ETSI TS 103 481 V11.1.0 (2019-03)

Smart Cards;
Test specification for the Remote APDU structure for UICC based applications;
UICC features
(Release 11)

Reference
RTS/SCP-00RAMtestv110100

Keywords
management, remote, smart card, testing

ETSI

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

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

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights 10
Foreword 10
Modal verbs terminology 10
Introduction 11
1 Scope 12
2 References 12
2.1 Normative references 12
2.2 Informative references 14
3 Definition of terms, symbols, abbreviations and formats 14
3.1 Terms 14
3.2 Symbols 14
3.3 Abbreviations 14
3.4 Formats 15
3.4.1 Format of the table of optional features 15
3.4.2 Format of the applicability table 16
3.4.3 Status and Notations 16
4 Test Environment 17
4.1 Test Applicability 17
4.1.1 Table of optional features 17
4.1.2 Applicability table 17
4.2 Test environment description 21
4.3 Tests format 21
4.3.1 Initial Conditions 21
4.3.2 Test procedure 22
4.4 General initial conditions 22
4.4.1 Common rules 22
4.4.2 File system and files content 22
4.4.3 AID and TAR coding 23
4.5 Test equipment / OTA server 24
4.5.1 Test equipment / OTA server requirements 24
4.5.2 Default conditions for DUT operation 24
4.5.3 Java Card™ Software Development Kit 24
5 Conformance Requirements 25
5.1 Overview of remote management 25
5.2 Remote APDU format 25
5.3 Security parameters assigned to applications 31
5.4 Remote File Management (RFM) 32
5.5 Remote Application Management (RAM) 34
5.6 Additional command for push 47
5.7 Confidential application management 50
6 Test Cases 51
6.1 Overview of remote management 51
6.2 Remote APDU format 51
6.2.1 Compact Remote Application data format 51
6.2.2 Expanded Remote Application data format 51
6.2.2.1 Test case 1: A command session with C-APDU TLV Structure with definite length coding 51
6.2.2.1.1 Initial Conditions 51
6.2.2.1.2 Test Procedure 52
6.2.2.2 Test case 2: A command session containing multiple commands with C-APDU TLV Structure with definite length coding - Bad Format 53
6.2.2.2.1 Initial Conditions 53
6.2.2.2.2 Test Procedure 53

6.2.2.3 Test case 3: A command session with C-APDU TLV Structure with indefinite length coding 54
6.2.2.3.1 Initial Conditions 54
6.2.2.3.2 Test Procedure 54
6.2.2.4 Test case 4: A command session with C-APDU TLV Structure with indefinite length coding - Bad Format 55
6.2.2.4.1 Initial Conditions 55
6.2.2.4.2 Test Procedure 56
6.2.2.5 Test case 5: A command session with Immediate Action TLV Structure with definite length coding - Normal Format 57
6.2.2.5.1 Initial Conditions 57
6.2.2.5.2 Test Procedure 57
6.2.2.6 Test case 6: A command session with Immediate Action TLV Structure with definite length coding - Referenced Format 58
6.2.2.6.1 Initial Conditions 58
6.2.2.6.2 Test Procedure 58
6.2.2.7 Test case 7: A command session with Immediate Action TLV Structure with definite length coding - Immediate Action Error 59
6.2.2.7.1 Initial Conditions 59
6.2.2.7.2 Test Procedure 59
6.2.2.8 Test case 8: A command session with Immediate Action TLV Structure with indefinite length coding - Normal Format 59
6.2.2.8.1 Initial Conditions 59
6.2.2.8.2 Test Procedure 59
6.2.2.9 Test case 9: A command session with Immediate Action TLV Structure with indefinite length coding - Referenced Format 60
6.2.2.9.1 Initial Conditions 60
6.2.2.9.2 Test Procedure 60
6.2.2.10 Test case 10: A command session with Immediate Action TLV Structure with indefinite length coding - Immediate Action Error 60
6.2.2.10.1 Initial Conditions 60
6.2.2.10.2 Test Procedure 60
6.2.2.11 Test case 11: A command session with Error Action TLV Structure with definite length coding - normal format 61
6.2.2.11.1 Initial Conditions 61
6.2.2.11.2 Test Procedure 61
6.2.2.12 Test case 12: A command session with Error Action TLV Structure with definite length coding - Referenced format 61
6.2.2.12.1 Initial Conditions 61
6.2.2.12.2 Test Procedure 62
6.2.2.13 Test case 13: A command session with Error Action TLV Structure with indefinite length coding - Normal format 62
6.2.2.13.1 Initial Conditions 62
6.2.2.13.2 Test Procedure 62
6.2.2.14 Test case 14: A command session with Error Action TLV Structure with indefinite length coding - Referenced format 63
6.2.2.14.1 Initial Conditions 63
6.2.2.14.2 Test Procedure 63
6.2.2.15 Test case 15: A command session with Script Chaining TLV Structure with definite length coding 63
6.2.2.15.1 Initial Conditions 63
6.2.2.15.2 Test Procedure 63
6.2.2.16 Test case 16: A command session with Script Chaining TLV Structure with definite length coding (Script Chaining Error) 64
6.2.2.16.1 Initial Conditions 64
6.2.2.16.2 Test Procedure 64
6.2.2.17 Test case 17: A command session with Script Chaining TLV Structure with indefinite length coding 64
6.2.2.17.1 Initial Conditions 64
6.2.2.17.2 Test Procedure 64
6.2.2.18 Test case 18: A command session with Script Chaining TLV Structure with indefinite length coding (Script Chaining Error) 65
6.2.2.18.1 Initial Conditions 65

6.2.2.18.2 Test Procedure 65
6.3 Security parameters assigned to applications 65
6.3.1 Minimum Security Level (MSL) 65
6.3.2 Access domain 65
6.4 Remote File Management (RFM) 66
6.4.1 UICC Shared File System Remote File Management 66
6.4.1.1 Test case 1: A command session with a single SELECT command. Check access to the file tree 66
6.4.1.1.1 Initial Conditions 66
6.4.1.1.2 Test Procedure 66
6.4.1.2 Test case 2: A command session with multiple commands (SELECT, UPDATE BINARY, READ BINARY). 67
6.4.1.2.1 Initial Conditions 67
6.4.1.2.2 Test Procedure 67
6.4.1.3 Test case 3: A command session with multiple commands (SEARCH RECORD, UPDATE RECORD, INCREASE, READ RECORD) 67
6.4.1.3.1 Initial Conditions 67
6.4.1.3.2 Test Procedure 67
6.4.1.4 Test case 4: A command session with multiple commands (SET DATA, RETRIEVE DATA). 68
6.4.1.4.1 Initial Conditions 68
6.4.1.4.2 Test Procedure 68
6.4.1.5 Test case 5: A command session with multiple commands (ACTIVATE FILE, DEACTIVATE FILE) 68
6.4.1.5.1 Initial Conditions 68
6.4.1.5.2 Test Procedure 69
6.4.1.6 Test case 6: A command session with multiple commands (VERIFY PIN, CHANGE PIN) 69
6.4.1.6.1 Initial Conditions 69
6.4.1.6.2 Test Procedure 69
6.4.1.7 Test case 7: A command session with multiple commands (DISABLE PIN, ENABLE PIN) 70
6.4.1.7.1 Initial Conditions 70
6.4.1.7.2 Test Procedure 70
6.4.1.8 Test case 8: A command session with multiple commands (UNBLOCK PIN) 70
6.4.1.8.1 Initial Conditions 70
6.4.1.8.2 Test Procedure 70
6.4.1.9 Test case 9: A command session with multiple commands (CREATE FILE, RESIZE FILE, DELETE FILE) 71
6.4.1.9.1 Initial Conditions 71
6.4.1.9.2 Test Procedure 71
6.4.2 ADF Remote File Management 72
6.4.2.1 Test case 1: A command session with a single SELECT command. Check access to the file tree 72
6.4.2.1.1 Initial Conditions 72
6.4.2.1.2 Test Procedure 72
6.4.2.2 Test case 2: A command session with multiple commands (SELECT, UPDATE BINARY, READ BINARY) 72
6.4.2.2.1 Initial Conditions 72
6.4.2.2.2 Test Procedure 72
6.4.2.3 Test case 3: A command session with multiple commands (SEARCH RECORD, UPDATE RECORD, INCREASE, READ RECORD) 73
6.4.2.3.1 Initial Conditions 73
6.4.2.3.2 Test Procedure 73
6.4.2.4 Test case 4: A command session with multiple commands (SET DATA, RETRIEVE DATA) 73
6.4.2.4.1 Initial Conditions 73
6.4.2.4.2 Test Procedure 73
6.4.2.5 Test case 5: A command session with multiple commands (ACTIVATE FILE, DEACTIVATE FILE) 74
6.4.2.5.1 Initial Conditions 74
6.4.2.5.2 Test Procedure 74
6.4.2.6 Test case 6: A command session with multiple commands (VERIFY PIN, CHANGE PIN) 74
6.4.2.6.1 Initial Conditions 74
6.4.2.6.2 Test Procedure 74
6.4.2.7 Test case 7: A command session with multiple commands (DISABLE PIN, ENABLE PIN) 75
6.4.2.7.1 Initial Conditions 75
6.4.2.7.2 Test Procedure 75

6.4.2.8 Test case 8: A command session with multiple commands (UNBLOCK PIN) 75
6.4.2.8.1 Initial Conditions 75
6.4.2.8.2 Test Procedure 75
6.4.2.9 Test case 9: A command session with multiple commands (CREATE FILE, RESIZE FILE, DELETE FILE) 76
6.4.2.9.1 Initial Conditions 76
6.4.2.9.2 Test Procedure 76
6.4.3 RFM implementation over HTTPS 76
6.5 Remote Application Management (RAM) 77
6.5.1 DELETE 77
6.5.1.1 Test case 1: DELETE command 77
6.5.1.1.1 Initial Conditions 77
6.5.1.1.2 Test Procedure 77
6.5.2 SET STATUS 77
6.5.2.1 Test case 1: SET STATUS command within a command session 77
6.5.2.1.1 Initial Conditions 77
6.5.2.1.2 Test Procedure 77
6.5.3 INSTALL 78
6.5.3.1 INSTALL [for load] 78
6.5.3.1.1 Test case 1: INSTALL [for load] as a single command in the session 78
6.5.3.1.2 Test case 2: INSTALL[for load] with memory management parameters 78
6.5.3.2 INSTALL [for install] 79
6.5.3.2.1 Test case 1: INSTALL[for install] with SIM File Access and Toolkit Application Specific Parameters 79
6.5.3.2.2 Test case 2: INSTALL[for install] with UICC System Specific Parameters and SIM File Access and Toolkit Application Specific Parameters 79
6.5.3.2.3 Test case 3: INSTALL[for install] with UICC System Specific Parameter "UICC Toolkit Application specific parameters field" 80
6.5.3.2.4 Test case 4: INSTALL[for install] with UICC System Specific Parameter "UICC Access Application specific parameters field" 80
6.5.3.2.5 Test case 5: INSTALL[for install] with UICC System Specific Parameter "UICC Administrative Access Application specific parameters field" 81
6.5.3.2.6 Test case 6: INSTALL[for install] with UICC System Specific Parameter "UICC Access Application specific parameters field" and "UICC Administrative Access Application specific parameters field" for the same ADF 81
6.5.3.2.7 Test case 7: INSTALL[for install] with UICC System Specific Parameter "UICC Access Application specific parameters field" and "UICC Administrative Access Application specific parameters field" for the same UICC file system 82
6.5.3.2.8 Test case 8: INSTALL[for install] with the maximum number of timers required for SIM Toolkit Application Specific Parameters set too high ('09') 83
6.5.3.2.9 Test case 9: INSTALL[for install] with the maximum number of timers required for UICC Toolkit Application Specific Parameters set too high ('09') 83
6.5.3.2.10 Test case 10: INSTALL[for install] with the maximum number of channels required for SIM Toolkit Application Specific Parameters set too high ('08') 84
6.5.3.2.11 Test case 11: INSTALL[for install] with the maximum number of channels required for UICC Toolkit Application Specific Parameters set too high ('08') 84
6.5.3.2.12 Test case 12: INSTALL[for install] with the maximum number of services required for UICC Toolkit Application Specific Parameters set too high ('09') 85
6.5.3.2.13 Test case 13: INSTALL[for install] with requested item identifier for SIM Toolkit Application Specific Parameters set to '128' 85
6.5.3.2.14 Test case 14: INSTALL[for install] with requested item identifier for UICC Toolkit Application Specific Parameters set to '128' 86
6.5.3.2.15 Test case 15: INSTALL[for install] with Minimum Security Level field of SIM Toolkit Application different from zero 86
6.5.3.2.16 Test case 16: INSTALL[for install] with Minimum Security Level field of UICC Toolkit Application different from zero 86
6.5.3.2.17 Test case 17: INSTALL[for install] with Minimum Security Level field of SIM Toolkit Application different from SPI1 87
6.5.3.2.18 Test case 18: INSTALL[for install] with Minimum Security Level field of UICC Toolkit Application different from SPI1 87
6.5.3.2.19 Test case 19: INSTALL[for install] SIM Toolkit Applications with Access Domain Parameter equal to '00' and 'FF' 88

