

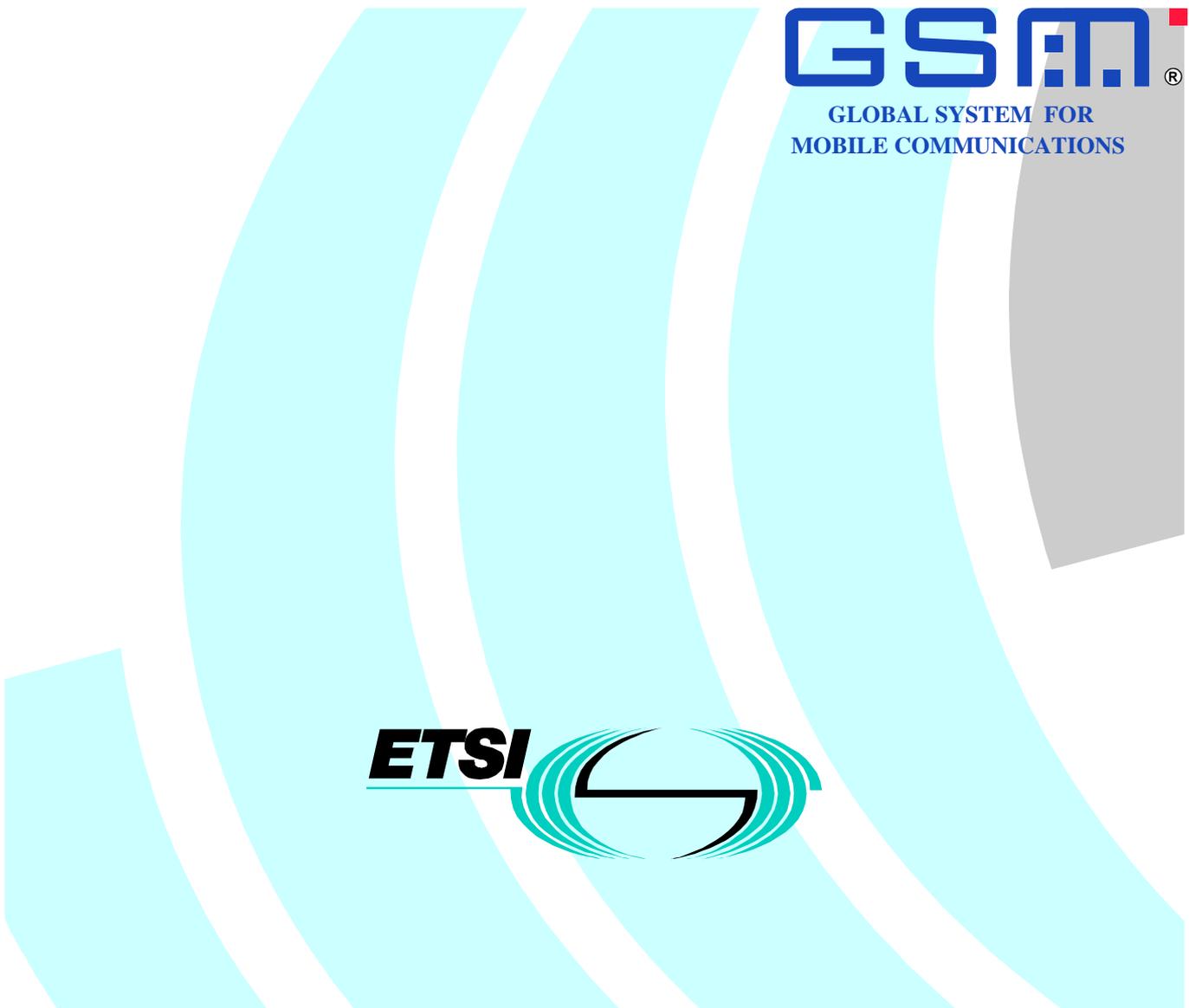
# ETSI EN 301 086 V7.0.2 (1999-12)

---

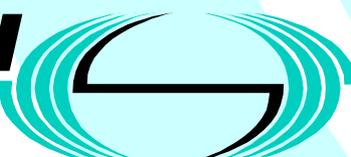
*European Standard (Telecommunications series)*

## **Digital cellular telecommunications system (Phase 2+) Subscriber Identity Module (SIM) conformance test specification (GSM 11.17 version 7.0.2 Release 1998)**

---



**GSM**®  
GLOBAL SYSTEM FOR  
MOBILE COMMUNICATIONS

**ETSI** 

---

Reference

---

DEN/SMG-091117P

Keywords

---

Digital cellular telecommunications system,  
Global System for Mobile communications (GSM)

**ETSI**

Postal address

---

F-06921 Sophia Antipolis Cedex - FRANCE

Office address

---

650 Route des Lucioles - Sophia Antipolis  
Valbonne - FRANCE  
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16  
Siret N° 348 623 562 00017 - NAF 742 C  
Association à but non lucratif enregistrée à la  
Sous-Préfecture de Grasse (06) N° 7803/88

Internet

---

secretariat@etsi.fr  
Individual copies of this ETSI deliverable  
can be downloaded from  
<http://www.etsi.org>  
If you find errors in the present document, send your  
comment to: editor@etsi.fr

**Important notice**

---

This ETSI deliverable may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

**Copyright Notification**

---

No part may be reproduced except as authorized by written permission.  
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 1999.  
All rights reserved.

# Contents

Intellectual Property Rights.....	9
Foreword.....	9
1 Scope.....	10
2 References.....	10
2.1 Normative references.....	10
2.2 Informative references.....	10
3 Definitions and abbreviations.....	11
3.1 Definitions.....	11
3.2 Abbreviations.....	11
4 Test environment.....	12
4.1 Test equipment.....	12
4.1.1 ME simulator.....	12
4.1.2 Signal generation device.....	12
4.1.2.1 VCC.....	12
4.1.2.2 RST.....	12
4.1.2.3 CLK.....	12
4.1.2.4 IO.....	13
4.1.3 Precision force-inducing contacting device.....	13
4.1.4 Temperature controllable environment.....	13
4.1.5 Temperature measuring device.....	13
4.1.6 Voltage measuring device.....	13
4.1.7 Precision measuring device.....	13
4.1.8 Current measuring device.....	13
4.1.9 Timing Measurements on contact IO.....	14
4.2 IUT default conditions.....	14
4.3 Default data formatting.....	14
4.4 Test definition and applicability.....	14
4.5 Test procedure.....	14
4.6 Test requirement.....	15
5 Test Group Hierarchy.....	15
5.1 Test groups under SIM.....	15
5.2 Test groups under PHY.....	16
5.3 Test groups under ELEC.....	16
5.4 Test groups under LOG.....	17
5.5 Test groups under SEC.....	17
5.6 Test groups under FN.....	18
5.7 Test groups under CMD.....	18
5.8 Test groups under CEF.....	18
5.9 Test groups under APP.....	19
6 Test Procedure.....	19
6.1 Physical characteristics.....	19
6.1.1 Format and layout.....	19
6.1.1.1 ID-1 SIM.....	19
6.1.1.1.1 Definition and applicability.....	19
6.1.1.1.2 Conformance requirement.....	19
6.1.1.1.3 Test purpose.....	20
6.1.1.1.4 Method of test.....	20
6.1.1.2 Plug-in SIM.....	20
6.1.1.2.1 Definition and applicability.....	20
6.1.1.2.2 Conformance requirement.....	20
6.1.1.2.3 Test purpose.....	21
6.1.1.2.4 Method of test.....	21

6.1.2	Temperature range for card operation.....	21
6.1.2.1	Definition and applicability.....	21
6.1.2.2	Conformance requirement.....	22
6.1.2.3	Test purpose.....	22
6.1.2.4	Method of test.....	22
6.1.3	Contacts.....	23
6.1.3.1	Definition and applicability.....	23
6.1.3.2	Conformance requirement.....	23
6.1.3.3	Test purpose.....	23
6.1.3.4	Method of test.....	23
6.2	Electronic signals and transmission protocols.....	23
6.2.1	Supply voltage Vcc (contact C1).....	24
6.2.1.1	Voltage limits.....	24
6.2.1.1.1	Definition and applicability.....	24
6.2.1.1.2	Conformance requirement.....	24
6.2.1.1.3	Test purpose.....	24
6.2.1.1.4	Method of test.....	24
6.2.1.2	Current limits.....	25
6.2.1.2.1	Definition and applicability.....	25
6.2.1.2.2	Conformance requirement.....	25
6.2.1.2.3	Test purpose.....	25
6.2.1.2.4	Method of test.....	25
6.2.1.3	Idle current limits.....	26
6.2.1.3.1	Definition and applicability.....	26
6.2.1.3.2	Conformance requirement.....	26
6.2.1.3.3	Test purpose.....	27
6.2.1.3.4	Method of test.....	27
6.2.1.3.5	Test requirement.....	27
6.2.1.4	Current limits at all frequencies.....	27
6.2.1.4.1	Definition and applicability.....	27
6.2.1.4.2	Conformance requirement.....	27
6.2.1.4.3	Test purpose.....	28
6.2.1.4.4	Method of test.....	28
6.2.1.5	Current limits in clk-stop-mode.....	28
6.2.1.5.1	Definition and applicability.....	28
6.2.1.5.2	Conformance requirement.....	28
6.2.1.5.3	Test purpose.....	29
6.2.1.5.4	Method of test.....	29
6.2.2	Reset RST (contact C2).....	29
6.2.2.1	Static operation.....	29
6.2.2.1.1	Definition and applicability.....	29
6.2.2.1.2	Conformance requirement.....	29
6.2.2.1.3	Test purpose.....	29
6.2.2.1.4	Method of test.....	30
6.2.3	Clock CLK (contact C3).....	30
6.2.3.1	Frequency and duty cycle.....	30
6.2.3.1.1	Definition and applicability.....	30
6.2.3.1.2	Conformance requirement.....	30
6.2.3.1.3	Test purpose.....	31
6.2.3.1.4	Method of test.....	31
6.2.3.2	Voltage and current.....	32
6.2.3.2.1	Definition and applicability.....	32
6.2.3.2.2	Conformance requirement.....	32
6.2.3.2.3	Test purpose.....	32
6.2.3.2.4	Method of test.....	32
6.2.4	I/O (contact C7).....	33
6.2.4.1	Voltage and current.....	33
6.2.4.1.1	Definition and applicability.....	33
6.2.4.1.2	Conformance requirement.....	33
6.2.4.1.3	Test purpose.....	33

6.2.4.1.4	Method of test.....	34
6.2.5	States.....	34
6.2.5.1	Definition and applicability.....	34
6.2.5.2	Conformance requirement.....	34
6.2.5.3	Test purpose.....	35
6.2.5.4	Method of test.....	35
6.2.6	Answer To Reset (ATR).....	36
6.2.6.1	ATR content.....	36
6.2.6.1.1	Definition and applicability.....	36
6.2.6.1.2	Conformance requirement.....	36
6.2.6.1.3	Test purpose.....	36
6.2.6.1.4	Method of test.....	36
6.2.6.2	PTS procedure.....	37
6.2.6.2.1	Definition and applicability.....	37
6.2.6.2.2	Conformance requirement.....	37
6.2.6.2.3	Test purpose.....	37
6.2.6.2.4	Method of test.....	38
6.2.7	Major Capabilities.....	38
6.2.7.1	Definition and applicability.....	38
6.2.7.2	Conformance requirement.....	38
6.2.7.3	Test purpose.....	38
6.2.7.4	Method of test.....	38
6.2.7.5	Test requirement.....	38
6.3	Logical Model.....	39
6.3.1	File identifier.....	39
6.3.1.1	File-type identification.....	39
6.3.1.1.1	Definition and applicability.....	39
6.3.1.1.2	Conformance requirement.....	39
6.3.1.1.3	Test purpose.....	39
6.3.1.1.4	Method of test.....	39
6.3.1.2	File ID assignments.....	40
6.3.1.2.1	Definition and applicability.....	40
6.3.1.2.2	Conformance requirement.....	40
6.3.1.2.3	Test purpose.....	40
6.3.1.2.4	Method of test.....	40
6.3.1.2.5	Test requirement.....	40
6.3.2	Dedicated files.....	40
6.3.2.1	Definition and applicability.....	40
6.3.2.2	Conformance requirement.....	40
6.3.2.3	Test purpose.....	41
6.3.2.4	Method of test.....	41
6.3.3	Elementary files.....	41
6.3.3.1	Definition and applicability.....	41
6.3.3.2	Conformance requirement.....	41
6.3.3.3	Test purpose.....	41
6.3.3.4	Method of test.....	42
6.3.4	Methods for selecting a file.....	42
6.3.4.1	Definition and applicability.....	42
6.3.4.2	Conformance requirement.....	42
6.3.4.3	Test purpose.....	43
6.3.4.4	Method of test.....	43
6.3.5	Reservation of file IDs.....	44
6.3.5.1	Definition and applicability.....	44
6.3.5.2	Conformance requirement.....	44
6.3.5.3	Test purpose.....	44
6.3.5.4	Method of test.....	45
6.4	Security features.....	45
6.4.1	Authentication and cipher key generation procedure.....	45
6.4.2	File access conditions.....	45
6.4.2.1	Definition and applicability.....	45

6.4.2.2	Conformance requirement .....	45
6.4.2.3	Test purpose .....	46
6.4.2.4	Method of test .....	46
6.5	Description of the functions.....	46
6.5.1	SELECT function .....	47
6.5.1.1	Definition and applicability.....	47
6.5.1.2	Conformance requirement.....	47
6.5.1.3	Test purpose .....	47
6.5.1.4	Method of test .....	47
6.5.2	STATUS function.....	49
6.5.2.1	Definition and applicability.....	49
6.5.2.2	Conformance requirement.....	49
6.5.2.3	Test purpose .....	49
6.5.2.4	Method of test .....	49
6.5.3	READ BINARY function.....	50
6.5.3.1	Definition and applicability.....	50
6.5.3.2	Conformance requirement.....	51
6.5.3.3	Test purpose .....	51
6.5.3.4	Method of test .....	51
6.5.4	UPDATE BINARY function.....	52
6.5.4.1	Definition and applicability.....	52
6.5.4.2	Conformance requirement.....	52
6.5.4.3	Test purpose .....	52
6.5.4.4	Method of test .....	52
6.5.5	READ RECORD function.....	53
6.5.5.1	Definition and applicability.....	53
6.5.5.2	Conformance requirement.....	53
6.5.5.3	Test purpose .....	54
6.5.5.4	Method of test .....	54
6.5.6	UPDATE RECORD function.....	56
6.5.6.1	Definition and applicability.....	56
6.5.6.2	Conformance requirement.....	56
6.5.6.3	Test purpose .....	57
6.5.6.4	Method of test .....	57
6.5.7	SEEK function.....	60
6.5.7.1	Definition and applicability.....	60
6.5.7.2	Conformance requirement.....	60
6.5.7.3	Test purpose .....	61
6.5.7.4	Method of test .....	61
6.5.8	INCREASE function.....	63
6.5.8.1	Definition and applicability.....	63
6.5.8.2	Conformance requirement.....	63
6.5.8.3	Test purpose .....	63
6.5.8.4	Method of test .....	63
6.5.9	VERIFY CHV function.....	64
6.5.9.1	Definition and applicability.....	64
6.5.9.2	Conformance requirement.....	64
6.5.9.3	Test purpose .....	65
6.5.10	CHANGE CHV function.....	66
6.5.10.1	Definition and applicability.....	66
6.5.10.2	Conformance requirement.....	66
6.5.10.3	Test purpose .....	67
6.5.10.4	Method of test .....	67
6.5.11	DISABLE CHV function.....	68
6.5.11.1	Definition and applicability.....	68
6.5.11.2	Conformance requirement.....	68
6.5.11.3	Test purpose .....	69
6.5.11.4	Method of test .....	69
6.5.12	ENABLE CHV function.....	70
6.5.12.1	Definition and applicability.....	70

6.5.12.2	Conformance requirement .....	70
6.5.12.3	Test purpose .....	70
6.5.12.4	Method of test .....	70
6.5.13	UNBLOCK CHV function.....	72
6.5.13.1	Definition and applicability.....	72
6.5.13.2	Conformance requirement .....	72
6.5.13.3	Test purpose .....	72
6.5.13.4	Method of test .....	73
6.5.14	INVALIDATE function.....	74
6.5.14.1	Definition and applicability.....	74
6.5.14.2	Conformance requirement .....	74
6.5.14.3	Test purpose .....	74
6.5.14.4	Method of test .....	74
6.5.15	REHABILITATE function .....	75
6.5.15.1	Definition and applicability.....	75
6.5.15.2	Conformance requirement .....	75
6.5.15.3	Test purpose .....	76
6.5.15.4	Method of test .....	76
6.5.16	RUN GSM ALGORITHM function .....	76
6.5.16.1	Definition and applicability.....	76
6.5.16.2	Conformance requirement .....	77
6.5.16.3	Test purpose .....	77
6.5.16.4	Method of test .....	77
6.5.17	SLEEP function .....	78
6.5.17.1	Definition and applicability.....	78
6.5.17.2	Conformance requirement .....	78
6.5.17.3	Test purpose .....	78
6.5.17.4	Method of test .....	78
6.6	Description of the commands .....	78
6.6.1	Mapping principles .....	78
6.6.1.1	Definition and applicability.....	78
6.6.1.2	Conformance requirement .....	78
6.6.1.3	Test purpose .....	79
6.6.1.4	Method of test .....	79
6.6.2	Coding of the commands .....	79
6.6.2.1	SELECT command .....	80
6.6.2.2	STATUS command .....	80
6.6.2.3	READ BINARY command .....	80
6.6.2.4	UPDATE BINARY command .....	80
6.6.2.5	READ RECORD command .....	80
6.6.2.6	UPDATE RECORD command .....	80
6.6.2.7	SEEK command .....	80
6.6.2.8	INCREASE command.....	80
6.6.2.9	VERIFY CHV command .....	80
6.6.2.10	CHANGE CHV command .....	80
6.6.2.11	DISABLE CHV command .....	80
6.6.2.12	ENABLE CHV command .....	81
6.6.2.13	UNBLOCK CHV command.....	81
6.6.2.14	INVALIDATE command.....	81
6.6.2.15	REHABILITATE command .....	81
6.6.2.16	RUN GSM ALGORITHM command .....	81
6.6.2.17	SLEEP command .....	81
6.6.2.18	GET RESPONSE command .....	81
6.6.2.18.1	Definition and applicability .....	81
6.6.2.18.2	Conformance requirement .....	81
6.6.2.18.3	Test purpose .....	81
6.6.2.18.4	Method of test.....	82
6.6.3	Definitions and coding.....	82
6.6.3.1	Definition and applicability.....	82
6.6.3.2	Conformance requirement .....	82

6.6.3.3 Test purpose .....82

6.6.3.4 Method of test .....82

6.6.4 Status conditions returned by the SIM .....83

6.6.4.1 Coding of the status words .....83

6.6.4.1.1 Definition and applicability .....83

6.6.4.1.2 Conformance requirement .....83

6.6.4.1.3 Test purpose .....83

6.6.4.1.4 Method of test.....83

6.6.4.2 Commands versus possible status responses .....85

6.6.4.2.1 Definition and applicability .....85

6.6.4.2.2 Conformance requirement .....85

6.6.4.2.3 Test purpose .....85

6.6.4.2.4 Method of test.....85

6.6.4.2.5 Test requirement .....85

6.7 Contents of the elementary files .....85

6.7.1 Definition and applicability .....85

6.7.2 Conformance requirement.....86

6.7.3 Test purpose.....86

6.7.4 Method of test.....86

6.8 Application Protocol.....87

6.8.1 FDN Procedure .....87

6.8.1.1 Definition and applicability.....87

6.8.1.2 Conformance requirement.....87

6.8.1.3 Test purpose .....87

6.8.1.4 Method of test .....87

**Annex A (informative): Change history .....90**

History .....91

---

## Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in 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 Web server (<http://www.etsi.org/ipr>).

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

---

## Foreword

This European Standard (Telecommunications series) has been produced by Special Mobile Group (SMG).

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

Version 7.x.y

where:

- 7 indicates GSM Release 1998 of Phase 2+
- x the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- y the third digit is incremented when editorial only changes have been incorporated in the specification

<b>National transposition dates</b>	
Date of adoption of this EN:	3 December 1999
Date of latest announcement of this EN (doa):	31 March 2000
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	30 September 2000
Date of withdrawal of any conflicting National Standard (dow):	30 September 2000

---

# 1 Scope

The present document provides the Conformance Test Specification for the Subscriber Identity Module defined in GSM 11.11 [1], GSM 11.12 [9] and GSM 11.18 [10].

---

## 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.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.
- For this Release 1998 document, references to GSM documents are for Release 1998 versions (version 7.x.y).

### 2.1 Normative references

- [1] GSM 11.11: "Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".
- [2] not used
- [3] ISO/IEC 7816-1 (1987): "Identification cards - Integrated circuit(s) cards with contacts, Part 1: Physical characteristics".
- [5] ISO/IEC 7816-2 (1988): "Identification cards - Integrated circuit(s) cards with contacts, Part 1: Dimensions and locations of the contacts".
- [6] ISO/IEC 7816-3 (1989): "Identification cards - Integrated circuit(s) cards with contacts, Part 1: Electronic signals and transmission protocols."
- [7] ISO/IEC 7811-1 (1995): "Identification cards - Recording technique - Part 1: Embossing"
- [8] ISO/IEC 7811-3 (1995): "Identification cards - Recording technique - Part 3: Location of embossed characters on ID-1 cards"
- [9] GSM 11.12: "Digital cellular telecommunications system (Phase 2); Specification of the 3 Volt Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".
- [10] GSM 11.18: "Digital cellular telecommunications system (Phase 2+); Specification of the 1.8 Volt Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

### 2.2 Informative references

All test cases included in GSM 11.17 are based on phase 2, except 1.8V electrical tests which are a phase 2+ feature. Enhancements will be done time by time.

---

## 3 Definitions and abbreviations

### 3.1 Definitions

For the purposes of the present document, the following terms and definitions apply in addition to the terms defined in GSM 11.11 [1];

**Implementation Conformance Statement (ICS):** A statement made by the supplier of an implementation or system claimed to conform to a given specification, stating which capabilities have been implemented. The ICS can take several forms: protocol ICS, profile ICS, profile specific ICS, information object ICS, etc.

**ICS proforma:** A document, in the form of a questionnaire, which when completed for an implementation or system becomes an ICS.

### 3.2 Abbreviations

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

CRn	Conformance Requirement 'n'
SIM	Subscriber Identity Module
ETS	European Telecommunication Standard
ICS	Implementation Conformance Statement
IUT	Implementation Under Test
FT	Fixed Termination
ME	Mobile Equipment
MS	Mobile Station
TS	Test Specification

---

## 4 Test environment

This clause specifies several requirements which shall be met, and a number of rules which shall be adhered to before testing can proceed.

### 4.1 Test equipment

This subclause recommends a minimum specification for each of the items of test equipment referenced in the tests.

#### 4.1.1 ME simulator

This item of equipment shall allow T=0 protocol communications to take place on both ID-1 and plug-in SIM cards. It shall be able to generate and send any command APDU and receive any of the possible responses. These commands may be generated manually, one at a time, or automatically from a predefined batch procedure containing one or more commands.

The ME simulator shall be able to support clock stop modes.

The ME simulator shall be able to accept an external clock signal to drive CLK (contact C3) of the SIM.

It shall be possible to access all the SIM contacts either directly or through test points.

#### 4.1.2 Signal generation device

##### 4.1.2.1 VCC

The voltage level for VCC (contact C1) of the SIM shall be adjustable between -0,5V and 6.0V to an accuracy of 1% of the nominal VCC voltage (e.g. 50mV for a 5V card).

The ME simulator shall be able to source current on the VCC contact in the range -2mA to 12mA statically and to deliver charges of > 400nAs without lowering the VCC-voltage for more than 10% of VCC nom.

##### 4.1.2.2 RST

The generated voltage level for RST (contact C2) of the SIM shall be adjustable between -0,5V and 6.0V to an accuracy of 50mV.

The rise and fall times shall be adjustable from 0 to 500 us with an accuracy of 5us. (*to check if the SIM works with the defined rise and fall times.*)

The beginning of the rising edge is programmable from 1 clk-cycle to 50000 clk-cycles after enabling the clk-line.

##### 4.1.2.3 CLK

This item of equipment shall be able to generate square wave signals for the clock on the SIM, any of which can be a single-shot or continuous signal, in the range 1MHz to 5MHz. The voltage levels for both high and low states shall be adjustable between -0,5V and 6,0V to an accuracy of 0,1V. The duty cycle of the clock signal shall be adjustable between 40% and 60% to an accuracy of 1%. It shall also provide control over the following parameters:

The voltage levels for both high and low states shall be adjustable between 0V and 6V to an accuracy of 1% of the nominal VCC voltage. The duty cycle of the clock signal shall be adjustable between 40% and 60% to an accuracy of 1% or 5ns whichever is the worst.

It shall also provide control over the following parameters:

- rise and fall time to an accuracy of 1% or 5ns whichever is the worst. ( $5ns = 2,5\% \text{ accuracy for } f_{max} = 5MHz$ ).

