			
7	UE<>TT	UE camps on NG-SS Cell and establishes RRC connection			
8	UE > TT	UE sends REGISTRATION REQUEST message with: - ngKSI: - NAS key set identifier: '111'	UE shall indicate in the REGISTRATION REQUEST that no key is available for the NAS key set identifier		
9	TT > UE	NG-SS sends AUTHENTICATION REQUEST with 5G AKA-Challenge message: - ngKSI: - NAS key set identifier: '000' - TSC: '0' - Authentication parameter RAND (5G authentication challenge): 128 bits value - Authentication parameter AUTN (5G Authentication challenge). 128 bits value	The NG-SS on the TT generates K <sub>AMF</sub> , K <sub>AUSF</sub> and K <sub>SEAF</sub> values, and initiates the 5G AKA authentication procedure		
10	UE	ME passes the RAND and AUTN values to the USIM	The ME provides the 5G AKA challenge data received in the AUTHENTICATION REQUEST to the USIM; the USIM calculates the response parameter K <sub>C</sub> (i.e. GPRS K <sub>c</sub> ) from CK and IK using conversion function c3		
11	UE > TT	UE sends AUTHENTICATION RESPONSE message with: - Authentication response parameter: 16 octets RES* value calculated according to TS 24.501 [25]	ME does not store GPRS K <sub>c</sub> on the USIM through step 10 to 15	CR 1	O
12	TT > UE	NG-SS sends SECURITY MODE COMMAND including the ngKSI of the new 5G NAS security context (as provided in step 8)			
13	UE > TT	UE send SECURITY MODE COMPLETE			
14	TT > UE	NG-SS sends REGISTRATION ACCEPT message with: - 5G-GUTI: 24408300010266436587 - TAI: 42 34 80 00 00 01			
15	UE > TT	UE sends REGISTRATION COMPLETE			

16	UE <> TT	The UE is powered off and/or deactivated, performs the DEREGISTRATION procedure			
17	UE	Run initial activation and/or activated			
18	UE<>TT	UE camps on NG-SS Cell and establishes RRC connection			
19	UE > TT	UE sends REGISTRATION REQUEST message that is Security protected (indicated by Security header) with - ngKSI: - NAS key set identifier: '000' - TSC: '0' - 5GS mobile identity: 5G-GUTI type with value 24408300010266436587		CR 1 CR 2 CR 3	
20	TT > UE	NG-SS sends REGISTRATION ACCEPT message with: - 5G-GUTI: 24408300010266436587 - TAI: 42 34 80 00 00 01			
21	UE > TT	UE sends REGISTRATION COMPLETE			

### 15.2.2.5 Acceptance criteria

CR 1, CR 2 and CR 3 can be implicitly verified in step 19) when UE sends REGISTRATION REQUEST message that is Security protected and includes ngKSI and 5G-GUTI type 5GS mobile identity as specified in the test procedure.

Optionally, CR 1 can be explicitly verified with methods A.2/1 or A.2/2 that ME does not store GPRS Kc on the USIM through steps 11) to 16).

## 15.2A.2 Authentication procedure for 5G AKA - Authentication is successful

### 15.2A.2.1 Definition and applicability

The purpose of the 5G AKA based primary authentication and key agreement procedure is to provide mutual authentication between the UE and the network and to agree on the keys  $K_{AUSF}$ ,  $K_{SEAF}$  and  $K_{AMF}$ . The UE and the AMF shall support the 5G AKA based primary authentication and key agreement procedure.

The 5G NAS security context parameters from a full native 5G NAS security context shall be stored on the USIM if the corresponding file is present on the USIM as specified in TS 31.102 [19]. If the corresponding file is not present on the USIM, this 5GMM parameters is stored in a non-volatile memory in the ME together with the SUPI from the USIM.

During the authentication procedure if the USIM computes a Kc (i.e. GPRS Kc) from CK and IK using conversion function c3 as described in TS 33.102 [53], and sends it to the ME, then the ME shall ignore such GPRS Kc and not store the GPRS Kc on USIM or in ME.

### 15.2A.2.2 Conformance requirement

- CR 1 The ME shall ignore the GPRS Kc and not store the GPRS Kc on USIM if the USIM computes a Kc (i.e. GPRS Kc) from CK and IK using conversion function c3 as described in TS 33.102 [53].
- CR 2 The ME shall ignore the GPRS Kc and not store the GPRS Kc in ME if the USIM computes a Kc (i.e. GPRS Kc) from CK and IK using conversion function c3 as described in TS 33.102 [53].
- CR 3 If Service n°122 and Service n°123 are not available on the USIM, the 5GS 3GPP access NAS security context parameters and the 5G authentication keys shall be stored in the non-volatile memory of the ME.

Reference:

- TS 33.501 [24], clause 6.1.3.1;
- TS 24.501 [25], clause 5.4.1.2 and Annex C.

### 15.2A.2.3 Test purpose

The purpose of this test is to verify that:

- 1) the ME will ignore the GPRS K<sub>c</sub> and will not store the GPRS K<sub>c</sub> on USIM or in ME when the USIM computes a K<sub>c</sub> (i.e. GPRS K<sub>c</sub>) from CK and IK.
- 2) the ME stores the 5GS 3GPP access NAS security context parameters and the 5G authentication keys inside the ME non-volatile memory when Services n°122, n°123 and n°133 are not available on the USIM.

### 15.2A.2.4 Method of test

#### 15.2A.2.4.1 Initial conditions

The values of the default UICC as defined in clause 4.5.2 of the present document are used.

The NR-SS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC):244/083/000001.
- Access control: unrestricted.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case.

#### 15.2A.2.4.2 Procedure

Step	Direction	Action	Comment	REQ	SA
1	TT	NG-SS Cell is powered up	The NG-SS on the TT is activated		
2	UE	Run initial activation			
3	UE<>TT	UE camps on NG-SS Cell and establishes RRC connection			
4	UE > TT	UE sends REGISTRATION REQUEST			
5	TT > UE	NG-SS sends REGISTRATION REJECT (cause: #13 Roaming not allowed in this tracking area) and release RRC connection	UE shall delete 5G-GUTI, last visited registered TAI, TAI list and ngKSI.		
6	UE	The UE is powered off and then on again			
7	UE<>TT	UE camps on NG-SS Cell and establishes RRC connection			
8	UE > TT	UE sends REGISTRATION REQUEST message with: - ngKSI: - NAS key set identifier: '111'	UE shall indicate in the REGISTRATION REQUEST that no key is available for the NAS key set identifier		
9	TT > UE	NG-SS sends AUTHENTICATION REQUEST with 5G AKA-Challenge message: - ngKSI: - NAS key set identifier: '000' - TSC: '0' - Authentication parameter RAND (5G authentication challenge): 128 bits value - Authentication parameter AUTN (5G Authentication challenge). 128 bits value	The NG-SS on the TT generates K <sub>AMF</sub> , K <sub>AUSF</sub> and K <sub>SEAF</sub> values, and initiates the 5G AKA authentication procedure		
10	UE	ME passes the RAND and AUTN values to the USIM	The ME provides the 5G AKA challenge data received in the AUTHENTICATION REQUEST to the USIM; the USIM calculates the response parameter K <sub>c</sub> (i.e. GPRS K <sub>c</sub> ) from CK and IK using conversion function c3		
11	UE > TT	UE sends AUTHENTICATION RESPONSE message with: - Authentication response parameter: 16 octets RES* value calculated according to TS 24.501 [25]	ME does not store GPRS K <sub>c</sub> , SOR counter or UE parameter update counter on the USIM through step 11 to 16	CR 1	

12	TT > UE	NG-SS sends SECURITY MODE COMMAND including the ngKSI of the new 5G NAS security context (as provided in step 8)			
13	UE > TT	UE send SECURITY MODE COMPLETE			
14	TT > UE	NG-SS sends REGISTRATION ACCEPT message with: - 5G-GUTI: 24408300010266436587 - TAI: 42 34 80 00 00 01			
15	UE > TT	UE sends REGISTRATION COMPLETE			
16	UE <> TT	The UE is powered off and/or deactivated, performs the DEREGISTRATION procedure			
17	UE	Run initial activation and/or activated			
18	UE<>TT	UE camps on NG-SS Cell and establishes RRC connection			
19	UE > TT	UE sends REGISTRATION REQUEST message that is Security protected (indicated by Security header) with - ngKSI: - NAS key set identifier: '000' - TSC: '0' - 5GS mobile identity: 5G-GUTI type with value 24408300010266436587		CR 1 CR 2 CR 3	
20	TT > UE	NG-SS sends REGISTRATION ACCEPT message with: - 5G-GUTI: 24408300010266436587 - TAI: 42 34 80 00 00 01			
21	UE > TT	UE sends REGISTRATION COMPLETE			

### 15.2A.2.5 Acceptance criteria

CR 1, CR 2 and CR 3 can be implicitly verified in step 19) when UE sends REGISTRATION REQUEST message that is security protected and includes ngKSI and 5G-GUTI type 5GS mobile identity as specified in the test procedure.

Optionally, CR 1 can be explicitly verified in steps 11) to 15) with methods A.2/1 or A.2/2 ensuring that the ME does not try to store GPRS Kc, SOR counter or UE parameter update counter on the USIM through steps 11) to 16).

## 15.2.3 Authentication procedure 5G AKA – AUTN fails on the USIM

### 15.2.3.1 Definition and applicability

The purpose of the primary authentication and key agreement procedure is to enable mutual authentication between the UE and the network and to provide keying material that can be used between the UE and network in subsequent security procedures. The UE and the AMF shall support the EAP based primary authentication and key agreement procedure.

At receipt of the RAND and AUTN, the USIM shall verify the freshness of the AV' by checking whether AUTN can be accepted as described in TS 33.102 [53]. If so, the USIM computes a response RES. The USIM shall return RES, CK, IK to the ME. If the verification of the AUTN fails on the USIM, then the USIM and ME shall proceed as described in clause 6.1.3. 3 in TS 33.501 [24].

When 5G AKA is used or when EAP-AKA' is used, at the receipt of the RAND and AUTN, if the verification of the AUTN fails, then the USIM indicates to the ME the reason for failure and in the case of a synchronisation failure passes the AUTS parameter (see TS 33.102 [53]) to the ME.

### 15.2.3.2 Conformance requirement

CR 1 The ME shall forward the RAND and AUTN received in 5G authentication challenge data in the AUTHENTICATION REQUEST message to the USIM.

CR 2 If the verification of the AUTN fails on the USIM, then ME shall send AUTHENTICATION FAILURE with 5GMM cause #21 "Synch failure" and includes the AUTS from USIM.

CR 3 If the verification of the AUTN success, the UE shall send AUTHENTICATION RESPONSE message contains the response calculated in the USIM (RES)

Reference:

- TS 33.501 [24], clause 6.1.3.2 and 6.1.3.3;
- TS 24.501 [25], clause 5.4.1.3.7

### 15.2.3.3 Test purpose

- 1) To verify that the ME forwards the RAND and AUTN received in the 5G authentication challenge message to the USIM.
- 2) To verify that the ME returns the Synchronization-Failure in the AUTHENTICATION FAILURE message if the verification of AUTN failed on the USIM due to a synchronisation failure.

### 15.2.3.4 Method of test

#### 15.2.3.4.1 Initial conditions

The NG-SS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC):244/083/000001.
- Access control: unrestricted.

The default 5G-NR UICC is used and installed into the ME.

#### 15.2.3.4.2 Procedure

Step	Direction	Action	Comment	REQ	SA
1	TT UE	NG-SS Cell is powered up Run initial activation	The NG-SS on the TT is activated		
2	UE<>TT	UE camps on NG-SS Cell and establishes RRC connection			
3	UE > TT	UE sends REGISTRATION REQUEST			
4	TT > UE	NG-SS sends AUTHENTICATION REQUEST with 5G AKA challenge message with: - ngKSI: - NAS key set identifier: '000' - TSC: '0' - Authentication parameter AUTN: '1111 1111 1111 1111' - Authentication parameter RAND (5G authentication challenge): 128 bits value - Authentication parameter AUTN (5G Authentication challenge). 128 bits value	AUTHENTICATION REQUEST with the AMF field in the IE "Authentication parameter AUTN" set to "AMF <sub>RESYNCH</sub> " value to trigger SQN re-synchronisation procedure in the USIM (see TS 34.108 [5], 8.1.2.2)		
5	UE	ME passes the RAND and AUTN values to the USIM	The ME provides the 5G AKA challenge data received in the AUTHENTICATION REQUEST at step 4 to the USIM	CR1	A.2/1 OR A.2/2
6	UE	The UICC returns AUTS parameter to the ME indicating that the verification of AUTN failed due to a synchronisation failure			
7	UE > TT	UE sends AUTHENTICATION FAILURE message with: - 5GMM cause: '0001 0101'	AUTHENTICATION RESPONSE message including 5GMM cause "Synch failure", with AUTS from USIM	CR2	

		- Authentication failure parameter: AUTS value calculated according to TS 34.108, 8.1.2.2 [5]			
8	TT > UE	NG-SS sends AUTHENTICATION REQUEST with 5G AKA challenge message with: - ngKSI: - NAS key set identifier: '000' - TSC: '0' - Authentication parameter RAND (5G authentication challenge): 128 bits value - Authentication parameter AUTN (5G Authentication challenge). 128 bits value			
9	UE	ME passes the RAND and AUTN values to the USIM	The ME provides the 5G AKA challenge data received in the AUTHENTICATION REQUEST at step 8 to the USIM	CR1	A.2/1 OR A.2/2
10	UE > TT	UE sends AUTHENTICATION RESPONSE message with: - Authentication response parameter: 4 - 16 octets RES value calculated according to TS 24.501 [25]	The UE shall return RES* equal to the XRES* calculated at the NG-SS with the parameters provided/indicated in the AUTHENTICATION REQUEST at step 8	CR3	
11	TT > UE	NG-SS sends SECURITY MODE COMMAND message including the ngKSI of the new 5G NAS security context (as provided in step 8)			
12	UE > TT	UE send SECURITY MODE COMPLETE			
13	TT > UE	NG-SS sends REGISTRATION ACCEPT message with: - 5G-GUTI: 24408300010266436587 - TAI: 42 34 80 00 00 01			
14	UE > TT	UE sends REGISTRATION COMPLETE			

### 15.2.3.5 Acceptance criteria

CR 1 can be verified at step 5) and 9).