6.5.3.2.20 Test case 20: INSTALL[for install] UICC Toolkit Applications with Access Domain Parameter equal to '00' and 'FF' 89
6.5.3.2.21 Test case 21: INSTALL[for install] SIM Toolkit Application with Access Domain Parameter equal to '00' and access condition set to 'NEVER' 89
6.5.3.2.22 Test case 22: INSTALL[for install] UICC Toolkit Application with Access Domain Parameter equal to '00' and access condition set to 'NEVER' 90
6.5.3.2.23 Test case 23: INSTALL[for install] SIM Toolkit Application with Access Domain Parameter not supported 90
6.5.3.2.24 Test case 24: INSTALL[for install] UICC Toolkit Application with Access Domain Parameter not supported 91
6.5.3.2.25 Test case 25: INSTALL[for install] UICC Toolkit Application with Access Domain Parameter equal to '02' 91
6.5.3.2.26 Test case 26: INSTALL[for install] SIM Toolkit Applications with Access Domain Parameter equal to '00' - independency from the PIN status at UICC-Terminal interface 92
6.5.3.2.27 Test case 27: INSTALL[for install] UICC Toolkit Applications with Access Domain Parameter equal to '00' - independency from the PIN status at UICC-Terminal interface 93
6.5.3.2.28 Test case 28: INSTALL[for install] of SIM Toolkit Applications with different Priority levels 94
6.5.3.2.29 Test case 29: INSTALL[for install] of UICC Toolkit Applications with different Priority levels 94
6.5.3.2.30 Test case 30: INSTALL[for install] SIM Toolkit Applets with same Priority levels 94
6.5.3.2.31 Test case 31: INSTALL[for install] UICC Toolkit Applets with same Priority levels 95
6.5.3.2.32 Test case 32: INSTALL[for install] two SIM Toolkit Applications with identical TAR value 95
6.5.3.2.33 Test case 33: INSTALL[for install] two UICC Toolkit Application with identical TAR value 96
6.5.3.2.34 Test case 34: INSTALL[for install] SIM Toolkit Application with multiple TAR values 97
6.5.3.2.35 Test case 35: INSTALL[for install] UICC Toolkit Application with multiple TAR values 98
6.5.3.2.36 Test case 36: INSTALL[for install] SIM Toolkit Application without TAR value in the Install parameters, the AID contains TAR value 98
6.5.3.2.37 Test case 37: INSTALL[for install] UICC Toolkit Application without TAR value in the Install parameters, the AID contains TAR value 99
6.5.3.2.38 Test case 38: INSTALL[for install] for contactless application with Reader mode protocol data type A 99
6.5.3.2.39 Test case 39: INSTALL[for install] for contactless application with Reader mode protocol data type B 99
6.5.3.2.40 Test case 40: INSTALL[for install] for contactless application with Card Emulation mode 100
6.5.4 LOAD 100
6.5.4.1 Test case 1: LOAD with DES for DAP verification 100
6.5.5 PUT KEY 101
6.5.5.1 Test case 1: PUT KEY - create new 3DES 2 keys 101
6.5.5.1.1 Initial Conditions 101
6.5.5.1.2 Test Procedure 101
6.5.5.2 Test case 2: PUT KEY - create new 3DES 3 keys 101
6.5.5.2.1 Initial Conditions 101
6.5.5.2.2 Test Procedure 101
6.5.5.3 Test case 3: PUT KEY - add and replace DES keys 102
6.5.5.3.1 Initial Conditions 102
6.5.5.3.2 Test Procedure 102
6.5.5.4 Test case 4: PUT KEY - create new 16 bytes AES keys 102
6.5.5.4.1 Initial Conditions 102
6.5.5.4.2 Test Procedure 102
6.5.5.5 Test case 5: PUT KEY - create new 24 bytes AES keys 102
6.5.5.5.1 Initial Conditions 102
6.5.5.5.2 Test Procedure 103
6.5.5.6 Test case 6: PUT KEY - create new 32 bytes AES keys 103
6.5.5.6.1 Initial Conditions 103
6.5.5.6.2 Test Procedure 103
6.5.6 GET STATUS 104
6.5.6.1 Test case 1: GET STATUS with different P1 values 104
6.5.6.1.1 Initial Conditions 104
6.5.6.1.2 Test Procedure 104
6.5.6.2 Test case 2: GET STATUS with optional P1 values 104
6.5.6.2.1 Initial Conditions 104
6.5.6.2.2 Test Procedure 104

6.5.6.3 Test case 3: GET STATUS returns Menu Entries in the LOCKED state 104
6.5.6.3.1 Initial Conditions 104
6.5.6.3.2 Test Procedure 105
6.5.7 GET DATA 105
6.5.7.1 Test case 1: GET DATA with different P1 values 105
6.5.7.1.1 Initial Conditions 105
6.5.7.1.2 Test Procedure 105
6.5.8 STORE DATA 105
6.5.8.1 Test case 1: STORE DATA 105
6.5.8.1.1 Initial Conditions 105
6.5.8.1.2 Test Procedure 106
6.5.8.2 Test case 2: STORE DATA with a Forbidden Load File List 106
6.5.8.2.1 Initial Conditions 106
6.5.8.2.2 Test Procedure 106
6.5.9 RAM implementation over HTTPS 106
6.6 Additional command for push 106
6.6.1 BIP 106
6.6.2 CAT_TP 106
6.6.2.1 Test case 1: Send Secured Data (READ BINARY) using Expanded and Compact format with the different TAR value 106
6.6.2.1.1 Initial Conditions 106
6.6.2.1.2 Test Procedure 106
6.6.2.2 Test case 2: Send Secured Data (READ BINARY) using Expanded and Compact format with the same TAR value 107
6.6.2.2.1 Initial Conditions 107
6.6.2.2.2 Test Procedure 107
6.6.2.3 Test case 3: PUSH Command, PoR required - No Error 107
6.6.2.3.1 Initial Conditions 107
6.6.2.3.2 Test Procedure 107
6.7 Confidential application management 108

Annex A (normative): BER-TLV tags 109

A.1 BER-TLV tags 109

Annex B (normative): Default file system and files content 110

B.1 DF_{TEST} (UICC Access Tests DF) 110
B.1.1 DF identifier 110
B.1.2 EF_{TNU} (Transparent Never Update) 110
B.1.3 EF_{TARU} (Transparent Always Read and Update) 110
B.1.4 EF_{TUACP} (Transparent Update Access Condition PIN) 111
B.1.5 EF_{TPRU} (Transparent PIN Read and Update) 111
B.1.6 EF_{LF4R4b} 111
B.1.7 $EF_{BER\text{-}TLV}$ 112
B.1.8 EF_{CY4R4b} 112

B.2 DF_{TESTB} (Tests DF under ADF_1) 113
B.2.1 DF identifier 113
B.2.2 EF_{TARUB} (Transparent Always Read and Update B) 113

B.3 $DF_{TELECOM}$ 113
B.3.1 EF_{RMA} (Remote Management Actions) 113

Annex C (normative): Secure data coding and command structure 115

C.1 Commands 115

C.2 Remote APDU Format 117
C.2.1 Compact Remote Application Data Format 117
C.2.2 Expanded Remote Application Data Format 117
C.2.2.1 C-APDU TLV 117
C.2.2.2 Immediate Action TLV 117
C.2.2.3 Error Action TLV 118

C.2.2.4 Script Chaining TLV 119
Annex D (informative): Full command structure sample 120
D.1 Formatted SMS with PoR required - default 120
D.2 CAT-TP - default 120
D.3 HTTPS - default 120
Annex E (normative): AID and TAR values 121
E.1 UICC shared file system remote file management application 121
E.2 ADF remote file management application 121
E.3 AID and TAR 121
Annex F (informative): FFS requirements 122
Annex G (informative): Core specification version information 124
Annex H (informative): Change History 125
History 126

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables 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 ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

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 ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

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

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Smart Card Platform (SCP).

The contents of the present document are subject to continuing work within TC SCP and may change following formal TC SCP approval. If TC SCP modifies 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 x.y.z

where:

x the first digit:

- 0 early working draft;
- 1 presented to TC SCP for information;
- 2 presented to TC SCP for approval;
- 3 or greater indicates TC SCP approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

Modal verbs terminology

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

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

Introduction

The present document defines test cases for the UICC relating to Remote APDU structure for UICC based applications as specified in ETSI TS 102 226 [1].

1 Scope

The present document covers the minimum characteristics considered necessary for the UICC in order to provide compliance to ETSI TS 102 226 [1].

It specifies conformance test cases for the UICC relating to Remote APDU structure for UICC based applications as specified in ETSI TS 102 226 [1].

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

- In the case of a reference to a TC SCP document, a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI TS 102 226: "Smart Cards; Remote APDU structure for UICC based applications".

[2] ETSI TS 102 225: "Smart Cards; Secured packet structure for UICC based applications".

[3] ETSI TS 102 221: "Smart Cards; UICC-Terminal interface; Physical and logical characteristics".

[4] ETSI TS 102 223: "Smart Cards; Card Application Toolkit (CAT) (Release 9)".

[5] GlobalPlatform: "Card Specification Version 2.2.1".

NOTE: Available at http://www.globalplatform.org/.

[6] ETSI TS 101 220: "Smart Cards; ETSI numbering system for telecommunication application providers".

[7] ETSI TS 102 241: "Smart Cards; UICC Application Programming Interface (UICC API) for Java Card (TM)".

[8] GlobalPlatform: "GlobalPlatform Card Specification Version 2.0.1".

NOTE: Available at http://www.globalplatform.org/.

[9] ETSI TS 102 222: "Integrated Circuit Cards (ICC); Administrative commands for telecommunications applications".

[10] ETSI TS 123 048: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Security mechanisms for the (U)SIM application toolkit; Stage 2 (3GPP TS 23.048)".

[11] ETSI TS 102 127: "Smart Cards; Transport protocol for CAT applications; Stage 2".

[12] ETSI TS 143 019: "Digital cellular telecommunications system (Phase 2+); Subscriber Identity Module Application Programming Interface (SIM API) for Java Card; Stage 2 (3GPP TS 43.019)".

[13] FIPS-197 (2001): "Advanced Encryption Standard (AES)".

NOTE: Available at http://csrc.nist.gov/publications/fips/index.html.

[14] NIST Special Publication 800-38A (2001): "Recommendation for Block Cipher Modes of Operation - Methods and Techniques".

NOTE: Available at http://csrc.nist.gov/publications/nistpubs/.

[15] NIST Special Publication 800-38B (2001): "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication".

NOTE: Available at http://csrc.nist.gov/publications/nistpubs/.

[16] GlobalPlatform: "Card UICC Configuration", Version 1.0.1.

NOTE: Available at http://www.globalplatform.org/.

[17] ETSI TS 102 588: "Smart Cards; Application invocation Application Programming Interface (API) by a UICC webserver for Java Card™ platform".

[18] GlobalPlatform: "Confidential Card Content Management Card Specification v2.2 - Amendment A V1.0.1".

NOTE: Available at http://www.globalplatform.org/.

[19] GlobalPlatform: "Card Specification Version 2.2, Amendment B" Version 1.1.

NOTE: Available at http://www.globalplatform.org/.

[20] ETSI TS 102 483: "Smart cards; UICC-Terminal interface; Internet Protocol connectivity between UICC and terminal".

[21] ISO/IEC 8825-1: "Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)".

[22] GlobalPlatform: "Card Specification Version 2.2, Amendment C: Contactless Services" Version 1.0.1.

NOTE: Available at http://www.globalplatform.org/.

[23] ETSI TS 102 622: "Smart Card; UICC - Contactless Front-end (CLF) Interface; Host Controller Interface (HCI)".

[24] GlobalPlatform: "Security Upgrade for Card Content Management - GlobalPlatform Card Specification v2.2 - Amendment E".

NOTE: Available at http://www.globalplatform.org/.

[25] GlobalPlatform: "Java Card API and Export File for Card Specification v2.2.1 (org.globalplatform) V1.5".

NOTE: Available at http://www.globalplatform.org/.

[26] Oracle "Application Programming Interface, Java Card™ Platform, 3.0.1 Classic Edition".

[27] Oracle "Runtime Environment Specification, Java Card™ Platform, 3.0.1 Classic Edition".

[28] Oracle "Virtual Machine Specification Java Card™ Platform, 3.0.1 Classic Edition".

NOTE: Oracle Java Card™ Specifications can be downloaded at http://docs.oracle.com/javame/javacard/javacard.html.

[29] ISO/IEC 9646-7:1995: "Information technology -- Open Systems Interconnection -- Conformance testing methodology and framework -- Part 7: Implementation Conformance Statements".

[30] ETSI TS 102 230-2: "Smart Cards; UICC-Terminal interface; Physical, electrical and logical test specification; Part 2: UICC features (Release 9)".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

- In the case of a reference to a TC SCP document, a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

Not applicable.

3 Definition of terms, symbols, abbreviations and formats

3.1 Terms

For the purposes of the present document, the terms given in ETSI TS 102 226 [1], ETSI TS 102 127 [11] and the following apply:

Controlling Authority Security Domain (CASD): on-card controlling entity representing an off card trusted third party

NOTE: It provides services to confidentially load or generate Secure Channel keys of the APSD.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TS 102 226 [1], ETSI TS 102 127 [11] and the following apply:

ACK	ACKnowledge
ADD	Access Domain Data
ADF	Application Data File
ADP	Access Domain Parameter
AES	Advanced Encryption Standard
AID	Application IDentifier
APDU	Application Protocol Data Unit
API	Application Programming Interface
APSD	Application Provider Security Domain
BER-TLV	Basic Encoding Rules - Tag, Length, Value
BIP	Bearer Independent Protocol
C-APDU	Command - Application Protocol Data Unit
CASD	Controlling Authority Security Domain
CBC	Cell Broadcast Centre

CLA	CLAss
CMAC	Cipher-based Message Authentication Code
DAP	Data Authentication Pattern
DEK	Data Encryption Key
DES	Data Encryption Standard
DF	Directory File
ECB	Electronic Code Book
ECKA	Elliptic Curve Key Agreement algorithm
ECKA	EG ElGamal ECKA
EF	Elementary File
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ICCID	Integrated Circuit Card IDentification
INS	INStruction
ISD	Issuer Security Domain
KIc	Key and algorithm Identifier for ciphering
KID	Key and algorithm IDentifier for RC/CC/DS
MAC	Message Authentication Code
MF	Management Field
MSL	Minimum Security Level
MSLD	Minimum Security Level Data
OTA	Over The Air
PDU	Packet Data Unit
RAM	Remote Application Management
R-APDU	Response - Application Protocol Data Unit
RF	Radio Frequency
RFM	Remote File Management
RFU	Reserved for Future Use
SCP02	Secure Channel Protocol 02
SD	Security Domain
SDU	Service Data Unit
TAR	Toolkit Application Reference
TCP	Transmission Control Protocol
TLV	Tag Length Value

3.4 Formats

3.4.1 Format of the table of optional features

The columns in table 4.1 have the following meaning.

Column	Meaning
Option	The optional feature supported or not by the IUT.
Status	See clause 3.4.3.
Support	The support columns are to be filled in by the supplier of the implementation. The following common notations, defined in ISO/IEC 9646-7 [29], are used for the support column in table 4.1. Y or y supported by the implementation. N or n not supported by the implementation. N/A, n/a or - no answer required (allowed only if the status is N/A, directly or after evaluation of a conditional status).
Mnemonic	The mnemonic column contains mnemonic identifiers for each item.

3.4.2 Format of the applicability table

The applicability of every test in table 4.2 is formally expressed by the use of Boolean expression defined in the following clause.

The columns in table 4.2 have the following meaning.

Column	Meaning
Clause	The "Clause" column identifies the clause containing the test case referenced in the "Test case number and description" column.
Test case number and description	The "Test case number and description" column gives a reference to the test case number (along with the corresponding description) detailed in the present document and required to validate the IUT.
Release	The "Release" column gives the Release applicable and onwards, for the corresponding test case.
Rel-x UICC	For a given Release, the corresponding "Rel-x UICC" column lists the tests required for a DUT to be declared compliant to this Release.
Support	The "Support" column is blank in the proforma, and is to be completed by the manufacturer in respect of each particular requirement to indicate the choices, which have been made in the implementation.

3.4.3 Status and Notations

The "Rel-x" columns show the status of the entries as follows:

The following notations, defined in ISO/IEC 9646-7 [29], are used for the status column:

M mandatory - the capability is required to be supported.

O optional - the capability may be supported or not.

N/A not applicable - in the given context, it is impossible to use the capability.

X prohibited (excluded) - there is a requirement not to use this capability in the given context.

O.i qualified optional - for mutually exclusive or selectable options from a set. "i" is an integer which identifies an unique group of related optional items and the logic of their selection which is defined immediately following the table.

Ci conditional - the requirement on the capability ("M", "O", "X" or "N/A") depends on the support of other optional or conditional items. "i" is an integer identifying an unique conditional status expression which is defined immediately following the table. For nested conditional expressions, the syntax "IF ... THEN (IF ... THEN ... ELSE...) ELSE ..." is to be used to avoid ambiguities.

References to items

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

EXAMPLE: 4.1/4 is the reference to the answer of item 4 in table 4.1.

The ID (identifier) of a test case consists of a main identifier and optionally a sub-identifier; for example, 2-1 and 3. A sub-identifier is used when there are multiple test cases with this same main identifier; otherwise, no sub-identifier is used. Reference to a main identifier when the relevant test cases also have sub-identifier are assumed to reference all of the test cases with that main identifier.