#### 4.1.2.4 IO

The equipment shall be able to generate IO-Signals according to 11.11

The voltage levels for high and low states shall be adjustable between -0,5V and 6V to an accuracy of 1% of the nominal VCC voltage. The IO line in transmission mode (high bit) shall be programmable between state A (active driven output) and state Z (IO-voltage-driver inactive, current source I-IO-high active).

It shall also provide control over the rise and fall time of 100ns to 1000ns with an accuracy of 50ns.

The ME simulator shall be able to source and sink currents on the IO contact in the range -20 to + 20uA in state high and 0 - -1mA in state low (receiving mode) and shall be able to switch in transmission mode (outputting a high Bit) between voltage and current driving mode.

The timing of the bitstream (jitter, guardtime, etu-value, etc.) on the IO-Line shall be programmable with an accuracy of  $\leq 0,01\text{etu}$  or  $2\text{clk-cycles}$  whichever is the worst.

#### 4.1.3 Precision force-inducing contacting device

This item of equipment shall be able to apply a prescribed and maintained level of force onto one or more contacts of a SIM. The range shall be between 0 and 0,5N and accurate to 0,01N.

#### 4.1.4 Temperature controllable environment

This item of equipment shall be able to control the temperature of a chamber large enough to enclose a SIM and card reader. The range of temperature control shall be between -25°C and +85°C to an accuracy of 0,5°C.

#### 4.1.5 Temperature measuring device

This item of equipment shall be able to measure the temperature of the SIM to within 0,5°C. The range of this device shall allow measurement of temperatures between -25°C and +85°C.

#### 4.1.6 Voltage measuring device

This item of equipment shall be able to measure static and transient voltages on any one of the contacts of the SIM. The measurable voltage range shall be between -2 and +7V to an accuracy of 1% of the nom. VCC voltage (e.g. 30mV for 3V cards) with a timebase accuracy of 25ns.

#### 4.1.7 Precision measuring device

This item of equipment shall be able to measure both linear and radius of curvature dimensions to an accuracy of 0,01mm.

#### 4.1.8 Current measuring device

This item of equipment shall be able to supervise the current levels for any one of the contacts of the SIM.

The Simulator shall be able to detect an over- or underload with a time resolution of  $\leq 100\text{ns}$ .

Channel	Minimum	Maximum	Resolution
VCC high	-2mA	+12,5mA	125uA
VCC high	-2mA	+12,5mA	125uA
VCC Burst	12mA	+250mA	2,5mA
RST/CLK high state	-50uA	+50 uA	1uA
RST/CLK low state	-250 uA	+250 uA	2,5uA
IO high state	-50 uA	+50 uA	1uA
IO low state	-1500	+1500 uA	15uA

### 4.1.9 Timing Measurements on contact IO

To verify the timing of the IO transmission from the SIM the ME Simulator shall be able to measure the IO-Bit-Timing in CLK-Cycles with an accuracy of  $\leq 0,01\text{etu}$  or  $2\text{clk-cycles}$  whichever is the worst.

## 4.2 IUT default conditions

Unless otherwise stated, the following is default:

- The voltage level for VCC (contact C1) is set to 5,0V.
- The voltage levels for CLK (contact C3) are set to 0V and 5,0V for low and high respectively.
- The clock frequency CLK (contact C3) is set to 5MHz with duty cycle 50%.
- The ME simulator generated low transmission voltage level for I/O (contact C7) is set to 0V and the current sources for high transmission and reception are set to  $\pm 20\text{uA}$  respectively
- CHV1 on the SIM is enabled and three VERIFY CHV1 attempts and ten UNBLOCK CHV1 attempts remain.
- Three VERIFY CHV2 attempts and ten UNBLOCK CHV2 attempts remain for CHV2.

## 4.3 Default data formatting

All numeric data enclosed in single quotes ( ' ) in the present document are hexadecimal data.

Where 'X' is used in place of a hexadecimal digit, X ranges from '0' to 'F'. For example, the data '6X' ranges from '60' to '6F' inclusive.

Where data is expressed as a group of bytes, it shall be in the following format: 'XX XX XX... XX', indicating first byte, second byte, third byte etc. in that order.

## 4.4 Test definition and applicability

The following statements are applicable to the Test definition and applicability clause for all test purposes contained within the present document:

- Unless otherwise stated, tests apply to both plug-in and ID-1 SIM cards.

## 4.5 Test procedure

The following statements are applicable to the Test Procedure clause for all test purposes contained within the present document:

- Unless otherwise stated, all steps with the test procedure are to be carried out in order.

- Where steps indicate that an ME simulator shall select a particular DF or EF using an unspecified number of SELECT commands, the ME simulator is to send the correct sequence of SELECT commands in order to select the required file ID from the current file ID (this may be achieved most easily by selecting from the MF down each time).
- Unless otherwise stated, the length (P3) for all READ RECORD and UPDATE RECORD commands sent by the ME simulator is to be that of the record length of the EF currently selected. In the case where an EF is not currently selected, the length sent is to be 1 unless otherwise stated.
- Unless otherwise stated, the offset for all READ BINARY and UPDATE BINARY commands sent by the ME simulator is to be '00 00'.
- Unless otherwise stated, the length (P3) for all STATUS and GET RESPONSE commands sent by the ME simulator is to be such that all available data is read.
- Unless otherwise stated, the CHV and UNBLOCK CHV presented for VERIFY CHV, CHANGE CHV, DISABLE CHV, ENABLE CHV and UNBLOCK CHV commands sent by the ME simulator is to be correct.
- Unless otherwise stated, the "CHV No." (P2) for VERIFY CHV, CHANGE CHV, DISABLE CHV, ENABLE CHV and UNBLOCK CHV commands sent by the ME simulator is to be 1.

### 4.6 Test requirement

Where steps within a test procedure involve an ME simulator sending one or more commands to the SIM, these commands are required to be correctly executed, with the SIM responding with status conditions of '90 00' or '9F XX', unless otherwise stated in the Test Requirements subclause for the test.

## 5 Test Group Hierarchy

This clause contains the Test Group Hierarchy diagrams which provide a structure for the test purposes and also a correlation between the base specification, ICS and this Test Specification.

The information contained in each node for each of the diagrams is as follows:

mnemonic for test group
reference to clause in TS

As the Test Group Hierarchy for the SIM is large, it has been broken into sections to aid presentation.

### 5.1 Test groups under SIM

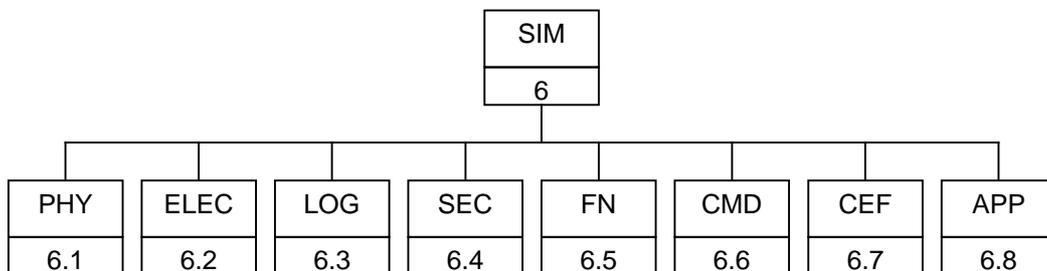


Figure 1: Top Level Test Group Hierarchy

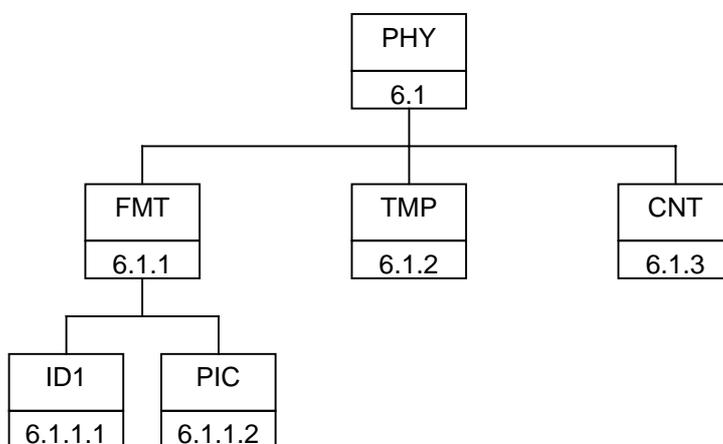
The mnemonics chosen for this test group are as follows:

- PHY: Physical characteristics - GSM 11.11 [1], clause 4
- ELEC: Electronic signals and transmission protocols - GSM 11.11 [1], clause 5

- LOG: Logical Model - GSM 11.11 [1], clause 6
- SEC: Security features - GSM 11.11 [1], clause 7
- FN: Description of the functions - GSM 11.11 [1], clause 8
- CMD: Description of the commands - GSM 11.11 [1], clause 9
- CEF: Contents of the elementary files - GSM 11.11 [1], clause 10
- APP: Application Protocol - GSM 11.11 [1], clause 11

The Test Groups "PHY", "ELEC", "LOG", "SEC", "CMD", "CEF" and "APP", shown in figure 1, are broken down further, as shown in the following diagrams.

## 5.2 Test groups under PHY

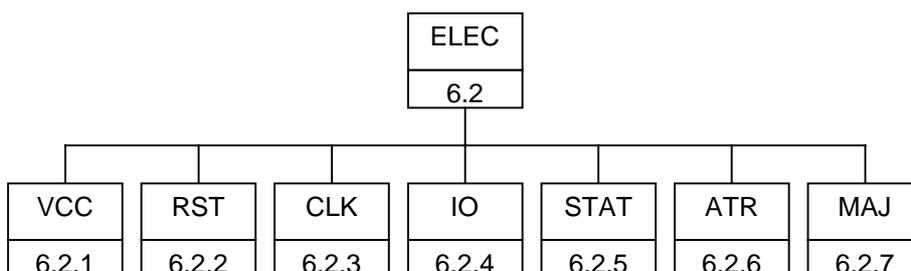


**Figure 2: Breakdown of "PHY" Test Group**

The mnemonics chosen for this test group are as follows:

- FMT: Format and layout - GSM 11.11 [1], subclause 4.1
- ID1: ID-1 card - GSM 11.11 [1], subclause 4.1.1
- PIC: Plug-in card - GSM 11.11 [1], subclause 4.1.2
- TMP: Temperature range for card operation - GSM 11.11 [1], subclause 4.2
- CNT: Contacts - GSM 11.11 [1], subclause 4.3

## 5.3 Test groups under ELEC

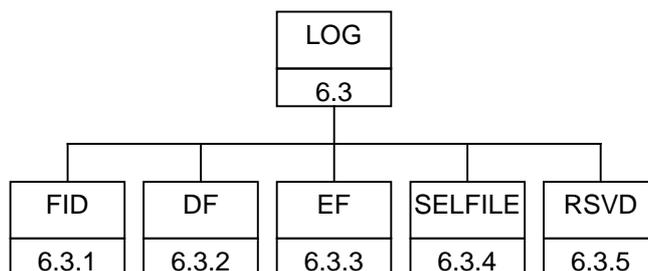


**Figure 3: Breakdown of "ELEC" Test Group**

The mnemonics chosen for this test group are as follows:

- VCC: Supply voltage Vcc (contact C1) - GSM 11.11 [1], subclause 5.1
- RST: Reset RST (contact C2) - GSM 11.11 [1], subclause 5.2
- CLK: Clock CLK (contact C3) - GSM 11.11 [1], subclause 5.4
- IO: I/O (contact C7) - GSM 11.11 [1], subclause 5.5
- STAT: States - GSM 11.11 [1], subclause 5.6
- ATR: Answer To Reset (ATR) - GSM 11.11 [1], subclause 5.8
- MAJ: Major Capabilities - GSM 11.11 [1], subclause 5, 5.7, 5.9, 5.10

## 5.4 Test groups under LOG

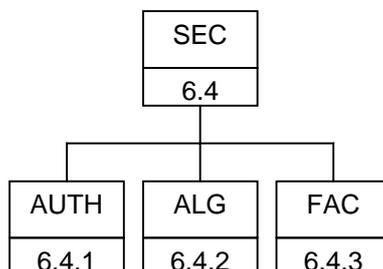


**Figure 4: Breakdown of "LOG" Test Group**

The mnemonics chosen for this test group are as follows:

- FID: File identifier - GSM 11.11 [1], subclause 6.2
- DF: Dedicated Files - GSM 11.11 [1], subclause 6.3
- EF: Elementary Files - GSM 11.11 [1], subclause 6.4
- SELFILE: Methods for selecting a file - GSM 11.11 [1], subclause 6.5
- RSVD: Reservation of file IDs - GSM 11.11 [1], subclause 6.6

## 5.5 Test groups under SEC

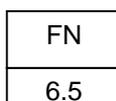


**Figure 5: Breakdown of "SEC" Test Group**

The mnemonics chosen for this test group are as follows:

- AUTH: Authentication and cipher key generation procedures - GSM 11.11 [1], subclause 7.1
- ALG: Algorithms and processes - GSM 11.11 [1], subclause 7.2
- FAC: File access conditions - GSM 11.11 [1], subclause 7.3

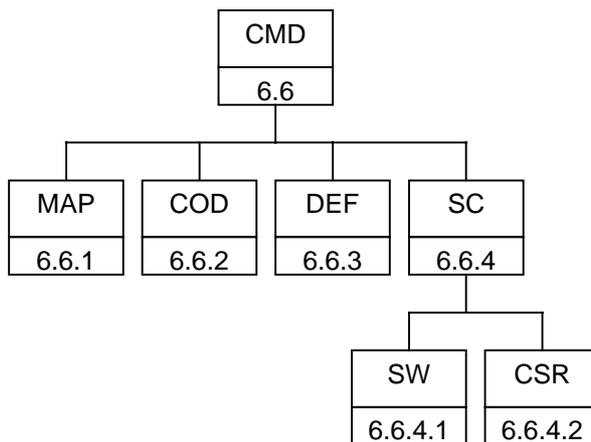
## 5.6 Test groups under FN



**Figure 6: Breakdown of "FN" Test Group**

All of the tests in the "FN" test group relate to GSM 11.11 [1], clause 8.

## 5.7 Test groups under CMD

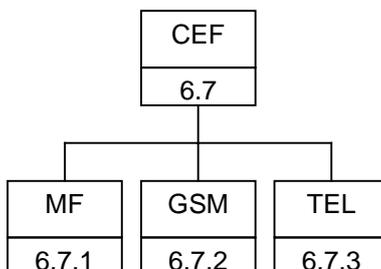


**Figure 7: Breakdown of "CMD" Test Group**

The mnemonics chosen for this test group are as follows:

- MAP: Mapping principles - GSM 11.11 [1], subclause 9.1
- COD: Coding of the commands - GSM 11.11 [1], subclause 9.2
- DEF: Definitions and coding - GSM 11.11 [1], subclause 9.3
- SC: Status conditions returned by the SIM - GSM 11.11 [1], subclause 9.4
- SW: Coding of the status words- GSM 11.11 [1], subclause 9.4.1-5
- CSR: Commands versus possible status responses - GSM 11.11 [1], subclause 9.4.6

## 5.8 Test groups under CEF



**Figure 8: Breakdown of "CEF" Test Group**

The mnemonics chosen for this test group are as follows:

- MF: Contents of the EFs at the MF level - GSM 11.11 [1], subclause 10.1

- GSM: Contents of EFs at the GSM application level - GSM 11.11 [1], subclause 10.2
- TEL: Contents of the EFs at the Telecom level - GSM 11.11 [1], subclause 10.3

## 5.9 Test groups under APP

[TBD]

**Figure 9: Breakdown of "APP" Test Group**

All of the tests in the "APP" test group relate to GSM 11.11 [1], clause 11.

---

# 6 Test Procedure

This clause details each of the tests in each of the test groups within the Test Group Hierarchy. This test suite allows testing of the IUT against the base specification with respect to:

- Physical characteristics
- Electronic signals and transmission protocols
- Logical model
- Security services and facilities
- Functions
- Commands
- Contents of the elementary files

The numbering of this clause correlates with the numbering of the accompanying ICS to allow for referencing between the documents.

## 6.1 Physical characteristics

The tests in this subclause ensure that the IUT conforms to the specification for both format and layout and contacts.

### 6.1.1 Format and layout

#### 6.1.1.1 ID-1 SIM

##### 6.1.1.1.1 Definition and applicability

The format and layout characteristics shall be adhered to, in order to ensure proper operation in the GSM environment.

This test applies to ID-1 SIM cards.

Currents defined as positive are flowing into the SIM

Voltages declared as  $V_O$  are delivered by the ME (ME Simulator)  $V_I$  is generated by the SIM

##### 6.1.1.1.2 Conformance requirement

CR1 Format and layout of the ID-1 card shall be in accordance with ISO 7816-1,2, unless otherwise specified.

CR2 The information on the exterior of the ID-1 SIM card shall include at least the individual account identifier and the check digit.

CR3 The card may have a polarisation mark which indicates how the user should insert the card into the ME.

CR4 Any embossing on the card shall be in accordance with ISO 7811-1,3 (conditional).

CR5 The contacts shall be located on the front (embossed face) of the card.

Reference: GSM 11.11 [1], clause 4, and subclauses 4.1, 4.1.1.

Test Group Reference (TGR): TGR\_SIM\_PHY\_FMT\_ID1

Test Procedure Reference (TPR): TPR\_SIM\_PHY\_FMT\_ID1

#### 6.1.1.1.3 Test purpose

To verify that the SIM conforms to the above requirements.

NOTE 1: The testing of CR1 is outside the scope of the present document. Please refer to the TS for ISO/IEC 7816-1,2.

NOTE 2: The testing of CR4 is outside the scope of the present document. Please refer to the TS for ISO 7811-1,3.

#### 6.1.1.1.4 Method of test

##### Initial conditions

None.

##### Test procedure

- a) The card is examined for the following:
- identification number,
  - polarisation mark,
  - contact location.

*The card shall have been observed to exhibit the following [CR2,3]:*

- identification number located on the exterior of the card,
- polarisation mark indicating how the user should insert the card into the ME,
- contact location on the front or the back of the card.

- b) The SIM is connected to an ME simulator.
- c) The ME simulator resets the SIM.
- d) The ME simulator sends a SELECT command to the SIM to select EF<sub>ICCID</sub>.
- e) The ME simulator sends a READ BINARY command to the SIM to read the identification number.

*The individual account identifier read from the SIM shall be identical with that on the exterior of the card [CR2].*

#### 6.1.1.2 Plug-in SIM

##### 6.1.1.2.1 Definition and applicability

The format and layout characteristics shall be adhered to, in order to ensure proper operation in the GSM environment.

This test applies to plug-in SIM cards.

##### 6.1.1.2.2 Conformance requirement

CR1 Format and layout of the plug-in card shall be in accordance with ISO 7816-1,2, unless otherwise specified. CR2 The information on the exterior of the plug-in card shall include at least the individual account identifier and the check digit.

CR3 The dimensions of the plug-in SIM shall be in accordance with Annex A of GSM 11.11 [1].

Reference: GSM 11.11 [1], clause 4, and subclauses 4.1, 4.1.2.

Test Group Reference (TGR): TGR\_SIM\_PHY\_FMT\_PIC

Test Procedure Reference (TPR): TPR\_SIM\_PHY\_FMT\_PIC

#### 6.1.1.2.3 Test purpose

To verify that the SIM conforms to the above requirements.

NOTE 1: The testing of CR1 is outside the scope of the present document. Please refer to the TS for ISO/IEC 7816-1,2.

#### 6.1.1.2.4 Method of test

##### **Initial conditions**

None.

##### **Test procedure**

- a) The card is examined for the following:
- individual account identifier and check digit,
  - width,
  - height,
  - thickness,
  - feature for orientation.

The card shall have been observed to exhibit the following [CR2]:

- at least the individual account identifier and check digit located on the exterior of the card,
  - correct width, height and thickness,
  - feature for orientation.
- b) The SIM is connected to an ME simulator.
- c) The ME simulator resets the SIM.
- d) The ME simulator sends a SELECT command to the SIM to select EF<sub>ICCID</sub>.
- e) The ME simulator sends a READ BINARY command to the SIM to read the identification number.

*The account identifier and check digit read from the SIM shall be present and identical with that on the exterior of the card [CR2]*

## 6.1.2 Temperature range for card operation

### 6.1.2.1 Definition and applicability

The temperature range for full operational use shall be adhered to, in order to ensure proper operation in the GSM environment.

### 6.1.2.2 Conformance requirement

CR1 The temperature range for full operational use shall be between  $-25^{\circ}\text{C}$  and  $+70^{\circ}\text{C}$  with occasional peaks of up to  $+85^{\circ}\text{C}$ , where "occasional" means not more than 4 hours each time and not over 100 times during the life time of the card.

Reference: GSM 11.11 [1], subclause 4.2.

Test Group Reference (TGR): TGR\_SIM\_PHY\_TMP

Test Procedure Reference (TPR): TPR\_SIM\_PHY\_TMP

### 6.1.2.3 Test purpose

To verify that the SIM conforms to the above requirements.

### 6.1.2.4 Method of test

#### Initial conditions

- 1) The SIM is placed in a temperature-controllable environment and connected to an ME simulator.
- 2) A temperature measuring device is connected to the surface of the SIM.
- 3) The SIM shall have passed the Format and Layout tests in subclause 6.1.1.

#### Test procedure

- a) The temperature of the SIM is set to  $+25^{\circ}\text{C}$ .
- b) The ME simulator resets the SIM.
- c) The ME simulator performs the SIM initialisation procedure, as defined in GSM 11.11 [1], subclause 11.2.1.

*The SIM shall operate successfully [CR1].*

- d) The temperature of the SIM is reduced to  $-25^{\circ}\text{C}$ .
- e) Steps b) and c) are repeated.

*The SIM shall operate successfully [CR1].*

- f) The temperature of the SIM is increased to  $+70^{\circ}\text{C}$ .
- g) Steps b) and c) are repeated.

*The SIM shall operate successfully [CR1].*

- h) The temperature of the SIM is increased to  $+85^{\circ}\text{C}$ .
- i) Steps b) and c) are repeated continually for a period of 4 hours.

*The SIM shall operate successfully [CR1].*

*The SIM shall have satisfied the test requirements of subclause 6.1.1.*

- j) The temperature of the SIM is reduced to  $+25^{\circ}\text{C}$ .
- k) Steps h), i) and j) are repeated a further 99 times.

*The SIM shall operate successfully [CR1].*

- l) Carry out the tests in subclause 6.1.1 again.

## 6.1.3 Contacts

### 6.1.3.1 Definition and applicability

The shape, robustness and provision of contacts shall be adhered to, in order to maintain good electrical contact with the ME, ensuring proper operation in the GSM environment.

### 6.1.3.2 Conformance requirement

CR2 Contact C6 shall not be bonded in the SIM for any function other than supplying  $V_{pp}$ .

Reference: GSM 11.11 [1], subclause 4.3.1., 4.3.,4

Test Group Reference (TGR): TGR\_SIM\_PHY\_CNT

Test Procedure Reference (TPR): TPR\_SIM\_PHY\_CNT

### 6.1.3.3 Test purpose

To verify that the SIM conforms to the above requirements.

NOTE: As the contacts specified in CR1 and CR3 are optional, the tests specified here shall only be performed on those contacts when the contacts are present.

### 6.1.3.4 Method of test

#### Initial conditions

- 1) The SIM shall have passed the Format and Layout tests in subclause 6.1.1.

#### Test procedure

- a) Contact C6 is connected to ground by the ME simulator
- b) VCC is applied to contact C1
- c) Contact C2 (RST) is kept at low level, ground
- d) A valid clock signal is applied to Contact C3

*The dc power consumption on Contact C1 shall not exceed 10 mA under any condition [CR2].*

NOTE: This test ensures that VPP and VCC are not bonded together in the SIM, if this would be the case VPP would also supply the SIM with current for its operation.

- e) The SIM is connected to an ME simulator.
- f) The ME simulator resets the SIM.

*The SIM shall have been reset successfully [CR4].*

## 6.2 Electronic signals and transmission protocols

The tests in this subclause ensure that the IUT conforms to the electrical specification for each of the contacts and also the protocol.

## 6.2.1 Supply voltage Vcc (contact C1)

### 6.2.1.1 Voltage limits

#### 6.2.1.1.1 Definition and applicability

In addition to the electronic signals and transmission protocols defined in ISO/IEC 7816-3, the SIM shall operate within the following supply voltage conditions to ensure proper operation in the GSM environment.

This test applies to all SIM implementations with 1.8V, 3V and 5V interfaces

#### 6.2.1.1.2 Conformance requirement

CR1 The SIM shall operate when the supply voltage on contact C1 (Vcc) is in the following ranges:

Card Type	Vmin /V	Vmax /V
5V type	4,5	5,5
3V type	2,7	3,3
1,8V type *	1,62	1,98

\* Draft EN 301 116 V0.2.0

Reference: GSM 11.11 [1], subclause 5.1.

Test Group Reference (TGR): TGR\_SIM\_ELEC\_VCC

Test Procedure Reference (TPR): TPR\_SIM\_ELEC\_VCC\_V

#### 6.2.1.1.3 Test purpose

To verify that the SIM conforms to the above requirements.

#### 6.2.1.1.4 Method of test

##### Initial conditions

- 1) The SIM is connected to an ME simulator.
- 2) The CHV1 value is 4 zeros.