CR 2 can be verified at step 7) with AUTS value verified according to TS 34.108 [5]), 8.1.2.2.

CR 3 can be verified at step 10).

## 15.2.4 Authentication procedure for 5G AKA - after SUPI is changed

### 15.2.4.1 Definition and applicability

The purpose of the 5G AKA based primary authentication and key agreement procedure is to provide mutual authentication between the UE and the network and to agree on the keys  $K_{\text{AUSF}}$ ,  $K_{\text{SEAF}}$  and  $K_{\text{AMF}}$ . The UE and the AMF shall support the 5G AKA based primary authentication and key agreement procedure.

The 5G NAS security context parameters from a full native 5G NAS security context shall be stored on the USIM if the corresponding file is present on the USIM as specified in TS 31.102 [19]. If the corresponding file is not present on the USIM, this 5GMM parameters is stored in a non-volatile memory in the ME together with the SUPI from the USIM. These 5GMM parameters can only be used if the SUPI from the USIM matches the SUPI stored in the non-volatile memory; else the UE shall delete the 5GMM parameters.

### 15.2.4.2 Conformance requirement

CR 1 The UE shall support the 5G AKA based primary authentication and key agreement procedure.

CR 2 The 5G NAS security context parameters shall be stored on the USIM or in a non-volatile memory in the ME together with the SUPI from the USIM.

CR 3 The UE shall delete the 5GMM parameters if the SUPI from the USIM does not match the SUPI stored in the non-volatile memory.

Reference:

- TS 33.501 [24], clause 6.1.3.2;
- TS 24.501 [25], clauses 5.4.1.3, Annex C.

### 15.2.4.3 Test purpose

- 1) To verify that the UE generates the 5G NAS security context parameters and stores them inside the non-volatile memory in the ME together with the SUPI from the USIM.
- 2) To verify that the UE rejects the SECURITY MODE COMMAND with the existing 5G NAS security context parameters if the SUPI is changed.

### 15.2.4.4 Method of test

#### 15.2.4.4.1 Initial conditions

The NG-SS transmits on the BCCH, with the following network parameters:

- TAI (MCC/MNC/TAC):244/083/000001.
- Access control: unrestricted.

The 5G-NR UICC as defined in clause 4.5.9 is used with the following exceptions and installed into the ME.

**EF<sub>UST</sub>** (USIM Service Table)

Logically:

Service n°122	5GS Mobility Management Information	not available
Service n°123:	5G Security Parameters	not available

Coding:

<b>Byte:</b>	<b>B1</b>	<b>B2</b>	<b>B3</b>	<b>B4</b>	<b>B5</b>	<b>B6</b>	<b>B7</b>	<b>B8</b>
Binary:	xxxx xx1x	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxx1 xx1x	xxxx xxxx	xxxx xxxx
	<b>B9</b>	<b>B10</b>	<b>B11</b>	...	<b>B16</b>	<b>B17</b>		
	xxxx xxxx	xxxx xxxx	xx11 xxxx	...	xxx0 100x	0000 0xxx		

#### 15.2.4.4.2 Procedure

Step	Direction	Action	Comment	REQ	SA
1	TT	NG-SS Cell is powered up	The NG-SS on the TT is activated		
	UE	Run initial activation with IMSI set as 246081685533963			
2	UE<>TT	UE camps on NG-SS Cell and establishes RRC connection			
3	UE > TT	UE sends REGISTRATION REQUEST			
4	TT > UE	NG-SS sends REGISTRATION REJECT (cause: #13 Roaming not allowed in this tracking area) and release RRC connection	UE shall delete 5G-GUTI, last visited registered TAI, TAI list and ngKSI.		
5	UE	The UE is powered off			
	TT	NG-SS Cell is powered off			
6	UE	Run initial activation, with default IMSI			
	TT	NG-SS Cell is powered on			

7	UE<>TT	UE camps on NG-SS Cell and establishes RRC connection			
8	UE > TT	UE sends REGISTRATION REQUEST message with: - ngKSI: - NAS key set identifier: '111' - 5GS mobile identity: SUCI of the UE	UE shall indicate in the REGISTRATION REQUEST that no key is available for the NAS key set identifier		
9	TT > UE	NG-SS sends AUTHENTICATION REQUEST with 5G AKA challenge message with: - ngKSI: - NAS key set identifier: '000' - TSC: '0' - Authentication parameter RAND (5G authentication challenge): 128 bits value - Authentication parameter AUTN (5G Authentication challenge). 128 bits value	The NG-SS on the TT generates $K_{AMF}$ , $K_{AUSF}$ and $K_{SEAF}$ values, and initiates 5G AKA authentication procedure		
10	UE > TT	UE sends AUTHENTICATION RESPONSE message with: - Authentication response parameter: 16 octets RES* value calculated according to TS 24.501 [25]	The UE shall return RES* equal to the XRES* calculated at the NG-SS with the parameters provided/indicated in the AUTHENTICATION REQUEST at step 9		
11	TT > UE	NG-SS sends SECURITY MODE COMMAND message including the ngKSI of the new 5G NAS security context (as provided in step 9)			
12	UE > TT	UE send SECURITY MODE COMPLETE			
13	TT > UE	NG-SS sends REGISTRATION ACCEPT message with: - 5G-GUTI: 24408300010266436587 - TAI: 42 34 80 00 00 01			
14	UE > TT	UE sends REGISTRATION COMPLETE		CR1	
15	UE <> TT	The UE is powered off and, performs the DEREGISTRATION procedure			
16	TT	NG-SS Cell is powered off			
17	UE TT	Run initial activation, with IMSI set as 246081685533963 NG-SS Cell is powered on			
18	UE<>TT	UE camps on NG-SS Cell and establishes RRC connection			
19	UE > TT	UE sends REGISTRATION REQUEST message with: - ngKSI: - NAS key set identifier: '111' - 5GS mobile identity: SUCI of the UE	UE shall indicate within the REGISTRATION REQUEST for the NAS key set identifier that no key is available, and use SUCI as 5GS mobile identity IE	CR3	
20	TT > UE	NG-SS sends AUTHENTICATION REQUEST with 5G AKA challenge message with: - ngKSI: - NAS key set identifier: '000' - TSC: '0' - Authentication parameter RAND (5G authentication challenge): 128 bits value - Authentication parameter AUTN (5G Authentication challenge). 128 bits value			
21	UE > TT	UE sends AUTHENTICATION RESPONSE message with: - Authentication response parameter: 16 octets RES* value calculated according to TS 24.501 [25]	The UE shall return RES* equal to the XRES* calculated at the NG-SS with the parameters provided/indicated in the AUTHENTICATION REQUEST at step 20		
22	TT > UE	NG-SS sends SECURITY MODE COMMAND with: - ngKSI: The ngKSI of the partial native 5G security context assigned in the			

		SECURITY MODE COMMAND message sent in step 11			
23	UE > TT	UE send SECURITY MODE REJECT with - 5GMM cause: '0001 1000'	Cause #24 - Security mode rejected, unspecified	CR2	
24	UE	The UE is powered off			

### 15.2.4.5 Acceptance criteria

CR 1 can be verified at step 14.

CR 3 can be implicitly verified at step 19 where REGISTRATION REQUEST includes NAS key set identifier that no key is available and use SUCI as 5GS mobile identity IE.

CR 2 can be verified at step 24.

## 15.2.5 Authentication procedure for registration on 3GPP accesses. successful 5G AKA - Authentication in different PLMNs

### 15.2.5.1 Definition and applicability

The purpose of the 5G AKA based primary authentication and key agreement procedure is to provide mutual authentication between the UE and the network and to agree on the keys  $K_{AUSF}$ ,  $K_{SEAF}$  and  $K_{AMF}$ . The UE and the AMF shall support the 5G AKA based primary authentication and key agreement procedure.

If the UE supports multiple records of NAS security context storage for multiple registration, the UE shall store the previously current 5G NAS security context in the second 5G security context of that access (see TS 31.102 [19]) and store the new 5G security context in the first 5G security context, when the UE activates the new 5G security context for a different PLMN over that access but the previously current 5G NAS security context is associated with the 5G-GUTI of the other access.

If the previously current 5G NAS security context is not associated with the 5G-GUTI of the other access (e.g. UE uses only 3GPP access) the second record will not be used.

The  $EF_{5GS3GPPNSC}$  contains the 5GS 3GPP access NAS security context as defined in TS 24.501 [25], consisting of  $K_{AMF}$  with the associated key set identifier, the UE security capabilities, and the uplink and downlink NAS COUNT values. This file shall contain two records if service n°136 is "available".

The  $EF_{5GAUTHKEYS}$  contains  $K_{AUSF}$  and  $K_{SEAF}$  that are generated on the ME using CK and IK as part of AKA procedures as described in TS 33.501 [24]. If service n°133 is "available" in  $EF_{UST}$ , the  $EF_{5GAUTHKEYS}$  also contains SOR counter and UE parameter update counter associated with the key  $K_{AUSF}$  as described in TS 33.501 [24] and TS 31.102 [19].

### 15.2.5.2 Conformance requirement

CR 1 The UE shall support the 5G AKA based primary authentication and key agreement procedure

Reference:

- TS 24.501 [25], clauses 4.4.2, 5.4.1.1 and 5.4.1.3

CR 2 The ME shall forward the RAND and AUTN received in AUTHENTICATION REQUEST message to the USIM.

Reference:

- TS 24.501 [25], clause 5.4.1.3.6

CR 3 The ME shall compute RES\* from RES according to TS 33.501 [24], Annex A.4 and return it in the AUTHENTICATION RESPONSE message.

Reference:

- TS 33.501 [24], Annex A.4

CR 4 As a result of the first successful authentication procedure in a PLMN (PLMN 1 over 3GPP access), the 5G 3GPP access NAS security context parameters shall be stored on the USIM in the first record of the EF<sub>5GS3GPPNSC</sub>.

Reference:

- TS 31.102 [19], clauses 4.4.11.4 and 5.2.32

CR 5 As a result of the second successful authentication procedure in another PLMN (PLMN 2 over 3GPP access), the 5G 3GPP access NAS security context parameters of PLMN 2 shall be stored on the USIM in the first record of the EF<sub>5GS3GPPNSC</sub> as the previously current 5G NAS security context is not associated with the 5G-GUTI of the other access.

Reference:

- TS 31.102 [19], clauses 4.4.11.4 and 5.2.32

CR 6 The 5G 3GPP access NAS security context parameters of PLMN 1 will be overwritten with the 5G 3GPP access NAS security context parameters of PLMN 2. The second record of the EF<sub>5GS3GPPNSC</sub> is not used.

Reference:

- TS 31.102 [19], clauses 4.4.11.4 and 5.2.32

### 15.2.5.3 Test purpose

The purpose of this test is to verify that:

- 1) the ME forwards the RAND and AUTN received in 5G authentication challenge data from the first PLMN to the USIM within the *AUTHENTICATION REQUEST* message;
- 2) the ME sends *AUTHENTICATION RESPONSE* message contains the calculated RES\* in response to *AUTHENTICATION REQUEST* message;
- 3) the ME stores 5G 3GPP access NAS security context parameters when entering state 5GMM-DEREGISTERED, consisting of K<sub>AMF</sub> with the associated key set identifier in the first record of the EF<sub>5GS3GPPNSC</sub> on the USIM;
- 4) the ME forwards the RAND and AUTN received in 5G authentication challenge data from the second PLMN to the USIM within the *AUTHENTICATION REQUEST* message;
- 5) the ME sends *AUTHENTICATION RESPONSE* message contains the calculated RES\* in response to *AUTHENTICATION REQUEST* message;
- 6) the ME stores 5G 3GPP access NAS security context parameters of a different PLMN when entering state 5GMM-DEREGISTERED, consisting of K<sub>AMF</sub> with the associated key set identifier in the first record of the EF<sub>5GS3GPPNSC</sub> on the USIM.

### 15.2.5.4 Method of test

#### 15.2.5.4.1 Initial conditions

The 5G-NR UICC - support of Rel-16 features as defined in clause 4.5.11 of the present document is used.

The TT (NG-SS) transmits on the BCCH, with the following network parameters:

Cell A:

TAI (MCC/MNC/TAC): 244/083/000001

CellIdentity: "000000001"

Access control: unrestricted.

Cell B :

TAI (MCC/MNC/TAC): 244/084/000001

CellIdentity: "000000001"

Access control: unrestricted.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case.