4 Test Environment

4.1 Test Applicability

4.1.1 Table of optional features

The device supplier shall state the support of possible options in table 4.1. See clause 3.3 for the format of table 4.1.

Table 4.1: Options

Item	Option	Status	Support	Mnemonic
1	CAT TP protocol is supported	O		O_CAT_TP
2	SMS protocol supported	O		O_SMS
3	HTTPS protocol supported	O		O_HTTPS
4	The TAR may be taken out of the AID	O		O_Default_TAR
5	Reader Mode, Type A	O		O_RM_A
6	Reader Mode, Type B	O		O_RM_B
7	DES used for ciphering	O		O_DES_CHP
8	STORE DATA command is supported	O		O_STORE_DATA_CMD
9	Additional combinations of the P1 parameter is supported for command GET STATUS; i.e. setting more than one bit of b5 to b8	O		O_P1_ADD_COM

4.1.2 Applicability table

Table 4.2 specifies the applicability of each test case to the device under test. See clause 3.3 for the format of table 4.2.

Table 4.2 a): Applicability of tests

Clause	Test case number and description	Release	Rel-11 UICC	Support
6.2.2.1	Test case 1: A command session with C-APDU TLV Structure with definite length coding	Rel-11	M	
6.2.2.2	Test case 2: A command session containing multiple commands with C-APDU TLV Structure with definite length coding - Bad Format	Rel-11	M	
6.2.2.3	Test case 3: A command session with C-APDU TLV Structure with indefinite length coding	Rel-11	M	
6.2.2.4	Test case 4: A command session with C-APDU TLV Structure with indefinite length coding - Bad Format	Rel-11	M	
6.2.2.5	Test case 5: A command session with Immediate Action TLV Structure with definite length coding - Normal Format	Rel-11	M	
6.2.2.6	Test case 6: A command session with Immediate Action TLV Structure with definite length coding - Referenced Format	Rel-11	M	
6.2.2.7	Test case 7: A command session with Immediate Action TLV Structure with definite length coding - Immediate Action Error	Rel-11	M	
6.2.2.8	Test case 8: A command session with Immediate Action TLV Structure with indefinite length coding - Normal Format	Rel-11	M	
6.2.2.9	Test case 9: A command session with Immediate Action TLV Structure with indefinite length coding - Referenced Format	Rel-11	M	
6.2.2.10	Test case 10: A command session with Immediate Action TLV Structure with indefinite length coding - Immediate Action Error	Rel-11	M	
6.2.2.11	Test case 11: A command session with Error Action TLV Structure with definite length coding - normal format	Rel-11	M	
6.2.2.12	Test case 12: A command session with Error Action TLV Structure with definite length coding - Referenced format	Rel-11	M	
6.2.2.13	Test case 13: A command session with Error Action TLV Structure with indefinite length coding - Normal format	Rel-11	M	
6.2.2.14	Test case 14: A command session with Error Action TLV Structure with indefinite length coding - Referenced format	Rel-11	M	

Clause	Test case number and description	Release	Rel-11 UICC	Support
6.2.2.15	Test case 15: A command session with Script Chaining TLV Structure with definite length coding	Rel-11	M	
6.2.2.16	Test case 16: A command session with Script Chaining TLV Structure with definite length coding (Script Chaining Error)	Rel-11	M	
6.2.2.17	Test case 17: A command session with Script Chaining TLV Structure with indefinite length coding	Rel-11	M	
6.2.2.18	Test case 18: A command session with Script Chaining TLV Structure with indefinite length coding (Script Chaining Error)	Rel-11	M	
6.4.1.1	Test case 1: A command session with a single SELECT command. Check access to the file tree.	Rel-11	M	
6.4.1.2	Test case 2: A command session with multiple commands (SELECT, UPDATE BINARY, READ BINARY).	Rel-11	M	
6.4.1.3	Test case 3: A command session with multiple commands (SEARCH RECORD, UPDATE RECORD, INCREASE, READ RECORD)	Rel-11	M	
6.4.1.4	Test case 4: A command session with multiple commands (SET DATA, RETRIEVE DATA).	Rel-11	M	
6.4.1.5	Test case 5: A command session with multiple commands (ACTIVATE FILE, DEACTIVATE FILE)	Rel-11	M	
6.4.1.6	Test case 6: A command session with multiple commands (VERIFY PIN, CHANGE PIN).	Rel-11	M	
6.4.1.7	Test case 7: A command session with multiple commands (DISABLE PIN, ENABLE PIN).	Rel-11	M	
6.4.1.8	Test case 8: A command session with multiple commands (UNBLOCK PIN).	Rel-11	M	
6.4.1.9	Test case 5: A command session with multiple commands (CREATE FILE, RESIZE FILE, DELETE FILE)	Rel-11	M	
6.5.1.1	Test case 1: DELETE command	Rel-11	M	
6.5.2.1	Test case 1: SET STATUS command within a command session	Rel-11	M	
6.5.3.1.1	Test case 1: INSTALL [for load] as a single command in the session	Rel-11	M	
6.5.3.1.2	Test case 2: INSTALL[for load] with memory management parameters	Rel-11	M	
6.5.3.2.1	Test case 1: INSTALL[for install] with SIM File Access and Toolkit Application Specific Parameters	Rel-11	M	
6.5.3.2.2	Test case 2: INSTALL[for install] with UICC System Specific Parameters and SIM File Access and Toolkit Application Specific Parameters	Rel-11	M	
6.5.3.2.3	Test case 3: INSTALL[for install] with UICC System Specific Parameter "UICC Toolkit Application specific parameters field"	Rel-11	M	
6.5.3.2.4	Test case 4: INSTALL[for install] with UICC System Specific Parameter "UICC Access Application specific parameters field"	Rel-11	M	
6.5.3.2.5	Test case 5: INSTALL[for install] with UICC System Specific Parameter "UICC Administrative Access Application specific parameters field"	Rel-11	M	
6.5.3.2.6	Test case 6: INSTALL[for install] with UICC System Specific Parameter "UICC Access Application specific parameters field" and "UICC Administrative Access Application specific parameters field" for the same ADF	Rel-11	M	
6.5.3.2.7	Test case 7: INSTALL[for install] with UICC System Specific Parameter "UICC Access Application specific parameters field" and "UICC Administrative Access Application specific parameters field" for the same UICC file system	Rel-11	M	
6.5.3.2.8	Test case 8: INSTALL[for install] with the maximum number of timers required for SIM Toolkit Application Specific Parameters set too high ('09')	Rel-11	M	
6.5.3.2.9	Test case 9: INSTALL[for install] with the maximum number of timers required for UICC Toolkit Application Specific Parameters set too high ('09')	Rel-11	M	
6.5.3.2.10	Test case 10: INSTALL[for install] with the maximum number of channels required for SIM Toolkit Application Specific Parameters set too high ('08')	Rel-11	M	
6.5.3.2.11	Test case 11: INSTALL[for install] with the maximum number of channels required for UICC Toolkit Application Specific Parameters set too high ('08')	Rel-11	M	

Clause	Test case number and description	Release	Rel-11 UICC	Support
6.5.3.2.12	Test case 12: INSTALL[for install] with the maximum number of services required for UICC Toolkit Application Specific Parameters set too high ('09')	Rel-11	M	
6.5.3.2.13	Test case 13: INSTALL[for install] with requested item identifier for SIM Toolkit Application Specific Parameters set to '128'	Rel-11	M	
6.5.3.2.14	Test case 14: INSTALL[for install] with requested item identifier for UICC Toolkit Application Specific Parameters set to '128'	Rel-11	M	
6.5.3.2.15	Test case 15: INSTALL[for install] with Minimum Security Level field of SIM Toolkit Application different from zero	Rel-11	C001	
6.5.3.2.16	Test case 16: INSTALL[for install] with Minimum Security Level field of UICC Toolkit Application different from zero	Rel-11	C001	
6.5.3.2.17	Test case 17: INSTALL[for install] with Minimum Security Level field of SIM Toolkit Application different from SPI1	Rel-11	C001	
6.5.3.2.18	Test case 18: INSTALL[for install] with Minimum Security Level field of UICC Toolkit Application different from SPI1	Rel-11	C001	
6.5.3.2.19	Test case 19: INSTALL[for install] SIM Toolkit Applications with Access Domain Parameter equal to '00' and 'FF'	Rel-11	M	
6.5.3.2.20	Test case 20: INSTALL[for install] UICC Toolkit Applications with Access Domain Parameter equal to '00' and 'FF'	Rel-11	M	
6.5.3.2.21	Test case 21: INSTALL[for install] SIM Toolkit Application with Access Domain Parameter equal to '00' and access condition set to 'NEVER'	Rel-11	M	
6.5.3.2.22	Test case 22: INSTALL[for install] UICC Toolkit Application with Access Domain Parameter equal to '00' and access condition set to 'NEVER'	Rel-11	M	
6.5.3.2.23	Test case 23: INSTALL[for install] SIM Toolkit Application with Access Domain Parameter not supported	Rel-11	M	
6.5.3.2.24	Test case 24: INSTALL[for install] UICC Toolkit Application with Access Domain Parameter not supported	Rel-11	M	
6.5.3.2.25	Test case 25: INSTALL[for install] UICC Toolkit Application with Access Domain Parameter equal to '02'	Rel-11	M	
6.5.3.2.26	Test case 26: INSTALL[for install] SIM Toolkit Applications with Access Domain Parameter equal to '00' - independency from the PIN status at UICC-Terminal interface	Rel-11	M	
6.5.3.2.27	Test case 27: INSTALL[for install] UICC Toolkit Applications with Access Domain Parameter equal to '00' - independency from the PIN status at UICC-Terminal interface	Rel-11	M	
6.5.3.2.28	Test case 28: INSTALL[for install] of SIM Toolkit Applications with different Priority levels	Rel-11	M	
6.5.3.2.29	Test case 29: INSTALL[for install] of UICC Toolkit Applications with different Priority levels	Rel-11	M	
6.5.3.2.30	Test case 30: INSTALL[for install] SIM Toolkit Applets with same Priority levels	Rel-11	M	
6.5.3.2.31	Test case 31: INSTALL[for install] UICC Toolkit Applets with same Priority levels	Rel-11	M	
6.5.3.2.32	Test case 32: INSTALL[for install] two SIM Toolkit Applications with identical TAR value	Rel-11	M	
6.5.3.2.33	Test case 33: INSTALL[for install] two UICC Toolkit Application with identical TAR value	Rel-11	M	
6.5.3.2.34	Test case 34: INSTALL[for install] SIM Toolkit Application with multiple TAR values	Rel-11	C001	
6.5.3.2.35	Test case 35: INSTALL[for install] UICC Toolkit Application with multiple TAR values	Rel-11	C001	
6.5.3.2.36	Test case 36: INSTALL[for install] SIM Toolkit Application without TAR value in the Install parameters, the AID contains TAR value	Rel-11	C002	
6.5.3.2.37	Test case 37: INSTALL[for install] UICC Toolkit Application without TAR value in the Install parameters, the AID contains TAR value	Rel-11	C002	
6.5.3.2.38	Test case 38: INSTALL[for install] for contactless application with Reader mode protocol data type A	Rel-11	C003	
6.5.3.2.39	Test case 39: INSTALL[for install] for contactless application with Reader mode protocol data type B	Rel-11	C004	
6.5.3.2.40	Test case 40: INSTALL[for install] for contactless application with Card Emulation mode	Rel-11	M	
6.5.4.1	Test case 1: LOAD with DES for DAP verification	Rel-11	M	
6.5.5.1	Test case 1: PUT KEY - create new 3DES 2 keys	Rel-11	M	

Clause	Test case number and description	Release	Rel-11 UICC	Support
6.5.5.2	Test case 2: PUT KEY - create new 3DES 3 keys	Rel-11	M	
6.5.5.3	Test case 3: PUT KEY - add and replace DES keys	Rel-11	C006	
6.5.5.4	Test case 4: PUT KEY - create new 16 bytes AES keys	Rel-11	M	
6.5.5.5	Test case 5: PUT KEY - create new 24 bytes AES keys	Rel-11	M	
6.5.5.6	Test case 6: PUT KEY - create new 32 bytes AES keys	Rel-11	M	
6.5.6.1	Test case 1: GET STATUS with different P1 values	Rel-11	M	
6.5.6.2	Test case 2: GET STATUS with optional P1 values	Rel-11	C008	
6.5.6.3	Test case 3: GET STATUS returns Menu Entries in the LOCKED state	Rel-11	M	
6.5.7.1	Test case 1: GET DATA with different P1 values	Rel-11	M	
6.5.8.1	Test case 1: STORE DATA	Rel-11	C007	
6.5.8.2	Test case 2: STORE DATA with a Forbidden Load File List	Rel-11	C007	
6.6.2.1	Test case 1: Send Secured Data (READ BINARY) using Expanded and Compact format with the same TAR value	Rel-11	C005	
6.6.2.2	Test case 2: Send Secured Data (READ BINARY) using Expanded and Compact format with the same TAR value	Rel-11	C005	
6.6.2.3	Test case 3: PUSH Command, PoR required - No Error	Rel-11	C005	
6.6.2.4	Test case 4: PUSH Command - Error Case	Rel-11	C005	

Table 4.2 b): Conditional items referenced by table 4.2 a)

Conditional item	Description
C001	IF (O_CAT_TP OR O_SMS) THEN M ELSE N/A
C002	If (O_CAT_TP OR O_SMS) AND (O_Default_TAR) THEN M ELSE N/A
C003	IF O_RM_A THEN M ELSE N/A
C004	IF O_RM_B THEN M ELSE N/A
C005	IF O_CAT_TP THEN M ELSE N/A
C006	IF(O_DES_CHP AND O_CAT_TP) THEN M ELSE N/A
C007	IF O_STORE_DATA_CMD THEN M ELSE N/A
C008	IF O_P1_ADD_COM THEN M ELSE N/A

4.2 Test environment description

The general architecture for the test environment is:

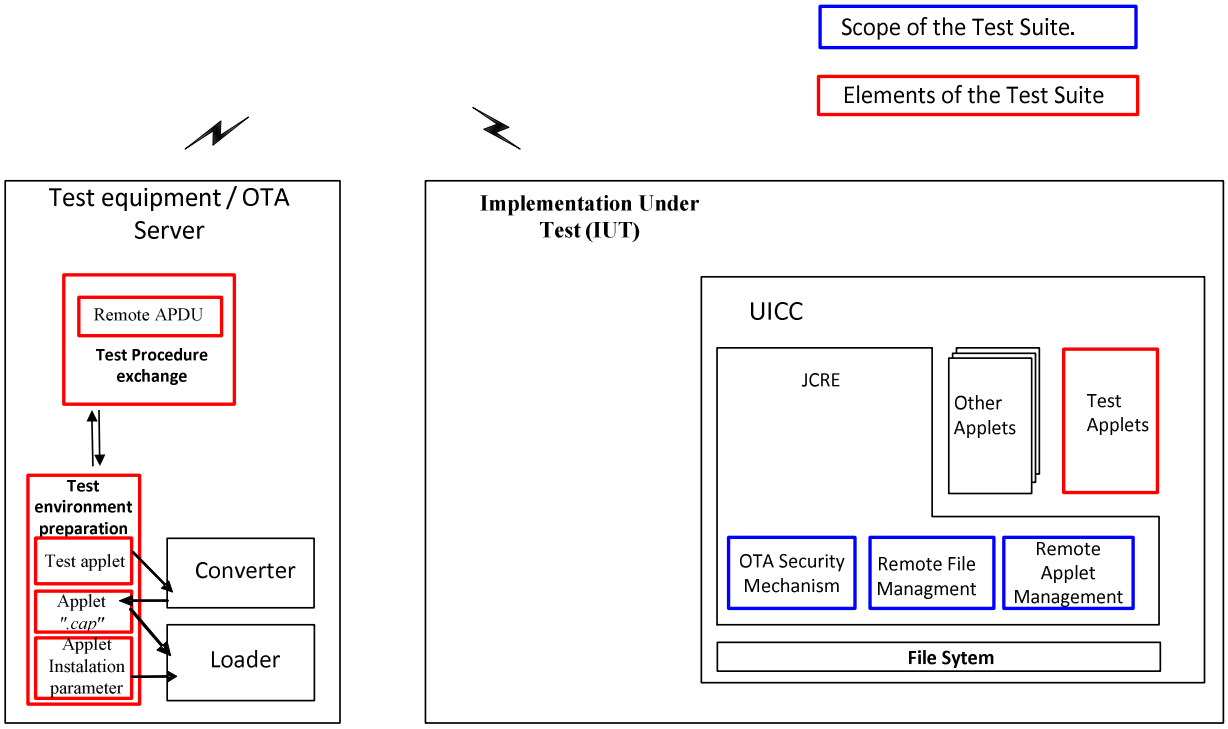


Figure 4.1

The general scheme for the Data Exchange:

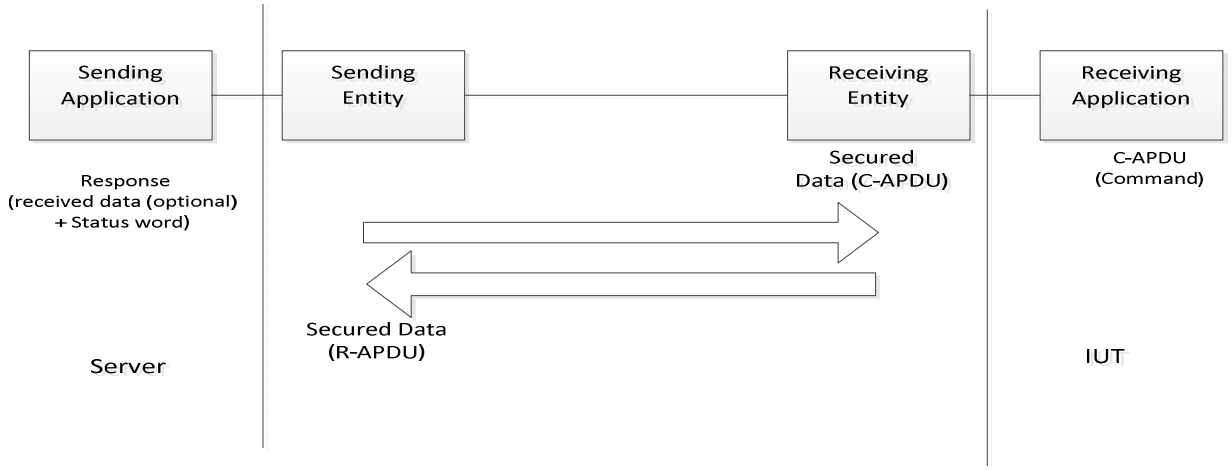


Figure 4.2

4.3 Tests format

4.3.1 Initial Conditions

In addition to the general preconditions defined in clause 4.3, this clause defines the initial conditions prior to the execution of each test case; i.e. for each ID.

4.3.2 Test procedure

Each test procedure contains a table to indicate the expected responses form the UICC as follows.

Step	Description	Expected Result	RQ
	Commands with Secured Data content description *Each step consist of a command which may contain a single command or a sequence of commands*	*Expected returned Response with Secured Data content description*	*Conformance Requirements Reference*

The detailed information on the Data Format of Secured data to be sent in the "Description" column shall be configured as specified in annex C under:

- clause C.2.1 for "Compact Remote Application Data Format"
- clause C.2.2 for "Expanded Remote Application Data Format"

The detailed information on the Command Coding of the Secured data to be sent in the "Description" shall be configured as specified in annex C under:

- clause C.1 Commands, table C.1

In case the expected returned Response with Secured Data in "Expected Result" shall contain Data in addition to the status word, the detailed description of the file contents for all system files used within the present document is specified in annex B.

4.4 General initial conditions

4.4.1 Common rules

The Initial Conditions are a set of general prerequisites for the IUT prior to the execution of testing. For each test procedure described in the present document, the following rules apply to the Initial Conditions:

- Unless otherwise stated, the file system and files content shall be restored to the contents definition in clause 4.3.1 and in annex B of the present document.
- Unless otherwise stated, before installing the applet(s) relevant to the current test procedure, no package specific to this test specification shall be present.
- Unless otherwise stated, all structured data shall be coded as Compact Remote Command Structure.
- Unless otherwise stated, all structured data sent via HTTP shall be coded as Expanded Remote command in indefinite length coding structure.
- Unless otherwise stated, the UICC shall be activated and a reset has been performed on ISO interface.
- Unless otherwise stated, the initial security conditions (i.e. PIN, ADM etc.) shall be set to the default value before running of the test case.
- Unless otherwise specified, the default SPI1 coding for a RAM application should be set to ‚17' or '16'.

4.4.2 File system and files content

Figure 4.3 shows the file system and the files content that the IUT shall contain to execute the test cases of this test specification, unless otherwise stated. The definition of other files is out of scope of the present document.

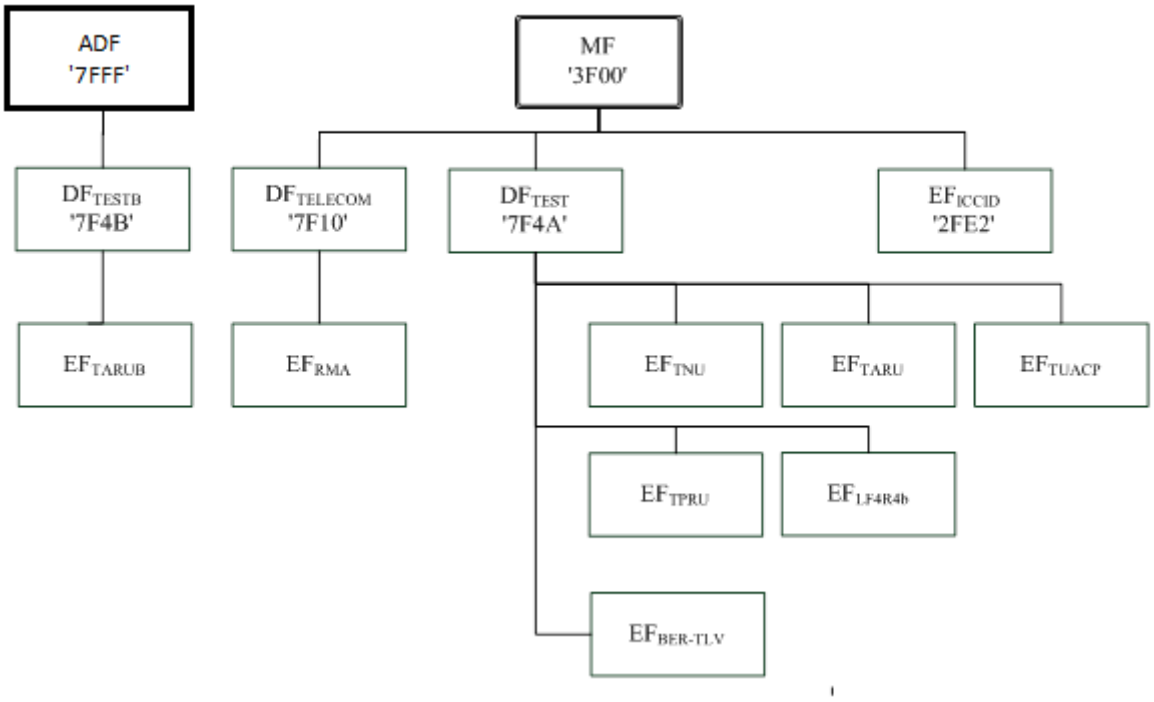


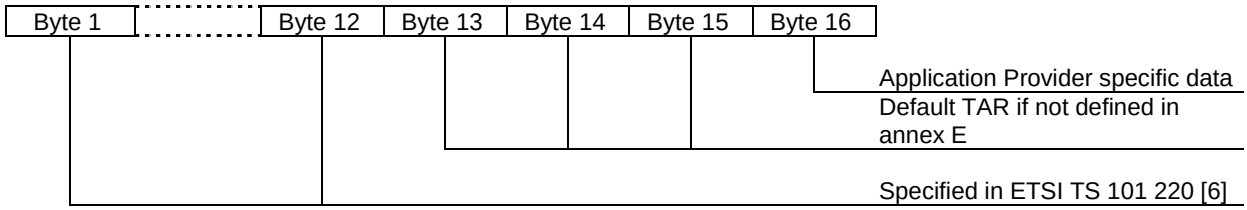
Figure 4.3

Further information can be found under annex B.

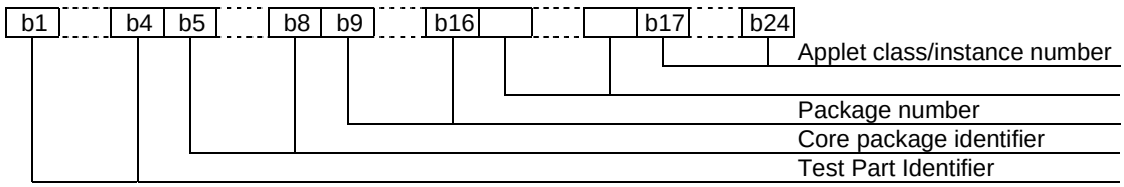
4.4.3 AID and TAR coding

The AID coding for the Test Packages, Applet classes and Applets shall be as specified in ETSI TS 101 220 [6]. In addition, the following TAR and Application Provider specific data values are defined for use within the present document.

AID coding



TAR coding (3 bytes / 24 bits):



Applet instance number, Applet Class number, Package number:

- For package AID, package number shall start from 0 and class and instance numbers shall be 0.
- For class AID, package number is the number of the class package, class number shall start from 1 and instance shall be 0.

- For instance AID, package and class number are the number of class and package of which instance belongs, and instance number shall start from 1.

Test Part and Core Package Identifier are defined in annex E, despite the values reserved in ETSI TS 101 220 [6].

Application Provider specific data (1 byte):

- '00' for Package.
- '01' for Applet class.
- '02' for Applet Instance.

Further information can be found under annex E.

4.5 Test equipment / OTA server

4.5.1 Test equipment / OTA server requirements

These sub-clauses recommend a minimum specification for each of the items of test equipment referenced in the tests.

The simulator shall meet the following requirements:

- be able to send and receive secure data commands to the IUT;
- the result of I/O commands shall be presented at the application layer;
- the structure of commands shall be according to the generalized structure defined ETSI TS 102 221 [3];
- be able to provide results of the tests;
- shall send and/or compare all data specified in test file;
- shall be able to accept all valid status codes returned.

Further requirement when the UICC interface shall be checked in the test case:

- shall provide the possibility to monitor the UICC on the ISO and SWP interfaces;
- the result of I/O commands shall be presented at the application layer.

4.5.2 Default conditions for DUT operation

- Any level 1 user verification requirement (PIN) on the IUT shall be enabled with three VERIFY PIN attempts and ten UNBLOCK PIN attempts remaining.
- The default PIN value shall be set on the IUT to '31 31 31 31 FF FF FF FF'.
- The default UNBLOCK PIN value shall be set on the IUT to '33 33 33 33 FF FF FF FF'.
- An application residing on the UICC shall support the required commands specified in ETSI TS 102 221 [3].

The following application could be used for this purpose:

- UICC toolkit application (applications using the uicc.toolkit.ToolkitInterface).
- SIM toolkit application (applications using the sim.toolkit.ToolkitInterface or sim.access.SIMView).

4.5.3 Java Card™ Software Development Kit

Java Card™ software development kit (SDK) version supported by Java Card 3.0.1 specifications ([26], [27] and [28]) is 1.5.

5 Conformance Requirements

5.1 Overview of remote management

Reference: ETSI TS 102 226 [1], clause 4.

RQ number	Clause	Description
RQ01_0001	4	All data exchanged between the Sending Entity and Receiving Entity shall be formatted as "Secured data" according to ETSI TS 102 225 [2].
RQ01_0002	4	The parameter(s) in the "Secured data" is either a single command, or a list of commands, which shall be processed sequentially.
RQ01_0003	4	The Remote Management application shall take parameters from the "Secured data" and shall act upon the files or applications or perform other actions according to these parameters.
RQ01_0004	4	Remote Management commands shall be executed by the dedicated Remote Management Application.
RQ01_0005	4	A "Command session" is defined as starting upon receipt of the parameter/command list, and ends when the parameter list in the "Secured data" is completed, or when an error (i.e. SW1 of the command indicates an error condition) is detected which shall halt further processing of the command list.
RQ01_0006	4	Warnings or procedure bytes do not halt processing of the command list.
RQ01_0007	4	A "Command session" shall be handled like an application session defined in ETSI TS 102 221 [3] (for RFM) and GlobalPlatform Card Specification [5] (for RAM).
RQ01_0008	4	Application selection at the beginning of the session happens implicitly based on the header information (TAR or HTTP header field X-Admin-Targeted-Application).
RQ01_0009	4	Unless defined otherwise in ETSI TS 102 226 [1], the session context shall be deleted when the "Command session" ends.
RQ01_0010	4	At the beginning and end of a Command "session" the logical state of the UICC as seen from the terminal shall not be changed to an extent sufficient to disrupt the behaviour of the terminal.
RQ01_0011	4	If changes in the logical state have occurred that the terminal needs to be aware of, the application on the UICC may issue a REFRESH command according to ETSI TS 102 223 [4].
NOTE: RQ01_0008 is implicitly tested in the present document.		

5.2 Remote APDU format

Reference: ETSI TS 102 226 [1], clause 5.

RQ number	Clause	Description
RQ02_0101	5.1.1	A command string may contain a single command or a sequence of commands.
RQ02_0102	5.1.1	The structure of each command shall be according to the generalized structure defined below; each element other than the Data field is a single octet (see ETSI TS 102 221 [3]). The format of the commands is the same as the one defined in ETSI TS 102 221 [3] for T = 0 TPDU commands. Class byte (CLA) | Instruction code (INS) | P1 | P2 | P3 | Data
RQ02_0103	5.1.1	If the sending application needs to retrieve the Response parameters/data of a case 4 command, then a GET RESPONSE command shall follow this command in the command string.
RQ02_0104	5.1.1	The GET RESPONSE and any case 2 command (i.e. READ BINARY, READ RECORD) shall only occur once in a command string and, if present, shall be the last command in the string.
RQ02_0105	5.1.1	For all case 2 commands and for the GET RESPONSE command, if P3 = '00', then the UICC shall send back all available response parameters/data e.g. if a READ RECORD command has P3 = '00' the whole record shall be returned.
RQ02_0106	5.1.1	In case the data is truncated in the response, the remaining bytes are lost and the status words shall be set to '62 F1'.