##### Test procedure

(the voltage Vcc min/max depends on the voltage class the SIM provides),

- a) The voltage source for contact C1 (Vcc) is set to Vcc min, and the SIM interface signals are powered from a Vcc min, source.
- b) The ME simulator resets the SIM.  
*The SIM shall send the correct ATR sequence [CR1].*
- c) The ME simulator sends an CHANGE CHV command to the SIM with new CHV1 value 8 zeros.
- d) The ME simulator sends an CHANGE CHV command to the SIM to return the CHV1 to its original value.
- e) The voltage source for contact C1 (Vcc) is set to Vcc max,.
- f) The ME simulator resets the SIM.

*The SIM shall send the correct ATR sequence [CR1].*

- g) The ME simulator sends an CHANGE CHV command to the SIM with new CHV1 value 8 zeros.
- h) The ME simulator sends an CHANGE CHV command to the SIM to return the CHV1 to its original value.

- i) Repeat the test for every voltage class the SIM provides

## 6.2.1.2 Current limits

### 6.2.1.2.1 Definition and applicability

In addition to the electronic signals and transmission protocols defined in ISO/IEC 7816-3, the current consumption shall not exceed the specified limit under normal operating conditions to ensure proper operation in the GSM environment.

**Table 1: Current consumption on VCC**

Card Type	$I_{max}$ /mA under normal conditions (average value *1)	$f_{max}$ /Mhz (max CLK-frequency under normal conditions)	$V_{cc_{max}}$ voltage on VCC during testing
5V type	10	5	5,5V
3V type	6	4	3,3V
1,8V type *	4	4	1,98V

**Table 2: Current spikes on VCC**

Card Type	$I_{max}$ /mA	max charge /nAs	max duration /ns
5V type	200	40	400
3V type	60	12	400
1,8V type *	60	12	400

\* Draft EN 301 116 V0.2.0

\*1  $I_{max}$  is the average value of the Vcc Current including the current spikes!

### 6.2.1.2.2 Conformance requirement

CR1 The current consumption of the SIM shall not exceed the max currents values ( $I_{max}$ ) as defined in table 1 and 2 at the max. frequency ( $f_{max}$ ) and the max. allowed voltage level  $V_{max}$ .

Reference: GSM 11.11 [1], subclause 5.1.

Test Group Reference (TGR): TGR\_SIM\_ELEC\_VCC

Test Procedure Reference (TPR): TPR\_SIM\_ELEC\_VCC\_I

### 6.2.1.2.3 Test purpose

To verify that the SIM conforms to the above requirements.

### 6.2.1.2.4 Method of test

#### Initial conditions

- 1) The SIM is connected to an ME simulator.
- 2) A current measuring device is connected to the SIM.
- 3) The CHV1 value is 4 zeros.

#### Test procedure

- a) The frequency of the clock source is set to 1MHz.
- b) The ME simulator resets the SIM.

- c) The ME simulator performs the SIM initialisation procedure during which time the current consumption is measured.
- d) The ME simulator sends an CHANGE CHV command to the SIM with new CHV1 value 8 zeros.
- e) The ME simulator sends an CHANGE CHV command to the SIM to return the CHV1 to its original value.
- f) The frequency of the clock source is set to 3.25MHz.
- g) The ME simulator resets the SIM.
- h) The ME simulator performs the SIM initialisation procedure during which time the current consumption is measured.
- i) The ME simulator sends an CHANGE CHV command to the SIM with new CHV1 value 8 zeros.
- j) The ME simulator sends an CHANGE CHV command to the SIM to return the CHV1 to its original value.
- k) The frequency of the clock source is set to  $f_{\max}$
- l) The ME simulator resets the SIM.
- m) The ME simulator performs the SIM initialisation procedure during which time the current consumption is measured.
- n) The ME simulator sends an CHANGE CHV command to the SIM with new CHV1 value 8 zeros.
- o) The ME simulator sends an CHANGE CHV command to the SIM to return the CHV1 to its original value.
- p) repeat tests a ) to o) for all voltage classes the SIM delivers.

*The current consumption of the SIM shall not exceed the max.current values given in table 1 and 2 according to the SIM class excluding spikes up to the defined maximum charges, durations and amplitudes during the whole test.*

### 6.2.1.3 Idle current limits

#### 6.2.1.3.1 Definition and applicability

In addition to the electronic signals and transmission protocols defined in ISO/IEC 7816-3, the current consumption shall not exceed the specified limit under idle conditions to ensure proper operation in the GSM environment.

**Table 3: Current consumption in idle mode**

Card Type	$I_{\max}$ / $\mu$ A in idle state clk frequency 1 Mhz	$V_{CC_{\max}}$ /V max. voltage on VCC during testing
5V type	200	5,5
3V type	200	3,3
1,8V type *	200	1,98

\* Draft EN 301 116 V0.2.0

#### 6.2.1.3.2 Conformance requirement

CR1 The idle current consumption of the SIM shall not exceed  $I_{\max}$  at 1MHz , +25°C and  $V_{\max}$ .

Reference: GSM 11.11 [1], subclause 5.1.

Reference: GSM 11.11 [1], subclause 5.

\*Reference: Draft EN 301126 V0.2.0 (1998-01) subclause 5.

Test Group Reference (TGR): TGR\_SIM\_ELEC\_VCC

Test Procedure Reference (TPR): TPR\_SIM\_ELEC\_VCC\_IDLE

### 6.2.1.3.3 Test purpose

To verify that the SIM conforms to the above requirements.

### 6.2.1.3.4 Method of test

#### Initial conditions

- 1) The SIM is connected to an ME simulator.
- 2) The frequency of the clock source is set to 1MHz.
- 3) The temperature of the SIM is +25°C.
- 4) The voltage on VCC is set to  $V_{CC_{max}}$ .

#### Test procedure

- a) The ME simulator resets the SIM.
- b) The idle current consumption is measured after receiving the ATR over a period of ten seconds.
- c) repeat test for all voltage classes the SIM supports.

### 6.2.1.3.5 Test requirement

- 1) During step b), the current consumption of the SIM shall not exceed  $I_{max}$

## 6.2.1.4 Current limits at all frequencies

### 6.2.1.4.1 Definition and applicability

In addition to the electronic signals and transmission protocols defined in ISO/IEC 7816-3, the current consumption shall not exceed the specified limit under idle conditions to ensure proper operation in the GSM environment.

**Table 4: Current consumption in idle mode at max frequency**

Card Type	$I_{max}$ / $\mu$ A in idle state (average value)	$V_{CC_{max}}$ /V max. voltage on VCC during testing	$f_{max}$ /Mhz max CLK frequency in idle mode
5V type	1000	5,5	5
3V type	1000	3,3	4
1,8V type *	1000	1,98	4

\* Draft EN 301 116 V0.2.0

### 6.2.1.4.2 Conformance requirement

- 1) The idle current consumption of the SIM shall not exceed  $I_{max}$  at any frequency  $f_{max}$

Reference: GSM 11.11 [1], subclause 5.1.

Reference: ETS 300 641 [1], subclause 5.

\*Reference: Draft EN 3011126 V0.2.0 (1998-01) subclause 5.

Test Group Reference (TGR): TGR\_SIM\_ELEC\_VCC

Test Procedure Reference (TPR): TPR\_SIM\_ELEC\_VCC\_IF

#### 6.2.1.4.3 Test purpose

To verify that the SIM conforms to the above requirements.

#### 6.2.1.4.4 Method of test

##### Initial conditions

- 1) The SIM is connected to an ME simulator.

##### Test procedure

- a) The frequency of the clock source is set to 1MHz.
- b) The ME simulator resets the SIM.
- c) The current consumption is measured after receiving the ATR over a period of ten seconds.
- d) The frequency of the clock source is set to 3.25MHz.
- e) The ME simulator resets the SIM.
- f) The current consumption is measured after receiving the ATR over a period of ten seconds.
- g) The frequency of the clock source is set to  $f_{max}$ .
- h) The ME simulator resets the SIM..
- i) The current consumption is measured after receiving the ATR over a period of ten seconds.

*The current consumption of the SIM shall not exceed 1mA [CR1] in average over the whole test*

#### 6.2.1.5 Current limits in clk-stop-mode

##### 6.2.1.5.1 Definition and applicability

In addition to the electronic signals and transmission protocols defined in ISO/IEC 7816-3, the current consumption shall not exceed the specified limit under clk-stop conditions to ensure proper operation in the GSM environment.

**Table 1: Current consumption in clk stop mode**

Card Type	$I_{max}$ / $\mu$ A in clk-stop mode (average value)	$V_{cc_{max}}$ /V max. voltage on VCC during testing
5V type	200	5,5
3V type	100	3,3
1,8V type *	100	1,98

\* Draft EN 301 116 V0.2.0

##### 6.2.1.5.2 Conformance requirement

- 1) The clk stop mode current consumption of the SIM shall not exceed  $I_{max}$  if clk stop mode is delivered by the SIM.

Reference: GSM 11.11 [1], subclause 5.1.

Reference: ETS 300 641 [1], subclause 5.

\*Reference: Draft EN 3011126 V0.2.0 (1998-01) subclause 5.

Test Group Reference (TGR): TGR\_SIM\_ELEC\_VCC

Test Procedure Reference (TPR): TPR\_SIM\_ELEC\_VCC\_CLKSTOP

### 6.2.1.5.3 Test purpose

To verify that the SIM conforms to the above requirements.

### 6.2.1.5.4 Method of test

#### Initial conditions

- 1) The SIM is connected to an ME simulator.

#### Test procedure

- a) The ME simulator resets the SIM.
- b) The ME simulator sends a SELECT command to the SIM to select the MF.
- c) The ME simulator sends a GET RESPONSE command to the SIM using the SW2 returned by the SIM following step b).
- d) The ME simulator stops the clock at least 744 clk according to the clock stop mode read in step c).
- f) The current consumption is measured during clk stop for min. 10s.

*The current consumption of the SIM shall not exceed  $I_{max}$  in average during clk stop.*

## 6.2.2 Reset RST (contact C2)

### 6.2.2.1 Static operation

#### 6.2.2.1.1 Definition and applicability

In addition to the electronic signals and transmission protocols defined in ISO/IEC 7816-3, the SIM shall operate within the following limits regarding the reset RST signal to ensure proper operation in the GSM environment.

#### 6.2.2.1.2 Conformance requirement

CR1 The SIM shall operate within the following limits for RST:

Card Type	$V_{OL}$ min/V	$V_{OL}$ max/V	$I_{OL}$ max/uA	$V_{OH}$ min/V	$V_{OH}$ max/V	$I_{OH}$ max/uA
5V type	-0,3	0,6	-200	$0,7 * V_{CC}$	$V_{CC} + 0,3V$	+20
3V type	-0,3	$0,2 * V_{CC}$	-200	$0,8 * V_{CC}$	$V_{CC} + 0,3V$	+20
1,8V type *	-0,3	$0,2 * V_{CC}$	-200	$0,8 * V_{CC}$	$V_{CC} + 0,3V$	+200

-  $t_R$  and  $t_F$  shall not exceeding 400µs, with  $C_{out}$  and  $C_{in}$  equal to 30pF.

Reference: GSM 11.11 [1], subclause 5.2.

Reference: ETS 300 641 [1], subclause 5.

\*Reference: Draft EN 3011126 V0.2.0 (1998-01) subclause 5.

Test Group Reference (TGR): TGR\_SIM\_ELEC\_RST

Test Procedure Reference (TPR): TPR\_SIM\_ELEC\_RST\_ST

### 6.2.2.1.3 Test purpose

To verify that the SIM conforms to the above requirements.

#### 6.2.2.1.4 Method of test

##### Initial conditions

- 1) The SIM is connected to an ME simulator.
- 2) A current measuring device is connected to RST (contact C2) of the SIM.
- 3) The capacitance,  $C_{in}$ , of RST (contact C2) is measured to be 30pF.

##### Test procedure

- a) The following parameters are set for RST:
  - $V_{OH}$  of the RST signal is set to  $V_{OH\ min}$ .
  - $V_{OL}$  of the RST signal is set to  $V_{OL\ min}$ .
  - $t_R$  and  $t_F$  are set to 400 $\mu$ S.
- b) The ME simulator resets the SIM.
- c) The following parameters are set for RST:
  - $V_{OH}$  of the RST signal is set to  $V_{OH\ max}$ .
  - $V_{OL}$  of the RST signal is set to  $V_{OL\ max}$ .
  - $t_R$  and  $t_F$  are set to 400 $\mu$ S.
- d) The ME simulator resets the SIM.
- e) Repeat the test for all voltage classes the card supports

*The following shall be true for all tests:*

- $I_{OLmax}$  is measured to be less than or equal to  $I_{OL\ max}$  [CR1b,c].
- $I_{OHmax}$  is measured to be less than or equal to  $I_{OH\ max}$  [CR1a,c].

### 6.2.3 Clock CLK (contact C3)

#### 6.2.3.1 Frequency and duty cycle

##### 6.2.3.1.1 Definition and applicability

In addition to the electronic signals and transmission protocols defined in ISO/IEC 7816-3, the SIM shall operate within the following limits regarding the reset RST signal to ensure proper operation in the GSM environment.

This test applies to all SIM implementations with 5V interface.

##### 6.2.3.1.2 Conformance requirement

- CR1 The SIM shall **not** support an internal clock.
- CR2 The SIM shall support a duty cycle between 40% and 60% of the period during stable operation.
- CR3 The SIM shall operate within the following limits for CLK:

Card Type	V <sub>OL</sub> min/V	V <sub>OL</sub> max/V	V <sub>OH</sub> min/V	V <sub>OH</sub> max/V	T <sub>R</sub> & T <sub>F</sub> max	f <sub>max</sub> /MHz
5V type	-0,3	0,5	0,7 * V <sub>CC</sub>	V <sub>CC</sub> +0,3V	9% with a max. of 0,5us	5
3V type	-0,3	0,2 * V <sub>CC</sub>	0,8*V <sub>CC</sub>	V <sub>CC</sub> +0,3V	50ns	4
1,8V type *	-0,3	0,2 * V <sub>CC</sub>	0,8*V <sub>CC</sub>	V <sub>CC</sub> +0,3V	50ns	4

Note: T<sub>R</sub> and T<sub>F</sub> has to be measured between 10% and 90% of V<sub>OL</sub> and V<sub>OH</sub>; C<sub>in</sub> is equal to 30pF.

Reference: GSM 11.11 [1], subclause 5.4.

Reference: ETS 300 641 [1], subclause 5.

\*Reference: Draft EN 3011126 V0.2.0 (1998-01) subclause 5.

Test Group Reference (TGR): TGR\_SIM\_ELEC\_CLK

Test Procedure Reference (TPR): TPR\_SIM\_ELEC\_CLK\_FREQ

### 6.2.3.1.3 Test purpose

To verify that the SIM conforms to the above requirements.

### 6.2.3.1.4 Method of test

#### Initial conditions

- 1) The SIM is connected to an ME simulator.

#### Test procedure

- a) The frequency of the clock source is set to 1MHz.
- b) The duty cycle of the clock source is set to 40% high.

V<sub>OH</sub> is set to V<sub>OHmax</sub>; V<sub>OL</sub> is set to V<sub>OLmin</sub>

- c) The ME simulator resets the SIM.
- d) The duty cycle of the clock source is set to 60% high.
- e) The ME simulator resets the SIM.

*The SIM shall send the correct ATR sequence [CR1,3].*

- f) The frequency of the clock source is set to f<sub>max</sub>.
- g) The duty cycle of the clock source is set to 40% high.
- h) The ME simulator resets the SIM.

*The SIM shall send the correct ATR sequence [CR1,3].*

- i) The duty cycle of the clock source is set to 60% high.
- j) The ME simulator resets the SIM.

*The SIM shall send the correct ATR sequence [CR1,3]*

- k) Repeat a) to i) with V<sub>OH</sub> set to V<sub>OHmin</sub>; V<sub>OL</sub> set to V<sub>OLmax</sub>

- l) Repeat a) to j) for all voltage classes supported by the SIM

## 6.2.3.2 Voltage and current

### 6.2.3.2.1 Definition and applicability

In addition to the electronic signals and transmission protocols defined in ISO/IEC 7816-3, the SIM shall operate within the following limits regarding the CLK signal to ensure proper operation in the GSM environment.

### 6.2.3.2.2 Conformance requirement

CR1 The SIM shall operate within the following limits for CLK:

Card Type	V <sub>OL</sub> min/V	V <sub>OL</sub> max/V	I <sub>OL</sub> max/uA	V <sub>OH</sub> min/V	V <sub>OH</sub> max/V	I <sub>OH</sub> max/uA	T <sub>R</sub> & T <sub>F</sub> max	fmax /MHz
5V type	-0,3	0,5	-200	0,7 * V <sub>CC</sub>	V <sub>CC</sub> +0,3V	+20	9% with a max. of 0,5us	5
3V type	-0,3	0,2 * V <sub>CC</sub>	-20	0,7*V <sub>CC</sub>	V <sub>CC</sub> +0,3V	+20	50ns	4
1,8V type *	-0,3	0,2 * V <sub>CC</sub>	-20	0,8*V <sub>CC</sub>	V <sub>CC</sub> +0,3V	+20	50ns	4

Reference: GSM 11.11 [1], subclause 5.4.

Reference: ETS 300 641 [1], subclause 5.

\*Reference: Draft EN 3011126 V0.2.0 (1998-01) subclause 5.

Test Group Reference (TGR): TGR\_SIM\_ELEC\_CLK

Test Procedure Reference (TPR): TPR\_SIM\_ELEC\_CLK\_VI

### 6.2.3.2.3 Test purpose

To verify that the SIM conforms to the above requirements.

### 6.2.3.2.4 Method of test

#### Initial conditions

- 1) The SIM is connected to an ME simulator.
- 2) A current measuring device is connected to CLK (contact C3) of the SIM.
- 3) The capacitance of CLK (contact C3) is measured to be  $\leq 30\text{pF}$ .

#### Test procedure

- a) The clock signal is set to 1MHz.
- b) The following parameters are set for CLK:
  - V<sub>OH</sub> at V<sub>OH</sub>max.
  - V<sub>OL</sub> at V<sub>OL</sub>min.
  - t<sub>R</sub> and t<sub>F</sub> is set to t<sub>R</sub>max and t<sub>F</sub>max
- c) The ME simulator resets the SIM.

*The following shall be true:*

*The SIM shall provide an ATR*

- d) The following parameters are set for CLK:
  - V<sub>OH</sub> at V<sub>OH</sub>min

- $V_{OL}$  at  $V_{OLmax}$
- e) The ME simulator resets the SIM.

The following shall be true:

- The SIM shall provide an ATR
- f) Repeat test a) to e) with  $f_{clk} = f_{max}$ ,  $T_R = T_{Rmax}$  and  $T_F = T_{Fmax}$ .
- f) Repeat test a) to f) for all voltage classes delivered by the SIM

The following shall be true for all tests:

- $I_{OHmax}$  is measured to be less than or equal to  $+20\mu A$  [CR1a].
- $I_{OLmax}$  is measured to be less than or equal to  $-200\mu A$  [CR1b].
- The SIM shall provide an ATR after a reset

## 6.2.4 I/O (contact C7)

### 6.2.4.1 Voltage and current

#### 6.2.4.1.1 Definition and applicability

In addition to the electronic signals and transmission protocols defined in ISO/IEC 7816-3, the SIM shall operate within the following limits regarding the I/O signal to ensure proper operation in the GSM environment.

#### 6.2.4.1.2 Conformance requirement

CR1 The SIM shall operate within the following limits for I/O:

Card Type	$V_{OL}$ min/V	$V_{OL}$ max/V	$I_{OL}$ max/ $\mu A$	$V_{OH}$ min/V	$V_{OH}$ max/V	$I_{OH}$ max/ $\mu A$	$T_R$ & $T_F$ max	fmax /MHz
5V type	-0,3	0,5	-1000	3,8	$V_{cc} +0,3V$	+20	1us	5
3V type	-0,3	0,4	-1000	0,7*VCC	$V_{cc} +0,3V$	+20	1us	4
1,8V type *	-0,3	0,3	-1000	0,7*VCC	$V_{cc} +0,3V$	+20	1us	4

Card Type	$V_{IL}$ min/V	$V_{IL}$ max/V	$I_{IL}$ max/ $\mu A$	$V_{IH}$ min/V	$V_{IH}$ max/V	$I_{IH}$ min/max / $\mu A$	$T_R$ & $T_F$ max	fmax /MHz
5V type	-0,3	0,8	+1000	0,7 * VCC	$V_{cc} +0,3V$	$\pm 20$	1us	5
3V type	-0,3	0,2 * VCC	+1000	0,7*VCC	$V_{cc} +0,3V$	$\pm 20$	1us	4
1,8V type *	-0,3	0,2 * VCC	+1000	0,7*VCC	$V_{cc} +0,3V$	$\pm 20$	1us	4

Reference: GSM 11.11 [1], subclause 5.5.

Reference: ETS 300 641 [1], subclause 5.

\*Reference: Draft EN 301126 V0.2.0 (1998-01) subclause 5.

Test Group Reference (TGR): TGR\_SIM\_ELEC\_IO

Test Procedure Reference (TPR): TPR\_SIM\_ELEC\_IO\_VI

#### 6.2.4.1.3 Test purpose

To verify that the SIM conforms to the above requirements.

#### 6.2.4.1.4 Method of test

##### Initial conditions

- 1) The SIM is connected to an ME simulator.
- 2) A current measuring device is connected to I/O (contact C7) of the SIM.
- 3) The capacitance,  $C_{out}$  and  $C_{in}$ , of I/O (contact C7) is measured to be 30pF.

##### Test procedure

- a) The ME simulator are set to the following max. ranges allowed by the SIM :

$V_{cc}$  to  $V_{cc}$  max

$V_{OL}$  to  $V_{OL}$  min,  $V_{OH}$  to  $V_{OH}$  max,

$I_{IL}$  to  $I_{IL}$ max,  $I_{IH}$  to  $I_{IH}$  max.

$T_R$  to  $T_R$  max and  $T_F$  to  $T_F$  maxb) The ME simulator resets the SIM.

- c) The ME simulator sends a STATUS command to the SIM.

- d) The ME simulator are set to the minimum ranges allowed by the SIM with  $V_{OH}$  inaktiv:

$V_{cc}$  to  $V_{cc}$  min

$V_{OL}$  to  $V_{OL}$  max,  $V_{OH}$  to  $V_{OH}$  min,

$I_{IL}$  to  $I_{IL}$ max,  $I_{IH}$  to  $I_{IH}$  min.

$T_R$  to  $T_R$  max and  $T_F$  to  $T_F$  max

- e) The ME simulator resets the SIM.

- f) The ME simulator sends a STATUS command to the SIM.

*m) repeat test a) to l) for all voltage classes*

*Acceptance criterium for all tests:*

*$I_{OL}$  has to be between 0mA and  $I_{OL}$  max.*

*$I_{OH}$  has to be  $\leq I_{OH}$  max..*

*$V_{IL}$  has to be between  $V_{IL}$  min and  $V_{IL}$  max.*

*$V_{IH}$  has to be between  $V_{IH}$  min and  $V_{IH}$  max*

*$T_R$  and  $T_R$  generated by the SIM have to be  $\leq T_R$  and  $T_F$  max*

## 6.2.5 States

### 6.2.5.1 Definition and applicability

There are two states for the while the power supply is on, operating state when the SIM is executing a command, and idle state at any other time.

### 6.2.5.2 Conformance requirement

CR1 The SIM shall support exactly one of these items:

- Clock stop allowed, no preferred level

- Clock stop allowed, high level preferred
- Clock stop allowed, low level preferred
- Clock stop not allowed
- Clock stop not allowed, unless at high level
- Clock stop not allowed, unless at low level

CR2 When the SIM is in idle state, all pertinent data shall be retained.

CR3 A SIM of Phase 2 or later shall always send the status information "normal ending of the command" after the successful interpretation of the command SLEEP received from a Phase 1 ME.

Reference: GSM 11.11 [1], subclauses 5.6 and 9.2.1.

Test Group Reference (TGR): TGR\_SIM\_ELEC\_STAT

Test Procedure Reference (TPR): TPR\_SIM\_ELEC\_STAT

### 6.2.5.3 Test purpose

To verify that the SIM conforms to the above requirements.

### 6.2.5.4 Method of test

#### Initial conditions

- 1) The SIM is connected to an ME simulator.

#### Test procedure

- a) The ME simulator resets the SIM.
- b) The ME simulator sends a SELECT command to the SIM to select the MF.
- c) The ME simulator sends a GET RESPONSE command to the SIM using the SW2 returned by the SIM following step b).

*The coding of bits 1, 3 and 4 of byte 14 in the response data shall be one in the table below only [CR1].*

- d) The ME simulator stops the clock according to the clock stop mode read in step c).
- e) The ME simulator pauses for 10 seconds, then starts the clock.
- f) The ME simulator sends a GET RESPONSE command to the SIM using the SW2 returned by the SIM following step b).

*The response data read shall be that indicating  $EF_{ICCID}$ .*

Table 1: (Title?)