#### 15.2.5.4.2 Procedure

Step	Direction	Action	Comment	REQ	SA
1	TT	Power up TT (NG-SS) Cell A is with SIB1 as defined in the initial conditions	The NG-SS on the TT is activated		
2	UE	Run initial activation	The ME reads EF <sub>UST</sub> , EF <sub>5GS3GPPNSC</sub> and EF <sub>5GAUTHKEYS</sub>	CR 1	A.2/1 OR A.2/2
3	UE > TT	Send RRCSetupRequest message	TT (NG-SS) transmits an RRCSetup message to the UE		
4	UE > TT	Send RRCSetupComplete message			
5	UE > TT	Send REGISTRATION REQUEST	Within the REGISTRATION REQUEST the UE indicates that no key is available.		
6	TT > UE	Send AUTHENTICATION REQUEST with 5G AKA-Challenge message: - ngKSI: - NAS key set identifier: '000' - TSC: '0' - Authentication parameter RAND (5G authentication challenge): 128 bits value - Authentication parameter AUTN (5G Authentication challenge). 128 bits value	TT (NG-SS) generates K <sub>AMF</sub> , K <sub>AUSF</sub> and K <sub>SEAF</sub> values, and initiates the 5G AKA authentication procedure	CR 1	
7	UE	Pass RAND and AUTN values to the USIM	The ME provides the authentication challenge data received in the AUTHENTICATION REQUEST to the USIM	CR 2	A.2/1 OR A.2/2
8	UE <> TT	Send AUTHENTICATION RESPONSE message with: - Authentication response parameter: 16 octets RES* value	The TT (NG-SS) sends a SECURITY MODE COMMAND message	CR 3	
9	UE > TT	Send SECURITY MODE COMPLETE message			
10	TT > UE	Send REGISTRATION ACCEPT message with: - 5G-GUTI: 24408300010266436587 - TAI: 42 34 80 00 00 01			
11	UE > TT	Send REGISTRATION COMPLETE			
12	UE > TT/USIM	The UE is powered off or deactivated, and performs the deregistration procedure	UE enters the 5GMM-DEREGISTERED during this step, and updates EF <sub>5GS3GPPNSC</sub>	CR 4	A.2/1 OR A.2/2
13	TT	Power down TT (NG-SS) Cell A Power up TT (NG-SS) Cell B with SIB1 as defined in the initial conditions			
14	UE	Run activation or switch on the UE's radio interface	The UE reads the first record of the 5G 3GPP NAS security context from the USIM		
15	UE > TT	Send RRCSetupRequest message	TT (NG-SS) transmits an RRCSetup message to the UE		
16	UE > TT	Send RRCSetupComplete message			
17	UE > TT	Send REGISTRATION REQUEST	TT (NG-SS) initiates the 5G AKA authentication procedure		
18	TT > UE	Send AUTHENTICATION REQUEST with 5G AKA-Challenge message: - ngKSI: - NAS key set identifier: '001' - TSC: '0'	The NG-SS on the TT generates K <sub>AMF</sub> , K <sub>AUSF</sub> and K <sub>SEAF</sub> values, and initiates the 5G AKA authentication procedure		

		- Authentication parameter RAND (5G authentication challenge): 128 bits value - Authentication parameter AUTN (5G Authentication challenge). 128 bits value			
19	UE	Pass RAND and AUTN values to the USIM	The ME provides the authentication challenge data received in the AUTHENTICATION REQUEST to the USIM	CR 5	A.2/1 OR A.2/2
20	UE <> TT	Send AUTHENTICATION RESPONSE message	The TT (NG-SS) sends a SECURITY MODE COMMAND message		
21	UE > TT	Send SECURITY MODE COMPLETE message			
22	TT > UE	Send REGISTRATION ACCEPT message with: - 5G-GUTI: 24408300010266436587 - TAI: 42 34 80 00 00 01			
23	UE > TT	Send REGISTRATION COMPLETE message			
24	UE > TT/USIM	Power off and/or deactivate the UE	UE enters the 5GMM-DEREGISTERED during this step, and updates EF <sub>5GS3GPPNSC</sub>	CR 6	A.2/1 OR A.2/2

### 15.2.5.5 Acceptance criteria

CR 1 can be explicitly verified by using methods A.2/1 or A.2/2 to check EF<sub>UST</sub>, EF<sub>5GS3GPPNSC</sub> and EF<sub>5GAUTHKEYS</sub> contents in step 2). With having sent the expected 5G AKA-Challenge message data within the AUTHENTICATION REQUEST in step 6) CR 1 is implicitly verified.

CR 2 can be implicitly verified in step 7) using methods A.2/1 or A.2/2. CR 2 is met if EF<sub>5GS3GPPNSC</sub> has the expected contents:

**EF<sub>5GS3GPPNSC</sub>** (5GS 3GPP Access NAS Security Context)

Logically:

5GS NAS Security Context:

ngKSI: 00  
 K<sub>AMF</sub>: 32 bytes, value not checked  
 Uplink NAS count: any value  
 Downlink NAS count: any value  
 Identifiers of selected NAS integrity and encryption algorithms: any value  
 Identifiers of selected EPS NAS integrity and encryption algorithms for use after mobility to EPS: any value

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	Bx
Hex	A0	xx	80	01	00	81	xx	xx	...	xx

CR 3 is implicitly verified in step 8). The requirement is met if the ME sends a SECURITY MODE COMPLETE message in step 9).

CR 4 is explicitly verified in step 12) using methods A.2/1 or A.2/2. The requirement is met if EF<sub>5GS3GPPNSC</sub> has the expected contents:

**EF<sub>5GS3GPPNSC</sub> (5GS 3GPP Access NAS Security Context)**

Logically:

5GS NAS Security Context first record:

ngKSI: 00

K<sub>AMF</sub>: value not checked

Uplink NAS count: any value

Downlink NAS count: any value

Identifiers of selected NAS integrity  
and encryption algorithms: any value

Identifiers of selected EPS NAS  
integrity and encryption algorithms  
for use after mobility to EPS: any value

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	Bx
Hex	A0	xx	80	01	00	81	xx	xx	...	xx

CR 5 can be explicitly verified in step 19) using methods A.2/1 or A.2/2. The requirement is met if EF<sub>5GAUTHKEYS</sub> has the expected contents:

**EF<sub>5GAUTHKEYS</sub> (5G authentication keys)**

Logically:

K<sub>AUSF</sub>: 32 bytes, value not checked

K<sub>SEAF</sub> for 3GPP access: 32 bytes, value not checked

K<sub>SEAF</sub> for non-3GPP access: 32 bytes, all values set to 'FF'

SOR counter: 2 bytes, value not checked

UE parameter update counter: 2 bytes, value not checked

Coding:

Byte	B1	B2	B3	..	B35	B36	B37	..
Hex	80	20	xx	xx	81	20	xx	xx
	<b>B69</b>	<b>B70</b>	<b>B71</b>	..	<b>B103</b>	<b>B104</b>	<b>B105</b>	<b>B106</b>
	82	20	FF	FF	83	02	xx	xx
	<b>B107</b>	<b>B108</b>	<b>B109</b>	<b>B110</b>				
	84	02	xx	xx				

CR 6 is explicitly verified if step 24) using methods A.2/1 or A.2/2. The requirement is met if EF<sub>5GS3GPPNSC</sub> has the expected contents:

**EF<sub>5GS3GPPNSC</sub> (5GS 3GPP Access NAS Security Context)**

Logically:

5GS NAS Security Context first record

ngKSI: 01

K<sub>AMF</sub>: value not checked

Uplink NAS count: any value

Downlink NAS count: any value

Identifiers of selected NAS integrity  
and encryption algorithms: any value

Identifiers of selected EPS NAS  
integrity and encryption algorithms  
for use after mobility to EPS: any value

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	Bx
Hex	A0	xx	80	01	01	81	xx	xx	...	xx

5GS NAS Security Context second record:

ngKSI: 07 (no key available)

K<sub>AMF</sub>: value not checked

Uplink NAS count: any value

Downlink NAS count: any value

Identifiers of selected NAS integrity  
and encryption algorithms: any value

Identifiers of selected EPS NAS  
integrity and encryption algorithms  
for use after mobility to EPS: any value

PLMN identifier: any value

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	Bx
Hex	A0	xx	80	01	07	81	xx	xx	...	xx

NOTE: Implicit verification using method A.2/3 is not possible for CR 2 and CR 4. Thus, A.2/3 is no valid verification method for this test.

---

## 16 UE Route Selection Policy (URSP) procedure

### 16.1 Pre-configured URSP rules

#### 16.1.1 Support for URSP by USIM

##### 16.1.1.1 Definition and applicability

As specified in TS 24.526 [38], if the UE has no signalled URSP, and the UE has pre-configured URSPs configured in both the USIM and the ME, then the UE shall use the pre-configured URSP in the USIM.

As specified in TS 31.102 [19], the EF<sub>URSP</sub> in the USIM contains UE Route Selection Policies per PLMN and shall be considered by the ME if EF<sub>UST</sub> service n° 132 "Support for URSP by USIM" is available.

##### 16.1.1.2 Conformance requirement

CR 1 The UE shall support the URSP procedure;

Reference:

- TS 31.102 [19], clause 5.2.34
- TS 24.526 [38], clause 4.2.2.2
- TS 23.503 [40], clause 6.6.2.1
- TS 23.501 [39], clause 5.15.5.2 and 5.15.5.3

CR 2 The URSP rules shall be read from USIM if service n°132 is available;

Reference:

- TS 31.102 [19], clause 4.4.11.12 and 5.2.3.34

CR 3 The ME shall use URSP rules stored on the USIM rather than any pre-configured USRP rules stored in the ME if service n°132 is available.

Reference:

- TS 31.102 [19], clause 5.1.1 and 5.2.34

### 16.1.1.3 Test purpose

The purpose of this test is to verify that:

- 1) To verify that the ME reads the URSP rules from USIM if service n°132 is available.
- 2) To verify that the ME uses the matching URSP rule from USIM to set the PDU session establishment parameters if service n°132 is available.

### 16.1.1.4 Method of test

#### 16.1.1.4.1 Initial conditions

The values of the 5G-NR UICC – support of Rel-16 features as defined in clause 4.5.11 of the present document are used with EF<sub>MSI</sub> as defined in clause 4.6.5 and the following exceptions:

**EF<sub>UST</sub>** (USIM Service Table)

Logically:

Service n°132: Support for URSP by USIM available

Coding:

<b>Byte:</b>	<b>B1</b>	<b>B2</b>	<b>B3</b>	<b>B4</b>	<b>B5</b>	<b>B6</b>	<b>B7</b>	<b>B8</b>
Binary:	xxxx xx1x	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxx1 xx1x	xxxx xxxx	xxxx xxxx
	<b>B9</b>	<b>B10</b>	<b>B11</b>	...	<b>B16</b>	<b>B17</b>		
	xxxx xxxx	xxxx xxxx	xx11 xxxx	...	xxx0 111x	0xxx 1xxx		

**EF<sub>URSP</sub>** (UE Route Selection Policies)

Logically:

URSP rules for one PLMN only

- PLMN: 246 081

Rule Precedence = 0

Traffic descriptor:

- DNN = TestGp.rs

Route Selection Descriptor:

- Precedence = 0
- Network Slice Selection, S-NSSAI: '01 01 01 03' (ST: MBB, SD: 010103)

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	80	22	42	16	80	1E	00	1C	00	00	0C	88
	<b>B13</b>	<b>B14</b>	<b>B15</b>	<b>B16</b>	<b>B17</b>	<b>B18</b>	<b>B19</b>	<b>B20</b>	<b>B21</b>	<b>B22</b>	<b>B23</b>	<b>B24</b>
	0A	06	54	65	73	74	47	70	02	72	73	00
	<b>B25</b>	<b>B26</b>	<b>B27</b>	<b>B28</b>	<b>B29</b>	<b>B30</b>	<b>B31</b>	<b>B32</b>	<b>B33</b>	<b>B34</b>	<b>B35</b>	<b>B36</b>
	0B	00	09	00	00	06	02	04	01	01	01	03

The ME is pre-configured with the following URSP rules:

USRP rules for one PLMN only

- PLMN: 246 081

Rule Precedence =1

Traffic descriptor:

- DNN=TestGp.rs

Route Selection Descriptor:

- Precedence=1
- Network Slice Selection, S-NSSAI: '01 01 01 02' (ST: MBB, SD: 010102)
- SSC Mode Selection: SSC Mode 1
- Access Type preference: 3GPP access

Rule Precedence = <lowest priority>

Traffic Descriptor: \*

Route Selection Descriptor:

- Precedence = 1
- Network Slice Selection, S-NSSAI: '01 01 01 01' (ST: MBB, SD: 010101)
- SSC Mode Selection: SSC Mode 1
- DNN Selection: internet

The TT (NG-SS) transmits on the BCCH, with the following network parameters:

- Mobile Country Code (MCC) = 246;
- Mobile Network Code (MNC) = 081;
- Tracking Area Code (TAC) = 000001;
- NG-SS Cell Id = 0001 (36 bits).

The Allowed S-NSSAI list is configured in NG-SS as '01 01 01 01', '01 01 01 02' and '01 01 01 03'.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case.