RQ number	Clause	Description
RQ02_0107	5.1.1	The limitation of 256 bytes does not apply for the length of the response data.
NOTE: RQ02_0102 is implicitly tested in the present document. All tests related to ETSI TS 102 221 [3] UICC compliance to be provided in ETSI TS 102 230-2 [30].		

RQ number	Clause	Description
RQ02_0201	5.1.2	If a proof of Receipt is required by the sending entity, the Additional Response Data sent by the Remote Management Application shall be formatted as following: Number of commands executed within the command script, with Length =1. This field shall be set to '01' if one command was executed within the command script, '02' if two commands were executed, etc. Status bytes or '61 xx' procedure bytes of last executed command/GET RESPONSE, of Length = 2. Response data of last executed command / GET RESPONSE if available (i.e. if the last command was a case 2 command or a GET RESPONSE), with Length = X.
NOTE: This field shall be set to '01' if one command was executed within the command script, '02' if two commands were executed, etc.		

RQ number	Clause	Description
RQ2_0301	5.2.1	For Expanded Remote command structure, the "Secured data" sent to a Remote Management Application shall be a BER-TLV data object formatted according to the table below for definite length coding: **Length in bytes** / **Name** 1 / Command Scripting template tag for definite length coding L / Length of Command Scripting template= A+B+…C A / Command TLV B / Command TLV … / … C / Command TLV Where the tag of this TLV is defined in annex A.
RQ02_0301a	5.2.1	For Expanded Remote command structure, the "Secured data" sent to a Remote Management Application shall be a BER-TLV data object formatted according to the table below for indefinite length coding: **Length in bytes** / **Name** 1 / Command Scripting template tag for indefinite length coding 1 / Indicator for indefinite length coding (value '80') A / Command TLV B / Command TLV … / … C / Command TLV 2 / End of content indicator (value '00 00') Where the tag of this TLV is defined in annex A.
RQ02_0302	5.2.1	A Remote Management application command string may contain a single or several Command TLVs.
RQ02_0303	5.2.1	If the Command TLV is a C-APDU it shall contain a remote management command
RQ02_0304	5.2.1	If the command TLV is an Immediate Action TLV it shall contain a proactive command or another action to be performed when it is encountered while processing the sequence of Command TLVs.
RQ02_0305	5.2.1	If the command TLV is an Error Action TLV it shall contain a proactive command to be performed only if an error is encountered in a C APDU following this TLV.
RQ02_0306	5.2.1	A Command TLV can be a script Chaining TLV as first Command TLV.
NOTE: For testing RQ02_0301 the tags of the TLVs are defined in ETSI TS 102 226 [1], in annex A.		

RQ number	Clause	Description
RQ02_0401	5.2.1.1	The structure of each C-APDU shall be a TLV structure coded according to the C-APDU COMPREHENSION-TLV data object coding defined in ETSI TS 102 223 [4]. The restriction on the length of the C-APDU mentioned in the note in ETSI TS 102 223 [4] shall not apply.
RQ02_0402	5.2.1.1	For all case 2 and case 4 C-APDUs, if Le='00' in the C-APDU, then the UICC shall send back all available response parameters/data in the R-APDU e.g. if a READ RECORD command has Le='00' the whole record shall be returned. The limitation of 256 bytes does not apply for the length of the response data.
RQ02_0403	5.2.1.1	In case the data is truncated in the response of a C-APDU, the status words for this C-APDU shall be set to '62 F1' in the corresponding R-APDU. This shall terminate the processing of the command list.
RQ02_0404	5.2.1.1	If a R-APDU fills the response buffer so that no further R-APDU can be included in the response scripting template, this shall terminate the processing of the command list.
RQ02_0405	5.2.1.1	If Le field is empty in the C-APDU, then no response data is expected in the R-APDU and in case of expanded format with definite length coding, no R-APDU shall be returned by the UICC in the application additional response data except if the corresponding C-APDU is the last command executed in the script.
NOTE: RQ02_0401 is verified in the present document for some C-APDUs. Further tests on TLV structure coding is out of the scope of the present document.		

RQ number	Clause	Description
RQ02_0501	5.2.1.2	If the normal format is used for the Immediate Action TLV it shall be formatted as: **Length in bytes** / **Name** 1 / Immediate Action tag (see annex A) L / Length of Immediate Action = A > 1 A / Set of COMPREHENSION-TLV data objects
RQ02_0502	5.2.1.2	If the referenced format is used for Immediate Action TLV it shall be formatted as: **Length in bytes** / **Name** 1 / Immediate Action tag (see annex A) 1 / Length of Immediate Action = 1 1 / '01' to '7F': Reference to a record in EF_{RMA} '81': Proactive session indication '82': Early response other values: RFU
RQ02_0503	5.2.1.2	In case Immediate Action TLV with reference format and in case of reference to a record in EF_{RMA}, the referenced record shall contain the set of COMPREHENSION-TLV data objects preceded by a length value as defined for a BER-TLV, see ETSI TS 102 222 [9].
RQ02_0504	5.2.1.2	If present, the Immediate Action TLV coding "proactive session indication" shall be: The first Command TLV in the script if there is no script chaining. The second Command TLV in the script if there is script chaining.
RQ02_0505	5.2.1.2	In case of "proactive session indication", execution of the remaining script shall be suspended if a proactive session is ongoing.
RQ02_0506	5.2.1.2	In case of "proactive session indication", execution of the remaining script shall be suspended if a proactive session is ongoing. Script processing shall be resumed after the end of the proactive session. If the UICC cannot suspend the script execution, e.g. because there is not enough internal resources available, the UICC shall terminate the processing of the script and return a "suspension error" in the response data.
RQ02_0507	5.2.1.2	If no "proactive session indication" is present as first Command TLV and another proactive session is ongoing, proactive commands in the script shall be silently ignored.
RQ02_0508a	5.2.1.2	In case of "early response", the response to the sending entity shall be sent before processing the rest of the command TLVs.
RQ02_0508b	5.2.1.2	In case of "early response", the number of executed commands TLV objects shall include all objects up to the immediate action TLV encoding the "early response".
RQ02_0508c	5.2.1.2	In case of "early response", no other response data shall be sent after the response sent due to the early response action TLV.

RQ number	Clause	Description
RQ02_0509	5.2.1.2	Proactive commands DISPLAY TEXT, PLAY TONE and REFRESH are allowed as Immediate Action.

RQ number	Clause	Description
RQ02_0601	5.2.1.3	The Error Action TLV - normal format shall be formatted as: **Length in bytes** / **Name** 1 / Error Action tag (see annex A) L / Length of Error Action = A > 1 A / Set of COMPREHENSION-TLV data objects
RQ02_0602	5.2.1.3	The Error Action TLV - referenced format shall be formatted as: **Length in bytes** / **Name** 1 / Error Action tag (see annex A) 1 / Length of Error Action = 1 1 / '01' to '7F': Reference to a record in EFRMA other values: RFU
RQ02_0603	5.2.1.3	The Error Action TLV - no action shall be formatted as: **Length in bytes** / **Name** 1 / Error Action tag (see annex A) 1 / Length of Error Action = 0
RQ02_0604	5.2.1.3	In case of referenced format, the referenced record in EF_{RMA} shall contain the set of COMPREHENSION-TLV data objects preceded by a length value as defined for a BER-TLV, see ETSI TS 123 048 [10].
RQ02_0605	5.2.1.3	Proactive commands for Error Action DISPLAY TEXT and PLAY TONE are allowed for Error Action
RQ02_0606	5.2.1.3	If there is an Error Action TLV between the start of the script and the C-APDU resulting in an error, the action defined in the last Error Action TLVs shall be performed. If this last Error Action TLV has zero length, no action shall be performed.
RQ02_0607	5.2.1.3	If there is no Error Action TLV between the start of the script and the C-APDU resulting in an error, no action shall be performed.

RQ number	Clause	Description
RQ02_0701	5.2.1.4	The optional Script Chaining TLV shall be coded as: **Length in bytes** / **Name** 1 / Script Chaining tag 1 / Script Chaining Length = 1 1 / Script Chaining Value The Script Chaining tag is defined in annex A.
RQ02_0702	5.2.1.4	If present, the Script Chaining TLV shall be present only once and shall be the first Command TLV in the Command Script. It may only be present for Remote File Management or Remote Application Management.
RQ02_0703	5.2.1.4	If it is received by any other application standardized in the present document, the error "Script Chaining not supported by this application" shall be sent back to the sending entity.
RQ02_0704	5.2.1.4	The Script Chaining Value is defined as follows: '01': first script - delete chaining information upon card reset - valid for RFM and RAM. '11': first script - keep chaining information across card reset - valid for RFM only. '02': subsequent script - subsequent script(s) will follow. '03': subsequent script - last script.
RQ02_0705	5.2.1.4	With script chaining, a command session is extended beyond the scope of one command scripting TLV; the session context is kept until the last script.

<table>
<tr><th>RQ number</th><th>Clause</th><th>Description</th></tr>
<tr><td>RQ02_0801</td><td>5.2.2</td><td>In case no Script Chaining is present in the command list or processing of the Script Chaining produces no error, it shall be formatted for Expanded Format of Remote Management application additional response data in case of definite length coding as:

<table><tr><th>Length in bytes</th><th>Name</th></tr><tr><td>1</td><td>Response Scripting template tag for definite length coding</td></tr><tr><td>L</td><td>Length of Response Scripting template= X+A+B…C</td></tr><tr><td>X</td><td>Number of executed Command TLV objects</td></tr><tr><td>A</td><td>R-APDU of first executed case 2/ case 4 C-APDU in the script</td></tr><tr><td>B</td><td>R-APDU of second executed case 2/ case 4 C-APDU in the script</td></tr><tr><td></td><td>…</td></tr><tr><td>C</td><td>R-APDU of last executed C-APDU (case 1, 2, 3 or 4) in the script or Bad format TLV</td></tr><tr><td colspan="2">NOTE: If the last executed C-APDU is a case 2 or case 4 command, its corresponding R-APDU TLV shall only be present once in the Response Scripting template.</td></tr></table>
Where the tag of this TLV is defined in annex A</td></tr>
<tr><td>RQ02_0801a</td><td>5.2.2</td><td>The Response Scripting template is a BER-TLV data object as defined in ETSI ETSI TS 101 220 [6], i.e. it uses definite length coding; see RQ02_0301 it shall be used if the command scripting template used definite length coding.</td></tr>
<tr><td>RQ02_0802</td><td>5.2.2</td><td>In case no Script Chaining is present in the command list or processing of the Script Chaining produces no error, it shall be formatted for Expanded Format of Remote Management application additional response data in case of indefinite length coding as:

<table><tr><th>Length in bytes</th><th>Name</th></tr><tr><td>1</td><td>Response Scripting template tag for indefinite length coding</td></tr><tr><td>1</td><td>Indicator for indefinite length coding (value '80')</td></tr><tr><td>A</td><td>R-APDU of first executed C-APDU in the script</td></tr><tr><td>B</td><td>R-APDU of second executed C-APDU in the script</td></tr><tr><td></td><td>…</td></tr><tr><td>C</td><td>R-APDU of last executed C-APDU in the script or Bad format TLV</td></tr><tr><td>2</td><td>End of content indicator (value '00 00')</td></tr></table>
Where the tag of this TLV is defined in annex A</td></tr>
<tr><td>RQ02_0802a</td><td>5.2.2</td><td>The Response Scripting template is a BER-TLV data object which uses indefinite length coding as defined in ISO/IEC 8825-1 [21]; see RQ02_0302. It shall be used if the command scripting template used indefinite length coding.</td></tr>
<tr><td>RQ02_0803</td><td>5.2.2</td><td>The Response Scripting template is a BER TLV data object as defined in ETSI TS 101 220 [6], i.e. it uses definite length coding; see table 5.2 [1]. It shall be used if the command scripting template used definite length coding.</td></tr>
<tr><td>RQ02_0804</td><td>5.2.2</td><td>The Response Scripting template is a BER-TLV data object which uses indefinite length coding as defined in ISO/IEC 8825-1 [21]; see table 5.2a [1]. It shall be used if the command scripting template used indefinite length coding.</td></tr>
<tr><td>RQ02_0805</td><td>5.2.2</td><td>In case the definite length coding is used, the Number of executed command TLV objects is a BER-TLV data object and shall be coded as shown below:

<table><tr><th>Length in bytes</th><th>Description</th></tr><tr><td>1</td><td>Number of executed command TLV objects tag</td></tr><tr><td>1</td><td>Length=X</td></tr><tr><td>X</td><td>Number of executed command TLV objects</td></tr></table>
Where the tag of this TLV is defined in annex A.</td></tr>
<tr><td>RQ02_0806</td><td>5.2.2</td><td>The structure of each R-APDU shall be a TLV structure coded according to the R-APDU COMPREHENSION-TLV data object coding defined in ETSI TS 102 223 [4].</td></tr>
<tr><td>RQ02_0807</td><td>5.2.2</td><td>The restriction on the length of the R-APDU mentioned in the note in ETSI TS 102 223 [4] shall not apply. For Le='00', the length of the R-APDU may be coded on more than two bytes.</td></tr>
</table>

<table>
<tr><th>RQ number</th><th>Clause</th><th>Description</th></tr>
<tr><td>RQ02_0809</td><td>5.2.2</td><td>In case of an unknown Tag, or TLV with a wrong format (e.g. length > length of BER-TLV or length < 4) is encountered while processing the command script, a Bad format TLV shall be put into the response data and processing of the command script shall be aborted at that point.</td></tr>
<tr><td>RQ02_0810</td><td>5.2.2</td><td>The Number of executed C-APDUs shall take into account the incorrectly formatted TLV.</td></tr>
<tr><td>RQ02_0811</td><td>5.2.2</td><td>The Bad format TLV is a BER-TLV data object and shall be coded as follow:
<table><tr><th>Length in bytes</th><th>Description</th></tr><tr><td>1</td><td>Bad format TLV tag</td></tr><tr><td>1</td><td>Length</td></tr><tr><td>1</td><td>Error type</td></tr></table>
Where the tag of this TLV is defined in annex A.</td></tr>
<tr><td>RQ02_0812</td><td>5.2.2</td><td>The Bad format TLV shall be coded with following error type coding:
• '01': Unknown Tag found.
• '02': Wrong length found.
• '03': Length not found.
• other values: RFU.</td></tr>
<tr><td>RQ02_0812a</td><td>5.2.2</td><td>For Expanded Format of Remote Management application additional response data in case of Immediate Action error - definite length coding and If "proactive session indication" is present in the script and a proactive session is ongoing and the UICC is unable to suspend script processing, the additional response application data shall be formatted according to table below and indicate "suspension error":
<table><tr><th>Length in bytes</th><th>Name</th></tr><tr><td>1</td><td>Response Scripting template tag for definite length coding</td></tr><tr><td>L</td><td>Length of Response Scripting template= X+A</td></tr><tr><td>X</td><td>Number of executed command TLV objects (value is 1)</td></tr><tr><td>A</td><td>Immediate Action Response</td></tr></table>
Where the tag of this TLV is defined in annex A.</td></tr>
<tr><td>RQ02_0812b</td><td>5.2.2</td><td>Expanded Format of Remote Management application additional response data in case of Immediate Action error - indefinite length coding and If "proactive session indication" is present in the script and a proactive session is ongoing and the UICC is unable to suspend script processing, the additional response application data shall be formatted according to table below and indicate "suspension error":
<table><tr><th>Length in bytes</th><th>Name</th></tr><tr><td>1</td><td>Response Scripting template tag for indefinite length coding</td></tr><tr><td>1</td><td>Indicator for indefinite length coding (value '80')</td></tr><tr><td>A</td><td>Immediate Action Response</td></tr><tr><td>2</td><td>End of content indicator (value '00 00')</td></tr></table>
Where the tag of this TLV is defined in annex A</td></tr>
<tr><td>RQ02_0813</td><td>5.2.2</td><td>The Immediate Action Response from RQ02_0812a and RQ02_0812b is an Immediate Action Response TLV which is a BER-TLV data object coded as follow:
<table><tr><th>Length in bytes</th><th>Description</th></tr><tr><td>1</td><td>Immediate Action Response tag (see annex A)</td></tr><tr><td>1</td><td>Length=X</td></tr><tr><td>X</td><td>Immediate Action Response Value</td></tr></table></td></tr>
<tr><td>RQ02_0814</td><td>5.2.2</td><td>The Immediate Action Response Value from RQ02_0813 is defined as follows:
• '01': Suspension error.</td></tr>
<tr><td>RQ02_0815</td><td>5.2.2</td><td>In case a Script Chaining TLV indicating "subsequent script - …" is present in the list, the following situation shall be considered as chaining errors:
The previous script did not contain a Script Chaining TLV indicating "first script - …" or "subsequent script - subsequent script(s) will follow".</td></tr>
<tr><td>RQ02_0816</td><td>5.2.2</td><td>In case a Script Chaining TLV indicating "subsequent script - …" is present in the list, the following situation shall be considered as chaining errors:
The first script of the chain indicating "first script - delete chaining information upon card reset" was processed in an earlier card session.</td></tr>
</table>