Bit 1	Bit 3	Bit 4	Clock stop mode
1	0	0	Clock stop allowed, no preferred level
1	1	0	Clock stop allowed, high level preferred
1	0	1	Clock stop allowed, low level preferred
0	0	0	Clock stop not allowed
0	1	0	Clock stop only allowed on high level
0	0	1	Clock stop only allowed on low level

## 6.2.6 Answer To Reset (ATR)

### 6.2.6.1 ATR content

#### 6.2.6.1.1 Definition and applicability

The ATR is information presented by the SIM to the ME at the beginning of the card session and gives operational requirements.

#### 6.2.6.1.2 Conformance requirement

- CR1 The ATR consists of at the most 33 characters.
- CR2 Initial character TS is sent by the SIM.
- CR3 Format character T0 is sent by the SIM.
- CR4 Interface character (global) TA1 is sent by the SIM (optional).
- CR5 Interface character (global) TB1 is sent by the SIM (optional).
- CR6 Interface character (global) TC1 is sent by the SIM (optional).
- CR7 Interface character TD1 is sent by the SIM (optional).
- CR8 Interface character (specific) TA2 is sent by the SIM (optional).
- CR9 Interface character (global) TB2 is **never** sent by the SIM.
- CR10 Interface character (specific) TC2 is sent by the SIM (optional).
- CR11 Interface character TD<sub>i</sub> is sent by the SIM (optional).
- CR12 Interface characters T<sub>Ai</sub>, T<sub>Bi</sub>, T<sub>Ci</sub> (i>2) are sent by the SIM (optional).
- CR13 Historical characters T1,...,TK are sent by the SIM (optional).
- CR14 Check character TCK is sent by the SIM (conditional).

Reference: GSM 11.11 [1], subclause 5.8.1

Test Group Reference (TGR): TGR\_SIM\_ELEC\_ATR

Test Procedure Reference (TPR): TPR\_SIM\_ELEC\_ATR\_CON

#### 6.2.6.1.3 Test purpose

To verify that the SIM conforms to the above requirements.

#### 6.2.6.1.4 Method of test

##### Initial conditions

- 1) The SIM is connected to an ME simulator.

### Test procedure

- a) The ME simulator resets the SIM.

*The SIM shall send the ATR sequence [CR1].*

*The total length of the ATR sequence shall not be more than 33 characters [CR1].*

*The following characters shall be present and in the following order:*

*Initial character TS [CR2].*

*Format character T0 [CR3].*

*Interface character (global) TA1, if its presence is indicated by T0 [CR4].*

*Interface character (global) TB1, if its presence is indicated by T0 [CR5].*

*Interface character (global) TC1, if its presence is indicated by T0 [CR6].*

*Interface character TD1, if its presence is indicated by T0 [CR7].*

*Interface character (specific) TA2, if its presence is indicated by TD1 [CR8].*

*Interface character (specific) TC2, if its presence is indicated by TD1 [CR10].*

*Interface character TD<sub>i</sub>, if its presence is indicated by TD(i-1, i>1) [CR11].*

*Interface characters TA<sub>i</sub>, TB<sub>i</sub>, TC<sub>i</sub> if their presence is indicated by TD(i-1, i>2) [CR12].*

*Historical characters T1,...,TK, if their presence is indicated by T0 [CR13].*

*Check character TCK, if an additional protocol type to T=0 is indicated by TD1 [CR14].*

*PII shall be equal to 0 if TB1 is sent [CR5].*

*TC1 shall be either 0 or 255, if sent [CR6].*

*The SIM shall never send Interface character (global) TB2 [CR9].*

## 6.2.6.2 PTS procedure

### 6.2.6.2.1 Definition and applicability

The ATR indicates which protocols are available for use during a session. The PTS procedure allows one of the available protocol types to be selected.

### 6.2.6.2.2 Conformance requirement

- CR1 The SIM shall respond to a PTS-Request from the ME with a PTS-Response (optional).

Reference: GSM 11.11 [1], subclause 5.8.2.

Test Group Reference (TGR): TGR\_SIM\_ELEC\_ATR

Test Procedure Reference (TPR): TPR\_SIM\_ELEC\_ATR\_PTS

### 6.2.6.2.3 Test purpose

To verify that the SIM conforms to the above requirements.

#### 6.2.6.2.4 Method of test

##### Initial conditions

- 1) The SIM is connected to an ME simulator.

##### Test Procedure

- a) The ME simulator resets the SIM.

*The SIM shall send the correct ATR sequence.*

- b) The ME simulator sends a PTS-Request to the SIM, selecting T=0 protocol.

*If the SIM supports PTS procedure it shall send a valid PTS-Response [CR1].*

### 6.2.7 Major Capabilities

#### 6.2.7.1 Definition and applicability

The SIM shall adhere to the electronic signals and transmission protocols defined in GSM 11.11 [1] and ISO/IEC 7816-3 to ensure proper operation in the GSM environment.

#### 6.2.7.2 Conformance requirement

CR1 Electronic signals and transmission protocols shall be in accordance with ISO/IEC 7816-3 unless otherwise specified.

CR2 The choice of the transmission protocol(s), to be used to communicate between the ME and the SIM, shall at least include that specified and denoted by T=0 in ISO/IEC 7816-3.

CR3 The baudrate for all communications shall be: (clock frequency)/372.

CR4 The bit/character duration and sampling time specified in ISO/IEC 7816-3, subclauses 6.1.1 and 6.1.2, are valid for all communications.

CR5 Error detection and character repetition is mandatory for the SIM for all communications.

Reference: GSM 11.11 [1], clauses 5, and subclauses 5.7, 5.9 and 5.10.

Test Group Reference (TGR): TGR\_SIM\_ELEC\_MAJOR

Test Procedure Reference (TPR): TPR\_SIM\_ELEC\_MAJOR

#### 6.2.7.3 Test purpose

To verify that the SIM conforms to the above requirements.

NOTE: The testing of CR1, CR2, CR3, CR4 and CR5 is outside the scope of the present document.

#### 6.2.7.4 Method of test

##### Initial conditions

N/A

##### Test procedure

N/A

#### 6.2.7.5 Test requirement

N/A

## 6.3 Logical Model

The tests in this subclause ensure that the IUT is tested against the specification of the logical structure, for a SIM, the code associated with it, and the structure of the files used.

### 6.3.1 File identifier

#### 6.3.1.1 File-type identification

##### 6.3.1.1.1 Definition and applicability

A file identifier is used to address or identify each specific file.

##### 6.3.1.1.2 Conformance requirement

CR1 For GSM, the Master File shall be coded as '3F 00'.

CR2 For GSM, file type '7F' shall be used to identify Dedicated Files.

CR3 For GSM, file type '2F' shall be used to identify Elementary Files under the Master File.

CR4 For GSM, file type '6F' shall be used to identify Elementary Files under a Dedicated File.

Reference: GSM 11.11 [1], subclause 6.2.

Test Group Reference (TGR): TGR\_SIM\_LOG\_FID

Test Procedure Reference (TPR): TPR\_SIM\_LOG\_FID\_FTI

##### 6.3.1.1.3 Test purpose

To verify that the SIM conforms to the above requirements.

##### 6.3.1.1.4 Method of test

#### Initial conditions

- 1) The SIM is connected to an ME simulator.

#### Test procedure

- a) The ME simulator resets the SIM.
- b) For each file in figure 7 of GSM 11.11 [1], subclause 10.4, the ME simulator sends SELECT commands to the SIM to select the file ID and, if selected successfully, the ME simulator sends a GET RESPONSE command to the SIM.

*After each successful SELECT and GET RESPONSE, byte 7 of the response data shall conform to the following table:*

<i>File ID</i>	<i>Type of File</i>
'3F 00'01'	
'7F XX'	'02'
'2F XX'	'04'
'6F XX'	'04'

### 6.3.1.2 File ID assignments

#### 6.3.1.2.1 Definition and applicability

A file identifier is used to address or identify each specific file. There are a number of rules regarding file ID assignment.

#### 6.3.1.2.2 Conformance requirement

- CR1 A file ID is assigned at the time of creation of the file concerned.
- CR2 Two files under the same parent shall never have the same ID.
- CR3 A child and any parent, either immediate or remote, in the hierarchy shall never have the same ID.

Reference: GSM 11.11 [1], subclause 6.2.

Test Group Reference (TGR): TGR\_SIM\_LOG\_FID

Test Procedure Reference (TPR): TPR\_SIM\_LOG\_FID\_FIA

#### 6.3.1.2.3 Test purpose

To verify that all files within the SIM structure conform to the above requirements.

NOTE 1: CR1 cannot be tested as the SELECT function requires the file ID in order to select files.

NOTE 2: CR2 and CR3 cannot be tested due to the operation of the SELECT function which should only ever select a single file for a given file ID.

#### 6.3.1.2.4 Method of test

##### Initial conditions

N/A

##### Test procedure

N/A

#### 6.3.1.2.5 Test requirement

N/A

### 6.3.2 Dedicated files

#### 6.3.2.1 Definition and applicability

Dedicated Files provide a functional grouping of Elementary Files. In this way a structured hierarchy of files can be established on the SIM.

#### 6.3.2.2 Conformance requirement

- CR1 The SIM shall contain  $DF_{GSM}$ .
- CR2 The SIM shall contain  $DF_{TELECOM}$  (optional).

Reference: GSM 11.11 [1], subclause 6.3., subclause 10.2, subclause 10.3

Test Group Reference (TGR): TGR\_SIM\_LOG\_DF

Test Procedure Reference (TPR): TPR\_SIM\_LOG\_DF

### 6.3.2.3 Test purpose

To verify that the Dedicated Files within the SIM file structure conform to the above requirements.

### 6.3.2.4 Method of test

#### Initial conditions

- 1) The SIM is connected to an ME simulator.

#### Test procedure

- a) The ME simulator resets the SIM.
- b) The ME simulator sends a SELECT command to the SIM to select DF<sub>GSM</sub>.

*The status condition returned by the SIM shall be SW1='9F', SW2='XX' - length 'XX' of the response data [CR1].*

- c) The ME simulator resets the SIM.
- d) The ME simulator sends a SELECT command to the SIM to select DF<sub>TELECOM</sub>.

*The status condition returned by the SIM shall be SW1='9F', SW2='XX' - length 'XX' of the response data, if the SIM supports DF<sub>TELECOM</sub>, otherwise the status condition returned by the SIM shall be SW1='94', SW2='04' - file ID not found [CR2].*

## 6.3.3 Elementary files

### 6.3.3.1 Definition and applicability

Elementary Files structure the way in which information is held on the SIM and provide security on how this information is accessed.

### 6.3.3.2 Conformance requirement

- CR1 The total data length of the body of an EF with transparent structure shall be indicated in the header of the EF.
- CR2 The record length of an EF with linear fixed structure shall be indicated in the header of the EF.
- CR3 The record length multiplied by the number of records of an EF with linear fixed structure shall be indicated in the header of the EF.
- CR4 The SIM shall be able to access records within a linear fixed EF using all of the methods given in subclause 6.4.2.
- CR5 For an EF with cyclic structure, when all the records have been used for storage, then the next storage of data shall overwrite the oldest information.
- CR6 The SIM shall be able to access records within a cyclic EF using all of the methods given in subclause 6.4.3.

Reference: GSM 11.11 [1], clause 6.4.1, 6.4.2 and 6.4.3.

Test Group Reference (TGR): TGR\_SIM\_LOG\_EF

Test Procedure Reference (TPR): TPR\_SIM\_LOG\_EF

### 6.3.3.3 Test purpose

To verify that the EFs within the SIM file structure conform to the above requirements.

NOTE: CR4, CR5 and CR6 are tested in subclauses 6.5.5 and 6.5.6.

### 6.3.3.4 Method of test

#### Initial conditions

- 1) The SIM is connected to an ME simulator, and the ME simulator has reset the SIM.

#### Test procedure

The following steps are performed for all EFs in figure 7 of GSM 11.11 [1], subclause 10.4.

- a) The ME simulator sends a SELECT command to select the required EF in the SIM.
- b) If the EF is successfully selected, the ME simulator sends a GET RESPONSE command to the SIM.
- c) The ME simulator fulfils the READ access condition of the EF.
- d) If the EF is transparent, the ME simulator sends a READ BINARY command to the SIM. The length used shall be that of bytes 3 and 4 of the response data in step b).

*The status condition returned by the SIM shall be SW1='90', SW2='00' - normal ending of command [CR1].*

- e) If the EF is transparent, the ME simulator sends a READ BINARY command with offset '00 01' to the SIM. The length used shall be that of bytes 3 and 4 of the response data in step b).

*The status condition returned by the SIM shall indicate an error [CR1].*

- f) If the EF is linear fixed or cyclic, the ME simulator sends a READ RECORD using ABSOLUTE mode with record 1 to the SIM. The length used shall be that of byte 15 of the response data in step b).

*The status condition returned by the SIM shall be SW1='90', SW2='00' - normal ending of command [CR2].*

- g) If the EF is linear fixed or cyclic, the ME simulator sends a READ RECORD using ABSOLUTE mode to the SIM. The record length used shall be that of byte 15 of the response data in step b) and the record number shall be that of bytes 3 and 4 of the response data in step b) divided by the record length.

*The status condition returned by the SIM shall be SW1='90', SW2='00' - normal ending of command [CR3].*

- h) If the EF is linear fixed or cyclic, the ME simulator sends a READ RECORD using ABSOLUTE mode to the SIM. The record length used shall be that of byte 15 of the response data in step b) and the record number shall be that of bytes 3 and 4 of the response data in step b) divided by the record length, plus 1.

*The status condition returned by the SIM shall be SW1='94', SW2='02' - out of range (invalid address) [CR3].*

## 6.3.4 Methods for selecting a file

### 6.3.4.1 Definition and applicability

The ME accesses information on the SIM navigating around the file structure by selecting DFs and EFs as required. There are a number of rules regarding which file elements may be selected from a given DF or EF.

### 6.3.4.2 Conformance requirement

- CR1 Selection of a DF or MF shall set the current Directory on the SIM.
- CR2 After a selection of a DF or MF there shall be no current EF.
- CR3 After a selection of an EF, the current EF shall be set to this EF and the current Directory shall remain the DF or MF which is the parent of this EF.
- CR4 Any application specific command shall only be operable if it is specific to the current Directory.
- CR5 It shall be possible to select the following from the last selected file:
  - a) any file which is an immediate child of the current Directory

- b) any DF which is an immediate child of the parent of the current DF
- c) the parent of the current Directory
- d) the current DF
- e) the MF

NOTE: Reselection of the last selected file is allowed.

CR6 It shall be possible to select any of the 'valid selections' in Table 6, subclause 6.5 of GSM 11.11 [1] for each of the 'last selected file' entries.

Reference: GSM 11.11 [1], subclause 6.5.

Test Group Reference (TGR): TGR\_SIM\_LOG\_SELFILE

Test Procedure Reference (TPR): TPR\_SIM\_LOG\_SELFILE

### 6.3.4.3 Test purpose

To verify that the SIM conforms to the above requirements with regard to file selection.

NOTE 2: CR5 is tested for function RUN GSM ALGORITHM in subclause 6.5.16.

### 6.3.4.4 Method of test

#### Initial conditions

- 1) The SIM is connected to an ME simulator.

#### Test procedure

- a) The ME simulator resets the SIM.
- b) The ME simulator sends SELECT commands to the SIM to select  $DF_{GSM}$ .
- c) The ME simulator sends a STATUS command to the SIM.

*Bytes 5 and 6 of the response data shall indicate that  $DF_{GSM}$  is the currently selected directory [CR1].*

- d) The ME simulator sends a READ BINARY command using a length of 1 byte to the SIM.

*The status condition returned by the SIM shall be  $SW1='94'$ ,  $SW2='00'$  - no EF selected [CR2].*

- e) The ME simulator sends a SELECT command to the SIM to select  $EF_{LP}$ .
- f) The ME simulator sends a GET RESPONSE command to the SIM.

*Bytes 5 and 6 of the response data shall indicate that  $EF_{LP}$  is the currently selected EF [CR3].*

- g) The ME simulator sends a STATUS command to the SIM.

*Bytes 5 and 6 of the response data shall indicate that  $DF_{GSM}$  is the currently selected directory [CR3].*

- h) Step i) is carried out for each line in Table 6, subclause 6.5 of GSM 11.11 [1].

- i) Step j) is carried out for each one of the 'valid selections' in that line of the table.

- j) Steps k) then l) are carried out in turn.

- k) The ME simulator sends SELECT commands to the SIM to select the 'last selected file'.

- l) The ME simulator sends a SELECT command to the SIM to select the 'valid selection'.

*The status condition returned by the SIM shall be  $SW1='9F'$ ,  $SW2='XX'$  [CR5,6].*

The following file IDs are used to represent the IDs in the table:

**Table 2: IDs**

Table	Actual
MF	MF
DF1	DF <sub>TELECOM</sub>
DF2	DF <sub>GSM</sub>
EF1	EF <sub>ICCID</sub>
EF2	EF <sub>ADN</sub>
EF3	EF <sub>LP</sub>
EF4	EF <sub>IMSI</sub>

NOTE: When EF<sub>ADN</sub> is not supported by the SIM, any supported EF in DF<sub>TELECOM</sub> may be chosen.

## 6.3.5 Reservation of file IDs

### 6.3.5.1 Definition and applicability

In order to accommodate planned and possible future requirements, certain file IDs are considered reserved, and may not be used in the SIM file structure.

### 6.3.5.2 Conformance requirement

CR1 The following Dedicated File IDs are reserved for operational use by GSM:

'7F 10'

'7F 2X'

CR2 The following Elementary File IDs are reserved for operational use by GSM:

'2F 1X' under MF

'6F 2X', '6F 3X' and '6F 4X' under '7F 10' and '7F 2X'

CR3 The following Dedicated File IDs are reserved for administrative use by GSM:

'7F 4X'

CR4 The following Elementary File IDs are reserved for administrative use by GSM:

'2F 01', '2F EX' under MF

'6F XX' under DFs '7F 4X'

'6F 1X' under '7F 10', '7F 20' and '7F 21'

Reference: GSM 11.11 [1], subclause 6.6.

Test Group Reference (TGR): TGR\_SIM\_LOG\_RSVD

Test Procedure Reference (TPR): TPR\_SIM\_LOG\_RSVD

### 6.3.5.3 Test purpose

To verify that the SIM conforms to the above requirements.

NOTE: CR3 and CR4 cannot be tested as the administrative functionality is outside the scope of GSM 11.11 [1].

#### 6.3.5.4 Method of test

##### Initial conditions

- 1) The SIM is connected to an ME simulator.

##### Test procedure

- a) The ME simulator resets the SIM.
- b) For all possible EFs on the SIM, the ME simulator sends SELECT commands to the SIM to select each EF in sequence.

*For all successful selections, the ID of the selected file shall be one of those in Figure 7, clause 10 of GSM 11.11 [1] or shall not be one of those listed as reserved for operational use. [CR1,2]*

## 6.4 Security features

The tests in this subclause ensure that the IUT conforms with the security aspects which are related to the SIM.

### 6.4.1 Authentication and cipher key generation procedure

The authentication mechanism employed in the GSM system between the network and SIM to authenticate a SIM, results in a finite interaction with the SIM, through the use of the function RUN GSM ALGORITHM. In order to test the behaviour of the SIM during this authentication mechanism, it is sufficient to test the function which operates on the SIM during the authentication mechanism. The test procedure for the function itself shall be executed, as defined in subclause 6.5.16 ("RUN GSM ALGORITHM" function).

### 6.4.2 File access conditions

#### 6.4.2.1 Definition and applicability

Every file has its own specific access condition for each command which shall be fulfilled before the command can take place.

#### 6.4.2.2 Conformance requirement

CR1 For access condition ALWAYS, the command can be performed without any restriction.

CR2 For access condition CHV1, the command shall only be possible if one of the following three conditions is fulfilled:

- a) a correct CHV1 value has already been presented to the SIM during the current session
- b) the CHV1 enabled/disabled indicator is set to "disabled"
- c) UNBLOCK CHV1 has been successfully performed during the current session

CR3 For access condition CHV2, the command shall only be possible if one of the following two conditions is fulfilled:

- a) a correct CHV2 value has already been presented to the SIM during the current session
- b) UNBLOCK CHV2 has been successfully performed during the current session

CR4 For access condition NEVER, the command shall not be possible over the SIM/ME interface.

Reference: GSM 11.11 [1], subclause 7.6.

Test Group Reference (TGR): TGR\_SIM\_SEC\_FAC

Test Procedure Reference (TPR): TPR\_SIM\_SEC\_FAC

### 6.4.2.3 Test purpose

To verify that the SIM conforms to the above requirements.

NOTE 1: Allocation of ADM levels and the respective requirements for their fulfilment are the responsibility of the appropriate administrative authority.

NOTE 2: CR2b and CR2c are tested in subclauses 6.5.11, 6.5.12 and 6.5.13.

NOTE 3: CR3b is not tested here although the UNBLOCK CHV function in subclause 6.5.13 intrinsically tests for CHV2.

### 6.4.2.4 Method of test

#### Initial conditions

- 1) The SIM is connected to an ME simulator.
- 2) EF<sub>ADN</sub> is present and not invalidated.

#### Test procedure

- a) The ME simulator resets the SIM.
- b) The ME simulator sends a SELECT command to the SIM to select EF<sub>ICCID</sub>.
- c) The ME simulator sends a READ BINARY command to the SIM to read the first 1 byte in EF<sub>ICCID</sub>.  
*The status condition returned by the SIM shall be SW1='90', SW2='00' - normal ending of command [CR1].*
- d) The ME simulator sends SELECT commands to the SIM to select EF<sub>ADN</sub> under DF<sub>TELECOM</sub>.
- e) The ME simulator sends a READ RECORD command to the SIM to read the first record in EF<sub>ADN</sub>.  
*The status condition returned by the SIM shall be SW1='98', SW2='04' - access condition not fulfilled [CR2a].*
- f) The ME simulator gains CHV1 security access.
- g) The ME simulator sends a READ RECORD command to the SIM to read the first record in EF<sub>ADN</sub>.  
*The status condition returned by the SIM shall be SW1='90', SW2='00' - normal ending of command [CR2a].*
- h) The ME simulator sends an INVALIDATE command to the SIM to invalidate EF<sub>ADN</sub>.  
*The status condition returned by the SIM shall be SW1='98', SW2='04' - access condition not fulfilled [CR3a].*
- i) The ME simulator gains CHV2 security access.
- j) The ME simulator sends an INVALIDATE command to the SIM to invalidate EF<sub>ADN</sub>.  
*The status condition returned by the SIM shall be SW1='90', SW2='00' - normal ending of command [CR3a].*
- k) The ME simulator sends SELECT commands to the SIM to select EF<sub>ICCID</sub> under MF.
- l) The ME simulator sends an UPDATE BINARY command to the SIM to update the byte in EF<sub>ICCID</sub> with the byte read in step c).  
*The status condition returned by the SIM shall be SW1='98', SW2='04' - access condition not fulfilled [CR4].*

## 6.5 Description of the functions

The tests in this subclause ensure that the IUT conforms to the functional specification for all the commands and their respective responses.

## 6.5.1 SELECT function

### 6.5.1.1 Definition and applicability

It shall be mandatory for all cards complying with GSM 11.11 [1] to support all functions described therein.

### 6.5.1.2 Conformance requirement

- CR1 The SELECT function shall select a file according to the methods described in clause 6 of GSM 11.11 [1].
- CR2 The function shall accept as an input, a file ID.
- CR3 If the selected file is the MF or a DF, then the function shall output the file ID, total memory space available, CHV enabled/disabled indicator and CHV status.
- CR4 If the selected file is an EF, then the function shall output the file ID, access conditions, invalidation indicator, structure of EF and the length of the records in the case of linear fixed or cyclic structure.
- CR5 The record pointer in a cyclic file shall address the last record which has been updated or increased.

Reference: GSM 11.11 [1], subclause 8.1.

Test Group Reference (TGR): TGR\_SIM\_FN

Test Procedure Reference (TPR): TPR\_SIM\_FN\_SEL

### 6.5.1.3 Test purpose

To verify that the SELECT function conforms to the above requirements for the different file types available.

NOTE: CR1 is tested in subclause 6.3.5.

### 6.5.1.4 Method of test

#### Initial conditions

- 1) The SIM is connected to an ME simulator.
- 2) The records in EF<sub>ACM</sub> contain the following data:
  - Record 1: '11 11 11' (last updated record)
  - Record 2: '22 22 22'
  - Record 3: '33 33 33'
- 4) The record length of EF<sub>ADN</sub> is known.

#### Test procedure and Requirements

- a) The ME simulator resets the SIM.
- b) The ME simulator sends a SELECT command to select DF<sub>GSM</sub>.
 

*The status returned by the SIM shall be SW1='9F', SW2='XX' - length 'XX' of the response data [CR2].*
- c) The ME simulator sends a GET RESPONSE command to the SIM.
 