#### 16.1.1.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	Run initial activation.			
2	UE > TT	Authenticate at the TT	The UE successful authenticates to PLMN 246 081.	CR 1	

			The TT indicates Allowed S-NSSAI list as: - '01 01 01 01' - '01 01 01 02' - '01 01 01 03'.		
3	UE	READ EF <sub>UST</sub> and EF <sub>URSP</sub>	No URSP rules are provisioned by the PCF	CR 2 (CR 1)	A.2/1 OR A.2/2
3	UE > TT	Initiate a connection to DNN=TestGp.rs			
4	UE > TT	Send a PDU SESSION ESTABLISHMENT REQUEST	The UE sends the PDU SESSION ESTABLISHMENT REQUEST to the network via UL NAS TRANSPORT with: - DNN: TestGp.rs - S-NSSAI: '01 01 01 03'		
5	TT > UE	Send PDU SESSION ESTABLISHMENT ACCEPT message		CR 3 (CR 1)	
6	UE	UE is soft powered down			
<b>Optional step if CR 2 verification cannot be performed at step 3)</b>					
7	UE	READ EF <sub>UST</sub> and EF <sub>URSP</sub>		CR 2	A.2/3

### 16.1.1.5 Acceptance criteria

CR 1 is implicitly verified. The requirement is met if the test sequence can be executed as expected.

CR 2 is explicitly verified at step 3) by using the methods A.2/1 or A.2/2. Optional it can be verified in step 7) using method A.2/3.

CR 3 is implicitly verified if the PDU SESSION ESTABLISHMENT ACCEPT message is sent by the UE.

## 16.1.2 Support for URSP by ME

### 16.1.2.1 Definition and applicability

If the UE has no signalled URSP and the UE has only pre-configured URSPs configured in the ME, then the UE shall use the pre-configured URSP in the ME.

The pre-configured URSP can only be used if the SUPI from the USIM matches the SUPI stored in the non-volatile memory of the ME.

### 16.1.2.2 Conformance requirement

CR 1 The UE shall support the URSP procedure.

CR 2 The ME shall use the pre-configured URSP rules in the ME if there is no signalled URSP and UE has only pre-configured URSP in the ME.

CR 3 The URSP can only be used if the SUPI from the USIM matches the SUPI stored in the non-volatile memory of the ME.

Reference:

- TS 24.526 [50], clause 4.2.2.2 and 5.2;
- TS 23.503 [52], clause 6.6.2.

### 16.1.2.3 Test purpose

The purpose of this test is to verify that the ME uses the matching URSP rule from ME to set the PDU session establishment parameters if there is no signalled URSP and there is no pre-configured URSP in the USIM.

## 16.1.2.4 Method of test

### 16.1.2.4.1 Initial conditions

The values of the 5G-NR UICC – support of Rel-16 features as defined in clause 4.5.11 of the present document are used with EF<sub>IMSI</sub> as defined in clause 4.6.5.

The ME is pre-configured with the following URSP rules:

USRP rules for one PLMN only

- PLMN: 244 083

Rule Precedence = 1

Traffic descriptor:

- DNN = TestGp.rs

Route Selection Descriptor:

- Precedence = 1
- Network Slice Selection, S-NSSAI: '01 01 01 02' (ST: MBB, SD: 010102)
- SSC Mode Selection: SSC Mode 1
- Access Type preference: 3GPP access

Rule Precedence = <lowest priority>

Traffic Descriptor: \*

Route Selection Descriptor:

- Precedence =1
- Network Slice Selection, S-NSSAI: '01 01 01 01' (ST: MBB, SD: 010101)
- SSC Mode Selection: SSC Mode 1
- DNN Selection: internet

The TT (NG-SS) transmits on the BCCH, with the following network parameters:

- Mobile Country Code (MCC) = 244;
- Mobile Network Code (MNC) = 083;
- Tracking Area Code (TAC) = 000001;
- NG-SS Cell Id = 0001 (36 bits).

The Allowed S-NSSAI list is configured in NG-SS to include S-NSSAIs ('01 01 01 01', '01 01 01 01'), and ('01 01 01 02', '01 01 01 02').

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case.

### 16.1.2.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	Run initial activation.			
2	UE > TT	Authenticate at the TT	The UE successful authenticates to PLMN 244 083.	CR 1	

			The TT indicates Allowed S-NSSAI list as: - '01 01 01 01' - '01 01 01 02'.		
3	UE	READ EF <sub>UST</sub>	No URSP rules are provisioned by the PCF	CR 2 (CR 1)	A.2/1 OR A.2/2
3	UE > TT	Initiate a connection to DNN=TestGp.rs			
4	UE > TT	Send a PDU SESSION ESTABLISHMENT REQUEST	The UE sends the PDU SESSION ESTABLISHMENT REQUEST to the network via UL NAS TRANSPORT with: - DNN: TestGp.rs - S-NSSAI: '01 01 01 02'		
5	TT > UE	Send PDU SESSION ESTABLISHMENT ACCEPT message		CR 3 (CR 1)	
6	UE	UE is soft powered down			
<b>Optional step if CR 2 verification cannot be performed at step 3)</b>					
7	UE	READ EF <sub>UST</sub>		CR 2	A.2/3

### 16.1.2.5 Acceptance criteria

CR 1 is implicitly verified. The requirement is met if the test sequence can be executed as expected.

CR 2 is explicitly verified at step 3) by using the methods A.2/1 or A.2/2. Optional it can be verified in step 7) using method A.2/3.

CR 3 is implicitly verified if the PDU SESSION ESTABLISHMENT ACCEPT message is sent by the UE.

## 16.1.3 Support of Signalled URSP

### 16.1.3.1 Definition and applicability

The HPLMN pre-configured URSP in the ME and the HPLMN signalled URSP shall be stored in a non-volatile memory in the ME together with the SUPI from the USIM.

If the UE has both pre-configured URSP(s) and signalled URSP, the UE shall only use the signalled URSP. For a UE not operating in SNPN access mode, if the UE has no signalled URSP, and the UE has pre-configured URSPs configured in both the USIM and the ME, then the UE shall use the pre-configured URSP in the USIM. The HPLMN pre-configured URSP in the ME shall be stored until a new URSP is configured by HPLMN or the USIM is removed.

### 16.1.3.2 Conformance requirement

CR 1 The UE shall support the URSP procedure.

CR 2 If the UE has both pre-configured URSP(s) and signalled URSP, the UE shall only use the signalled URSP.

Reference:

- TS 24.526 [50], clause 4.2.2.2 and 5.2;
- TS 23.503 [52], clause 6.6.2.

### 16.1.3.3 Test purpose

The purpose of this test is to verify that the ME uses signalled URSP when provided rather than pre-configured URSP in the USIM or the ME.

### 16.1.3.4 Method of test

#### 16.1.3.4.1 Initial conditions

The values of the 5G-NR UICC – support of Rel-16 features as defined in clause 4.5.11 of the present document are used with EF<sub>IMSI</sub> as defined in clause 4.6.5 and the following exceptions:

##### EF<sub>UST</sub> (USIM Service Table)

Logically:

Service n°132: Support for URSP by USIM available

Coding:

Byte:	B1	B2	B3	B4	B5	B6	B7	B8
Binary:	xxxx xx1x	xxxx xxxx	xxxx 1x00	xxxx x1xx	xxxx xx11	xxx1 xx1x	xxxx xxxx	xxxx xxxx
	B9	B10	B11	...	B16	B17		
	xxxx xxxx	xxxx xxxx	xx11 xxxx	...	xxx0 111x	0xxx 1xxx		

##### EF<sub>URSP</sub> (UE Route Selection Policies)

Logically:

URSP rules for one PLMN only

- PLMN: 246 081

Rule Precedence = 0

Traffic descriptor:

- DNN = TestGp.rs

Route Selection Descriptor:

- Precedence = 0
- Network Slice Selection, S-NSSAI: '01 01 01 02' (ST: MBB, SD: 010102)

Coding:

Byte	B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12
Hex	80	22	42	16	80	1E	00	1C	00	00	0C	88
	B13	B14	B15	B16	B17	B18	B19	B20	B21	B22	B23	B24
	0A	06	54	65	73	74	47	70	02	72	73	00
	B25	B26	B27	B28	B29	B30	B31	B32	B33	B34	B35	B36
	0B	00	09	00	00	06	02	04	01	01	01	02

The ME is pre-configured with the following URSP rules:

URSP rules for one PLMN only

- PLMN: 246 081

Rule Precedence =1

Traffic descriptor:

- DNN=TestGp.rs

Route Selection Descriptor:

- Precedence=1
- Network Slice Selection, S-NSSAI: '01 01 01 01' (ST: MBB, SD: 010101)
- SSC Mode Selection: SSC Mode 1
- Access Type preference: 3GPP access

The TT (NG-SS) transmits on the BCCH, with the following network parameters:

- Mobile Country Code (MCC) = 246;

- Mobile Network Code (MNC) = 081;
- Tracking Area Code (TAC) = 000001;
- NG-SS Cell Id = 0001 (36 bits).

The Allowed S-NSSAI list is configured in NG-SS as '01 01 01 01', '01 01 01 02' and '01 01 01 03'.

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case.

#### 16.1.3.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	Run initial activation.			
2	UE > TT	Authenticate at the TT	The UE successful authenticates to PLMN 246 081. The TT indicates Allowed S-NSSAI list as: - '01 01 01 01' - '01 01 01 02' - '01 01 01 03'.	CR 1	
3	UE	READ EF <sub>UST</sub> and EF <sub>URSP</sub>	No URSP rules are provisioned by the PCF	CR 2 (CR 1)	A.2/1 OR A.2/2
3	UE > TT	Initiate a connection to DNN=TestGp.rs			
4	UE > TT	Send a PDU SESSION ESTABLISHMENT REQUEST	The UE sends the PDU SESSION ESTABLISHMENT REQUEST to the network via UL NAS TRANSPORT with: - DNN: TestGp.rs - S-NSSAI: '01 01 01 02'		
5	TT > UE	Send PDU SESSION ESTABLISHMENT ACCEPT message		(CR 1)	
6	TT > UE	Release the PDU Session			
7	TT > UE	Send MANAGE UE POLICY COMMAND	The UE should update the URSP rule for DNN: "TestGp.rs" Traffic Descriptor: - DNN: 'TestGp.rs' - S-NSSAI: '01 01 01 03'	CR 1	
8	UE > TT	Initiate a connection to DNN=TestGp.rs			
9	UE > TT	Send a PDU SESSION ESTABLISHMENT REQUEST	The UE sends the PDU SESSION ESTABLISHMENT REQUEST to the network via UL NAS TRANSPORT with: - DNN: TestGp.rs - S-NSSAI: '01 01 01 03'		
10	TT > UE	Send PDU SESSION ESTABLISHMENT ACCEPT message		(CR 1)	
<b>Optional step if CR 2 verification cannot be performed at step 3)</b>					
11	UE	READ EF <sub>UST</sub> and EF <sub>URSP</sub>		CR 2	A.2/3

#### 16.1.3.5 Acceptance criteria

CR 1 is implicitly verified. The requirement is met if the test sequence can be executed as expected.

CR 2 is explicitly verified at step 3) by using the methods A.2/1 or A.2/2. Optional it can be verified in step 11) using method A.2/3.

## 17 CAG list handling

### 17.1 CAG list handling for 5G

#### 17.1.1 Automatic CAG selection with preconfigured CAG list on USIM

##### 17.1.1.1 Definition and applicability

If MS supports CAG and is pre-configured with a non-empty "CAG information list" stored in the USIM, the MS in automatic PLMN selection mode shall consider a PLMN indicated by an NG-RAN cell only if:

- A) the cell is a CAG cell and broadcasts a CAG-ID for the PLMN such that there exists an entry with the PLMN ID of the PLMN in the "CAG information list" and the CAG-ID is included in the "Allowed CAG list" of the entry;

or

- B) the cell is not a CAG cell and:

- there is no entry with the PLMN ID of the PLMN in the "CAG information list";

or

- there exists an entry with the PLMN ID of the PLMN in the "CAG information list" but the "indication that the MS is only allowed to access 5GS via CAG cells" is not included in the entry.

##### 17.1.1.2 Conformance requirement

CR 1 If service n°137 is available in EF<sub>UST</sub> and a preconfigured "CAG information list" is available on the USIM, then an ME that supports CAG shall read EF<sub>CAG</sub> and consider the PLMN indicated by the NG-RAN to perform automatic PLMN selection procedure.

Reference:

- TS 31.102 [4], clause 4.4.11.14.

CR 2 If the available CAG cell broadcasts a CAG-ID for the PLMN such that there exists an entry with the PLMN ID of the PLMN in the "CAG information list" and the CAG-ID is included in the "Allowed CAG list" of the entry, then UE shall select the CAG cell.

Reference:

- TS 23.122 [31], clauses 3.8, 4.4.3.1.1
- TS 24.501 [42], clauses 9.11.3.18A

##### 17.1.1.3 Test purpose

The purpose of this test is to verify that the ME only selects the CAG cell if the PLMN ID and CAG ID of the cell are found in the EF<sub>CAG</sub> (Pre-configured CAG information list) available on USIM.

##### 17.1.1.4 Method of tests

###### 17.1.1.4.1 Initial conditions

The values of the 5G-NR UICC – CAG support as defined in clause 4.5.13 of the present document are used.

The TT (NG-SS) is configured to transmit on the BCCH, with the following network parameters:

Cell A

- TAI (MCC/MNC/TAC): 244/083/000001.
- cag-Identity: 00 00 00 02

Cell B

- TAI (MCC/MNC/TAC): 244/083/000002.
- cag-Identity: 00 00 00 09

Ensure that the UE has installed and is using the UICC/USIM configuration defined for this test case and that both cells on the TT are switched off.