<table>
<tr><th>RQ number</th><th>Clause</th><th>Description</th></tr>
<tr><td>RQ02_0817a</td><td>5.2.2</td><td>In case of chaining errors, the additional response application data shall be formatted according to table below, for definite length coding:

<table><tr><th>Length in bytes</th><th>Name</th></tr><tr><td>1</td><td>Response Scripting template tag for definite length coding</td></tr><tr><td>L2</td><td>Length of Response Scripting template= X+A</td></tr><tr><td>X</td><td>Number of executed Command TLV objects</td></tr><tr><td>A</td><td>Script Chaining Response</td></tr></table>
Where the Script Chaining Response tag is defined in annex A.</td></tr>
<tr><td>RQ02_0817b</td><td>5.2.2</td><td>In case of chaining errors, the additional response application data shall be formatted according to table below, for indefinite length coding:

<table><tr><th>Length in bytes</th><th>Name</th></tr><tr><td>1</td><td>Response Scripting template tag for indefinite length coding</td></tr><tr><td>1</td><td>Indicator for indefinite length coding (value '80')</td></tr><tr><td>A</td><td>Script Chaining Response</td></tr><tr><td>2</td><td>End of content indicator (value '00 00')</td></tr></table>
Where the Script Chaining Response tag is defined in annex A.</td></tr>
<tr><td>RQ02_0818</td><td>5.2.2</td><td>The Script Chaining Response TLV is a BER-TLV data object and shall be coded as:

<table><tr><th>Length in bytes</th><th>Description</th></tr><tr><td>1</td><td>Script Chaining Response tag</td></tr><tr><td>1</td><td>Length=X</td></tr><tr><td>X</td><td>Script Chaining Result Value</td></tr></table>
Where the Script Chaining Response tag is defined in annex A.</td></tr>
<tr><td>RQ02_0819</td><td>5.2.2</td><td>The Script Chaining Result Value is defined as follows:
'01': No previous script.
'02': Script Chaining not supported by this application.
'03': Unable to process script chaining (e.g. no resources to store chaining context).</td></tr>
</table>

RQ number	Clause	Description
RQ02_0901	5.3	If a TAR is configured for multiple data formats, the following automatic application data format detection shall apply: If b2b1 of the first data byte of the application data are 00, the format of the application data shall be the compact remote application data format.
RQ02_0902	5.3	If b2b1 of the first data byte of the application data are not 00, and if a TAR is configured for multiple data formats, the following automatic application data format detection shall apply: the first data byte of the application data shall indicate the format of the data packet.

5.3 Security parameters assigned to applications

Reference: ETSI TS 102 226 [1], clause 6.

RQ number	Clause	Description
RQ03_0101	6.1	The Receiving Entity shall check the Minimum Security Level, set for the Receiving Application, before processing the security of the Command Packet.
RQ03_0102	6.1	If the check fails, the Receiving Entity shall reject the messages and a Response Packet with the "Insufficient Security Level" Response Status Code (see ETSI TS 102 225 [2]) shall be sent if required.
RQ03_0103	6.1	According to UICC Configuration [16], if the Receiving Application is a Security Domain which has no own secure channel key set, then the security will be processed by the closest ascendant Security Domain (= Receiving Entity) that has a suitable secure channel key set.
RQ03_0104	6.1	A Minimum Security Level as described in clause 8.2.1.3.2.4 in ETSI TS 102 226 [1] shall be assigned to each Remote Management application (RFM/RAM).
NOTE 1: Development of test cases for RQ03_0103 is out of scope for the present document. NOTE 2: RQ03_0101 is for information only.		

RQ number	Clause	Description
RQ03_0201	6.2	The access rights granted to an application by its Access Domain shall be independent from the access rights granted at the UICC/Terminal interface.
RQ03_0202	6.2	An Access Domain as described in clause 8.2.1.3.2.5 in ETSI TS 102 226 [1] shall be assigned to each Remote File Management Application.

5.4 Remote File Management (RFM)

Reference: ETSI TS 102 226 [1], clause 7.

RQ number	Clause	Description
RQ04_0101	7	The concept of embedding APDUs in a command packet and the Additional Response data in a response packet shall be as defined in the previous clauses describing the Compact and expanded Remote Application data format.
RQ04_0102	7	Unless a TAR is used that is configured for automatic application data format detection, the Compact and expanded Remote Application data formats shall be distinguished by different TAR values.
RQ04_0103	7	For the Expanded Remote Application data format, it is possible to chain two or more scripts using Script Chaining TLVs.
RQ04_0104	7	If a Script Chaining TLV indicating "first script - …" or "subsequent script - subsequent script(s) will follow" is processed successfully, the file context (current directory, current file, current tag pointer, etc.) and the PIN verification status at the end of the script shall be remembered until the next script is processed by the Remote File Management application.
RQ04_0105	7	If the next script received successfully contains a Script Chaining TLV indicating "subsequent script - …", the remembered file context and PIN verification status shall be restored. Else the default context shall be used.
RQ04_0106	7	If a non-shareable file is selected by the remembered file context, the mechanisms defined in ETSI TS 102 221 [3] limiting the access to non-shareable files shall apply.

RQ number	Clause	Description
RQ04_0201	7.1	The SELECT command shall not include the selection by DF name corresponding to P1='04' in the Command Parameters of SELECT (see ETSI TS 102 221 [3]).
RQ04_0202	7.1	The Response Data shall be placed in the Additional Response Data element of the Response Packet. If P3/Le = '00' in the READ RECORD command, then the UICC shall send back all data until the end of the data object from the current BER-TLV structure EF.
RQ04_0203	7.1	The Response Data shall be placed in the Additional Response Data element of the Response Packet. If P3/Le = '00' in the READ BINARY command, then the UICC shall send back all data until the end of the file, according to clause 5.1.
RQ04_0204	7.1	The Response Data shall be placed in the Additional Response Data element of the Response Packet. If P3/Le = '00' in the RETRIEVE DATA command, then the UICC shall send back all data until the end of the data object from the current BER-TLV structure EF.

<table>
<tr><th>RQ number</th><th>Clause</th><th>Description</th></tr>
<tr><td>RQ04_0301</td><td>7.2</td><td>A UICC Shared File System Remote File Management application shall have access only to the MF and all DFs and EFs that are located under the MF (see note 2).</td></tr>
<tr><td>RQ04_0302</td><td>7.2</td><td>Unless Script Chaining is used, the MF shall be implicitly selected and be the current directory at the beginning of a "Command session".</td></tr>
<tr><td>RQ04_0303</td><td>7.2</td><td>No ADF shall be accessed by the UICC Shared File System Remote File Management application.</td></tr>
<tr><td>RQ04_0304</td><td>7.2</td><td>The following commands shall apply for UICC Shared File System Remote File Management:
<table>
<tr><th>Operational command</th></tr>
<tr><td>SELECT (see below)</td></tr>
<tr><td>UPDATE BINARY</td></tr>
<tr><td>UPDATE RECORD</td></tr>
<tr><td>SEARCH RECORD</td></tr>
<tr><td>INCREASE</td></tr>
<tr><td>VERIFY PIN</td></tr>
<tr><td>CHANGE PIN</td></tr>
<tr><td>DISABLE PIN</td></tr>
<tr><td>ENABLE PIN</td></tr>
<tr><td>UNBLOCK PIN</td></tr>
<tr><td>DEACTIVATE FILE</td></tr>
<tr><td>ACTIVATE FILE</td></tr>
<tr><td>READ BINARY</td></tr>
<tr><td>READ RECORD</td></tr>
<tr><td>CREATE FILE</td></tr>
<tr><td>DELETE FILE</td></tr>
<tr><td>RESIZE FILE</td></tr>
<tr><td>SET DATA</td></tr>
<tr><td>RETRIEVE DATA</td></tr>
</table>
The SELECT command shall not include the selection by DF name corresponding to P1='04' in the Command Parameters of SELECT.</td></tr>
<tr><td>RQ04_0305</td><td>7.2</td><td>The TAR value of the UICC Shared File System Remote File Management application is defined in ETSI TS 101 220 [6].</td></tr>
<tr><td colspan="3">NOTE 1: RQ04_0305 is for information only.
NOTE 2: ADFs are not considered to be files located under the MF.</td></tr>
</table>

<table>
<tr><th>RQ number</th><th>Clause</th><th>Description</th></tr>
<tr><td>RQ04_0406</td><td>7.3</td><td>An ADF Remote File Management application shall have access to the DFs and EFs located under the ADF.</td></tr>
<tr><td>RQ04_0407</td><td>7.3</td><td>Unless Script Chaining is used, the ADF shall be implicitly selected and be the current directory at the beginning of a "Command session".</td></tr>
<tr><td>RQ04_0408</td><td>7.3</td><td>The UICC Shared File System, i.e. the MF and all DFs and EFs that are located under the MF, may also be accessed, depending on the access rights granted to the ADF Remote File Management application.</td></tr>
<tr><td>RQ04_0409</td><td>7.3</td><td>The following commands shall apply for ADF Remote File Management:
<table><tr><th>Operational command</th></tr><tr><td>SELECT (see below)</td></tr><tr><td>UPDATE BINARY</td></tr><tr><td>UPDATE RECORD</td></tr><tr><td>SEARCH RECORD</td></tr><tr><td>INCREASE</td></tr><tr><td>VERIFY PIN</td></tr><tr><td>CHANGE PIN</td></tr><tr><td>DISABLE PIN</td></tr><tr><td>ENABLE PIN</td></tr><tr><td>UNBLOCK PIN</td></tr><tr><td>DEACTIVATE FILE</td></tr><tr><td>ACTIVATE FILE</td></tr><tr><td>READ BINARY</td></tr><tr><td>READ RECORD</td></tr><tr><td>CREATE FILE</td></tr><tr><td>DELETE FILE</td></tr><tr><td>RESIZE FILE</td></tr><tr><td>SET DATA</td></tr><tr><td>RETRIEVE DATA</td></tr></table>
The SELECT command shall not include the selection by DF name corresponding to P1='04' in the Command Parameters of SELECT.</td></tr>
<tr><td>RQ04_0410</td><td>7.3</td><td>The TAR of an ADF RFM application shall be linked to the AID of the application to which the ADF belongs.</td></tr>
<tr><td>RQ04_0411</td><td>7.3</td><td>The TAR value of an ADF Remote File Management application is defined in ETSI TS 101 220 [6].</td></tr>
<tr><td colspan="3">NOTE: RQ04_0411 is for information only.</td></tr>
</table>

RQ number	Clause	Description
RQ04_0501	7.4	When using remote APDUs to perform RFM over HTTPS, the header values defined in ETSI TS 102 225 [2] apply. The RFM / HTTP communication flow is illustrated in annex B.

5.5 Remote Application Management (RAM)

Reference: ETSI TS 102 226 [1], clause 8.

RQ number	Clause	Description
RQ05_0101	8	Remote Application Management on a UICC card includes the ability to load, install, and remove applications.
RQ05_0102	8	The Remote Application Management is under the control of a security domain with card content management capabilities, such as the Issuer Security Domain or any Security Domain with Delegated Management privileges or Authorized Management as described in GlobalPlatform Card Specification [5].
RQ05_0103	8	All GlobalPlatform features and functionality that are described in the present clause, as well as the assignment of GlobalPlatform privileges shall comply with GlobalPlatform Card Specification [5] as detailed in the UICC Configuration [16].
RQ05_0104	8	A RAM Application shall support all features and functionality described in the present clause unless they are specifically described as optional.
RQ05_0105	8	The support of the APIs related to GlobalPlatform Card Specification [5] (Java Card API [25] or Multos API) is optional. If implemented, it shall follow the specification in the UICC Configuration [16], especially concerning the Secure Channel Interface usage.

<table>
<tr><th>RQ number</th><th>Clause</th><th>Description</th></tr>
<tr><td>RQ05_0106</td><td>8</td><td>Remote Application Management commands shall be executed according to table "Authorized GlobalPlatform Commands per Card Life Cycle State" of GlobalPlatform Card Specification [5].</td></tr>
<tr><td>RQ05_0107</td><td>8</td><td>The TAR value allocated for the Issuer Security Domain are defined in ETSI TS 101 220 [6]. The concept of embedding APDUs in a command packet and the Additional Response data in a response packet shall be as defined in the previous clauses describing the Compact and expanded Remote Application data format.</td></tr>
<tr><td>RQ05_0108</td><td>8</td><td>Unless a TAR is used that is configured for automatic application data format detection, the Compact and expanded Remote Application data formats shall be distinguished by different TAR values.</td></tr>
<tr><td>RQ05_0109</td><td>8</td><td>The Minimum Security Level of a RAM Application shall require at least integrity using CC or DS. It applies to all data formatted as secured data according to clause 4 of the present document and including all commands listed below:
<table>
<tr><th>Operational command</th></tr>
<tr><td>DELETE</td></tr>
<tr><td>SET STATUS</td></tr>
<tr><td>INSTALL</td></tr>
<tr><td>LOAD</td></tr>
<tr><td>PUT KEY</td></tr>
<tr><td>GET STATUS</td></tr>
<tr><td>GET DATA as case 2 command
GET DATA as case 4 command
(for Menu parameters)</td></tr>
<tr><td>STORE DATA</td></tr>
</table></td></tr>
<tr><td>RQ05_0110</td><td>8</td><td>A complying card shall support at least the triple DES algorithm in outer CBC mode for cryptographic computations.</td></tr>
<tr><td colspan="3">NOTE 1: RQ05_0102 is not testable.
NOTE 2: Development of test cases for RQ05_0103, RQ05_0105 and RQ05_0106 is out of scope for the present document.</td></tr>
</table>

RQ number	Clause	Description
RQ05_0201	8.1	Remote Load File loading, Application installation, Load File removal, Application removal, Application locking/unlocking, Application information retrieval shall be compliant to GlobalPlatform Card Specification [5] as detailed in the UICC Configuration [16].
RQ05_0202	8.1	Support of the application personalization described in Global Platform Card Specification [5] is optional.
RQ05_0203	8.1	As a RAM Application is a Receiving Application per clause 4, application selection (SELECT command) and command dispatching as described in GlobalPlatform Card Specification [5] do not apply to Remote Application Management.
NOTE: Development of test cases for RQ05_0201, RQ05_0202 and RQ05_0203 is out of scope for the present document.		