*The following shall be true of the response data [CR3]:*

  - Bytes 5 and 6 shall indicate that DF<sub>GSM</sub> is the currently selected file
  - Byte 7 shall be '02' indicating a DF

- Byte 13 shall be less than or equal to SW2 from step b) minus 13
  - Bit 8 of byte 14 shall be 0 indicating that CHV1 is enabled
  - Byte 15 shall indicate the correct number of DFs which are a direct child of DF<sub>GSM</sub>
  - Byte 16 shall indicate the correct number of EFs which are a direct child of DF<sub>GSM</sub>
  - Bits 1 through 4 of byte 19 shall indicate three VERIFY CHV1 attempts remaining
  - Bits 1 through 4 of byte 21 shall indicate three VERIFY CHV2 attempts remaining.
  - Bits 1 through 4 of byte 20 shall indicate ten UNBLOCK CHV1 attempts remaining
  - Bits 1 through 4 of byte 22 shall indicate ten UNBLOCK CHV2 attempts remaining
- d) The ME simulator sends a SELECT command to the SIM to select the MF.
- e) The ME simulator sends a GET RESPONSE command to the SIM.
- The following shall be true of the response data [CR3]:*
- Byte 7 shall be '01' indicating MF
  - Byte 15 shall indicate the correct number of DFs which are a direct child of MF
  - Byte 16 shall indicate the correct number of EFs which are a direct child of MF
- f) The ME simulator sends a VERIFY CHV command with **incorrect** CHV1 to the SIM.
- g) The ME simulator send a SELECT command to the SIM to select DF<sub>GSM</sub>.
- h) The ME simulator sends a GET RESPONSE command to the SIM.
- The following shall be true of the response data [CR3]:*
- Bits 1 through 4 of byte 19 shall indicate two VERIFY CHV1 attempts remaining
- i) The ME simulator sends a DISABLE CHV command to the SIM.
- j) The ME simulator send a SELECT command to the SIM to select DF<sub>GSM</sub>.
- k) The ME simulator sends a GET RESPONSE command to the SIM.
- The following shall be true of the response data [CR3]:*
- Bit 8 of byte 14 shall be 1 indicating that CHV1 is disabled
  - Bits 1 through 4 of byte 19 shall indicate three VERIFY CHV1 attempts remaining.
- l) The ME simulator sends a SELECT command to the SIM to select the MF.
- m) The ME simulator sends a SELECT command to the SIM to select DF<sub>TELECOM</sub>.
- n) The ME simulator sends a ENABLE CHV command to the SIM.
- o) The ME simulator sends a SELECT command to the SIM to select EF<sub>ADN</sub>.
- p) The ME simulator sends a GET RESPONSE command to the SIM.
- The following shall be true of the response data [CR4]:*
- Bytes 5 and 6 shall indicate that EF<sub>ADN</sub> is the currently selected file.
  - Bytes 9 through 11 shall state the access conditions in subclause 10.3.1 of GSM 11.11 [1].
  - Bit 1 of byte 12 shall be 1 indicating that the file is not invalidated.

- Byte 14 shall be '01' indicating linear fixed structure.
  - Byte 15 shall indicate the length of the records.
- q) The ME simulator sends a VERIFY CHV command to the SIM with **correct** CHV2.
- r) The ME simulator sends an INVALIDATE command to the SIM.
- s) The ME simulator sends a SELECT command to the SIM to re-select EF<sub>ADN</sub>.
- t) The ME simulator sends a GET RESPONSE command to the SIM.
- The response data shall indicate the following [CR4]:*
- Bit 1 of byte 12 shall be 0 indicating that the file is invalidated.
- u) The ME simulator sends a REHABILITATE command to the SIM.
- v) The ME simulator sends a SELECT command to the SIM to select DF<sub>GSM</sub>.
- w) The ME simulator sends a SELECT command to the SIM to select EF<sub>ACM</sub>.
- x) The ME simulator sends a GET RESPONSE command to the SIM.
- The following shall be true of the response data [CR4]:*
- Byte 14 shall be '03' indicating cyclic structure.
- y) The ME simulator sends a READ RECORD command using CURRENT mode to the SIM.
- The response data shall be '11 11 11' [CR5].*

## 6.5.2 STATUS function

### 6.5.2.1 Definition and applicability

It shall be mandatory for all cards complying with GSM 11.11 [1] to support all functions described therein.

### 6.5.2.2 Conformance requirement

- CR1 The STATUS function shall output the file ID, total memory space available, CHV enabled/disabled indicator and CHV status of the currently selected MF or DF.

Reference: GSM 11.11 [1], subclause 8.2.

Test Group Reference (TGR): TGR\_SIM\_FN

Test Procedure Reference (TPR): TPR\_SIM\_FN\_STATUS

### 6.5.2.3 Test purpose

To verify that the SIM conforms to the above requirements.

### 6.5.2.4 Method of test

#### Initial conditions

- 1) The SIM is connected to an ME simulator.

#### Test procedure and Requirements

- a) The ME simulator resets the SIM.
- b) The ME simulator sends a SELECT command to select DF<sub>GSM</sub>.

- c) The ME simulator sends a STATUS command to the SIM.

*The following shall be true of the response data [CR1]:*

- Bytes 5 and 6 shall indicate that  $DF_{GSM}$  is the currently selected file
- Byte 7 shall be '02' indicating a DF
- Byte 13 shall be less than or equal to SW2 from step b) minus 13
- Bit 8 of byte 14 shall be 0 indicating that CHV1 is enabled
- Byte 15 shall indicate the correct number of DFs which are a direct child of  $DF_{GSM}$
- Byte 16 shall indicate the correct number of EFs which are a direct child of  $DF_{GSM}$
- Bits 1 through 4 of byte 19 shall indicate three VERIFY CHV1 attempts remaining if CHV1 is initialised
- Bits 1 through 4 of byte 21 shall indicate three VERIFY CHV2 attempts remaining if CHV2 is initialised
- Bits 1 through 4 of byte 20 shall indicate ten UNBLOCK CHV1 attempts remaining if CHV1 is initialised
- Bits 1 through 4 of byte 22 shall indicate ten UNBLOCK CHV2 attempts remaining if CHV2 is initialised

- d) The ME simulator sends a SELECT command to the SIM to select the MF.

- e) The ME simulator sends a STATUS command to the SIM.

*The following shall be true of the response data [CR1]:*

- Byte 7 shall be '01' indicating MF
- Byte 15 shall indicate the correct number of DFs which are a direct child of MF
- Byte 16 shall indicate the correct number of EFs which are a direct child of MF

- f) The ME simulator sends a VERIFY CHV command with **incorrect** CHV1 to the SIM.

- g) The ME simulator send a SELECT command to the SIM to select  $DF_{GSM}$ .

- h) The ME simulator sends a STATUS command to the SIM.

*The following shall be true of the response data [CR1]:*

- Bits 1 through 4 of byte 19 shall indicate two VERIFY CHV1 attempts remaining

- i) The ME simulator sends a DISABLE CHV command to the SIM.

- j) The ME simulator send a SELECT command to the SIM to select  $DF_{GSM}$ .

- k) The ME simulator sends a STATUS command to the SIM.

*The following shall be true of the response data [CR1]:*

- Bit 8 of byte 14 shall be 1 indicating that CHV1 is disabled
- Bits 1 through 4 of byte 19 shall indicate three VERIFY CHV1 attempts remaining.

## 6.5.3 READ BINARY function

### 6.5.3.1 Definition and applicability

It shall be mandatory for all cards complying with GSM 11.11 [1] to support all functions described therein.

### 6.5.3.2 Conformance requirement

- CR1 The READ BINARY function shall read a string of bytes from the current transparent EF.
- CR2 The function shall accept as an input, the relative address (offset) and the length (in bytes) of the string.
- CR3 The function shall output the string of bytes.
- CR4 The function shall only be performed if the READ access condition for the current EF is satisfied.

Reference: GSM 11.11 [1], subclause 8.3.

Test Group Reference (TGR): TGR\_SIM\_FN

Test Procedure Reference (TPR): TPR\_SIM\_FN\_RDBIN

### 6.5.3.3 Test purpose

To verify that the READ BINARY function conforms to the above requirements.

### 6.5.3.4 Method of test

#### Initial conditions

- 1) The SIM is connected to an ME simulator.
- 2) EF<sub>Kc</sub> contains the data string: 'A1 A2 A3 A4 A5 A6 A7 A8 A9'.

#### Test procedure

- a) The ME simulator resets the SIM.
- b) The ME simulator sends SELECT commands to the SIM to select EF<sub>Kc</sub> under DF<sub>GSM</sub>.
- c) The ME simulator sends a READ BINARY command using a length of 9 bytes to the SIM.  
*The status condition returned by the SIM shall be SW1='98', SW2='04' - access condition not fulfilled [CR4].*
- d) The ME simulator sends a VERIFY CHV command to the SIM.
- e) The ME simulator sends a READ BINARY command using a length of 9 bytes to the SIM.  
*The status condition returned by the SIM shall be SW1='90', SW2='00' - normal ending of command [CR1-4].*  
*The data string returned shall be 'A1 A2 A3 A4 A5 A6 A7 A8 A9' [CR1-4].*
- f) The ME simulator sends a READ BINARY command using a length of 1 byte to the SIM.  
*The data string returned shall be 'A1'.*
- g) The ME simulator sends a READ BINARY command using an offset of '00 01' and length 8 byte to the SIM.  
*The data string returned shall be 'A2 A3 A4 A5 A6 A7 A8 A9' [CR1-4].*
- h) The ME simulator sends a READ BINARY command using a length of 10 bytes to the SIM.  
*The status condition returned by the SIM shall be SW1='67', SW2='09' or '00' - incorrect parameter P3.*
- i) The ME simulator sends a READ BINARY command using an offset of '00 0A' and length 1 byte to the SIM.  
*The status condition returned by the SIM shall be SW1='6B', SW2='XX' - incorrect parameter P1 or P2.*
- j) The ME simulator sends a READ BINARY command using an offset of '00 05' and length 5 bytes to the SIM.  
*An error status condition shall be returned by the SIM.*

## 6.5.4 UPDATE BINARY function

### 6.5.4.1 Definition and applicability

It shall be mandatory for all cards complying with GSM 11.11 [1] to support all functions described therein.

### 6.5.4.2 Conformance requirement

- 1) The UPDATE BINARY function shall update the current transparent EF with a string of bytes.
- 2) The function shall accept as an input, the relative address (offset), the length (in bytes) of the string, and the string of bytes.
- 3) The function shall only be performed if the UPDATE access condition for the current EF is satisfied.

Reference: GSM 11.11 [1], subclause 8.4.

Test Group Reference (TGR): TGR\_SIM\_FN

Test Procedure Reference (TPR): TPR\_SIM\_FN\_UPBIN

### 6.5.4.3 Test purpose

To verify that the UPDATE BINARY function conforms to the above requirements.

### 6.5.4.4 Method of test

#### Initial conditions

- 1) The SIM is connected to an ME simulator.
- 2) EF<sub>Kc</sub> contains the data string: 'FF FF FF FF FF FF FF FF FF'.

#### Test procedure

- a) The ME simulator resets the SIM.
- b) The ME simulator sends SELECT commands to the SIM to select EF<sub>Kc</sub> under DF<sub>GSM</sub>.
- c) The ME simulator sends an UPDATE BINARY command using a length of 9 bytes, and data string 'A1 A2 A3 A4 A5 A6 A7 A8 A9' to the SIM.

*The status condition returned by the SIM shall be SW1='98', SW2='04' - access condition not fulfilled [CR3].*

- d) The ME simulator sends a VERIFY CHV command to the SIM.
- e) The ME simulator sends a READ BINARY command using a length of 9 bytes to the SIM.

The data string returned shall be 'FF FF FF FF FF FF FF FF FF'.

- f) The ME simulator sends an UPDATE BINARY command using a length of 9 bytes, and data string 'A1 A2 A3 A4 A5 A6 A7 A8 A9' to the SIM.

*The status condition returned by the SIM shall be SW1='90', SW2='00' [CR3].*

- g) The ME simulator sends a READ BINARY command using a length of 9 bytes to the SIM.

*The data string returned shall be 'A1 A2 A3 A4 A5 A6 A7 A8 A9' [CR1].*

- h) The ME simulator sends an UPDATE BINARY command using a length of 1 byte, and data string 'E4' to the SIM.
- i) The ME simulator sends a READ BINARY command using a length of 9 bytes to the SIM.

The data string returned shall be 'E4 A2 A3 A3 A4 A5 A6 A7 A8 A9' [CR1].

- j) The ME simulator sends an UPDATE BINARY command using an offset of '00 01', a length 1 byte, and data string 'E5' to the SIM.
- k) The ME simulator sends a READ BINARY command using a length of 9 bytes to the SIM.

*The data string returned shall be 'E4 E5 A3 A3 A4 A5 A6 A7 A8 A9' [CR1].*

## 6.5.5 READ RECORD function

### 6.5.5.1 Definition and applicability

It shall be mandatory for all cards complying with GSM 11.11 [1] to support all functions described therein.

### 6.5.5.2 Conformance requirement

- CR1 The READ RECORD function shall read one complete record in the current linear fixed or cyclic EF.
- CR2 The function shall accept as an input, the mode, record number if absolute mode, and the length of the record.
- CR3 The function shall output the record specified by the mode.
- CR4 The function shall only be performed if the READ access condition for the current EF is satisfied.
- CR5 If the mode is CURRENT, the current record is read.
- CR6 If the mode is CURRENT, the record pointer is not affected.
- CR7 If the mode is ABSOLUTE, the record given by the record number is read.
- CR8 If the mode is ABSOLUTE, the record pointer is not affected.
- CR9 If the mode is NEXT, the record pointer is incremented before the function is performed and the pointed record is read.
- CR10 If the mode is NEXT, and the record pointer has not been previously been set within the selected EF, the **first** record shall be read and the record pointer set to this record.
- CR11 If the mode is NEXT, and the record pointer addresses the last record in a linear fixed EF, the record pointer shall not change and no data shall be read.
- CR12 If the mode is NEXT, and the record pointer addresses the last record in a cyclic EF, the **first** record shall be read and the record pointer set to this record.
- CR13 If the mode is PREVIOUS, the record pointer is decremented before the function is performed and the pointed record is read.
- CR14 If the mode is PREVIOUS, and the record pointer has not been previously been set within the selected EF, the **last** record shall be read and the record pointer set to this record.
- CR15 If the mode is PREVIOUS, and the record pointer addresses the first record in a linear fixed EF, the record pointer shall not change and no data shall be read.
- CR16 If the mode is PREVIOUS, and the record pointer addresses the first record in a cyclic EF, the **last** record shall be read and the record pointer set to this record.
- CR17 The record pointer shall not be changed if the function is unsuccessful.
- CR18 For modes NEXT and PREVIOUS, P1 has no significance and shall not be interpreted by the SIM.

Reference: GSM 11.11 [1], subclause 8.5.

Test Group Reference (TGR): TGR\_SIM\_FN

Test Procedure Reference (TPR): TPR\_SIM\_FN\_RDREC

### 6.5.5.3 Test purpose

To verify that the READ RECORD function conforms to the above requirements using two test procedures.

NOTE: CR12 and CR16 can only be tested if EF<sub>ACM</sub> is present.

### 6.5.5.4 Method of test

#### Initial conditions

- 1) The SIM is connected to an ME simulator.
- 2) The records in EF<sub>ADN</sub> contain the following data for the first 16 bytes:
  - First record: '10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F'
  - Second record: '20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F'
  - Second last record: 'E0 E1 E2 E3 E4 E5 E6 E7 E8 E9 EA EB EC ED EE EF'
  - Last record: 'F0 F1 F2 F3 F4 F5 F6 F7 F8 F9 FA FB FC FD FE FF'

The data for the remainder of these two records and for all other records (if any) is 'FF'.

- 3) The records in EF<sub>ACM</sub> contain the following data:

Record 1: '01 01 01' (last updated record)

Record 2: '02 02 02'

Record 3: '03 03 03'

...and so on for all records...

Record X: '0X 0X 0X' (first updated record)

#### Test procedure 1 and Requirements

- a) The ME simulator resets the SIM.
- b) The ME simulator sends SELECT commands to the SIM to select EF<sub>ADN</sub> under DF<sub>TELECOM</sub>.
- c) The ME simulator sends a READ RECORD command using ABSOLUTE mode with record 1 to the SIM.
 

*The status condition returned by the SIM shall be SW1='98', SW2='04' - access condition not fulfilled [CR4].*
- d) The ME simulator sends a VERIFY CHV command to the SIM.
- e) The ME simulator sends a READ RECORD command using ABSOLUTE mode with record 1 to the SIM.
 

*The status condition returned by the SIM shall be SW1='90', SW2='00' - normal ending of command [CR4].*

*The record data returned shall be that of the first record in EF<sub>ADN</sub> [CR1-4,7].*
- f) The ME simulator sends SELECT commands to the SIM to select EF<sub>ADN</sub> under DF<sub>TELECOM</sub>.
- g) The ME simulator sends a READ RECORD command using NEXT mode to the SIM.
- h) The ME simulator sends a READ RECORD command using ABSOLUTE mode with record 2 to the SIM.
 

*The record data returned shall be that of the second record in EF<sub>ADN</sub> [CR7].*
- i) The ME simulator sends a READ RECORD command using CURRENT mode to the SIM.
 

*The record data returned shall be that of the first record in EF<sub>ADN</sub> [CR5,8].*

- j) The ME simulator sends a READ RECORD command using NEXT mode to the SIM.  
*The record data returned shall be that of the second record in EF<sub>ADN</sub> [CR6].*
- k) The ME simulator sends a READ RECORD command using ABSOLUTE mode with the last record to the SIM.  
*The record data returned shall be that of the last record in EF<sub>ADN</sub> [CR7].*
- l) The ME simulator sends a READ RECORD command using ABSOLUTE mode with the last record + 1 to the SIM.  
*The status condition returned by the SIM shall be SW1='94', SW2='02' - out of range.*
- m) The ME simulator sends a READ RECORD command using CURRENT mode to the SIM.  
*The record data returned shall be that of the second record in EF<sub>ADN</sub> [CR17].*
- n) The ME simulator sends SELECT commands to the SIM to select EF<sub>ACM</sub> under DF<sub>GSM</sub>.
- o) The ME simulator sends a READ RECORD command using CURRENT mode to the SIM.  
*The record data returned shall be that of the first record in EF<sub>ACM</sub> [CR1,5].*
- p) The ME simulator sends a READ RECORD command using ABSOLUTE mode with record 3 to the SIM.  
*The record data returned shall be that of the record 3 in EF<sub>ACM</sub> [CR1,7].*
- q) The ME simulator sends a READ RECORD command using ABSOLUTE mode with the last record + 1 to the SIM.  
*The status condition returned by the SIM shall be SW1='94', SW2='02' - out of range.*
- r) The ME simulator sends a READ RECORD command using CURRENT mode to the SIM.  
*The record data returned shall be that of the first record in EF<sub>ACM</sub> [CR17].*

### Test procedure 2 and Requirements

- a) The ME simulator resets the SIM.
- b) The ME simulator sends a VERIFY CHV command to the SIM.
- c) The ME simulator sends SELECT commands to the SIM to select EF<sub>ADN</sub> under DF<sub>TELECOM</sub>.
- d) The ME simulator sends a READ RECORD command using NEXT mode to the SIM.  
*The record data returned shall be that of the first record in EF<sub>ADN</sub> [CR10].*
- e) The ME simulator sends a READ RECORD command using CURRENT mode to the SIM.  
*The record data returned shall be that of the first record in EF<sub>ADN</sub> [CR10].*
- f) The ME simulator sends a READ RECORD command using NEXT mode to the SIM with P1 = 'FF'.  
*The status condition returned by the SIM shall be SW1='90', SW2='00' - normal ending of command [CR18].*  
*The record data returned shall be that of the second record in EF<sub>ADN</sub> [CR9].*
- g) The ME simulator sends a READ RECORD command using CURRENT mode to the SIM.  
*The record data returned shall be that of the second record in EF<sub>ADN</sub> [CR9].*
- h) The ME simulator sends a SELECT command to the SIM to select EF<sub>ADN</sub>.
- i) The ME simulator sends a READ RECORD command using PREVIOUS mode to the SIM.  
*The record data returned shall be that of the last record in EF<sub>ADN</sub> [CR14].*

- j) The ME simulator sends a READ RECORD command using NEXT mode to the SIM.  
*The status condition returned by the SIM shall be SW1='94', SW2='02' - out of range [CR11].*
- k) The ME simulator sends a READ RECORD command using CURRENT mode to the SIM.  
*The record data returned shall be that of the last record in EF<sub>ADN</sub> [CR11].*
- l) The ME simulator sends a READ RECORD command using PREVIOUS mode with P1 = 'FF' to the SIM.  
*The status condition returned by the SIM shall be SW1='90', SW2='00' - normal ending of command [CR18].*  
*The record data returned shall be that of the second last record in EF<sub>ADN</sub> [CR13].*
- m) The ME simulator sends a SELECT command to the SIM to select EF<sub>ADN</sub>.
- n) The ME simulator sends a READ RECORD command using NEXT mode to the SIM.
- o) The ME simulator sends a READ RECORD command using PREVIOUS mode to the SIM.  
*The status condition returned by the SIM shall be SW1='94', SW2='02' - out of range [CR15].*
- p) The ME simulator sends a READ RECORD command using CURRENT mode to the SIM.  
*The record data returned shall be that of the first record in EF<sub>ADN</sub> [CR15].*
- q) The ME simulator sends SELECT commands to the SIM to select EF<sub>ACM</sub>.
- r) The ME simulator sends a READ RECORD command using PREVIOUS mode to the SIM.  
*The record data returned shall be that of the last record (record X) in EF<sub>ACM</sub> [CR16].*
- s) The ME simulator sends a READ RECORD command using CURRENT mode to the SIM.  
*The record data returned shall be that of the last record (record X) in EF<sub>ACM</sub> [CR16].*
- t) The ME simulator sends a READ RECORD command using NEXT mode to the SIM.  
*The record data returned shall be that of the first record (record 1) in EF<sub>ACM</sub> [CR12].*
- u) The ME simulator sends a READ RECORD command using CURRENT mode to the SIM.  
*The record data returned shall be that of the first record (record 1) in EF<sub>ACM</sub> [CR12].*

## 6.5.6 UPDATE RECORD function

### 6.5.6.1 Definition and applicability

It shall be mandatory for all cards complying with GSM 11.11 [1] to support all functions described therein.

### 6.5.6.2 Conformance requirement

- CR1 The UPDATE RECORD function shall update one complete record in the current linear fixed or cyclic EF.
- CR2 The function shall accept as an input, the mode, record number if absolute mode, the length of the record, and the data used for updating the record.
- CR3 The function shall only be performed if the UPDATE access condition for the current EF is satisfied.
- CR4 For cyclic files, only PREVIOUS mode is allowed.
- CR5 If the mode is CURRENT, the current record is updated
- CR6 If the mode is CURRENT, the record pointer is not affected.
- CR7 If the mode is ABSOLUTE, the record given by the record number is updated.

- CR8 If the mode is ABSOLUTE, the record pointer is not affected.
- CR9 If the mode is NEXT, the record pointer is incremented before the function is performed and the pointed record is updated.
- CR10 If the mode is NEXT, and the record pointer has not previously been set within the selected EF, the **first** record shall be updated and the record pointer set to this record.
- CR11 If the mode is NEXT, and the record pointer addresses the last record, the record pointer shall not change and no record shall be updated.
- CR12 If the mode is PREVIOUS, the record pointer is decremented before the function is performed and the pointed record is updated.
- CR13 If the mode is PREVIOUS, and the record pointer has not previously been set within the selected EF, the **last** record shall be updated and the record pointer set to this record.
- CR14 If the mode is PREVIOUS, and the record pointer addresses the first record, the record pointer shall not change and no record shall be updated.
- CR15 If the mode is PREVIOUS and the EF is a cyclic file, the oldest record is updated, the record pointer set to this record, and this record shall become the first record.
- CR16 The record pointer shall not be changed if the function is unsuccessful.
- CR17 For modes NEXT and PREVIOUS, P1 has no significance and shall not be interpreted by the SIM.

Reference: GSM 11.11 [1], subclause 8.6.

Test Group Reference (TGR): TGR\_SIM\_FN

Test Procedure Reference (TPR): TPR\_SIM\_FN\_UPREC

### 6.5.6.3 Test purpose

To verify that the UPDATE RECORD function conforms to the above requirements for the different modes available.

NOTE: CR4 and CR13 can only be tested if EF<sub>ACM</sub> is present.

### 6.5.6.4 Method of test

#### Initial conditions

- 1) The SIM is connected to an ME simulator.
- 2) The records in EF<sub>ADN</sub> contain the following data for the first 16 bytes:
  - First record: '10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F'
  - Second record: '20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F'
  - Second last record: 'E0 E1 E2 E3 E4 E5 E6 E7 E8 E9 EA EB EC ED EE EF'
  - Last record: 'F0 F1 F2 F3 F4 F5 F6 F7 F8 F9 FA FB FC FD FE FF'

The data for the remainder of these two records and for all other records (if any) is 'FF'.
- 3) The records in EF<sub>ACM</sub> contain the following data:
  - Record 1: '01 01 01' (last updated record)
  - Record 2: '02 02 02'
  - Record 3: '03 03 03'

...and so on for all records...

Record X: '0X 0X 0X' (first updated record)

### Test procedure 1 and Requirements

- a) The ME simulator resets the SIM.
- b) The ME simulator sends SELECT commands to the SIM to select EF<sub>ADN</sub> under DF<sub>TELECOM</sub>.
- c) The ME simulator sends an UPDATE RECORD command using ABSOLUTE mode with record 1 to the SIM. The data used is 'C1' for all bytes.