#### 17.1.1.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	TT	Activate NG-SS Cell B	The NG-SS Cell B on the TT is activated as defined in the initial conditions		
2	UE	Run initial activation			
3		Wait for 5 minutes	While waiting, the ME shall not attempt to registration to Cell B	CR 1	
4	TT	Activate NG-SS Cell A, deactivate NG-SS Cell B			
5	UE > TT	Send REGISTRATION REQUEST to Cell A	The UE sends a REGISTRATION REQUEST with 5GS registration type IE as "initial registration"	CR 2	
6	TT > UE	Send REGISTRATION ACCEPT from Cell A	The TT sends a REGISTRATION ACCEPT with 5G-GUTI		
7	UE > TT	Send REGISTRATION COMPLETE			
8	UE	Power off/deactivate the UE			
9	TT	Deactivate NG-SS Cell A			
10	TT	Activate NG-SS Cell B with SIB1 modified to indicate new cag-identity 00 00 00 07			
11	UE	Power on/activate the UE			
12	UE > TT	Send REGISTRATION REQUEST to Cell B	The UE sends a REGISTRATION REQUEST with 5GS registration type IE as "initial registration"	CR 2	
13	TT > UE	Send REGISTRATION ACCEPT from Cell B	The TT sends a REGISTRATION ACCEPT with 5G-GUTI		
14	UE > TT	Send REGISTRATION COMPLETE			
15	UE	Power off/deactivate the UE			
16	TT	Deactivate NG-SS Cell A and Cell B			

#### 17.1.1.5 Acceptance criteria

CR 1 can be implicitly verified in step 3). The requirement is met if the UE is not sending a REGISTRATION REQUEST message to Cell B.

CR 2 can be implicitly verified in steps 5) and 12). The requirement is met if the UE sends REGISTRATION REQUEST message to Cell A in step 5) and to Cell B in step 6).

## 18 NSSAA procedure with SSIM

### 18.1 SSIM management procedures

#### 18.1.1 SSIM identification, S-NSSAI list request

##### 18.1.1.1 Definition and applicability

If the decision of HPLMN, the SNPN or the slice owner is to require Network Slice-Specific Authentication and Authorization with a Credentials holder AAA Server (AAA-S) during the NSSAA procedure (see TS 23.502 [61] and TS 23.501 [39]) for a certain S-NSSAI and to require that the ME shall use the SSIM for this authentication and authorization, then the HPLMN (respectively SNPN or slice owner) shall provision a list of S-NSSAI in the SSIM that the HPLMN (respectively SNPN or slice owner) allows.

Prior to the slice establishment with AMF, the ME shall select the SSIM on the UICC to retrieve the S-NSSAI list supported by the SSIM.

##### 18.1.1.2 Conformance requirement

CR 1 If SSIM is supported on the UICC and declared in  $EF_{DIR}$  then the ME shall read  $EF_{NSSAI}$  from  $ADF_{SSIM}$  to identify the S-NSSAIs supported by the SSIM.

Reference:

- TS 31.105 [59], clauses 5.1.0, 5.1.1, 5.1.5, 7.2

CR 2 Network slice-specific authentication shall be performed if the UE indicates the support in the network slice-specific authentication and authorization in the 5GMM Capability IE in the REGISTRATION REQUEST message.

Reference:

- TS 24.501 [25], clauses 4.6.2.4, 5.5.1.2.2 and 5.5.1.3.2

CR 3 The network slice-specific authentication and authorization procedure shall not be performed unless the primary authentication and key agreement procedure has successfully been completed.

Reference:

- TS 24.501 [25], clauses 4.6.2.4, 5.4.1

CR 4 If one of the S-NSSAI supported by the SSIM requires authentication and authorization during NSSAA procedure with the network then the ME shall relay the EAP packets between the AAA Server (AAA-S) and the SSIM using the SSIM AUTHENTICATE command and associated NSSAA procedure NAS messages (i.e. NETWORK SLICE-SPECIFIC AUTHENTICATION COMMAND, NETWORK SLICE-SPECIFIC AUTHENTICATION COMPLETE and NETWORK SLICE-SPECIFIC AUTHENTICATION RESULT).

Reference:

- TS 33.501 [24], clause 16.3
- TS 23.501 [39], clauses 5.15.5.2.1, 5.15.10
- TS 23.502 [61], clause 4.2.9
- TS 24.501 [25], clauses 4.6.2.4, 5.4.7, 8.2.31, 8.2.32, 8.2.33

##### 18.1.1.3 Test purpose

The purpose of this test is to verify that:

- 1) the ME identifies and selects the SSIM supported on the UICC
- 2) the ME retrieves from the SSIM the supported S-NSSAI list from EF<sub>NSSAI</sub>
- 3) during the NSSAA procedure requiring authentication and authorization during NSSAA procedure on a specific S-NSSAI supported by the SSIM, the ME relays the EAP packets between the AAA Server (AAA-S) and the SSIM using the SSIM AUTHENTICATE command and associated NSSAA procedure NAS messages.

#### 18.1.1.4 Method of tests

##### 18.1.1.4.1 Initial conditions

The browser's cache shall be cleared before execution of the test sequence.

The ME memory shall be cleared from all formerly stored Allowed-NSSAI and Rejected-NSSAI.

The values of the 5G-NR SSIM-UICC as defined in clause 4.5.16 of the present document are used.

The ME is pre-configured with the following Configured-NSSAI:

PLMN: 001 01

- S-NSSAI: 01 01 01 01 (SST: eMBB, SD: 010101)
- S-NSSAI: 01 01 01 02 (SST: eMBB, SD: 010102)
- S-NSSAI: 01 01 01 03 (SST: eMBB, SD: 010103)

The ME is pre-configured with the following URSP rules for one PLMN only (PLMN: 244 83):

Rule Precedence = 1

Traffic Descriptor:

- DNN = TestGp.rs

Route Selection Descriptor:

- Precedence = 1
- Network Slice Selection: S-NSSAI: 01 01 01 03 (SST: eMBB, SD: 010103)
- SSC Mode Selection: SSC Mode 1
- Access Type preference: 3GPP access

Rule Precedence =2

Traffic Descriptor:

- DNN = Test12.rs

Route Selection Descriptor:

- Precedence = 1
- Network Slice Selection: S-NSSAI: 01 01 01 02 (SST: eMBB, SD: 010102)
- SSC Mode Selection: SSC Mode 1
- Access Type preference: 3GPP access

Rule Precedence = <lowest priority>

Traffic Descriptor: \*

Route Selection Descriptor:

- Precedence = 1
- SSC Mode Selection: SSC Mode 1
- Access Type preference: 3GPP access

The TT (NG-SS) is configured to transmit on the BCCH with the following network parameters:

#### Cell A

- Mobile Country Code (MCC): 244;
- Mobile Network Code (MNC): 83;
- Tracking Area Code (TAC): 000001;
- NG-RAN Cell Identity value: 0001 (36 bits);
- Subscribed S-NSSAIs: 01010102 (SST: eMBB, SD: 010102) and S-NSSAI is subject to NSSAA;

#### Cell B

- Mobile Country Code (MCC): 244;
- Mobile Network Code (MNC): 83;
- Tracking Area Code (TAC): 000002;
- NG-RAN Cell Identity value: 0002 (36 bits);
- Subscribed S-NSSAIs: 01010103 (SST: eMBB, SD: 010103) and S-NSSAI is subject to NSSAA;

The ME is connected to Cell A.

Ensure that the UE has installed and is using the UICC/SSIM configuration defined for this test case.

#### 18.1.1.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	Run initial activation.		CR 1	A.2/1 OR A.2/2
2	UE > TT	Send REGISTRATION REQUEST	The UE sends a REGISTRATION REQUEST including Requested NSSAI: - S-NSSAI 01010101 (SST: eMBB, SD: 010101) - S-NSSAI 01010102 (SST: eMBB, SD: 010102) - S-NSSAIs 01010103 (SST: eMBB, SD: 010103) and indicating NSSAA support in 5GMM capability	CR 2	
3	TT > UE	Send REGISTRATION ACCEPT	The NG-SS sends a REGISTRATION ACCEPT without Allowed NSSAI and indicating "NSSAA to be performed" in 5GS registration result		
4	TT < > UE	Initiate the primary authentication	The primary authentication and key agreement procedure is successfully completed	CR 3	A.2/1 OR A.2/2
5	ME > SSIM	Send SSIM AUTHENTICATE command	The ME relays the EAP-Request packet from EAP message IE to the SSIM using AUTHENTICATE command.		
6	SSIM > ME	Send SSIM AUTHENTICATE response	The ME retrieves the EAP-Response packet from the SSIM AUTHENTICATE command response	CR 3	A.2/1 OR A.2/2
7	UE > TT	Send NETWORK SLICE-SPECIFIC AUTHENTICATION COMPLETE	The NETWORK SLICE-SPECIFIC AUTHENTICATION COMPLETE message includes an EAP-Response:		

			- S-NSSAI IE set to 01010102 (SST: eMBB, SD: 010102)		
8	TT > UE	Send NETWORK SLICE-SPECIFIC AUTHENTICATION RESULT	The NETWORK SLICE-SPECIFIC AUTHENTICATION RESULT message includes: - S-NSSAI IE set to 01010102 (SST: eMBB, SD: 010102) - EAP message IE containing an EAP-success or EAP-failure message	CR 4	

#### 18.1.1.4.2 Acceptance criteria

CR 1 can be explicitly verified using methods A.2/1 or A.2/2 during UE initialization (step 1)). The requirement is met if the ME selects the SSIM and reads  $EF_{NSSAI}$ .

CR 2 can be verified in step 2). The requirement is met if the UE indicates the support in the network slice-specific authentication and authorization in the 5GMM Capability IE in the REGISTRATION REQUEST message

CR 3 can explicitly be verified in steps 4) and 6) using methods A.2/1 or A.2/2.

CR 4 can be verified in step 8). It is met if the NETWORK SLICE-SPECIFIC AUTHENTICATION RESULT message includes:

- S-NSSAI IE set to 01010102 (SST: eMBB, SD: 010102);
- EAP message IE containing an EAP-success or EAP-failure message.

## 18.2 SSIM commands

### 18.2.1 AUTHENTICATE command, Identity EAP-Request/EAP-Response messages

#### 18.2.1.1 Definition and applicability

If the decision of HPLMN, the SNPN or the slice owner is to require Network Slice-Specific Authentication and Authorization with a Credentials holder AAA Server (AAA-S) during the NSSAA procedure (see TS 23.502 [61] and TS 23.501 [39]) for a certain S-NSSAI and to require that the ME shall use SSIM for this authentication and authorization, then the HPLMN (respectively SNPN or slice owner) shall provision associated identifier (i.e. EAP Identifier).

At the beginning of the Network Slice-Specific Authentication and Authorization with a Credentials holder AAA Server (AAA-S) on supported S-NSSAI for a given SSIM, the ME shall:

- relay the EAP-Request/Identity packet from EAP message IE in the first NETWORK SLICE-SPECIFIC AUTHENTICATION COMMAND NAS message to the SSIM using AUTHENTICATE command.
- relay the EAP-Response/Identity packet returned by the SSIM on AUTHENTICATE command to EAP message IE in the first NETWORK SLICE-SPECIFIC AUTHENTICATION COMPLETE NAS message.

#### 18.2.1.2 Conformance requirement

CR 1 If one of the S-NSSAI supported by the SSIM requires authentication and authorization during NSSAA procedure with the network, then the ME shall relay the EAP-Request/Identity packet included in the first NETWORK SLICE-SPECIFIC AUTHENTICATION COMMAND NAS message from the network to the appropriate SSIM using the SSIM AUTHENTICATE command.

CR 2 If one of the S-NSSAI supported by the SSIM requires authentication and authorization during NSSAA procedure with the network, then the ME shall relay the EAP-Response/Identity packet included in the response of the first SSIM AUTHENTICATE command sent to the appropriate SSIM to the first NETWORK SLICE-SPECIFIC AUTHENTICATION COMPLETE NAS message sent to the network.

Reference:

- TS 31.105 [59], clauses 4.2.2, 7.2
- TS 33.501 [24], clause 16.3
- TS 23.501 [39], clauses 5.15.5.2.1, 5.15.10
- TS 23.502 [61], clause 4.2.9
- TS 24.501 [25], clauses 5.4.7, 8.2.31, 8.2.32, 8.2.33

### 18.2.1.3 Test purpose

The purpose of this test is to verify that at the beginning of the NSSAA procedure at the beginning of the NSSAA procedure requiring authentication and authorization during NSSAA procedure on a specific S-NSSAI supported by the SSIM,:

- 1) the ME relays the EAP-Request/Identity packet from EAP message IE in the first NETWORK SLICE-SPECIFIC AUTHENTICATION COMMAND NAS message to the SSIM using AUTHENTICATE command.
- 2) the ME relays the EAP-Response/Identity packet returned by the SSIM on AUTHENTICATE command to EAP message IE in the first NETWORK SLICE-SPECIFIC AUTHENTICATION COMPLETE NAS message.

### 18.2.1.4 Method of tests

#### 18.2.1.4.1 Initial conditions

The initial conditions defined in 18.1.1.4.1 apply.