RQ number	Clause	Description
RQ05_3801	8.2	Commands and responses shall be coded according to GlobalPlatform Card Specification [5] as detailed in the UICC Configuration [16] unless otherwise specified in the present document.
RQ05_3802	8.2	Secure messaging shall be based on ETSI TS 102 225 [2].
RQ05_3803	8.2	if additional application provider security as defined in clause 10.2 is applied, the secure messaging as defined in GlobalPlatform Card Specification [5] shall not apply to RAM APDU commands and responses (e.g. MAC shall not be present in the command data field).
RQ05_3804	8.2	if additional application provider security as defined in clause 10.2 is applied, the class byte shall indicate that an APDU command includes no secure messaging.
RQ05_3805	8.2	The logical channel number indicated in the class byte shall be zero.
RQ05_3806	8.2	Command status words placed in the Additional Response Data element of the Response Packet shall be coded according to the GlobalPlatform Card Specification [5] as detailed in the UICC Configuration [16].
NOTE: RQ05_3801, RQ05_3802, RQ05_3805 and RQ05_3806 are implicitly tested in the present document. Further detailed tests are out of the scope of the present document.		

RQ number	Clause	Description
RQ05_0301	8.2.1	The following standardized Application management commands shall be supported: **Operational command** DELETE SET STATUS INSTALL LOAD PUT KEY GET STATUS GET DATA as case 2 command GET DATA as case 4 command (for Menu parameters)
RQ05_0302	8.2.1	The Response Data shall be placed in the Additional Response Data element of the Response Packet
RQ05_0303	8.2.1	Script chaining may be used for confidential application management as specified in clause 10 or to chain a sequence of STORE DATA commands. It has no effect for other commands.
RQ05_0304	8.2.1	Whenever Script chaining is present for RAM, it shall be processed as defined in the present document.
RQ05_0305	8.2.1	When using the Compact Remote Application data format and if an application session is saved beyond a command session as defined below, this session context shall be deleted upon card reset.

RQ number	Clause	Description
RQ05_0401	8.2.1.1	The Removal of Applications, of Executable Load Files, and of Executable Load Files and its related Applications shall be supported via DELETE command.
RQ05_0402	8.2.1.1	The warning status word '6200' (Application has been logically deleted) as defined in Open Platform Card Specification 2.0.1 [8] may be returned.

RQ number	Clause	Description
RQ05_0501	8.2.1.2	The management of Applications, Issuer Security Domain and Security Domains Life Cycle States shall be supported via SET STATUS.

RQ number	Clause	Description
RQ05_0601	8.2.1.3	INSTALL [for load], INSTALL [for install] and INSTALL [for make selectable] commands shall be supported.
RQ05_0602	8.2.1.3	INSTALL [for personalization] and Install [for extradition] command described in GlobalPlatform Card Specification [5] are optional.
RQ05_0603	8.2.1.3	A UICC supporting confidential application management as specified in clause 10 [1] shall support INSTALL [for personalization].
RQ05_0604	8.2.1.3	If INSTALL [for personalization] and Install [for extradition] implemented, both commands shall follow the specification in the UICC Configuration [16].
RQ05_0605	8.2.1.3	The support of the combined [for install and make selectable] within the same INSTALL command is mandatory.
RQ05_0606	8.2.1.3	When using the Compact Remote Application data format, the context established by INSTALL [for load] shall be saved across command sessions until the last LOAD command.
RQ05_0607	8.2.1.3	When using the Compact Remote Application data format, the context established by INSTALL [for personalization] (if supported) shall be saved across command sessions until the STORE DATA command containing the last block.

RQ number	Clause	Description
RQ05_0701	8.2.1.3.1	Support and presence of the Load File Data Block Hash according to GlobalPlatform Card Specification [5] shall be as specified in the UICC Configuration [16].
RQ05_0702	8.2.1.3.1	If present, the Load Parameter Field of the INSTALL [for load] command shall be coded according to GlobalPlatform Card Specification [5].
RQ05_0703	8.2.1.3.1	If the System Specific parameters "Non volatile code space limit" (Tag 'C6'), "Volatile data space limit" (Tag 'C7') and "Non volatile data space limit" (Tag 'C8') are present, the UICC shall be able to handle them.

<table>
<tr><th>RQ number</th><th>Clause</th><th>Description</th></tr>
<tr><td>RQ05_0801</td><td>8.2.1.3.2</td><td>If present, the Install Parameter Field of the INSTALL [for install] command shall be coded according to GlobalPlatform Card Specification [5].</td></tr>
<tr><td>RQ05_0802</td><td>8.2.1.3.2</td><td>If the System Specific parameters "Volatile data space limit" (Tag 'C7') and "Non volatile data space limit" (Tag 'C8') are present, the UICC shall be able to handle them.</td></tr>
<tr><td>RQ05_0803</td><td>8.2.1.3.2</td><td>The application instance shall be registered with the instance AID present in the INSTALL [for install] command.</td></tr>
<tr><td>RQ05_0804</td><td>8.2.1.3.2</td><td>In case of JavaCardTM applications, the application may invoke the register(bArray, bOffset, bLength) or the register() method.</td></tr>
<tr><td>RQ05_0805</td><td>8.2.1.3.2</td><td>In case of JavaCardTM applications, If the register (bArray, bOffset, bLength) is invoked, the AID passed in the parameters shall be the instance AID provided in the install method buffer.</td></tr>
<tr><td>RQ05_0806</td><td>8.2.1.3.2</td><td>In case of JavaCardTM applications, If the register() method is invoked the instance AID present in the INSTALL [for install] command and the AID within the Load File, as specified in GlobalPlatform Card Specification [5], should be the same.</td></tr>
<tr><td>RQ05_0807</td><td>8.2.1.3.2</td><td>The "UICC System Specific Parameters" TLV object (Tag 'EA', as defined below) is included in the Install Parameter Field and shall be coded as follows:
<table>
<tr><th>Presence</th><th>Length</th><th>Name</th><th>Value</th></tr>
<tr><td>Optional</td><td>1</td><td>Tag of UICC System Specific Parameters constructed field</td><td>'EA'</td></tr>
<tr><td></td><td>1 to 3</td><td>Length of UICC System Specific Parameters constructed field as specified in GlobalPlatform Card Specification [5] for TLV data objects. Coded as defined in ETSI TS 101 220 [6] for a BER-TLV data object</td><td></td></tr>
<tr><td></td><td>0 to n</td><td>UICC System Specific Parameters constructed value field</td><td></td></tr>
</table></td></tr>
</table>

<table>
<tr><th>RQ number</th><th>Clause</th><th>Description</th></tr>
<tr><td>RQ05_0901</td><td>8.2.1.3.2.1</td><td>The "SIM File Access and Toolkit Application Specific Parameters" TLV object (Tag 'CA', as defined below) is included in the "System Specific Parameters" (Tag 'EF') and shall be coded as follow:
<table>
<tr><th>Presence</th><th>Length</th><th>Name</th><th>Value</th></tr>
<tr><td>Optional</td><td>1</td><td>Tag of SIM file access and toolkit application specific parameters field</td><td>'CA'</td></tr>
<tr><td></td><td>1 to 3</td><td>Length of SIM file access and toolkit application specific parameters field.
Coded as defined in ETSI TS 101 220 [6] for a BER-TLV data object</td><td></td></tr>
<tr><td></td><td>6 to n</td><td>SIM file access and toolkit Application specific Parameters</td><td></td></tr>
</table></td></tr>
<tr><td>RQ05_0902</td><td>8.2.1.3.2.1</td><td>The SIM file access and toolkit application specific parameters field is used to specify the terminal and UICC resources the application instance can use. These resources include the timers, the Bearer Independent protocol channels, menu items for the Set Up Menu, the Minimum Security Level and the TAR Value(s) field.</td></tr>
</table>

<table>
<tr><th>RQ number</th><th>Clause</th><th>Description</th></tr>
<tr><td>RQ05_0903</td><td>8.2.1.3.2.1</td><td>The SIM file access and toolkit parameters are mandatory for applications using the sim.toolkit.ToolkitInterface or sim.access.SIMView interface as defined in ETSI TS 143 019 [12]. The Access Domain is applicable to applications using the sim.access.SIMView interface as defined in ETSI TS 143 019 [12]:
<table>
<tr><th>Length</th><th>Name</th><th>Value</th></tr>
<tr><td>1</td><td>Length of Access Domain field</td><td></td></tr>
<tr><td>1 to p</td><td>Access Domain</td><td></td></tr>
<tr><td>1</td><td>Priority level of the Toolkit application instance</td><td></td></tr>
<tr><td>1</td><td>Maximum number of timers allowed for this application instance</td><td></td></tr>
<tr><td>1</td><td>Maximum text length for a menu entry</td><td></td></tr>
<tr><td>1</td><td>Maximum number of menu entries allowed for this application instance</td><td>= m</td></tr>
<tr><td>1</td><td>Position of the first menu entry</td><td>\</td></tr>
<tr><td>1</td><td>Identifier of the first menu entry ('00' means do not care)</td><td>|</td></tr>
<tr><td></td><td>….</td><td>| = 2 × m bytes</td></tr>
<tr><td>1</td><td>Position of the last menu entry</td><td>|</td></tr>
<tr><td>1</td><td>Identifier of the last menu entry ('00' means do not care)</td><td>/</td></tr>
<tr><td>1</td><td>Maximum number of channels for this application instance</td><td></td></tr>
<tr><td>1</td><td>Length of Minimum Security Level field</td><td></td></tr>
<tr><td>0 to q</td><td>Minimum Security Level (MSL)</td><td></td></tr>
<tr><td>1</td><td>Length of TAR Value(s) field</td><td></td></tr>
<tr><td>3 × y</td><td>TAR Value(s) of the Toolkit Application instance</td><td></td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>RQ number</th><th>Clause</th><th>Description</th></tr>
<tr><td>RQ05_1001</td><td>8.2.1.3.2.2</td><td>If the SIM file access and toolkit parameters TLV object (tag 'CA') is present and the UICC System Specific Parameters TLV object (tag 'EA') is present, the card shall return the Status Word '6A80', incorrect parameters in data field, to the INSTALL [for install] command.</td></tr>
<tr><td>RQ05_1002</td><td>8.2.1.3.2.2</td><td>The UICC System Specific Parameters constructed value field of the INSTALL [for Install] command shall be coded as follows:
<table>
<tr><th>Presence</th><th>Length</th><th>Name</th><th>Value</th></tr>
<tr><td>Optional</td><td>1</td><td>Tag of UICC Toolkit Application specific parameters field</td><td>'80'</td></tr>
<tr><td></td><td>1</td><td>Length of UICC Toolkit Application specific parameters field</td><td></td></tr>
<tr><td></td><td>N</td><td>UICC Toolkit Application specific parameters</td><td></td></tr>
<tr><td>Optional</td><td>1</td><td>Tag of UICC Toolkit parameters DAP</td><td>'C3'</td></tr>
<tr><td></td><td>1</td><td>Length of UICC Toolkit parameters DAP</td><td></td></tr>
<tr><td></td><td>N</td><td>UICC Toolkit parameters DAP</td><td></td></tr>
<tr><td>Optional</td><td>1</td><td>Tag of UICC Access Application specific parameters field</td><td>'81'</td></tr>
<tr><td></td><td>1</td><td>Length of UICC Access Application specific parameters field</td><td></td></tr>
<tr><td></td><td>N</td><td>UICC Access Application specific parameters</td><td></td></tr>
<tr><td>Optional</td><td>1</td><td>Tag of UICC Administrative Access Application specific parameters field</td><td>'82'</td></tr>
<tr><td></td><td>1</td><td>Length of UICC Administrative Access Application specific parameters field</td><td></td></tr>
<tr><td></td><td>N</td><td>UICC Administrative Access Application specific parameters</td><td></td></tr>
</table>
</td></tr>
<tr><td>RQ05_1003</td><td>8.2.1.3.2.2</td><td>Access parameters for the same ADF may be present in both the UICC Access Application specific parameters field and the UICC Administrative Access Application specific parameters field.</td></tr>
<tr><td>RQ05_1004</td><td>8.2.1.3.2.2</td><td>Access parameters for the same UICC file system may be present in both the UICC Access Application specific parameters field and the UICC Administrative Access Application specific parameters field.</td></tr>
</table>

<table>
<tr><th>RQ number</th><th>Clause</th><th>Description</th></tr>
<tr><td>RQ05_1101</td><td>8.2.1.3.2.2.1</td><td>The UICC toolkit application specific parameters field is used to specify the terminal and UICC resources the application instance can use. These resources include the timers, the Bearer Independent Protocol channels, the services for local bearers, menu items for the Set Up Menu, the Minimum Security Level and the TAR Value(s) field.</td></tr>
<tr><td>RQ05_1102</td><td>8.2.1.3.2.2.1</td><td>The UICC Toolkit Application specific parameters are mandatory for applications using the uicc.toolkit.ToolkitInterface defined in ETSI TS 102 241 [7] and for Applets extending the SCWSExtension interface as defined in ETSI TS 102 588 [17] that make use of the ProactiveHandler and the ProactiveResponseHandler.</td></tr>
<tr><td>RQ05_1103</td><td>8.2.1.3.2.2.1</td><td>None of the toolkit resources will be accessible if the UICC Toolkit Application specific parameters are missing.</td></tr>
<tr><td>RQ05_1104</td><td>8.2.1.3.2.2.1</td><td>UICC Toolkit Application specific parameters shall be coded as follows:
<table>
<tr><th>Length</th><th>Name</th><th>Value</th></tr>
<tr><td>1</td><td>Priority level of the Toolkit application instance</td><td></td></tr>
<tr><td>1</td><td>Maximum number of timers allowed for this application instance</td><td></td></tr>
<tr><td>1</td><td>Maximum text length for a menu entry</td><td></td></tr>
<tr><td>1</td><td>Maximum number of menu entries allowed for this application instance</td><td>= m</td></tr>
<tr><td>1</td><td>Position of the first menu entry</td><td>\</td></tr>
<tr><td>1</td><td>Identifier of the first menu entry ('00' means do not care)</td><td>|</td></tr>
<tr><td></td><td>….</td><td>| = 2 × m bytes</td></tr>
<tr><td>1</td><td>Position of the last menu entry</td><td>|</td></tr>
<tr><td>1</td><td>Identifier of the last menu entry ('00' means do not care)</td><td>/</td></tr>
<tr><td>1</td><td>Maximum number of channels for this application instance</td><td></td></tr>
<tr><td>1</td><td>Length of Minimum Security Level field</td><td></td></tr>
<tr><td>0-q</td><td>Minimum Security Level (MSL)</td><td></td></tr>
<tr><td>1</td><td>Length of TAR Value(s) field</td><td></td></tr>
<tr><td>3 × y</td><td>TAR Value(s) of the Toolkit Application instance</td><td></td></tr>
<tr><td>1</td><td>Maximum number of services for this application instance</td><td></td></tr>
</table></td></tr>
<tr><td>RQ05_1105</td><td>8.2.1.3.2.2.1</td><td>Any additional parameters shall be ignored by the card.</td></tr>
<tr><td colspan="3">NOTE: RQ05_1101 is for information only.</td></tr>
</table>