*The status condition returned by the SIM shall be SW1='98', SW2='04' - access condition not fulfilled [CR3].*

- d) The ME simulator sends a VERIFY CHV command to the SIM.
- e) The ME simulator sends an UPDATE RECORD command using ABSOLUTE mode with record 1 to the SIM. The data used is 'C2' for all bytes.

*The status condition returned by the SIM shall be SW1='90', SW2='00' - normal ending of command [CR3].*

- f) The ME simulator sends a READ RECORD command using ABSOLUTE mode with record 1 to the SIM.

*The record data returned shall be 'C2' for all bytes [CR1-3,7].*

- g) The ME simulator sends SELECT commands to the SIM to select EF<sub>ADN</sub> under DF<sub>TELECOM</sub>.
- h) The ME simulator sends an UPDATE RECORD command using NEXT mode to the SIM. The data used is 'D0' for all bytes.
- i) The ME simulator sends an UPDATE RECORD command using ABSOLUTE mode with record 2 to the SIM. The data used is 'C3' for all bytes.

- j) The ME simulator sends a READ RECORD command using ABSOLUTE mode with record 2 to the SIM.

*The record data returned shall be 'C3' for all bytes [CR7].*

- k) The ME simulator sends an UPDATE RECORD command using CURRENT mode to the SIM. The data used is 'C4' for all bytes.

- l) The ME simulator sends a READ RECORD command using ABSOLUTE mode with record 1 to the SIM.

*The record data returned shall be 'C4' for all bytes [CR5,8].*

- m) The ME simulator sends an UPDATE RECORD command using NEXT mode to the SIM. The data used is 'C5' for all bytes.

- n) The ME simulator sends a READ RECORD command using ABSOLUTE mode with record 2 to the SIM.

*The record data returned shall be 'C5' for all bytes [CR8].*

- o) The ME simulator sends an UPDATE RECORD command using ABSOLUTE mode with the last record to the SIM. The data used is 'C7' for all bytes.

- p) The ME simulator sends a READ RECORD command using ABSOLUTE mode with the last record to the SIM.

*The record data returned shall be 'C7' for all bytes [CR7].*

- q) The ME simulator sends an UPDATE RECORD command using ABSOLUTE mode with the last record + 1 to the SIM. The data used is 'C8' for all bytes.

*The status condition returned by the SIM shall be SW1='94', SW2='02' - out of range.*

- r) The ME simulator sends an UPDATE RECORD command using CURRENT mode to the SIM. The data used is 'C9' for all bytes.

- s) The ME simulator sends a READ RECORD command using ABSOLUTE mode with record 2 to the SIM.

*The record data returned shall be 'C9' for all bytes [CR16].*

- t) The ME simulator sends SELECT commands to the SIM to select EF<sub>ACM</sub> under DF<sub>GSM</sub>.
- u) The ME simulator sends an UPDATE RECORD command using CURRENT mode to the SIM. The data used is 'CA' for all bytes.

*The status condition returned by the SIM shall be SW1='6B', SW2='XX' - file is inconsistent with the command [CR4].*

- v) The ME simulator sends an UPDATE RECORD command using ABSOLUTE mode with record 3 to the SIM. The data used is 'CB' for all bytes.

*The status condition returned by the SIM shall be SW1='6B', SW2='XX' - file is inconsistent with the command [CR4].*

## Test procedure 2 and Requirements

- a) The ME simulator resets the SIM.
- b) The ME simulator sends a VERIFY CHV command to the SIM.
- c) The ME simulator sends SELECT commands to the SIM to select EF<sub>ADN</sub> under DF<sub>TELECOM</sub>.
- d) The ME simulator sends an UPDATE RECORD command using NEXT mode to the SIM. The data used is 'C2' for all bytes.
- e) The ME simulator sends a READ RECORD command using ABSOLUTE mode with record 1 to the SIM.

*The record data returned shall be 'C2' for all bytes [CR10].*

- f) The ME simulator sends an UPDATE RECORD command using CURRENT mode to the SIM. The data used is 'C3' for all bytes.
- g) The ME simulator sends a READ RECORD command using ABSOLUTE mode with record 1 to the SIM.

*The record data returned shall be 'C3' for all bytes [CR10].*

- h) The ME simulator sends an UPDATE RECORD command using NEXT mode to the SIM with P1 = 'FF'. The data used is 'C4' for all bytes.

*The status condition returned by the SIM shall be SW1='90', SW2='00' - normal ending of command [CR17].*

- i) The ME simulator sends a READ RECORD command using ABSOLUTE mode with record 2 to the SIM.

*The record data returned shall be 'C4' for all bytes [CR9,17].*

- j) The ME simulator sends an UPDATE RECORD command using CURRENT mode to the SIM. The data used is 'C5' for all bytes.

- k) The ME simulator sends a READ RECORD command using ABSOLUTE mode with record 2 to the SIM.

*The record data returned shall be 'C5' for all bytes [CR9].*

- l) The ME simulator sends a SELECT command to the SIM to select EF<sub>ADN</sub>.

- m) The ME simulator sends an UPDATE RECORD command using PREVIOUS mode to the SIM. The data used is 'C6' for all bytes.

- n) The ME simulator sends a READ RECORD command using ABSOLUTE mode with the last record to the SIM.

*The record data returned shall be 'C6' for all bytes [CR13].*

- o) The ME simulator sends an UPDATE RECORD command using NEXT mode to the SIM. The data used is 'C7' for all bytes.

*The status condition returned by the SIM shall be SW1='94', SW2='02' - out of range [CR11].*

- p) The ME simulator sends an UPDATE RECORD command using CURRENT mode to the SIM. The data used is 'C8' for all bytes.
- q) The ME simulator sends a READ RECORD command using ABSOLUTE mode with the last record to the SIM.  
*The record data returned shall be 'C8' for all bytes [CR16].*
- r) The ME simulator sends an UPDATE RECORD command using PREVIOUS mode with P1 = 'FF' to the SIM. The data used is 'C9' for all bytes.  
*The status condition returned by the SIM shall be SW1='90', SW2='00' - normal ending of command [CR17].*
- s) The ME simulator sends a READ RECORD command using ABSOLUTE mode with the second last record to the SIM.  
*The record data returned shall be 'C9' for all bytes [CR12,17].*
- t) The ME simulator sends a SELECT command to the SIM to select EF<sub>ADN</sub>.
- u) The ME simulator sends an UPDATE RECORD command using NEXT mode to the SIM. The data used is 'CA' for all bytes.
- v) The ME simulator sends an UPDATE RECORD command using PREVIOUS mode to the SIM. The data used is 'CB' for all bytes.  
*The status condition returned by the SIM shall be SW1='94', SW2='02' - out of range [CR13].*
- w) The ME simulator sends an UPDATE RECORD command using CURRENT mode to the SIM. The data used is 'CC' for all bytes.
- x) The ME simulator sends a READ RECORD command using ABSOLUTE mode with record 1 to the SIM.  
*The record data returned shall be 'CC' for all bytes [CR16].*
- y) The ME simulator sends SELECT commands to the SIM to select EF<sub>ACM</sub> under DF<sub>GSM</sub>.
- z) The ME simulator sends an UPDATE RECORD command using PREVIOUS mode to the SIM. The data used is 'CD' for all bytes.
- aa) The ME simulator sends a READ RECORD command using ABSOLUTE mode with the first record (record 1) to the SIM.  
*The record data returned shall be 'CD' for all bytes [CR15].*
- ab) The ME simulator sends an UPDATE RECORD command using NEXT mode to the SIM. The data used is 'C2' for all bytes.  
*The status condition returned by the SIM shall be SW1='6B', SW2='XX' - file is inconsistent with the command [CR4].*

## 6.5.7 SEEK function

### 6.5.7.1 Definition and applicability

It shall be mandatory for all cards complying with GSM 11.11 [1] to support all functions described therein.

### 6.5.7.2 Conformance requirement

- CR1 The SEEK function shall search through the current linear fixed EF to find a record starting with the given pattern.
- CR2 The function shall accept as an input, the type and mode, pattern and length of pattern.
- CR3 The SEEK function shall support both type 1 and type 2.

- CR4 For a type 2 SEEK, the function shall output the record number.
- CR5 The SEEK function shall support the following modes:
- from the beginning forwards
  - from the end backwards
  - from the next location forwards
  - from the previous location backwards
- CR6 The function shall only be performed if the READ access condition for the current EF is satisfied.
- CR7 If the parameter P3 indicates a pattern-length greater than the record length, the SIM shall send the status information 'incorrect parameter P3'.
- CR8 The SIM shall be able to accept any pattern length from 1 to 16 bytes inclusive.
- CR9 For a SEEK function of next location forwards, if the record pointer has not been previously set within the selected linear fixed EF, the search begins with the **first** record.
- CR10 For a SEEK function of previous location backwards, if the record pointer has not been previously set within the selected linear fixed EF, the search begins with the **last** record.
- CR11 After a successful SEEK function, the record pointer shall be set to the record in which the pattern was found.
- CR12 The record pointer shall not be changed by an unsuccessful SEEK function.

Reference: GSM 11.11 [1], subclause 8.7.

Test Group Reference (TGR): TGR\_SIM\_FN

Test Procedure Reference (TPR): TPR\_SIM\_FN\_SEEK

### 6.5.7.3 Test purpose

To verify that the SEEK function conforms to the above requirements for the different modes available.

### 6.5.7.4 Method of test

#### Initial conditions

- The SIM is connected to an ME simulator.
- The records in EF<sub>ADN</sub> contain the following data for the first 16 bytes:

record 1: 'A0 A1 A2 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D'

record 2: 'A0 A1 A2 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D'

The data for the remainder of these two records and for all other records is 'FF'.

#### Test procedure

- The ME simulator resets the SIM.
- The ME simulator sends SELECT commands to the SIM to select EF<sub>ADN</sub> under DF<sub>TELECOM</sub>.
- The ME simulator sends a type 1 SEEK command using the 'from the beginning forwards' mode, a pattern-length of 1, and pattern 'A0' to the SIM.

*The status condition returned by the SIM shall be SW1='98', SW2='04' - access condition not fulfilled [CR6].*

- The ME simulator sends a VERIFY CHV command to the SIM.

- e) The ME simulator sends a type 1 SEEK command using the 'from the beginning forwards' mode, a pattern-length of 1, and pattern 'A0' to the SIM.

*The status condition returned by the SIM shall be SW1='90', SW2='00' - normal ending of command [CR1-3,6].*

- f) The ME simulator sends SELECT commands to the SIM to select EF<sub>ADN</sub> under DF<sub>TELECOM</sub>.

- g) The ME simulator sends a type 2 SEEK command using the 'from the beginning forwards' mode, a pattern-length of 1, and pattern 'A0' to the SIM.

*The status condition returned by the SIM shall be SW1='9F', SW2='01' [CR1-3,8].*

- h) The ME simulator sends a GET RESPONSE command to the SIM.

*The response data shall be '01' indicating that the first record has been found [CR4].*

- i) The ME simulator sends a type 2 SEEK command using the 'from the beginning forwards' mode, a pattern-length of 3, and pattern 'A0 A1 A2' to the SIM.

- j) The ME simulator sends a GET RESPONSE command to the SIM.

*The response data shall be '01' indicating that the first record has been found [CR5a].*

- k) The ME simulator sends a type 2 SEEK command using the 'from the end backwards' mode, a pattern-length of 3, and pattern 'A0 A1 A2' to the SIM.

- l) The ME simulator sends a GET RESPONSE command to the SIM.

*The response data shall be '02' indicating that the second record has been found [CR5b].*

- m) The ME simulator sends a type 2 SEEK command using the 'from the previous location backwards' mode, a pattern-length of 16, and the following pattern to the SIM:

'A0 A1 A2 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D'

*The status condition returned by the SIM shall be SW1='9F', SW2='01' [CR8].*

- n) The ME simulator sends a GET RESPONSE command to the SIM.

*The response data shall be '01' indicating that the first record has been found [CR5d].*

- o) The ME simulator sends a type 2 SEEK command using the 'from the next location forwards' mode, a pattern-length of 3, and pattern 'A0 A1 A2' to the SIM.

- p) The ME simulator sends a GET RESPONSE command to the SIM.

*The response data shall be '02' indicating that the second record has been found [CR5c].*

- q) The ME simulator sends a SELECT command to the SIM to select EF<sub>ADN</sub> again.

- r) The ME simulator sends a type 2 SEEK command using the 'from the next location forwards' mode, a pattern-length of 3, and pattern 'A0 A1 A2' to the SIM.

- s) The ME simulator sends a GET RESPONSE command to the SIM to retrieve the single byte of response data.

*The response data shall be '01' indicating that the first record has been found [CR9].*

- t) The ME simulator sends a SELECT command to the SIM to select EF<sub>ADN</sub> again.

- u) The ME simulator sends a type 2 SEEK command using the 'from the previous location backwards' mode, a pattern-length of 3, and pattern 'A0 A1 A2' to the SIM.

- v) The ME simulator sends a GET RESPONSE command to the SIM.

*The response data shall be '02' indicating that the second record has been found [CR10].*

- w) The ME simulator sends a READ RECORD command using CURRENT mode to the SIM.

*The record data returned shall be that of the second record in EF<sub>ADN</sub> [CR11].*

- x) The ME simulator sends a type 2 SEEK command using the 'from the beginning forwards' mode, a pattern-length of 5, and pattern 'A1 A2 11 12 13' to the SIM.

The status condition returned by the SIM shall be SW1='94', SW2='04' - pattern not found [CR1].

- y) The ME simulator sends a READ RECORD command using CURRENT mode to the SIM.

*The record data returned shall be that of the second record in EF<sub>ADN</sub> [CR12].*

- z) The ME simulator sends SELECT commands to the SIM to select EF<sub>ADN</sub> under DF<sub>TELECOM</sub>.

- aa) The ME simulator sends a type 2 SEEK command using the 'from the beginning forwards' mode, a pattern-length of one more than the record size of EF<sub>ADN</sub>, and 'FF' for all pattern bytes to the SIM.

*The status condition returned by the SIM shall be SW1='67', SW2='XX' - incorrect parameter P3 [CR7].*

## 6.5.8 INCREASE function

### 6.5.8.1 Definition and applicability

It shall be mandatory for all cards complying with GSM 11.11 [1] and containing EF<sub>ACM</sub> and EF<sub>ACMMAX</sub> to support all functions described therein.

### 6.5.8.2 Conformance requirement

- CR1 This function shall add the value given to the value of the last increased/updated record of the current cyclic EF and store the result into the oldest record.
- CR2 The record pointer shall be set to this record and this record becomes the first record.
- CR3 The function shall only be used if the INCREASE access condition is fulfilled.
- CR4 The function shall accept as an input, the value to be added.
- CR5 The function shall output the value of the increased record and the value which has been added.
- CR6 The SIM shall not perform the INCREASE if the result would exceed the maximum value of the record (represented by all bytes set to 'FF').

Reference: GSM 11.11 [1], subclause 8.8.

Test Group Reference (TGR): TGR\_SIM\_FN

Test Procedure Reference (TPR): TPR\_SIM\_FN\_INC

### 6.5.8.3 Test purpose

To verify that the INCREASE function conforms to the above requirements.

### 6.5.8.4 Method of test

#### Initial conditions

- 1) The SIM is connected to an ME simulator.
- 2) Each record in EF<sub>ACM</sub> contains the data '00 00 01'.

#### Test procedure

- a) The ME simulator resets the SIM.

- b) The ME simulator sends SELECT commands to the SIM to select EF<sub>ACM</sub> under DF<sub>GSM</sub>.
- c) The ME simulator sends an INCREASE command with value '00 00 02' to the SIM.  
*The status condition returned by the SIM shall be SW1='98', SW2='04' - access condition not fulfilled [CR3].*
- d) The ME simulator sends a VERIFY CHV command to the SIM.
- e) The ME simulator sends an INCREASE command with value '00 00 03' to the SIM.  
*The status condition returned by the SIM shall be SW1='9F', SW2='06' [CR4].*
- f) The ME simulator sends a GET RESPONSE command to the SIM.  
*The response data shall be '00 00 04 00 00 03' [CR1,5].*
- g) The ME simulator sends an INCREASE command with value '01 02 00' to the SIM.
- h) The ME simulator sends a GET RESPONSE command to the SIM.  
*The response data shall be '01 02 04 01 02 00' [CR1].*
- i) The ME simulator sends a READ RECORD command using ABSOLUTE mode with record 1 to the SIM.  
*The data read shall be '01 02 04' [CR2].*
- j) The ME simulator sends an INCREASE command with value ' FF 00 00' to the SIM.  
*The status condition returned by the SIM shall be SW1='98', SW2='50' - increase cannot be performed - Max value reached [CR6].*
- k) The ME simulator sends an INCREASE command with value '00 FF FD' to the SIM.
- l) The ME simulator sends a GET RESPONSE command to the SIM.  
*The response data shall be '02 02 01 00 FF FD' [CR5].*

## 6.5.9 VERIFY CHV function

### 6.5.9.1 Definition and applicability

It shall be mandatory for all cards complying with GSM 11.11 [1] to support all functions described therein.

### 6.5.9.2 Conformance requirement

- CR1 This function shall verify the CHV presented by comparing it with the one stored in the SIM.
- CR2 The function shall accept as input, an indication of CHV1/CHV2 and the CHV.
- CR3 The verification process shall be subject to the following conditions being fulfilled:
- a) CHV is not disabled
  - b) CHV is not blocked
- CR4 If the access condition for a function to be performed on a file is CHV1 or CHV2, then a successful verification of the relevant CHV shall be required prior to the use of the function on this file unless the CHV is disabled.
- CR5 If the CHV presented is correct, the number of remaining CHV attempts for that CHV shall be reset to its initial value 3.
- CR6 If the CHV presented is false, the number of remaining CHV attempts for that CHV shall be decremented.

CR7 After 3 consecutive false CHV attempts, not necessarily in the same card session, the respective CHV shall be blocked and the access condition never fulfilled until the UNBLOCK CHV function has been successfully performed on the respective CHV.

Reference: GSM 11.11 [1], subclause 8.9.

Test Group Reference (TGR): TGR\_SIM\_FN

Test Procedure Reference (TPR): TPR\_SIM\_FN\_VERCHV

### 6.5.9.3 Test purpose

To verify that the VERIFY CHV function conforms to the above requirements.

NOTE: This function is only tested for CHV1. It is assumed that if the function operates correctly for CHV1, it will also operate correctly for CHV2 or other CHV.

#### Initial conditions

- 1) The SIM is connected to an ME simulator.
- 2) CHV1 on the SIM is set to '00000000'.

#### Test procedure

- a) The ME simulator resets the SIM.
- b) The ME simulator sends SELECT commands to the SIM to select EF<sub>Kc</sub> under DF<sub>GSM</sub>.
- c) The ME simulator sends a READ BINARY command using a length of 2 bytes to the SIM.  
*The status condition returned by the SIM shall be SW1='98', SW2='04' - access condition not fulfilled [CR4].*
- d) The ME simulator sends a VERIFY CHV command to the SIM.  
*The status condition returned by the SIM shall be SW1='90', SW2='00' - normal ending of command [CR1,2].*
- e) The ME simulator sends a READ BINARY command using a length of 2 bytes to the SIM.  
*The status condition returned by the SIM shall be SW1='90', SW2='00' - normal ending of command [CR4].*
- f) The ME simulator sends a VERIFY CHV command with **incorrect** CHV1 to the SIM.  
*The status condition returned by the SIM shall be SW1='98', SW2='04' -unsuccessful CHV verification, at least one attempt left.*
- g) The ME simulator sends a STATUS command to the SIM.  
*The following shall be true of the response data [CR6]:*
  - Bits 1 through 4 of byte 19 shall indicate two VERIFY CHV1 attempts remaining.
- h) The ME simulator sends a VERIFY CHV command to the SIM.
- i) The ME simulator sends a STATUS command to the SIM.  
*The following shall be true of the response data [CR5]:*
  - Bits 1 through 4 of byte 19 shall indicate three VERIFY CHV1 attempts remaining.
- j) The ME simulator sends a VERIFY CHV command with **incorrect** CHV1 to the SIM.  
*The status condition returned by the SIM shall be SW1='98', SW2='04' -unsuccessful CHV verification, at least one attempt left.*
- k) The ME simulator sends a VERIFY CHV command with **incorrect** CHV1 to the SIM.

*The status condition returned by the SIM shall be SW1='98', SW2='04' -unsuccessful CHV verification, at least one attempt left.*

- l) The ME simulator resets the SIM.
- m) The ME simulator sends a VERIFY CHV command with **incorrect** CHV1 to the SIM.

*The status condition returned by the SIM shall be SW1='98', SW2='40' - unsuccessful CHV verification, no attempt left[CR7].*

- n) The ME simulator resets the SIM.
- o) The ME simulator sends a VERIFY CHV command to the SIM.

*The status condition returned by the SIM shall be SW1='98', SW2='40' - CHV blocked [CR3b,7].*

- p) The ME simulator sends SELECT commands to the SIM to select EF<sub>Kc</sub> under DF<sub>GSM</sub>.
- q) The ME simulator sends a READ BINARY command using a length of 2 bytes to the SIM.

*The status condition returned by the SIM shall be SW1='98', SW2='04' - CHV blocked [CR7].*

- r) The ME simulator sends an UNBLOCK CHV command to the SIM.

*The status condition returned by the SIM shall be SW1='90', SW2='00' - normal ending of command [CR7].*

- s) The ME simulator sends a DISABLE CHV command to the SIM.
- t) The ME simulator resets the SIM.

- u) The ME simulator sends SELECT commands to the SIM to select EF<sub>Kc</sub> under DF<sub>GSM</sub>.

- v) The ME simulator sends a READ BINARY command using a length of 2 bytes to the SIM.

*The status condition returned by the SIM shall be SW1='90', SW2='00' - normal ending of command [CR4].*

- w) The ME simulator sends a VERIFY CHV command to the SIM.

*The status condition returned by the SIM shall be SW1='98', SW2='08' - in contradiction with CHV status [CR3].*

## 6.5.10 CHANGE CHV function

### 6.5.10.1 Definition and applicability

It shall be mandatory for all cards complying with GSM 11.11 [1] to support all functions described therein.

### 6.5.10.2 Conformance requirement

CR1 This function shall assign a new value to the relevant CHV, subject to the following conditions being fulfilled:

- a) CHV is not disabled
- b) CHV is not blocked

CR2 The function shall accept as input, an indication of CHV1/CHV2 and the old and new CHV.

CR3 If the old CHV presented is correct, the number of remaining CHV attempts for that CHV shall be reset to its initial value 3 and the new value for the CHV shall become valid.

CR4 If the old CHV presented is false, the number of remaining CHV attempts for that CHV shall be decremented and the value of the CHV shall remain unchanged.

CR5 After 3 consecutive false CHV presentations, not necessarily in the same card session, the respective CHV shall be blocked and the access condition never fulfilled until the UNBLOCK CHV function has been successfully performed on the respective CHV.

Reference: GSM 11.11 [1], subclause 8.10.

Test Group Reference (TGR): TGR\_SIM\_FN

Test Procedure Reference (TPR): TPR\_SIM\_FN\_CHCHV

### 6.5.10.3 Test purpose

To verify that the CHANGE CHV function conforms to the above requirements.

NOTE: This function is only tested for CHV1. It is assumed that if the function operates correctly for CHV1, it will also operate correctly for CHV2 or other CHV.

### 6.5.10.4 Method of test

#### Initial conditions

- 1) The SIM is connected to an ME simulator.
- 2) CHV1 on the SIM is set to '00000000'.

#### Test procedure

- a) The ME simulator resets the SIM.
- b) The ME simulator sends a CHANGE CHV command with an **incorrect** old CHV1 of '11111111' and new CHV1 of '33333333' to the SIM.

*The status condition returned by the SIM shall be SW1='98', SW2='04' - unsuccessful CHV verification, at least one attempt left.*

- c) The ME simulator sends a STATUS command to the SIM.

*The following shall be true of the response data [CR4]:*

- *Bits 1 through 4 of byte 19 shall indicate two VERIFY CHV1 attempts remaining.*

- d) The ME simulator sends a CHANGE CHV command with an old CHV1 of '00000000' and new CHV1 of '33333333' to the SIM.

*The status condition returned by the SIM shall be SW1='90', SW2='00' - normal ending of command [CR2].*

- e) The ME simulator sends a STATUS command to the SIM.

*The following shall be true of the response data [CR3]:*

- *Bits 1 through 4 of byte 19 shall indicate three VERIFY CHV1 attempts remaining.*

- f) The ME simulator sends a CHANGE CHV command with an **incorrect** old CHV1 of '00000000' and new CHV1 of '55555555' to the SIM.

*The status condition returned by the SIM shall be SW1='98', SW2='04' - unsuccessful CHV verification, at least one attempt left.*

- g) The ME simulator sends a CHANGE CHV command with an **incorrect** old CHV1 of '55555555' and new CHV1 of '33333333' to the SIM.

*The status condition returned by the SIM shall be SW1='98', SW2='04' - unsuccessful CHV verification, at least one attempt left.*

- h) The ME simulator resets the SIM.