#### 18.2.1.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	Run initial activation.			
2	UE > TT	Send REGISTRATION REQUEST	The UE sends a REGISTRATION REQUEST including Requested NSSAI: - S-NSSAI 01010101 (SST: eMBB, SD: 010101) - S-NSSAI 01010102 (SST: eMBB, SD: 010102) - S-NSSAI 01010103 (SST: eMBB, SD: 010103) and indicating NSSAA support in 5GMM capability		
3	TT > UE	Send REGISTRATION ACCEPT	The NG-SS sends a REGISTRATION ACCEPT without Allowed NSSAI and indicating "NSSAA to be performed" in 5GS registration result		
4	TT < > UE	Initiate the primary authentication	The primary authentication and key agreement procedure is successfully completed		
5	ME > SSIM	Send SSIM AUTHENTICATE command	The ME relays the EAP-Request packet from EAP message IE to the SSIM using AUTHENTICATE command.	CR 1	A.2/1 OR A.2/2
6	SSIM > ME	Send SSIM AUTHENTICATE response	The ME retrieves the EAP-Response packet from the SSIM AUTHENTICATE command response		
7	UE > TT	Send NETWORK SLICE-SPECIFIC AUTHENTICATION COMPLETE	The NETWORK SLICE-SPECIFIC AUTHENTICATION COMPLETE message includes an EAP-Response: - S-NSSAI IE set to 01010102 (SST: eMBB, SD: 010102)	CR 2	

8	TT > UE	Send NETWORK SLICE-SPECIFIC AUTHENTICATION RESULT	The NETWORK SLICE-SPECIFIC AUTHENTICATION RESULT message includes: - S-NSSAI IE set to 01010102 (SST: eMBB, SD: 010102) - EAP message IE containing an EAP-success or EAP-failure message		
---	---------	---	---	--	--

### 18.2.1.4.3 Acceptance criteria

CR 1 can be verified in step 5) using methods A.2/1 or A.2/2. The requirement is met if the ME relays the EAP-Request packet from EAP message IE to the SSIM using AUTHENTICATE command.

CR 2 can be verified in step 7). The requirement is met if:

- 1) the returned EAP-Response/Identity is verylongusername1@3gpp.com
- 2) all AUTHENTICATE commands are ODD INS only with a BER-TLV structure,
- 3) only for 'First block of authentication data' (b8b7b6 of P1 set to '100') AUTHENTICATE command the S-NSSAI field is present in command data and set to 01010102.

## 18.2.2 AUTHENTICATE command, other EAP-Request/EAP-Response messages

### 18.2.2.1 Definition and applicability

If the decision of HPLMN, the SNPN or the slice owner is to require Network Slice-Specific Authentication and Authorization with a Credentials holder AAA Server (AAA-S) during the NSSAA procedure (see TS 23.502 [61] and TS 23.501 [39]) for a certain S-NSSAI and to require that the ME shall use SSIM for this authentication and authorization, then the HPLMN (respectively SNPN or slice owner) shall provision associated identifier (i.e. EAP Identifier) and credentials in the SSIM that the HPLMN (respectively SNPN or slice owner) allows.

During the Network Slice-Specific Authentication and Authorization with a Credentials holder AAA Server (AAA-S) on supported S-NSSAI for a given SSIM, the ME shall:

- relay the EAP-Request packet from EAP message IE in the NETWORK SLICE-SPECIFIC AUTHENTICATION COMMAND NAS message to the SSIM using AUTHENTICATE command.
- relay the EAP-Response packet returned by the SSIM on AUTHENTICATE command to EAP message IE in the NETWORK SLICE-SPECIFIC AUTHENTICATION COMPLETE NAS message.

### 18.2.2.2 Conformance requirement

CR 1 If one of the S-NSSAI supported by the SSIM requires authentication and authorization during NSSAA procedure with the network, then the ME shall relay the EAP-Request packet included in the NETWORK SLICE-SPECIFIC AUTHENTICATION COMMAND NAS message from the network to the appropriate SSIM using the SSIM AUTHENTICATE command.

CR 2 If one of the S-NSSAI supported by the SSIM requires authentication and authorization during NSSAA procedure with the network, then the ME shall relay the EAP-Response packet included in the response of the SSIM AUTHENTICATE command from the SSIM to the NETWORK SLICE-SPECIFIC AUTHENTICATION COMPLETE NAS message sent to the network.

Reference:

- TS 31.105 [59], clauses 7.2
- TS 33.501 [24], clause 16.3
- TS 23.501 [39], clauses 5.15.5.2.1, 5.15.10

- TS 23.502 [61], clause 4.2.9
- TS 24.501 [25], clauses 5.4.7, 8.2.31, 8.2.32, 8.2.33

### 18.2.2.3 Test purpose

The purpose of this test is to verify that during the NSSAA procedure requiring authentication and authorization on a specific S-NSSAI supported by the SSIM, the ME relays:

- 1) the EAP-Request packet from EAP message IE in the NETWORK SLICE-SPECIFIC AUTHENTICATION COMMAND NAS message to the SSIM using AUTHENTICATE command.
- 2) the EAP-Response packet returned by the SSIM on AUTHENTICATE command to EAP message IE in the NETWORK SLICE-SPECIFIC AUTHENTICATION COMPLETE NAS message.

### 18.2.2.4 Method of tests

#### 18.2.2.4.1 Initial conditions

The initial conditions defined in 18.2.1.4.1 apply.

#### 18.2.2.4.2 Procedure

The procedure defined in 18.2.1.4.2 is used.

#### 18.2.2.4.3 Acceptance criteria

CR 1 can be verified in step 5) using methods A.2/1 or A.2/2. The requirement is met if the ME relays the EAP-Request packet from EAP message IE to the SSIM using AUTHENTICATE command.

CR 2 can be verified in step 7). The requirement is met if:

- 1) the returned EAP-Response from the AUTHENTICATE command response to EAP message IE is included in the NETWORK SLICE-SPECIFIC AUTHENTICATION COMPLETE message,
- 2) all AUTHENTICATE commands are ODD INS only with a BER-TLV structure
- 3) only for 'First block of authentication data' (b8b7b6 of P1 set to '100') AUTHENTICATE command the S-NSSAI field is present in command data and set to 01010102
- 4) the EAP message does not fit in one single SSIM AUTHENTICATE command, following data of the EAP message are sent segmented using 'Next block of authentication data' (b8b7b6 of P1 set to '000') AUTHENTICATE command and the S-NSSAI field is not present in command data.

## 18.2.3 AUTHENTICATE command, EAP-Success/EAP-Failure messages

### 18.2.3.1 Definition and applicability

At the end of the Network Slice-Specific Authentication and Authorization with a Credentials holder AAA Server (AAA-S) on supported S-NSSAI for a given SSIM, the ME shall:

- relay the EAP-success/EAP-failure packet from EAP message IE in the NETWORK SLICE-SPECIFIC AUTHENTICATION RESULT NAS message to the SSIM using AUTHENTICATE command.

### 18.2.3.2 Conformance requirement

CR 1 If one of the S-NSSAI supported by the SSIM requires authentication and authorization during NSSAA procedure with the network, then the ME shall relay the EAP-success/EAP-failure packet included in EAP message IE from the NETWORK SLICE-SPECIFIC AUTHENTICATION RESULT NAS message issued by the network to the appropriate SSIM using the SSIM AUTHENTICATE command.

Reference:

- TS 31.105 [59], clauses 7.2
- TS 33.501 [24], clause 16.3
- TS 23.501 [39], clauses 5.15.5.2.1, 5.15.10
- TS 23.502 [61], clause 4.2.9
- TS 24.501 [25], clauses 5.4.7, 8.2.31, 8.2.32, 8.2.33

### 18.2.3.3 Test purpose

The purpose of this test is to verify that, at the end of the NSSAA procedure requiring authentication and authorization on a specific S-NSSAI supported by the SSIM, the ME relays EAP-success/EAP-failure packet from EAP message IE in the NETWORK SLICE-SPECIFIC AUTHENTICATION RESULT NAS message to the SSIM using AUTHENTICATE command.

### 18.2.3.4 Method of tests

#### 18.2.3.4.1 Initial conditions

The initial conditions defined in 18.2.1.4.1 apply.

#### 18.2.3.4.2 Procedure

Step	Direction	Action	Information	REQ	SA
1	UE	Run initial activation.			
2	UE > TT	Send REGISTRATION REQUEST	The UE sends a REGISTRATION REQUEST including Requested NSSAI: - S-NSSAI 01010101 (SST: eMBB, SD: 010101) - S-NSSAI 01010102 (SST: eMBB, SD: 010102) - S-NSSAIs 01010103 (SST: eMBB, SD: 010103) and indicating NSSAA support in 5GMM capability		
3	TT > UE	Send REGISTRATION ACCEPT	The NG-SS sends a REGISTRATION ACCEPT without Allowed NSSAI and indicating "NSSAA to be performed" in 5GS registration result		
4	TT < > UE	Initiate the primary authentication	The primary authentication and key agreement procedure is successfully completed		
5	ME > SSIM	Send SSIM AUTHENTICATE command	The ME relays the EAP-Request packet from EAP message IE to the SSIM using AUTHENTICATE command.		
6	SSIM > ME	Send SSIM AUTHENTICATE response	The ME retrieves the EAP-Response packet from the SSIM AUTHENTICATE command response		
7	UE > TT	Send NETWORK SLICE-SPECIFIC AUTHENTICATION COMPLETE	The NETWORK SLICE-SPECIFIC AUTHENTICATION COMPLETE message includes an EAP-Response: - S-NSSAI IE set to 01010102 (SST: eMBB, SD: 010102)		
8	TT > UE	Send NETWORK SLICE-SPECIFIC AUTHENTICATION RESULT	The NETWORK SLICE-SPECIFIC AUTHENTICATION RESULT message includes: - S-NSSAI IE set to 01010102 (SST: eMBB, SD: 010102) - EAP message IE containing an EAP-success or EAP-failure message	CR 1	

### 18.2.3.4.3 Acceptance criteria

CR 1 can be verified in step 8). The requirement is met if:

- 1) the ME relays the EAP-Request packet from EAP message IE to the SSIM using AUTHENTICATE command,
- 2) the ME relays to the appropriate SSIM supporting the S-NSSAI 01010102 the EAP-success or EAP-failure from EAP message IE received on NETWORK SLICE-SPECIFIC AUTHENTICATION RESULT message using AUTHENTICATE command,
- 3) the AUTHENTICATE command is ODD INS only with a BER-TLV structure.
- 4) only for 'First block of authentication data' (b8b7b6 of P1 set to '100') AUTHENTICATE command the S-NSSAI field is present in command data and set to 01010102.

## Annex A (informative): Suggested requirements lists for Test Applet functionality

A Test Applet should be installed on to a nrUICC for testing USAT functionalities or testing USIM functionalities (e.g. test environment in clause 4.1.5) if toolkit applet is required. Test Applet and TT should support general requirements in clause A.1 and the requirements in either the List-1 or List-2 in clause A.2 for test execution.

### A.1 General requirements

General requirements	
A.1.1	Test instructions or Test Input data for test case execution should be read from Test EFs.
A.1.2	Format of the test instructions input data should be defined as per the applet implementation.
A.1.3	Applet should be able to trigger proactive commands using test case instructions or input data Test EFs.
A.1.4	Applet should be able to handle Call Control events from ME and return treatments using test case instructions or input data Test EFs.
A.1.5	TT should be able to instruct the applet when to read individual test instructions for executing them sequentially and should maintain proper synchronization with the test steps executed on the TT (Network Simulator).
A.1.6	Applet should be capable of resuming test steps in a test case after a device reset or UICC RESET refresh if required (e.g. Device reset or the REREFRESH is part of the test case).
A.1.7	Applet should be able to register or deregister for toolkit events in the ME - nrUICC interface.  NOTE 1: A SETUP EVENT LIST proactive command will be triggered by the nrUICC due to the event registration or deregistration. NOTE 2: Applet may not receive the TERMINAL RESPONSE (TR) for the SETUP EVENT LIST proactive command. TT may use other methods to verify the TR content if required.
A.1.8	Applet should be capable of processing concatenated envelopes (e.g., in the case of Long SoR) and to take the necessary actions according to the test requirements.
A.1.9	Applet should be able to read EF contents from a specific test file (e.g. EF <sub>EF_RESET</sub> ) to restore data in dedicated / standard EFs to its values in the original TS.48 configuration (e.g. prior to executing a test case).  NOTE 3: Applet may trigger UICC RESET after restoring the EF data.
A.1.10	Loading Test toolkit applets onto the nrUICC should be possible by using widely available tools.
A.1.11	Test applet should support events defined in ETSI TS 102 241 Rel-18 and 3GPP 31.130,

### A.2 Test instruction or input data requirements

Test applet should be able to read test instruction or input data from EFs under DF<sub>TEST</sub> or from EF<sub>TC\_IN</sub>. as defined in requirements list 1 or list 2 below.

#### A.2.1 Test instruction or input data requirements list-1

Requirements in the following list are suggested to be supported within the test environment for seamless testing as defined in clause 4.1.4 of the present document.

Requirements for Seamless testing environment	
A.2.1.1	TT or User should be able to configure the necessary Elementary Files (EF <sub>STK</sub> , EF <sub>SETSTK</sub> , EF <sub>CC</sub> , EF <sub>EVENTLIST</sub> ) of the activated USIM/ISIM application using test specific configuration data prior to execution of the test procedure.

## A.2.2 Test instruction or input data requirements list-2

Requirements in the following list are suggested to be supported within the test environment for Test toolkit events-based testing as defined in clause 4.1.5 of the present document.

Requirements for Test events-based testing	
A.2.2.1	Test instructions or Input data for test case execution should be read from the test EF (EF <sub>TC_IN</sub> ) configurable by the TT prior to execution of the test procedure (during test case initialization).

## A.3 APDU content verification requirements

### A.3.1 APDU content verification requirements list-1

Requirements in the following list are suggested to be supported within the test environment for seamless testing as defined in clause 4.1.4 of the present document.