- i) The ME simulator sends a CHANGE CHV command with an **incorrect** old CHV1 of '00000000' and new CHV1 of '55555555' to the SIM.

*The status condition returned by the SIM shall be SW1='98', SW2='40' - unsuccessful CHV verification, no attempt left [CR5].*

- j) The ME simulator resets the SIM.

- k) The ME simulator sends a CHANGE CHV command with an old CHV1 of '33333333' and new CHV1 of '55555555' to the SIM.

*The status condition returned by the SIM shall be SW1='98', SW2='40' - CHV blocked [CR1b,5].*

- l) The ME simulator sends an UNBLOCK CHV command with new CHV1 of '55555555' to the SIM.

*The status condition returned by the SIM shall be SW1='90', SW2='00' - normal ending of command [CR5].*

- m) The ME simulator sends a DISABLE CHV command to the SIM.

- n) The ME simulator resets the SIM.

- o) The ME simulator sends a CHANGE CHV command with an old CHV1 '55555555' and new CHV1 of '77777777' to the SIM.

*The status condition returned by the SIM shall be SW1='98', SW2='08' - in contradiction with CHV status [CR1a].*

- p) The ME simulator sends an ENABLE CHV command to the SIM with CHV1 '55555555'.

*The status condition returned by the SIM shall be SW1='90', SW2='00' - normal ending of command [CR1a].*

## 6.5.11 DISABLE CHV function

### 6.5.11.1 Definition and applicability

It shall be mandatory for all cards complying with GSM 11.11 [1] to support all functions described therein.

### 6.5.11.2 Conformance requirement

CR1 The successful execution of this function shall have the effect that files protected by CHV1 are now accessible as if they were marked 'ALWAYS'.

CR2 The function shall accept as input, CHV1.

CR3 This function shall not be executed by the SIM when CHV1 is already disabled or blocked.

CR4 If the CHV1 presented is correct, the number of remaining CHV1 attempts shall be reset to its initial value 3 and CHV1 shall be disabled.

CR5 If the CHV1 presented is false, the number of remaining CHV1 attempts shall be decremented and CHV1 shall remain enabled.

CR6 After 3 consecutive false CHV1 presentations, not necessarily in the same card session, CHV1 shall be blocked and the access condition never fulfilled until the UNBLOCK CHV function has been successfully performed on CHV1.

Reference: GSM 11.11 [1], subclause 8.11.

Test Group Reference (TGR): TGR\_SIM\_FN

Test Procedure Reference (TPR): TPR\_SIM\_FN\_DISCHV

### 6.5.11.3 Test purpose

To verify that the DISABLE CHV function conforms to the above requirements.

### 6.5.11.4 Method of test

#### Initial conditions

- 1) The SIM is connected to an ME simulator.

#### Test procedure

- a) The ME simulator resets the SIM.
- b) The ME simulator sends SELECT commands to the SIM to select EF<sub>LOC1</sub> under DF<sub>GSM</sub>.
- c) The ME simulator sends a READ BINARY command using a length of 2 bytes to the SIM.

*The status condition returned by the SIM shall be SW1='98', SW2='04' - access condition not fulfilled.*

- d) The ME simulator sends a DISABLE CHV command with **incorrect** CHV1 to the SIM.

*The status condition returned by the SIM shall be SW1='98', SW2='04' - unsuccessful CHV verification, at least one attempt left [CR5].*

- e) The ME simulator sends a READ BINARY command using a length of 2 bytes to the SIM.

*The status condition returned by the SIM shall be SW1='98', SW2='04' - access condition not fulfilled [CR5].*

- f) The ME simulator sends a STATUS command to the SIM.

*The following shall be true of the response data [CR5]:*

- Bit 8 of byte 14 shall be 0 indicating that CHV1 is still enabled.
- Bits 1 through 4 of byte 19 shall indicate two VERIFY CHV1 attempts remaining.

- g) The ME simulator sends a DISABLE CHV command to the SIM.

*The status condition returned by the SIM shall be SW1='90', SW2='00' - normal ending of command [CR2].*

- h) The ME simulator sends a STATUS command to the SIM.

*The following shall be true of the response data [CR4]:*

- Bit 8 of byte 14 shall be 1 indicating that CHV1 is now disabled.
- Bits 1 through 4 of byte 19 shall indicate three VERIFY CHV1 attempts remaining.

- i) The ME simulator sends an ENABLE CHV command to the SIM.

*The status condition returned by the SIM shall be SW1='90', SW2='00' - normal ending of command.*

- j) The ME simulator sends a READ BINARY command using a length of 2 bytes to the SIM.

*The status condition returned by the SIM shall be SW1='90', SW2='00' - normal ending of command [CR1].*

- k) The ME simulator sends a DISABLE CHV command with **incorrect** CHV1 to the SIM.

*The status condition returned by the SIM shall be SW1='98', SW2='04' - unsuccessful CHV verification, at least one attempt left.*

- l) The ME simulator sends a DISABLE CHV command with **incorrect** CHV1 to the SIM.

*The status condition returned by the SIM shall be SW1='98', SW2='04' - unsuccessful CHV verification, at least one attempt left.*

- m) The ME simulator resets the SIM.
- n) The ME simulator sends a DISABLE CHV command with **incorrect** CHV1 to the SIM.

*The status condition returned by the SIM shall be SW1='98', SW2='40' - unsuccessful CHV verification, no attempt left [CR6].*

- o) The ME simulator resets the SIM.
- p) The ME simulator sends a DISABLE CHV command to the SIM.

*The status condition returned by the SIM shall be SW1='98', SW2='40' - CHV blocked [CR3,6].*

- q) The ME simulator sends an UNBLOCK CHV command to the SIM.

*The status condition returned by the SIM shall be SW1='90', SW2='00' - normal ending of command [CR6].*

- r) The ME simulator sends a DISABLE CHV command to the SIM.
- s) The ME simulator sends a DISABLE CHV command to the SIM.

*The status condition returned by the SIM shall be SW1='98', SW2='08' - in contradiction with CHV status [CR3].*

## 6.5.12 ENABLE CHV function

### 6.5.12.1 Definition and applicability

It shall be mandatory for all cards complying with GSM 11.11 [1] to support all functions described therein.

### 6.5.12.2 Conformance requirement

CR1 The successful execution of this function shall have the effect that files accessible as if they were marked 'ALWAYS' due to CHV1 being disabled are now protected by CHV1.

CR2 The function shall accept as input, CHV1.

CR3 This function shall not be executed by the SIM when CHV1 is already enabled or blocked.

CR4 If the CHV1 presented is correct, the number of remaining CHV1 attempts shall be reset to its initial value 3 and CHV1 shall be enabled.

CR5 If the CHV1 presented is false, the number of remaining CHV1 attempts shall be decremented and CHV1 shall remain disabled.

CR6 After 3 consecutive false CHV1 presentations, not necessarily in the same card session, CHV1 shall be blocked and the access condition never fulfilled until the UNBLOCK CHV function has been successfully performed on CHV1.

Reference: GSM 11.11 [1], subclause 8.12.

Test Group Reference (TGR): TGR\_SIM\_FN

Test Procedure Reference (TPR): TPR\_SIM\_FN\_ENCHV

### 6.5.12.3 Test purpose

To verify that the ENABLE CHV function conforms to the above requirements.

### 6.5.12.4 Method of test

#### Initial conditions

- 1) The SIM is connected to an ME simulator.
- 2) CHV1 on the SIM is disabled.

### Test procedure

- a) The ME simulator resets the SIM.

- b) The ME simulator sends SELECT commands to the SIM to select EF<sub>LOC1</sub> under DF<sub>GSM</sub>.

- c) The ME simulator sends a READ BINARY command using a length of 2 bytes to the SIM.

*The status condition returned by the SIM shall be SW1='90', SW2='00' - normal ending of command.*

- d) The ME simulator sends an ENABLE CHV command with **incorrect** CHV1 to the SIM.

*The status condition returned by the SIM shall be SW1='98', SW2='04' - unsuccessful CHV verification, at least one attempt left.*

- e) The ME simulator sends a READ BINARY command using a length of 2 bytes to the SIM.

*The status condition returned by the SIM shall be SW1='90', SW2='00' - access condition not fulfilled [CR1].*

- f) The ME simulator sends a STATUS command to the SIM.

*The following shall be true of the response data [CR5]:*

- Bit 8 of byte 14 shall be 1 indicating that CHV1 is still disabled.
- Bits 1 through 4 of byte 19 shall indicate two VERIFY CHV1 attempts remaining.

- g) The ME simulator sends an ENABLE CHV command to the SIM.

*The status condition returned by the SIM shall be SW1='90', SW2='00' - normal ending of command [CR2].*

- h) The ME simulator sends a STATUS command to the SIM.

*The following shall be true of the response data [CR4]:*

- Bit 8 of byte 14 shall be 0 indicating that CHV1 is now enabled.
- Bits 1 through 4 of byte 19 shall indicate three VERIFY CHV1 attempts remaining.

- i) The ME simulator resets the SIM.

- j) The ME simulator sends SELECT commands to the SIM to select EF<sub>LOC1</sub> under DF<sub>GSM</sub>.

- k) The ME simulator sends a READ BINARY command using a length of 2 bytes to the SIM.

*The status condition returned by the SIM shall be SW1='98', SW2='04' - access condition not fulfilled [CR1].*

- l) The ME simulator sends a DISABLE CHV command to the SIM.

- m) The ME simulator sends an ENABLE CHV command with **incorrect** CHV1 to the SIM.

*The status condition returned by the SIM shall be SW1='98', SW2='04' - unsuccessful CHV verification, at least one attempt left.*

- n) The ME simulator sends an ENABLE CHV command with **incorrect** CHV1 to the SIM.

*The status condition returned by the SIM shall be SW1='98', SW2='04' - unsuccessful CHV verification, at least one attempt left.*

- o) The ME simulator resets the SIM.

- p) The ME simulator sends an ENABLE CHV command with **incorrect** CHV1 to the SIM.

*The status condition returned by the SIM shall be SW1='98', SW2='40' - unsuccessful CHV verification, no attempt left [CR6].*

q) The ME simulator resets the SIM.

r) The ME simulator sends an ENABLE CHV command to the SIM.

*The status condition returned by the SIM shall be SW1='98', SW2='40' or SW1='98', SW2='08' -CHV blocked [CR3,6].*

s) The ME simulator sends an UNBLOCK CHV command to the SIM.

*The status condition returned by the SIM shall be SW1='90', SW2='00' - normal ending of command [CR6].*

t) The ME simulator sends ENABLE CHV command to the SIM.

*The status condition returned by the SIM shall be SW1='98', SW2='08' - in contradiction with CHV status [CR3].*

## 6.5.13 UNBLOCK CHV function

### 6.5.13.1 Definition and applicability

It shall be mandatory for all cards complying with GSM 11.11 [1] to support all functions described therein.

### 6.5.13.2 Conformance requirement

CR1 This function shall unblock a CHV which has been blocked by 3 consecutive wrong CHV presentations.

CR2 The function shall accept as input, an indication of CHV1/CHV2, the UNBLOCK CHV and the new CHV.

CR3 This function shall be performed regardless of whether or not the relevant CHV is blocked.

CR4 If the UNBLOCK CHV presented is correct, the new CHV value, presented together with the UNBLOCK CHV is stored in the relevant EFCHV, the number of remaining UNBLOCK CHV attempts for that UNBLOCK CHV is reset to its initial value 10 and the number of remaining CHV attempts for that CHV is reset to its initial value 3.

CR5 After a successful unblocking attempt, the CHV shall be enabled, and the relevant access condition level satisfied.

CR6 If the presented UNBLOCK CHV is false, the number of remaining UNBLOCK CHV attempts for that UNBLOCK CHV shall be decremented.

CR7 After 10 consecutive false UNBLOCK CHV presentations, not necessarily in the same card session, the respective UNBLOCK CHV shall be blocked.

CR8 A false UNBLOCK CHV shall have no effect on the status of the respective CHV itself.

Reference: GSM 11.11 [1], subclause 8.13.

Test Group Reference (TGR): TGR\_SIM\_FN

Test Procedure Reference (TPR): TPR\_SIM\_FN\_UNCHV

### 6.5.13.3 Test purpose

To verify that the UNBLOCK CHV function conforms to the above requirements.

NOTE 1: CR1 is tested in subclauses 6.5.9, 6.5.10, 6.5.11 and 6.5.12..

NOTE 2: This function is only tested for CHV1. It is assumed that if the function operates correctly for CHV1, it will also operate correctly for CHV2 or other CHV.

#### 6.5.13.4 Method of test

##### Initial conditions

- 1) The SIM is connected to an ME simulator.

##### Test procedure 1

- a) The ME simulator resets the SIM.  
 b) The ME simulator sends SELECT commands to the SIM to select EF<sub>Kc</sub> under DF<sub>GSM</sub>.  
 c) The ME simulator sends a VERIFY CHV command to the SIM.  
 d) The ME simulator sends an UNBLOCK CHV command with **incorrect** UNBLOCK CHV1 to the SIM.

*The status condition returned by the SIM shall be SW1='98', SW2='04' - unsuccessful UNBLOCK CHV verification, at least one attempt left.*

- e) The ME simulator sends a STATUS command to the SIM.

*The following shall be true of the response data [CR6,8]:*

- Bit 8 of byte 14 shall be 0 indicating that CHV1 is enabled.
- Bits 1 through 4 of byte 19 shall indicate three VERIFY CHV1 attempts remaining.
- Bits 1 through 4 of byte 20 shall indicate nine UNBLOCK CHV1 attempts remaining.

- f) The ME simulator sends a DISABLE CHV command to the SIM.

- g) The ME simulator sends an UNBLOCK CHV command with **incorrect** UNBLOCK CHV1 to the SIM.

*The status condition returned by the SIM shall be SW1='98', SW2='04' - unsuccessful UNBLOCK CHV verification, at least one attempt left.*

- h) The ME simulator sends a STATUS command to the SIM.

*The following shall be true of the response data [CR6,8]:*

- Bit 8 of byte 14 shall be 1 indicating that CHV1 is still disabled.
- Bits 1 through 4 of byte 19 shall indicate three VERIFY CHV1 attempts remaining.
- Bits 1 through 4 of byte 20 shall indicate eight UNBLOCK CHV1 attempts remaining.

- i) The ME simulator sends an UNBLOCK CHV command to the SIM.

*The status condition returned by the SIM shall be SW1='90', SW2='00' - normal ending of command [CR2].*

- j) The ME simulator sends a STATUS command to the SIM.

*The following shall be true of the response data [CR4,5]:*

- Bit 8 of byte 14 shall be 0 indicating that CHV1 is enabled
- Bits 1 through 4 of byte 19 shall indicate three VERIFY CHV1 attempts remaining.
- Bits 1 through 4 of byte 20 shall indicate ten UNBLOCK CHV1 attempts remaining.

- k) The ME simulator sends a VERIFY CHV command with **incorrect** CHV1 to the SIM.

*The status condition returned by the SIM shall be SW1='98', SW2='04' - unsuccessful CHV verification, at least one attempt left.*

- l) The ME simulator resets the SIM.

- m) The ME simulator sends an UNBLOCK CHV command to the SIM.

- n) The ME simulator sends a STATUS command to the SIM.

*The following shall be true of the response data [CR4]:*

- Bits 1 through 4 of byte 19 shall indicate three VERIFY CHV1 attempts remaining.

- o) The ME simulator sends SELECT commands to the SIM to select EF<sub>Kc</sub> under DF<sub>GSM</sub>.
- p) The ME simulator sends a READ BINARY command using a length of 2 bytes to the SIM.

*The status condition returned by the SIM shall be SW1='90', SW2='00' - normal ending of command [CR5].*

#### **Test procedure 2 - \*\*\* Destructive test \*\*\***

- a) The ME simulator resets the SIM.
- b) The ME simulator sends nine UNBLOCK CHV command with **incorrect** UNBLOCK CHV1 to the SIM.

*The status condition returned by the SIM each time shall be SW1='98', SW2='04' - unsuccessful UNBLOCK CHV verification, at least one attempt left.*

- c) The ME simulator resets the SIM.
- d) The ME simulator sends an UNBLOCK CHV command with **incorrect** UNBLOCK CHV1 to the SIM.

*The status condition returned by the SIM shall be SW1='98', SW2='40' - unsuccessful UNBLOCK CHV verification, no attempt left.*

- e) The ME simulator sends an UNBLOCK CHV command to the SIM.

*The status condition returned by the SIM shall be SW1='98', SW2='40' - UNBLOCK CHV blocked.*

## 6.5.14 INVALIDATE function

### 6.5.14.1 Definition and applicability

It shall be mandatory for all cards complying with GSM 11.11 [1] to support all functions described therein.

### 6.5.14.2 Conformance requirement

- CR1 This function shall invalidate the current EF.
- CR2 After an INVALIDATE function the respective flag in the file status shall be changed accordingly.
- CR3 The function shall only be performed if the INVALIDATE access condition for the current EF is satisfied.
- CR4 An invalidated file shall no longer be available within the application for any function except for the SELECT and REHABILITATE functions.

Reference: GSM 11.11 [1], subclause 8.14.

Test Group Reference (TGR): TGR\_SIM\_FN

Test Procedure Reference (TPR): TPR\_SIM\_FN\_INVALID

### 6.5.14.3 Test purpose

To verify that the INVALIDATE function conforms to the above requirements.

### 6.5.14.4 Method of test

#### **Initial conditions**

- 1) The SIM is connected to an ME simulator.

- 2) EF<sub>LOCI</sub> on the SIM is not invalidated.

### Test procedure

- a) The ME simulator resets the SIM.  
 b) The ME simulator sends SELECT commands to the SIM to select EF<sub>LOCI</sub> under DF<sub>GSM</sub>.  
 c) The ME simulator sends an INVALIDATE command to the SIM.

*The status condition returned by the SIM shall be SW1='98', SW2='04' - access condition not fulfilled [CR3].*

- d) The ME simulator gains the security access condition(s) specified for both INVALIDATE and REHABILITATE on EF<sub>LOCI</sub>.  
 e) The ME simulator sends a SELECT command to the SIM to select EF<sub>LOCI</sub> once more.  
 f) The ME simulator sends a GET RESPONSE command to the SIM.

*The following shall be true of the response data:*

- Bit 1 of byte 12 shall be 1 indicating that the file is **not** invalidated.

- g) The ME simulator sends an INVALIDATE command to the SIM.

*The status condition returned by the SIM shall be SW1='90', SW2='00' - normal ending of command [CR3].*

- h) The ME simulator sends a SELECT command to the SIM to select EF<sub>LOCI</sub> again.

*The status condition returned by the SIM shall be SW1='9F', SW2='XX' - length 'XX' of the response data [CR4].*

- i) The ME simulator sends a GET RESPONSE command to the SIM.

*The following shall be true of the response data [CR1,2]:*

- Bit 1 of byte 12 shall be 0 indicating that the file is invalidated.

- j) The ME simulator sends a VERIFY CHV command to the SIM.

- k) The ME simulator sends a UPDATE BINARY command using a length of 1 byte and data 'C1' to the SIM.

*The status condition returned by the SIM shall be SW1='98', SW2='10' - in contradiction with invalidation status [CR4].*

- l) The ME simulator sends a READ BINARY command to the SIM.

*The status condition returned by the SIM shall be SW1='98', SW2='10' - in contradiction with invalidation status [CR4].*

- m) The ME simulator sends a REHABILITATE command to the SIM.

*The status condition returned by the SIM shall be SW1='90', SW2='00' - normal ending of command [CR4].*

## 6.5.15 REHABILITATE function

### 6.5.15.1 Definition and applicability

It shall be mandatory for all cards complying with GSM 11.11 [1] to support all functions described therein.

### 6.5.15.2 Conformance requirement

CR1 This function shall rehabilitate an invalidated current EF.

CR2 After a REHABILITATE function the respective flag in the file status byte shall be changed accordingly.

CR3 The function shall only be performed if the REHABILITATE access condition for the current EF is satisfied.

Reference: GSM 11.11 [1], subclause 8.15.

Test Group Reference (TGR): TGR\_SIM\_FN

Test Procedure Reference (TPR): TPR\_SIM\_FN\_REHAB

### 6.5.15.3 Test purpose

To verify that the REHABILITATE function conforms to the above requirements.

### 6.5.15.4 Method of test

#### Initial conditions

- 1) The SIM is connected to an ME simulator.
- 2) EF<sub>LOCI</sub> on the SIM is invalidated.

#### Test procedure

- a) The ME simulator resets the SIM.
- b) The ME simulator sends SELECT commands to the SIM to select EF<sub>LOCI</sub> under DF<sub>GSM</sub>.
- c) The ME simulator sends a REHABILITATE command to the SIM.

*The status condition returned by the SIM shall be SW1='98', SW2='04' - access condition not fulfilled [CR3].*

- d) The ME simulator gains the security access condition(s) specified for both INVALIDATE and REHABILITATE on EF<sub>LOCI</sub>.
- e) The ME simulator sends a SELECT command to the SIM to select EF<sub>LOCI</sub> once more.
- f) The ME simulator sends a GET RESPONSE command to the SIM.

*The following shall be true of the response data:*

- Bit 1 of byte 12 shall be 0 indicating that the file is invalidated.

- g) The ME simulator sends a REHABILITATE command to the SIM.

*The status condition returned by the SIM shall be SW1='90', SW2='00' - normal ending of command [CR1,3].*

- h) The ME simulator sends a SELECT command to the SIM to select EF<sub>LOCI</sub> again.
- i) The ME simulator sends a GET RESPONSE command to the SIM.

*The following shall be true of the response data [CR1,2]:*

- Bit 1 of byte 12 shall be 1 indicating that the file is **no longer** invalidated.

- j) The ME simulator sends a VERIFY CHV command to the SIM.

- k) The ME simulator sends a UPDATE BINARY command using a length of 1 byte and data 'D1' to the SIM.

*The status condition returned by the SIM shall be SW1='90', SW2='00' - normal ending of command [CR1].*

## 6.5.16 RUN GSM ALGORITHM function

### 6.5.16.1 Definition and applicability

It shall be mandatory for all cards complying with GSM 11.11 [1] to support all functions described therein.

### 6.5.16.2 Conformance requirement

- CR1 This function shall cause the SIM to run the A3 and A8 algorithms using a 16 byte random number and the subscriber authentication key  $K_i$  stored in the SIM.
- CR2 The function shall return the signed response SRES and cipher key  $K_c$ .
- CR3 The function shall not be executable unless  $DF_{GSM}$  has been selected as the current directory.
- CR4 The function shall not be executable unless a successful CHV1 verification procedure has been performed.

Reference: GSM 11.11 [1], subclause 8.16.

Test Group Reference (TGR): TGR\_SIM\_FN

Test Procedure Reference (TPR): TPR\_SIM\_FN\_RUNGSM

### 6.5.16.3 Test purpose

To verify that the SIM conforms to the above requirements.

### 6.5.16.4 Method of test

#### Initial conditions

- 1) The SIM is connected to an ME simulator.

#### Test procedure

- a) The ME simulator resets the SIM.
- b) The ME simulator sends a SELECT command to the SIM to select  $DF_{GSM}$ .
- c) The ME simulator sends a RUN GSM ALGORITHM command to the SIM with random number:  
 '00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F'  
*The status condition returned by the SIM shall be SW1='98', SW2='04' - access condition not fulfilled [CR4].*
- d) The ME simulator resets the SIM.
- e) The ME simulator sends a VERIFY CHV command to the SIM.
- f) The ME simulator sends a RUN GSM ALGORITHM command to the SIM with random number:  
 '00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F'  
*The status condition returned by the SIM shall be SW1='94', SW2='08' - file inconsistent with command [CR3].*
- g) The ME simulator sends a SELECT command to the SIM to select  $DF_{GSM}$ .
- h) The ME simulator sends a RUN GSM ALGORITHM command to the SIM with random number:  
 '00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F'  
*The status condition returned by the SIM shall be SW1='9F', SW2='0C' - length 'XX' of the response data [CR3,4].*
- i) The ME simulator sends a GET RESPONSE command to the SIM.  
*The data returned shall be correct for the given A3 and A8 algorithms and  $K_i$  stored in the SIM [CR1,2].*

## 6.5.17 SLEEP function

### 6.5.17.1 Definition and applicability

It shall be mandatory for all cards complying with GSM 11.11 [1] to support all functions described therein.

This function is an obsolete GSM function which was issued by Phase 1 MEs.

### 6.5.17.2 Conformance requirement

CR1 The function shall always return a good status.

Reference: GSM 11.11 [1], subclause 8.17.

Test Group Reference (TGR): TGR\_SIM\_FN

Test Procedure Reference (TPR): TPR\_SIM\_FN\_SLEEP

### 6.5.17.3 Test purpose

To verify that the SLEEP function conforms to the above requirement.

### 6.5.17.4 Method of test

#### Initial conditions

- 1) The SIM is connected to an ME simulator.

#### Test procedure

- a) The ME simulator resets the SIM.
- b) The ME simulator sends a SLEEP command to the SIM.

*The status condition returned by the SIM shall be SW1='90', SW2='00' - normal ending of command [CR1].*

## 6.6 Description of the commands

The tests in this subclause ensure that the IUT conforms to the specification for the mapping of functions onto Application Protocol Data Units (APDUs) which are used by the transmission protocol.

### 6.6.1 Mapping principles

#### 6.6.1.1 Definition and applicability

The transmission protocol requires that the command and response Application Protocol Data Units (APDUs) are mapped using certain principles, in order to ensure correct operation in the GSM environment.

#### 6.6.1.2 Conformance requirement

CR1 The command APDU shall have format (CLA, INS, P1, P2, P3 {, data}).

CR2 The response APDU shall have format ({data}, SW1, SW2).

CR3 The class 'A0' shall be accepted by the SIM.

Reference: GSM 11.11 [1], subclause 9.1.

Test Group Reference (TGR): TGR\_SIM\_CMD\_MAP

Test Procedure Reference (TPR): TPR\_SIM\_CMD\_MAP

### 6.6.1.3 Test purpose

To verify that the SIM conforms to the above requirements.

### 6.6.1.4 Method of test

#### Initial conditions

- 1) The SIM is connected to an ME simulator.

#### Test procedure

- a) The ME simulator resets the SIM.
- b) The ME simulator gains the security access condition(s) specified by the administrative authority for both INVALIDATE and REHABILITATE on EF<sub>LOCAL</sub>.
- c) The ME simulator sends SELECT commands to the SIM to select DF<sub>GSM</sub>.
- d) The ME simulator sends a VERIFY CHV command to the SIM.
- e) The ME simulator sends a SELECT command to the SIM to select EF<sub>LOCAL</sub>.

[Bytes sent: CLA='A0', INS='A4', P1='00', P2='00', P3='02', data='6F 7E']

[Bytes received: SW1, SW2<sub>1</sub>]

*The SIM shall have sent SW1='9F' and SW2='lgth' [CR1].*

- f) The ME simulator sends a GET RESPONSE command to the SIM, requesting all of the available response data, as indicated by SW2<sub>1</sub>.

[Bytes sent: CLA='A0', INS='C0', P1='00', P2='00', P3=SW2<sub>1</sub>]

[Bytes received: data, SW1, SW2]

*The SIM shall have sent 'lgth' bytes followed by SW1='90' and SW2='00' [CR2].*

- g) The ME simulator sends a READ BINARY command to the SIM to read both bytes.

[Bytes sent: CLA='A0', INS='B0', P1='00', P2='00', P3='02']

[Bytes received: data, SW1, SW2]

*The SIM shall have sent 2 bytes followed by SW1='90' and SW2='00'.*

- h) The ME simulator sends an INVALIDATE command to the SIM.

[Bytes sent: CLA='A0', INS='04', P1='00', P2='00', P3='00']

[Bytes received: SW1, SW2]

*The SIM shall have sent SW1='90' and SW2='00'.*

- i) The ME simulator sends a REHABILITATE command to the SIM.

## 6.6.2 Coding of the commands

The test procedures defined in subclause 6.5 of the present document, "Descriptions of the functions", intrinsically test most the coding of the associated commands. Therefore, test purposes exist in this subclause only to cover areas of testing not already covered by subclause 6.5.

### 6.6.2.1 SELECT command

The test procedure defined in subclause 6.5.1 of the present document, "SELECT function" intrinsically tests the coding of this command and so is not replicated here.

### 6.6.2.2 STATUS command

The test procedure defined in subclause 6.5.2 of the present document, "STATUS function" intrinsically tests the coding of this command and so is not replicated here.

### 6.6.2.3 READ BINARY command

The test procedure defined in subclause 6.5.3 of the present document, "READ BINARY function" intrinsically tests the coding of this command and so is not replicated here.

### 6.6.2.4 UPDATE BINARY command

The test procedure defined in subclause 6.5.4 of the present document, "UPDATE BINARY function" intrinsically tests the coding of this command and so is not replicated here.

### 6.6.2.5 READ RECORD command

The test procedure defined in subclause 6.5.5 of the present document, "READ RECORD function" intrinsically tests the coding of this command and so is not replicated here.

### 6.6.2.6 UPDATE RECORD command

The test procedure defined in subclause 6.5.6 of the present document, "UPDATE RECORD function" intrinsically tests the coding of this command and so is not replicated here.

### 6.6.2.7 SEEK command

The test procedure defined in subclause 6.5.7 of the present document, "SEEK function" intrinsically tests the coding of this command and so is not replicated here.

### 6.6.2.8 INCREASE command

The test procedure defined in subclause 6.5.8 of the present document, "VERIFY CHV function" intrinsically tests the coding of this command and so is not replicated here.

### 6.6.2.9 VERIFY CHV command

The test procedure defined in subclause 6.5.9 of the present document, "VERIFY CHV function" intrinsically tests the coding of this command and so is not replicated here.

### 6.6.2.10 CHANGE CHV command

The test procedure defined in subclause 6.5.10 of the present document, "CHANGE CHV function" intrinsically tests the coding of this command and so is not replicated here.

### 6.6.2.11 DISABLE CHV command

The test procedure defined in subclause 6.5.11 of the present document, "DISABLE CHV function" intrinsically tests the coding of this command and so is not replicated here.

### 6.6.2.12 ENABLE CHV command

The test procedure defined in subclause 6.5.12 of the present document, "ENABLE CHV function" intrinsically tests the coding of this command and so is not replicated here.

### 6.6.2.13 UNBLOCK CHV command

The test procedure defined in subclause 6.5.13 of the present document, "UNBLOCK CHV function" intrinsically tests the coding of this command and so is not replicated here.

### 6.6.2.14 INVALIDATE command

The test procedure defined in subclause 6.5.14 of the present document, "INVALIDATE function" intrinsically tests the coding of this command and so is not replicated here.

### 6.6.2.15 REHABILITATE command

The test procedure defined in subclause 6.5.15 of the present document, "REHABILITATE function" intrinsically tests the coding of this command and so is not replicated here.

### 6.6.2.16 RUN GSM ALGORITHM command

The test procedure defined in subclause 6.5.16 of the present document, "RUN GSM ALGORITHM function" intrinsically tests the coding of this command and so is not replicated here.

### 6.6.2.17 SLEEP command

The test procedure defined in subclause 6.5.17 of the present document, "SLEEP function" intrinsically tests the coding of this command and so is not replicated here.

### 6.6.2.18 GET RESPONSE command

#### 6.6.2.18.1 Definition and applicability

It shall be mandatory for all cards complying with GSM 11.11 [1] to support all functions described therein.

#### 6.6.2.18.2 Conformance requirement

CR1 The GET RESPONSE command shall provide response data after the execution of commands RUN GSM ALGORITHM, SEEK (type 2), SELECT, and INCREASE.

CR2 It is required that the GET RESPONSE command is executed immediately after the command it is related to (no other command shall come between the command/response pair and the command GET RESPONSE). If this sequence is not respected, the SIM shall send the Status Information "technical problem with no diagnostic given" as a reaction to the GET RESPONSE.

CR3 Since the MF is implicitly selected after the activation of the SIM, GET RESPONSE shall be allowed as the first command after activation.

Reference: GSM 11.11 [1], subclause 9.2.18.

Test Group Reference (TGR): TGR\_SIM\_CMD

Test Procedure Reference (TPR): TPR\_SIM\_CMD\_GET

#### 6.6.2.18.3 Test purpose

To verify that the coding of the GET RESPONSE command conforms to the above requirements.

NOTE: CR1 is tested in subclauses 6.5.1, 6.5.7, 6.5.8, 6.5.16 and 6.5.17.

#### 6.6.2.18.4 Method of test

##### Initial conditions

- 1) The SIM is connected to an ME simulator.

##### Test procedure

- a) The ME simulator resets the SIM.
- b) The ME simulator sends a GET RESPONSE command to the SIM.

[Bytes sent: CLA='A0', INS='C0', P1='00', P2='00', P3='08']

[Bytes received: P3 bytes of data, SW1, SW2]

*Bytes 5 and 6 of the response data shall indicate that MF is the currently selected file [CR3].*

- c) The ME simulator sends a STATUS command to the SIM with correct P3.
- d) The ME simulator sends a GET RESPONSE command to the SIM.

[Bytes sent: CLA='A0', INS='C0', P1='00', P2='00', P3='05']

[Bytes received: SW1, SW2]

*The status condition returned by the SIM shall be SW1='6F', SW2='XX' - technical problem with no diagnostic given [CR2].*

### 6.6.3 Definitions and coding

#### 6.6.3.1 Definition and applicability

Certain definitions and coding are used in the response parameters/data of the commands.

#### 6.6.3.2 Conformance requirement

CR1 The file structure indicator byte shall be one of the following values within the specified range: '00', '01' or '03'.

CR2 The file type indicator byte shall be one of the following values within the specified range: '00', '01', '02' or '04'.

Reference: GSM 11.11 [1], subclause 9.3.

Test Group Reference (TGR): TGR\_SIM\_CMD\_DEF

Test Procedure Reference (TPR): TPR\_SIM\_CMD\_DEF

#### 6.6.3.3 Test purpose

To verify that the response parameters/data conform to the above requirements for all file IDs on the SIM.

NOTE: CR2 is covered in subclause 6.3.1.1, "File-type identification".

#### 6.6.3.4 Method of test

##### Initial conditions

- 1) The SIM is connected to an ME simulator.

##### Test procedure

- a) The ME simulator resets the SIM.

- b) For every possible selectable file ID in the file structure, the ME simulator sends SELECT commands to select the file ID. When a file is selected successfully, the ME simulator sends a GET RESPONSE command to the SIM.

*For all EFs found, the following shall be true of the response data:*

- *Byte 15 shall be '00' if the EF is Transparent.*

*The file structure indicator byte shall be coded as follows, according to the specification in clause 10 of GSM 11.11 [1] [CR1]:*

- *'00' = Transparent*
- *'01' = Linear Fixed*
- *'03' = Cyclic*

## 6.6.4 Status conditions returned by the SIM

### 6.6.4.1 Coding of the status words

#### 6.6.4.1.1 Definition and applicability

The status words SW1 and SW2 provide the method with which the SIM can respond to the ME after executing a command.

#### 6.6.4.1.2 Conformance requirement

- CR1 The SIM shall respond with the correct SW1 and SW2 status words for commands which are correctly executed.
- CR2 The SIM shall respond with the correct SW1 and SW2 status words for commands which produce memory management errors.
- CR3 The SIM shall respond with the correct SW1 and SW2 status words for commands which produce referencing management errors.
- CR4 The SIM shall respond with the correct SW1 and SW2 status words for commands which produce security management errors.
- CR5 The SIM shall respond with the correct SW1 and SW2 status words for commands which produce application independent errors.

Reference: GSM 11.11 [1], subclause 9.4.

Test Group Reference (TGR): TGR\_SIM\_CMD\_SC\_SW

Test Procedure Reference (TPR): TPR\_SIM\_CMD\_SC\_SW

#### 6.6.4.1.3 Test purpose

To verify that the SIM conforms to the above requirements when issuing SW1 and SW2 status words.

NOTE 1: CR2 cannot be tested as there is no mechanism to force the SIM to produce memory errors.

NOTE 2: CR4 is already tested in subclause 6.5.8.

#### 6.6.4.1.4 Method of test

##### Initial conditions

- 1) The SIM is connected to an ME simulator.

- 2) EF<sub>ADN</sub> on the SIM is not invalidated.

### Test procedure

- a) The ME simulator resets the SIM.
- b) The ME simulator sends a VERIFY CHV command to the SIM.
- c) The ME simulator sends SELECT commands to the SIM to select DF<sub>GSM</sub>.
- The status condition returned by the SIM shall be SW1='9F', SW2='XX' - length 'XX' of the response data [CR1].*
- d) The ME simulator sends a GET RESPONSE command to the SIM.
- The status condition returned by the SIM shall be SW1='90', SW2='00' - normal ending of command [CR1].*
- e) The ME simulator sends a READ BINARY command using a length of 1 byte to the SIM.
- The status condition returned by the SIM shall be SW1='94', SW2='00' - no EF selected [CR3].*
- f) The ME simulator sends SELECT commands to the SIM to select EF<sub>ADN</sub>.
- g) The ME simulator sends an UPDATE RECORD command using PREVIOUS mode to the SIM. The data used is 'E1' for all bytes.
- h) The ME simulator sends an UPDATE RECORD command using NEXT mode to the SIM. The data used is 'E2' for all bytes.
- The status condition returned by the SIM shall be SW1='94', SW2='02' - out of range (invalid address) [CR3].*
- i) The ME simulator sends a READ BINARY command using a length of 1 byte to the SIM.
- The status condition returned by the SIM shall be SW1='94', SW2='08' - file type inconsistent with the command [CR3].*
- j) The ME simulator sends a VERIFY CHV command with **incorrect** CHV1 to the SIM.
- The status condition returned by the SIM shall be SW1='98', SW2='04' - unsuccessful CHV verification, at least one attempt left.*
- k) The ME simulator sends an ENABLE CHV command to the SIM.
- The status condition returned by the SIM shall be SW1='98', SW2='08' - in contradiction with CHV status [CR3].*
- l) The ME simulator sends VERIFY CHV command with **incorrect** CHV1 to the SIM.
- m) The ME simulator sends VERIFY CHV command with **incorrect** CHV1 to the SIM.
- The status condition returned by the SIM shall be SW1='98', SW2='40' - unsuccessful CHV verification, no attempt left.*
- n) The ME simulator sends an UPDATE RECORD command using ABSOLUTE mode with record 1 to the SIM. Parameter P3 is set to 1 and the data used is 'E3'.
- The status condition returned by the SIM shall be SW1='67', SW2='XX' or SW1='98', SW2='04' - incorrect parameter P3 [CR3].*
- o) The ME simulator sends an UPDATE RECORD command using mode '44' to the SIM. The data used is 'E4' for all bytes.
- The status condition returned by the SIM shall be SW1='6B', SW2='00' or SW1='98', SW2='04' - incorrect parameter P1 or P2 [CR3].*
- p) The ME simulator sends the following APDU to the SIM.

[Bytes sent: CLA='A0', INS='1E', P1='00', P2='00', P3='00']

*The status condition returned by the SIM shall be SW1='6D', SW2='00' - unknown instruction code given in the command [CR5].*

- s) The ME simulator sends a GET RESPONSE command to the SIM.

*The status condition returned by the SIM shall be SW1='6F', SW2='XX' - technical problem with no diagnostic given [CR5].*

## 6.6.4.2 Commands versus possible status responses

### 6.6.4.2.1 Definition and applicability

Limiting the status conditions for each command to a defined set allows the ME to efficiently manage the handling of the status condition.

### 6.6.4.2.2 Conformance requirement

CR1 Table 10 in GSM 11.11 [1], subclause 9.4.6 shows for each command the possible status conditions returned (marked by an asterisk \*). The SIM shall not generate status conditions other than those allowed for each command.

Reference: GSM 11.11 [1], subclause 9.4.6.

Test Group Reference (TGR): TGR\_SIM\_CMD\_SC\_CSR

Test Procedure Reference (TPR): TPR\_SIM\_CMD\_SC\_CSR

### 6.6.4.2.3 Test purpose

To verify for each command that the SIM will only generate the allowed status conditions.

NOTE: CR1 cannot be tested as it is not possible to force the SIM to generate all of the allowed status conditions for each command and there is no way of forcing the SIM to generate disallowed status conditions for each command.

### 6.6.4.2.4 Method of test

#### Initial conditions

N/A

#### Test procedure

N/A

### 6.6.4.2.5 Test requirement

N/A

## 6.7 Contents of the elementary files

The subclause provides tests to ensure that the IUT contains all of the EFs need for a GSM session.

### 6.7.1 Definition and applicability

The Elementary Files described in clause 10 of GSM 11.11 [1] are required on the SIM card in order for a GSM session to be carried out.

The contents of these files are not tested as they are card/personalisation specific.

## 6.7.2 Conformance requirement

The following conformance requirements refer to the tables for each EF in clause 10 of GSM 11.11 [1].

CR1 Each existing EF shall be selectable under the respective DF using the identifier given in the table for that EF.

CR2 All mandatory EFs shall exist on the SIM card.

CR3 The identifier of the EF shall be that given in the table for that EF. CR4 The type and structure of the EF shall be that given in the table for that EF.

CR5 The file size shall be at least that given in the table for that EF.

CR6 The access conditions shall be those given in the table for that EF.

Reference: GSM 11.11 [1], clause 10.

Test Group Reference (TGR): TGR\_SIM\_CEF

Test Procedure Reference (TPR): TPR\_SIM\_CEF

## 6.7.3 Test purpose

To verify that the SIM conforms to the above requirements.

NOTE: The contents and coding of the data within the files are not tested, but shall conform to the respective contents and coding of the data given for each file in clause 10 of GSM 11.11 [1].

## 6.7.4 Method of test

### Initial conditions

- 1) The SIM is connected to an ME simulator.

### Test procedure

- a) The ME simulator resets the SIM.
- b) The ME simulator sends SELECT commands to the SIM to select the respective DF for the first EF in clause 10 of GSM 11.11 [1].

*The status condition returned by the SIM shall be SW1='9F', SW2='XX' - length 'XX' of the response data [CR1].*

- c) The ME simulator sends a SELECT command to the SIM to select the first EF in clause 10 of GSM 11.11 [1].

*The status condition returned by the SIM shall be SW1='9F', SW2='XX' - length 'XX' of the response data [CR1,2].*

- d) The ME simulator sends a GET RESPONSE command to the SIM.

*The following shall be true of the response data:*

- Bytes 5 and 6 shall indicate the identifier of the file selected. [CR3].
- Byte 7 shall be '04' indicating EF [CR4].
- Byte 14 shall indicate the structure given in the table for the file in clause 10 of GSM 11.11 [1] [CR4].
- Bytes 3 and 4 shall be at least the minimum file size given in the table for the file in clause 10 of GSM 11.11 [1] if the EF is transparent [CR5].
- Byte 15 shall be in accordance with the record length given in the table for the file in clause 10 of GSM 11.11 [1] if the EF is linear fixed or cyclic [CR5].

- Bytes 3 and 4 shall be an integer multiple of the record length if the EF is linear fixed or cyclic [CR5].
  - Bytes 9, 10 and 11 shall indicate the access conditions given in the table for the file in clause 10 of GSM 11.11 [1] [CR6].
- e) Steps a) to d) are repeated for the remaining mandatory EFs in clause 10 of GSM 11.11 [1].
- f) Steps a) to d) are repeated for the existing optional EFs in clause 10 of GSM 11.11 [1].

## 6.8 Application Protocol

The tests in this subclause ensure that the IUT conforms to the functional specification for application protocol - in particular the internal management of AND/FDN switching in the SIM.

### 6.8.1 FDN Procedure

#### 6.8.1.1 Definition and applicability

It shall be mandatory for all cards complying with GSM 11.11 [1] to support all internal management processing required for the GSM application.

#### 6.8.1.2 Conformance requirement

- CR1 If FDN is enabled, the SIM shall invalidate both EF<sub>IMSI</sub> and EF<sub>LOCI</sub> once during each GSM session at least before the next command following selection of either EF.

Reference: GSM 11.11 [1], subclause 10.2.7, 11.2.1.

Test Group Reference (TGR): TGR\_SIM\_APP

Test Procedure Reference (TPR): TPR\_SIM\_APP\_FDN

#### 6.8.1.3 Test purpose

To verify that the FDN feature conforms to the above requirements.

#### 6.8.1.4 Method of test

##### Initial conditions

- 1) FDN feature is allocated and activated.
- 2) ADN feature is allocated and activated.
- 3) EF<sub>ADN</sub> is invalidated.

##### Test procedure

- a) The ME simulator resets the SIM.
- b) The ME simulator sends a VERIFY CHV1 to the SIM.
- c) The ME simulator sends SELECT commands to the SIM to select EF<sub>IMSI</sub> under DF<sub>GSM</sub>.
- d) The ME simulator sends a GET RESPONSE command to the SIM.

*Bit 1 of byte 12 of the data returned shall be 0 indicating that EF<sub>IMSI</sub> is invalidated [CR1].*

- e) The ME simulator sends a REHABILITATE command to the SIM.
- f) The ME simulator sends a SELECT command to the SIM to select EF<sub>LOCI</sub>.

g) The ME simulator sends a GET RESPONSE command to the SIM.

*Bit 1 of byte 12 of the data returned shall be 0 indicating that EF<sub>LOCI</sub> is invalidated [CR1].*

h) The ME simulator sends a REHABILITATE command to the SIM.

i) The ME simulator sends SELECT commands to the SIM to select EF<sub>ADN</sub> under DF<sub>TELECOM</sub>.

j) The ME simulator sends a VERIFY CHV2 to the SIM.

k) The ME simulator sends a REHABILITATE command to the SIM.

l) The ME simulator sends a SELECT command to the SIM to select EF<sub>SST</sub>.

m) The ME simulator gains the access condition for UPDATE policy.

n) The ME simulator sends an UPDATE BINARY command to the SIM to deactivate the ADN service.

o) The ME simulator resets the SIM.

p) The ME simulator sends a VERIFY CHV1 to the SIM.

q) The ME simulator sends SELECT commands to the SIM to select EF<sub>LOCI</sub> under DF<sub>GSM</sub>.

r) The ME simulator sends a GET RESPONSE command to the SIM.

*Bit 1 of byte 12 of the data returned shall be 0 indicating that EF<sub>LOCI</sub> is invalidated [CR1].*

s) The ME simulator sends a REHABILITATE command to the SIM.

t) The ME simulator sends a SELECT command to the SIM to select EF<sub>IMSI</sub>.

u) The ME simulator sends a GET RESPONSE command to the SIM.

*Bit 1 of byte 12 of the data returned shall be 0 indicating that EF<sub>IMSI</sub> is invalidated [CR1].*

v) The ME simulator sends a REHABILITATE command to the SIM.

w) The ME simulator sends a SELECT command to the SIM to select EF<sub>SST</sub>.

x) The ME simulator gains the access condition for UPDATE policy.

y) The ME simulator sends an UPDATE BINARY command to the SIM to deallocate the ADN service.

z) The ME simulator resets the SIM.

aa) The ME simulator sends a VERIFY CHV1 to the SIM.

ab) The ME simulator sends SELECT commands to the SIM to select EF<sub>LOCI</sub> under DF<sub>GSM</sub>.

ac) The ME simulator sends a GET RESPONSE command to the SIM.

*Bit 1 of byte 12 of the data returned shall be 0 indicating that EF<sub>LOCI</sub> is invalidated [CR1].*

ad) The ME simulator sends a REHABILITATE command to the SIM.

ae) The ME simulator sends a SELECT command to the SIM to select EF<sub>IMSI</sub>.

af) The ME simulator sends a GET RESPONSE command to the SIM.

*Bit 1 of byte 12 of the data returned shall be 0 indicating that EF<sub>IMSI</sub> is invalidated [CR1].*

ag) The ME simulator sends a REHABILITATE command to the SIM.

ah) The ME simulator sends a SELECT command to the SIM to select EF<sub>SST</sub>.

ai) The ME simulator sends an UPDATE BINARY command to the SIM to allocate and activate the ADN service.

aj) The ME simulator resets the SIM.

ak) The ME simulator sends a SELECT command to the SIM to select EF<sub>LOCI</sub>.

al) The ME simulator sends a GET RESPONSE command to the SIM.

*Bit 1 of byte 12 of the data returned shall be 1 indicating that EF<sub>LOCI</sub> is not invalidated [CR1].*

am) The ME simulator sends a SELECT command to the SIM to select EF<sub>IMSI</sub>.

an) The ME simulator sends a GET RESPONSE command to the SIM.

*Bit 1 of byte 12 of the data returned shall be 1 indicating that EF<sub>IMSI</sub> is not invalidated [CR1].*

ao) The ME simulator sends a SELECT command to the SIM to select EF<sub>SST</sub>.

ap) The ME simulator gains the access condition for UPDATE policy.

aq) The ME simulator sends an UPDATE BINARY command to the SIM to deactivate the FDN service.

ar) The ME simulator sends SELECT commands to the SIM to select EF<sub>ADN</sub> under DF<sub>TELECOM</sub>.

as) The ME simulator sends a VERIFY CHV2 to the SIM.

at) The ME simulator sends a INVALIDATE command to the SIM.

au) The ME simulator resets the SIM.

av) The ME simulator sends a SELECT command to the SIM to select EF<sub>LOCI</sub>.

aw) The ME simulator sends a GET RESPONSE command to the SIM.

*Bit 1 of byte 12 of the data returned shall be 1 indicating that EF<sub>LOCI</sub> is not invalidated [CR1].*

ax) The ME simulator sends a SELECT command to the SIM to select EF<sub>IMSI</sub>.

ay) The ME simulator sends a GET RESPONSE command to the SIM.

*Bit 1 of byte 12 of the data returned shall be 1 indicating that EF<sub>IMSI</sub> is not invalidated [CR1].*

---

## Annex A (informative): Change history

This annex lists all change requests approved for the present document since the the present document was approved by ETSI SMG.

SMG#	SMG tdoc	SMG9 tdoc	VERS	CR	RV	PH	CAT	SUBJECT	Resulting Version
s28	P-99-179	98p440	2.0.0			R98		Approval of final draft by SMG	7.0.0
			7.0.1					Update to Version 7.0.2 for Publication	7.0.2

---

# History

<b>Document history</b>		
V7.0.1	July 1999	One-step Approval Procedure OAP 9952: 1999-07-28 to 1999-11-26
V7.0.2	December 1999	Publication