Requirements for Seamless testing environment	
A.3.1.1	TT should be able to receive and process the APDU TX/RX data exchanged between UICC and ME while maintaining proper synchronization with the test steps executed in the TT.
A.3.1.2	Verification of APDU TX/RX data for the respective EF should be possible by the TT during or after the test case execution.

### A.3.2 APDU content verification requirements list-2

Requirements in the following list are suggested to be supported within the test environment for seamless testing as defined in clause 4.1.5 of the present document.

Requirements for Test events-based testing	
A.3.2.1	Applet should be capable of writing the contents of selected APDUs (e.g.: TERMINAL RESPONSE, ENVELOPE data, any selected APDUs etc), received from the ME - nrUICC interface to a test output file (e.g. EF <sub>TC_OUT</sub> ).
A.3.2.2	TT should read EF <sub>TC_OUT</sub> file after the test case execution to verify the acceptance criteria.
A.3.2.3	Format of the verification data in the test output file should be defined as per the applet implementation.
A.3.2.4	Applet should be able to process the TERMINAL RESPONSE received from the ME upon triggering a proactive command from the Applet.
A.3.2.5	When required by a test case, applet should be able to register or deregister for receiving an ADPU to verify its content.  NOTE 1: Test events based APDU verification (clause 4.1.5) will require additional test applet support for the events EVENT_TEST_EXTERNAL_FILE_READ and EVENT_TEST_RX_APDU defined in ETSI TS 102 241 Rel 18.

# Annex B (informative): Examples of Test EFs in the Test-nrUICC configuration

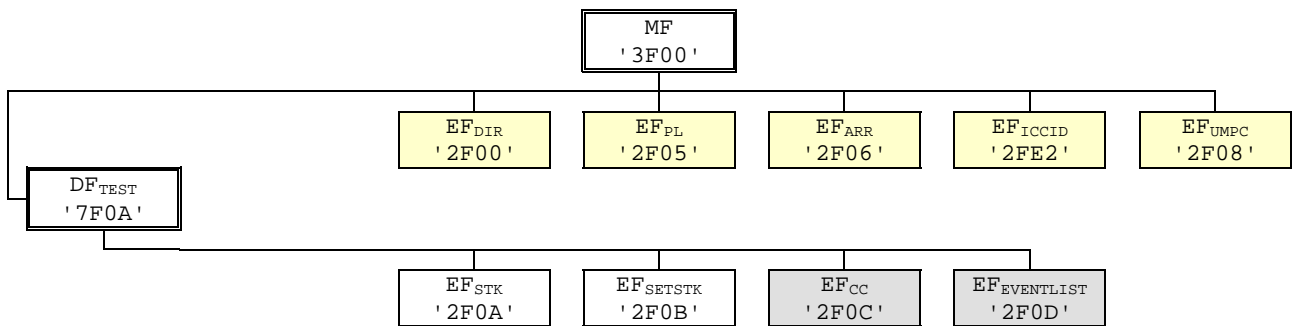
The details provided for the Test-SIM (Default UICC) in TS 31.121 [2] clause 4 apply to the Test-nrUICC configuration used with this test specification, with the following addition.

Test Tool or device manufacturer may provide the Test EF structure on the GSMA TS.48 [9] configuration depending on the test applet used for the testing.

## B.1 Test EF structure - 1

DF<sub>TEST</sub> shall be present at the Master File (MF) level to be used for testing purpose. The general structure of DF<sub>TEST</sub> and associated EF is defined below.

This EF structure is suggested to be used with the test environment defined in clause 4.1.4 of the present document in case USAT functionality is required to operate the test case.



The information in EF<sub>STK</sub>, EF<sub>SETSTK</sub>, EF<sub>CC</sub>, EF<sub>EVENTLIST</sub> shall be used. A Generic STK Applet that utilizes the test data configured by tester in these new EFs to trigger the required commands from the UICC shall be used.

NOTE: File ID for DF<sub>TEST</sub> is implementation specific.

### B.1.1 EF<sub>STK</sub> (SIMToolkit data)

Identifier: '2F0A'		Structure: linear fixed		Optional	
Record length: X bytes (see note)			Update activity: low		
Access Conditions:					
READ		ALW			
UPDATE		ALW			
DEACTIVATE		ALW			
ACTIVATE		ALW			
Bytes	Description	Default Value	M/O	Length	
1 to X	Test Data - Record 1	'FF FF .. FF FF'	M	X bytes	
..	..	..	M	X bytes	
39*X+1 to 40*X	Test Data - Record 40	'FF FF .. FF FF'	M	Xbytes	

Each individual record can hold the tester configured data, specific to the proactive command that needs to be issued by the ME referenced by EF<sub>SETSTK</sub>, for structure and coding details of the proactive command refer TS 31.111 [26].

NOTE: The record length is implementation specific. It is recommended to configure a record length allowing to entirely store each of the toolkit commands required for testing.

## B.1.2 EF<sub>SETSTK</sub> (Set SIM Toolkit)

Identifier: '2F0B'		Structure: transparent		Optional	
File size: 1 byte			Update activity: low		
Access Conditions:					
READ		ALW			
UPDATE		ALW			
DEACTIVATE		ALW			
ACTIVATE		ALW			
Bytes	Description	Default Value	M/O	Length	
1	Test Data	'00'	M	1 byte	

Test Data is either set by the tester to the default value '0x00' or a specific record number of EF<sub>STK</sub>. When read whilst set to a specific record number of EF<sub>STK</sub>, it will imply to trigger the respective SIM toolkit command.

Example:

EF<sub>STK</sub> is configured as '0x01':

- the test toolkit applet will issue the command stored at record 01 of EF<sub>STK</sub>.
- Once the command is issued successfully, the applet will set EF<sub>SETSTK</sub> to the default value.

EF<sub>STK</sub> is configured as '0x80':

- the test toolkit applet will issue all available commands stored in records of EF<sub>STK</sub> in sequence.

NOTE: This is helpful for tests where multiple proactive commands are required to be issued in sequence (from record 1 to n of EF<sub>STK</sub>) after receiving the Terminal Response from the prior command.

## B.1.3 EF<sub>CC</sub> (CALL CONTROL)

Identifier: '2F0C'		Structure: transparent		Optional	
Record length: 255 bytes			Update activity: low		
Access Conditions:					
READ		ALW			
UPDATE		ALW			
DEACTIVATE		ALW			
ACTIVATE		ALW			
Bytes	Description	Default Value	M/O	Length	
1 to 255	Test Data	'00 .. 00'	M	255 bytes	

Test Data is configured by the tester with the Call control response (as defined in TS 31.111 [26]) to process the Call Control Envelope commands received from the ME based on the Call Control service configured in UST.

For example:

1. '00 00' implies allowed not modified.
2. '01 00' implies not allowed.
3. '02 LL...XX' implies allowed with modifications. (LL denotes the length of the TLV).

### B.1.4 EF<sub>EVENTLIST</sub> (EVENT LIST)

Identifier: '2F0D'		Structure: transparent		Optional	
Record length: 255 bytes			Update activity: low		
Access Conditions: READ ALW UPDATE ALW DEACTIVATE ALW ACTIVATE ALW					
Bytes	Description	Default Value	M/O	Length	
1 to 255	Test Data	'FF .. FF'	M	255 bytes	

The Test data is of format <length><event1><event2>..<event n>.. FF FF, where the length indicates the number of configured events as configured by the tester. Supported events are defined in TS 31.111 [26].

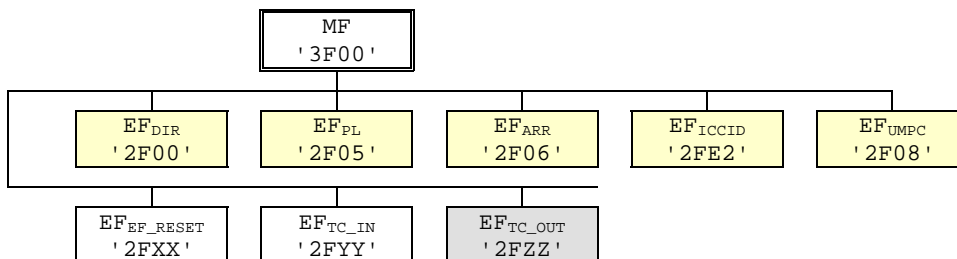
The data persist even after the card reset. Hence this data needs to be cleared by the tester by reverting the contents to default values (FF..FF)

---

## B.2 Test EF structure - 2

EF<sub>TC\_IN</sub>, EF<sub>TC\_OUT</sub>, and EF<sub>EF\_RESET</sub> files may be used for testing purpose and if used, shall be present at the Master File (MF) level. A Generic STK Test Applet can make use of the data configured in those files by the TT.

The general structure for the EFs is defined as below.



NOTE: File IDs for EF<sub>TC\_IN</sub>, EF<sub>TC\_OUT</sub>, and EF<sub>EF\_RESET</sub> files are implementation specific.

This EF structure is suggested to be used with the test environment defined in clause 4.1.5 of the present document in case USAT functionality is required to operate the test case.

EF<sub>TC\_IN</sub> and EF<sub>TC\_OUT</sub> files are used during test case execution, and it shall be updated fresh for each test case.

EF<sub>EF\_RESET</sub> file is used for saving EF content required to restore the TS.48 configuration to its original content before initializing test specific data.

### B.2.1 EF<sub>TC\_IN</sub> (Test Case Input)

This file contains data required for a test applet to handle test case execution. Content and format of the data may be changed depending on the Applet implementation.

Identifier: '2FXX'		Structure: transparent		Optional	
Record length: 255 bytes			Update activity: low		
Access Conditions:					
READ		ALW			
UPDATE		ALW			
DEACTIVATE		ALW			
ACTIVATE		ALW			
Bytes	Description	Default Value	M/O	Length	
1 to 255	Test Data	'FF .. FF'	M	255 bytes	

The EF may include data related to:

Test step control

- TT can update this data to direct test applet to move to next step in the test case.

Toolkit command data

- This can be a sequence of TLVs related to proactive commands or event registrations or call control response data or any other action required for the test case.

Different tags can be defined for this purpose.

Example:

Bytes	Description	M/O	Length
1	Test step control	M	1 byte
2	Tag 1: Wait for new step tag	M	1 byte
3	Tag 1 length	M	1 byte
4 to 4+X-1	Tag 1 data	M	X bytes
4+X	Tag 2: Proactive command tag	O	1 byte
5+X	Tag 2 length	O	1 byte
6+X to 6+X+Y-1	Tag 2 data	O	Y bytes

NOTE: X and Y is greater than zero if the Tag is present.

## B.2.2 EF<sub>TC\_OUT</sub> (Test Case Output)

This file contains data received from the ME and it can be read by the TT to verify if meeting the acceptance criteria of a test case. Additionally, few leading bytes can be used for tracking EF<sub>TC\_IN</sub> and EF<sub>TC\_OUT</sub> current offsets if required by the applet. Content and format of the data may be changed depending on the Applet implementation.

Identifier: '2FYY'		Structure: transparent		Optional	
Record length: 255 bytes			Update activity: low		
Access Conditions:					
READ		ALW			
UPDATE		ALW			
DEACTIVATE		ALW			
ACTIVATE		ALW			
Bytes	Description	Default Value	M/O	Length	
1 to 255	Test Data	'FF .. FF'	M	255 bytes	

The EF can include data related to,

Test EFs offset control,

- TT can update initial offsets during test case initialization.
- TT can track and update the test EF offsets as applet executes test steps.

Toolkit command response data received from the ME,

- This can be a sequence of TLVs related to proactive command responses (TERMINAL RESPONSE) or envelope commands (EVENTs).
- Different Tags can be used for this purpose.

Example:

Bytes	Description	M/O	Length
1-2	Test EFs offset control bytes	M	2 bytes
3-4	Length	M	2 bytes
5	Tag 1: Proactive command 1 tag (for TERMINAL RESPONSE 1)	O	1 byte
6	Tag 1 length	O	1 byte
7 to 7+X-1	Tag 1 data	O	X bytes
7+X	Tag 2: Proactive command 2 tag (for TERMINAL RESPONSE 2)	O	1 byte
8+X	Tag 2 length	O	1 byte
9+X to 9+X+Y-1	Tag 2 data	O	Y bytes

NOTE: X and Y is greater than zero if the Tag is present.

### B.2.3 EF<sub>EF\_RESET</sub> (EF\_RESET)

This file contains data required for updating EFs in the TS.48 configuration in order to restore the original content of it as part of test case initialization. TT can request the applet through test control byte to read the content from this EF and update required EFs in the TS.48 configuration. Content and format of the data may be changed depending on the Applet implementation.

[...]

Identifier: '2FZZ'		Structure: linear fixed		Optional	
Record length: 128 bytes		Update activity: low			
File size: 128 * n, (n = 25)					
Access Conditions:					
READ		ALW			
UPDATE		ALW			
DEACTIVATE		ALW			
ACTIVATE		ALW			
Byte	Description	Default Value	M/O	Length	
1 to X <sup>(1)</sup>	EF content read control data	'FF FF .. FF FF'	M	X bytes	
X+1 to X+1+128-1	Sequence of EF content data - 1	'FF FF .. FF FF'	M	128 bytes	
X+1+128 to X+1+128*2-1	Sequence of EF content data - 2	'FF FF .. FF FF'	O	128 bytes	
..	..	..	O	128 bytes	
X+1+128*23 to X+1+128*24-1	Sequence of EF content data - 24	'FF FF .. FF FF'	O	128 bytes	

NOTE 1: X depends on applet implementation and is greater than zero.

The EF can include data related to,

EF content read control data,

- TT can update this record with an instruction on what records to be read to update the EFs in the nrUICC.

Sequence of EF content data,

- This can be a sequence of TLVs related to EF content in the TS.48 configuration.
- Each sequence can include data related to more than one EF in the TS.48 configuration.
- Applet can choose a format to include number of padding pattern (eg 'FF') or unused bytes instead of updating with a sequence of same pattern to save the size of data in a record.

Example format:

Record number	Data format
1	<instruction to read all none empty records>, <REFRESH flag> OR <read from start record>, <read end record>, <REFRESH flag>
2	<path length 1>,< EF id 1>,<0 (for Transparent EF)>,<length of data 1>,<data 1>,<no of repeated pattern>,<length of pattern>,<repeated pattern>, <path length 2>,< EF id 2>,<1, (for record# 1)>,<length of actual data 2.1>,<data 2.1>,<no of repeated pattern>,<length of pattern>,<repeated pattern>, <path length 2>,< EF id 2>,<2, (for record# 2)>,<length of actual data 2.2>,<data 2.2>,<no of repeated pattern>,<length of pattern>,<repeated pattern>, .....
3	<path length 5>,< EF id 5>,<0 (Transparent EF)>,<length of data 5>,<data 5>,0, <path length 6>,< EF id 6>,<1 (Record# 1)>,<no. of FF>,<length of actual data 6.1>,<data 6.1>,0, <path length 7>,< EF id 7>,<0 (Transparent E)>,<no. of FF>,<length of actual data 7>,<data 7>,0, .....

NOTE: <length of pattern> and <repeated pattern> is not required if <no of repeated pattern> is 0.

Example data:

Record number	Data format
1	FD,1 OR 2,3,0
2	'02 6F C9 01 04 01 02 03 04 00.....'
3	'02 6F CE 05 01 09 07 01 FF 02 6F D2 00 03 03 03 03 00 61 01 FF.....'

## Annex C (informative): 5G-NR generic procedure for 5G Registration on 3GPP access with IMS service

### C.1 5G-NR generic procedure for 5G Registration on 3GPP access with IMS service

#### C.1.1 'voice centric' Procedure

Step	Direction	Action	Information
1	TT	NG-SS Cell is powered up with SIB1 as defined in the test case initial conditions and the additional requirements as defined in clause 4.7.	pc_VOICE_CENTRIC is TRUE. The NG-SS on the TT is activated.
2	UE	Run initial activation	
3	UE <> TT	UE camps on NG-SS Cell and establishes RRC connection	
4	UE > TT	Send REGISTRATION REQUEST	
5	TT > UE	Send AUTHENTICATION REQUEST	
6	UE	UE passes the RAND and AUTN values to the USIM	
7	UE > TT	Send AUTHENTICATION RESPONSE	The RES value in AUTHENTICATION RESPONSE message is calculated according to TS 24.501 [25]. It is equal to the XRES calculated at the TT
8	TT > UE	Send SECURITY MODE COMMAND	
9	UE > TT	Send SECURITY MODE COMPLETE	
10	TT > UE	Send REGISTRATION ACCEPT	
11	UE > TT	Send REGISTRATION COMPLETE	
12	UE > TT	Send an ULInformationTransfer message with a PDU SESSION ESTABLISHMENT REQUEST for the DNN type 'ims'.	5GMM: UL NAS TRANSPORT 5GSM: PDU SESSION ESTABLISHMENT REQUEST (DNN=IMS)
13	TT > UE	Send a RRCReconfiguration message with an PDU SESSION ESTABLISHMENT ACCEPT	5GMM: DL NAS TRANSPORT 5GSM: PDU SESSION ESTABLISHMENT ACCEPT
14	UE > TT	Send RRCReconfigurationComplete	
15	UE <> TT	Run IMS Registration	The IMS Registration procedure is executed in accordance with TS 34.229-5 [58] clause A.2 (steps 1-8).

# Annex D (informative): APDU logging in seamless testing

If the device manufacturer provides the option to facilitate the APDU logging in seamless testing (see Table A.2), the monitoring of data transfer seamlessly between ME and nrUSIM can be transferred to the TT to determine if conformance requirements are met.

## D.1 Example of SIM APDU logging via AT interface

In this example, the AT command (enable logging) starts the APDU logging, and AT command (disable logging) stops the APDU logging as defined in TS 27.007 [16]). The APDU data is made available to TT directly or indirectly via the AT interface.

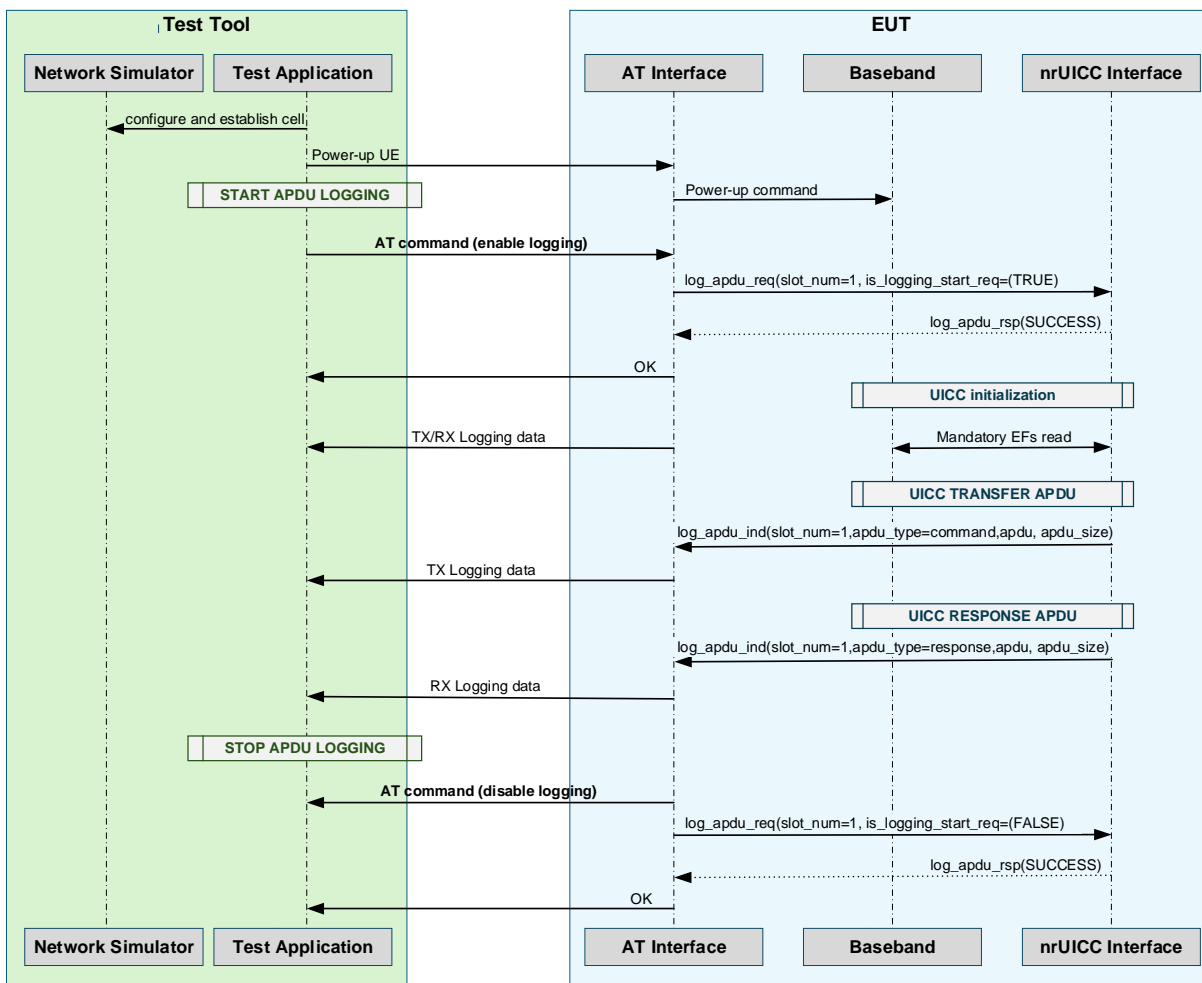


Figure D.1: Example of APDU logging via AT interface

## Annex E (informative): Change history

Date	Meeting	TDoc	CR	Rev	Cat	Subject/Comment	New version
2023-08	CT6#116	C6-230499				Initial version for information	
2023-11	CT6#117	C6-230664				Release candidate	1.1.0
2023-11	CT6#117	C6-230738				Version in CT6 meeting	2.0.0
2023-12	CT#102	CP-233094				Presented for information and approval	2.0.1
2023-12	CT#102					TS approved in TSG#102	17.0.0
2024-03	CT#103	CP-240135	0001	-	F	Correction of codings in the 5G test UICC definitions	17.1.0
2024-03	CT#103	CP-240135	0002	-	F	Addition of test case	17.1.0
2024-03	CT#103	CP-240135	0003	-	F	Insertion of a clause 17 header and correction of TC 17.1.1	17.1.0
2024-06	CT#104	CP-241209	0004	1	F	Correction of PIN handling tests	17.2.0
2024-12	CT#106	CP-243162	0007	2	F	TS 31.127 Annex Z Test toolkit applet requirements	17.3.0
2024-12	CT#106	CP-243163	0008	2	F	TS 31.127 Correction to Test Env in section 4 and Annex A	18.0.0
2025-03	CT#107	CP-250065	0009	-	F	Correction in default value definitions	18.1.0
2025-03	CT#107	CP-250065	0010	-	F	Correction in 15.xA.x test cases	18.1.0
2025-03	CT#107	CP-250065	0011	-	F	Correction to Unified Access Control Testcases 5.4.x	18.1.0
2025-03	CT#107	CP-250065	0012	-	B	Introduction of voice centric support for TS 31.127 5G tests	18.1.0
2025-03	CT#107	CP-250065	0013	-	B	UE recognising the search period of the Higher priority PLMN - NG-RAN	18.1.0
2025-03	CT#107	CP-250065	0014	-	B	Addition of SSIM test cases	18.1.0
2025-03	CT#107	CP-250065	0015	-	F	Correction to EFIMSI in clauses 4.3 and 4.6.x	18.1.0
2025-03	CT#107	CP-250065	0016	-	F	Correction to CSG TC 10.1.8	18.1.0
2025-06	CT#108	CP-251023	0017	-	F	Correction to EFIMSI in clause 4.6.2	18.2.0
2025-06	CT#108	CP-251023	0018	-	F	Correction to EF5GS3GPPLOCI for TC 7.4.7	18.2.0
2025-06	CT#108	CP-251023	0019	-	F	Correction to EFEPSLOCI in clause 4.5.4	18.2.0
2025-06	CT#108	CP-251023	0020	-	F	Correction to EFEPSLOCI for TC 10.1.2	18.2.0
2025-06	CT#108	CP-251023	0021	-	F	Correction to default EF5GS3GPPNSC and EF5GSN3GPPNSC	18.2.0
2025-06	CT#108	CP-251023	0022	-	F	Correction to 5G AKA TC 15.2.5	18.2.0
2025-06	CT#108	CP-251023	0026	-	F	Correction to SUCI calculation TC 5.3.16	18.2.0
2025-06	CT#108	CP-251023	0027	-	D	Change reference from ETSI TS 102 223 to TS 31.111	18.2.0
2025-06	CT#108	CP-251032	0024	3	B	Example test environment for seamless testing	18.2.0
2025-09	CT#109	CP-252019	0028	-	F	Correction to SUCI calculation TC 5.3.17	18.3.0
2025-09	CT#109	CP-252019	0029	-	F	Correction to SUCI calculation TC 5.3.12	18.3.0
2025-09	CT#109	CP-252019	0030	-	F	Correction to UE identification TC 5.3.9	18.3.0
2025-09	CT#109	CP-252019	0031	2	D	Clarification of Coding Conventions	18.3.0
2025-09	CT#109	CP-252026	0032	2	F	Missing figure in Clause D.1	18.3.0
2025-12	CT#110	CP-253177	0033		F	Update to spec reference in clause 2	18.4.0
2025-12	CT#110	CP-253177	0034		F	Align the Mnemonic in Applicability conditions	18.4.0
2025-12	CT#110	CP-253177	0036	1	F	Update to IMS related clauses	18.4.0
2025-12	CT#110	CP-253177	0037		F	Correction to the applicability of TC 5.4.xA	18.4.0
2025-12	CT#110	CP-253177	0038		F	Correction to clause 4.5.6	18.4.0
2025-12	CT#110	CP-253177	0039		F	Correction to the title of TC 5.6.6	18.4.0
2025-12	CT#110	CP-253177	0040		F	Correction to the message direction in CAG TC	18.4.0
2025-12	CT#110	CP-253177	0041		F	Add the title of Annex C	18.4.0
2025-12	CT#110	CP-253177	0042		F	Correction to coding of EFFDN	18.4.0
2025-12	CT#110	CP-253177	0043		F	Correction to UAC TC 5.4.6 and 5.4.7	18.4.0
2026-06	CT#112	CP-261076	0045	1	F	Update to the applicability table	18.5.0

---

## History

<b>Version</b>	<b>Date</b>	<b>Status</b>
V18.0.0	January 2025	Publication
V18.1.0	April 2025	Publication
V18.2.0	June 2025	Publication
V18.3.0	October 2025	Publication
V18.4.0	February 2026	Publication
V18.5.0	July 2026	Publication