<table>
<tr><th>RQ number</th><th>Clause</th><th>Description</th></tr>
<tr><td>RQ05_1201</td><td>8.2.1.3.2.2.2</td><td>The UICC access application specific parameters field is used to specify the access rights. The application instance is granted access rights to files only according to these UICC access parameters.</td></tr>
<tr><td>RQ05_1202</td><td>8.2.1.3.2.2.2</td><td>The UICC access application specific parameters are applicable to applications using the uicc.access.FileView defined in ETSI TS 102 241 [7]. These parameters shall be coded as follows:
<table>
<tr><th>Presence</th><th>Name</th><th>Length</th></tr>
<tr><td rowspan="6">O</td><td>Length of UICC file system AID</td><td>1</td></tr>
<tr><td>Empty UICC file system AID</td><td>0</td></tr>
<tr><td>Length of Access Domain for UICC file system</td><td>1</td></tr>
<tr><td>Access Domain for UICC file system</td><td>n</td></tr>
<tr><td>Length of Access Domain DAP</td><td>1</td></tr>
<tr><td>Access Domain DAP</td><td>0 or n</td></tr>
<tr><td rowspan="6">O</td><td>Length of ADF #1 AID</td><td>1</td></tr>
<tr><td>ADF #1 AID</td><td>5 to 16</td></tr>
<tr><td>Length of Access Domain for ADF #1</td><td>1</td></tr>
<tr><td>Access Domain for ADF #1</td><td>N</td></tr>
<tr><td>Length of Access Domain DAP #1</td><td>1</td></tr>
<tr><td>Access Domain DAP #1</td><td>0 or n</td></tr>
<tr><td>…</td><td>…</td><td>…</td></tr>
<tr><td>…</td><td>…</td><td>…</td></tr>
<tr><td rowspan="6">O</td><td>Length of ADF #n AID</td><td>1</td></tr>
<tr><td>ADF #n AID</td><td>5 to 16</td></tr>
<tr><td>Length of Access Domain for ADF #n</td><td>1</td></tr>
<tr><td>Access Domain for ADF #n</td><td>n</td></tr>
<tr><td>Length of Access Domain DAP #n</td><td>1</td></tr>
<tr><td>Access Domain DAP #n</td><td>0 or n</td></tr>
</table>
</td></tr>
<tr><td colspan="3">NOTE: RQ05_1201 is for information only.</td></tr>
</table>

RQ number	Clause	Description
RQ05_1301	8.2.1.3.2.2.3	The UICC toolkit parameters DAP is an optional signature. The card issuer's security policy may require the presence of this DAP.
RQ05_1302	8.2.1.3.2.2.3	The input data used to compute UICC toolkit parameters DAP is the concatenation of the following data: <table><tr><th>Description</th><th>Length</th></tr><tr><td>Length of instance AID</td><td>1</td></tr><tr><td>Instance AID</td><td>5 to 16</td></tr><tr><td>Length of UICC Toolkit parameters</td><td>1</td></tr><tr><td>UICC Toolkit parameters</td><td>n</td></tr></table> The key used to compute this DAP is: Key identifier '02' of Key Version number '11' in the Issuer Security Domain.
RQ05_1303	8.2.1.3.2.2.3	Depending on the key type for DAP, if padding is required by the algorithm, the data is appended by '80' and filled up with zero or more '00'.
RQ05_1304	8.2.1.3.2.2.3	Depending on the key type for DAP, if DES is used, MAC in CBC mode with initial chaining value set to zero shall be used.
RQ05_1305	8.2.1.3.2.2.3	Depending on the key type for DAP, if AES [13] is used, CMAC mode [15] shall be used. The length of the MAC shall be associated with the key.

RQ number	Clause	Description
RQ05_1401	8.2.1.3.2.2.4	The UICC Administrative access application specific parameters field is used to specify the access rights. The application instance is granted access rights to administrate files only according to these UICC Administrative access parameters.
RQ05_1402	8.2.1.3.2.2.4	The UICC Administrative access application specific parameters are applicable to applications using the uicc.access.fileadministration.AdminFileView defined in ETSI TS 102 241 [7]. These parameters shall be coded as defined in ETSI TS 102 226 [1], clause 8.2.1.3.2.2.2.

RQ number	Clause	Description
RQ05_1501	8.2.1.3.2.3	If the maximum number of timers required for Toolkit Application Specific Parameters is greater than '08' (maximum numbers of timers specified in ETSI TS 102 223 [4]), the card shall return the Status Word '6A80', incorrect parameters in data field, to the INSTALL [for install] command.
RQ05_1502	8.2.1.3.2.3	If the maximum number of channels required for Toolkit Application Specific Parameters is greater than '07' (maximum numbers of channels specified in ETSI TS 102 223 [4]), the card shall return the Status Word '6A80', incorrect parameters in data field, to the INSTALL [for install] command.
RQ05_1503	8.2.1.3.2.3	If the maximum number of services requested for Toolkit Application Specific Parameters is greater than '08' (maximum numbers of services specified in ETSI TS 102 223 [4]), the card shall return the Status Word '6A80', incorrect parameters in data field, to the INSTALL [for install] command.
RQ05_1504	8.2.1.3.2.3	The mechanism to manage the position of the Menu Entries for Toolkit Application Specific Parameters is defined in ETSI TS 102 241 [7].
RQ05_1505	8.2.1.3.2.3	A part of the item identifier for Toolkit Application Specific Parameters shall be under the control of the card system and the other part under the control of the card issuer. Item identifiers are split in two ranges: • [1...127] under control of the card issuer. • [128...255] under the control of the toolkit framework.
RQ05_1506	8.2.1.3.2.3	If the requested item identifier for Toolkit Application Specific Parameters is already allocated, or in the range [128...255], then the card shall reject the INSTALL command.
RQ05_1507	8.2.1.3.2.3	If the requested item identifier for Toolkit Application Specific Parameters is '00', the card shall take the first free value in the range [128...255].
NOTE: RQ05_1505 is for information only.		

RQ number	Clause	Description
RQ05_1601	8.2.1.3.2.4	If the length of the Minimum Security Level (MSL) field for Toolkit Application Specific Parameters is zero, no minimum security level check shall be performed by the Receiving Entity.
RQ05_1602	8.2.1.3.2.4	If the length of the Minimum Security Level (MSL) field for Toolkit Application Specific Parameters is greater than zero, the Minimum Security Level (MSL) field shall be coded according to the following table: **Length** | **Name** 1 | MSL Parameter q to 1 | MSL Data The MSL Data coding and length is defined for each MSL Parameter.

RQ number	Clause	Description
RQ05_1701	8.2.1.3.2.4.1	The possible values for the MSL Parameter for Toolkit Application Specific Parameters are:

Value	Name	Support	MSL Data length
'00'	RFU	RFU	N/A
'01'	Minimum SPI1	Optional	1
'02' to '7F'	RFU	RFU	N/A
'80' to 'FE'	Reserved for Proprietary Mechanisms	Optional	N/A
'FF'	RFU	RFU	N/A

RQ number	Clause	Description
RQ05_1801	8.2.1.3.2.4.2	The Minimum Security Level Data (MSLD) for the Minimum SPI1 MSL parameter for Toolkit Application Specific Parameters shall use the same coding as the first octet of the SPI of a command packet (see clause 5.1.1 of ETSI TS 102 225 [2]).
RQ05_1802	8.2.1.3.2.4.2	The first octet of the SPI field of MSL parameter in the incoming message Command Packet (SPI1) shall be checked against the Minimum Security Level Data (MSLD) byte by the receiving entity according to the following rules: • if SPI1.b2b1 is equal to or greater than MSLD.b2b1; • if SPI1.b3 is equal to or greater than MSLD.b3; and • if SPI1.b5b4 is equal to or greater than MSLD.b5b4. then the Message Security Level is sufficient and the check is successful, otherwise the check is failed.

RQ number	Clause	Description
RQ05_1901	8.2.1.3.2.5	The Access Domain field for Toolkit Application Specific Parameters is formatted as follows: **Length** / **Name** 1 / Access Domain Parameter (ADP) p to 1 / Access Domain Data (ADD) The Access Domain Data (ADD) coding and length is defined for each Access Domain Parameter (ADP).

RQ number	Clause	Description
RQ05_2001	8.2.1.3.2.5.1	The Access Domain Parameter indicates the mechanism used to control the application instance access to the File System :

Value	Name	Support	ADD length
'00'	Full access to the File System	Mandatory	0
'01'	Reserved (for APDU access mechanism)	-	-
'02'	UICC access mechanism	Mandatory	3
'03' to '7F'	RFU	RFU	RFU
'80' to 'FE'	Proprietary mechanism	-	-
'FF'	No access to the File System	Mandatory	0

RQ05_2002	8.2.1.3.2.5.1	The access rights granted to an application and defined in the access domain parameter shall be independent from the access rights granted at the UICC/Terminal interface.
RQ05_2003	8.2.1.3.2.5.1	The access rights granted to an application implies in particular that the status of a secret code (e.g. disabled PIN1, blocked PIN2, etc.) at the UICC/Terminal interface does not affect the access rights granted to an application.
RQ05_2004	8.2.1.3.2.5.1	If an application with Access Domain Parameter (ADP) 'FF' (i.e. No Access to the File System) tries to access a file the framework shall throw an exception.
RQ05_2005	8.2.1.3.2.5.1	If an application has Access Domain Parameter (ADP) '00' (i.e. Full Access to the File System), all actions can be performed on a file except the ones with NEVER access condition.
RQ05_2006	8.2.1.3.2.5.1	If the Access Domain Parameter (ADP) requested is not supported, the card shall return the Status Word '6A80', incorrect parameters in data field, to the INSTALL [for install] command.

RQ number	Clause	Description
RQ05_2101	8.2.1.3.2.5.2	The UICC access mechanism shall be coded as specified in clause 8.2.1.3.2.5.2 in ETSI TS 102 226 [1].
RQ05_2102	8.2.1.3.2.5.2	The Access Domain Data for UICC access mechanism shall be checked against SE ID 01 access rules as defined in ETSI TS 102 221 [3].

<table>
<tr><th>RQ number</th><th>Clause</th><th>Description</th></tr>
<tr><td>RQ05_2201</td><td>8.2.1.3.2.5.3</td><td>The Access Domain DAP is an optional signature. The security policy of the provider of the application to which the file system belongs may require the presence of this DAP.</td></tr>
<tr><td>RQ05_2202</td><td>8.2.1.3.2.5.3</td><td>The input data used to compute the Access Domain DAP is the concatenation of the following data:
<table>
<tr><th>Description</th><th>Length</th></tr>
<tr><td>Length of instance AID</td><td>1</td></tr>
<tr><td>Instance AID</td><td>5 to 16</td></tr>
<tr><td>Length of File System AID</td><td>1</td></tr>
<tr><td>File System AID</td><td>0 or n</td></tr>
<tr><td>Length of Access Domain</td><td>1</td></tr>
<tr><td>Access Domain</td><td>n</td></tr>
</table></td></tr>
<tr><td>RQ05_2203</td><td>8.2.1.3.2.5.3</td><td>In case of UICC shared File system, the Length of File System AID is 0 and the File System AID is not present in the Access Domain DAP.</td></tr>
<tr><td>RQ05_2204</td><td>8.2.1.3.2.5.3</td><td>The key used to compute the Access Domain DAP is: Key identifier '02' of Key Version number '11' in the Security Domain associated to the application to which the File System belongs. In case of UICC shared file system, the associated Security Domain may be the Issuer Security Domain or another Security Domain, depending on the card issuer's security policy.</td></tr>
<tr><td>RQ05_2205</td><td>8.2.1.3.2.5.3</td><td>Depending on the key type for the Access Domain DAP, if padding is required by the algorithm, the data is appended by '80' and filled up with zero or more '00'.</td></tr>
<tr><td>RQ05_2206</td><td>8.2.1.3.2.5.3</td><td>Depending on the key type for the Access Domain DAP, if DES is used, MAC in CBC mode with initial value set to zero shall be used.</td></tr>
<tr><td>RQ05_2207</td><td>8.2.1.3.2.5.3</td><td>Depending on the key type for the Access Domain DAP, if AES [13] is used, CMAC mode [15] shall be used. The length of the MAC shall be associated with the key.</td></tr>
</table>

RQ number	Clause	Description
RQ05_2301	8.2.1.3.2.6	The Priority level of the toolkit application specifies the order of activation of an application compared to the other application registered to, the same event.
RQ05_2302	8.2.1.3.2.6	If two or more applications are registered to the same event and have the same priority level, the applications are activated according to their installation date (i.e. the most recent application is activated first).
RQ05_2303	8.2.1.3.2.6	The following values are defined for priority level of the toolkit application: • '00': RFU. • '01': Highest priority level. • ... • 'FF': Lowest priority level.

<table>
<tr><th>RQ number</th><th>Clause</th><th>Description</th></tr>
<tr><td>RQ05_2401</td><td>8.2.1.3.2.7</td><td>The TAR is defined and coded according to ETSI TS 101 220 [6].</td></tr>
<tr><td>RQ05_2402</td><td>8.2.1.3.2.7</td><td>It is possible to define several TAR Values at the installation of a Toolkit Application.</td></tr>
<tr><td>RQ05_2403</td><td>8.2.1.3.2.7</td><td>The TAR Value(s) field shall be coded according to the following table:
<table>
<tr><th>Bytes</th><th>Description</th><th>Length</th></tr>
<tr><td>1 to 3</td><td>TAR Value 1</td><td>3</td></tr>
<tr><td>4 to 6</td><td>TAR Value 2</td><td>3</td></tr>
<tr><td>…</td><td>…</td><td>…</td></tr>
<tr><td>3 × y-2 to 3 × y</td><td>TAR Value y</td><td>3</td></tr>
</table></td></tr>
<tr><td>RQ05_2404</td><td>8.2.1.3.2.7</td><td>If the length of TAR Value(s) is zero, the TAR may be taken out of the AID if any.</td></tr>
<tr><td>RQ05_2405</td><td>8.2.1.3.2.7</td><td>If the length of the TAR Value(s) is greater than zero then the application instance shall be installed with the TAR Value(s) field defined above and the TAR indicated in the AID if any shall be ignored.</td></tr>
<tr><td>RQ05_2406</td><td>8.2.1.3.2.7</td><td>If a TAR Value(s) is already assigned on the card for a Toolkit Application instance or if the length of TAR Value(s) field is incorrect, the card shall return the Status Word '6A80', incorrect parameters in data field, to the INSTALL [for install] command.</td></tr>
</table>

<table>
<tr><th>RQ number</th><th>Clause</th><th>Description</th></tr>
<tr><td>RQ05_2501</td><td>8.2.1.3.2.8</td><td>An application intended to operate in contactless card emulation mode as defined in ETSI TS 102 622 [23] shall be installed as specified in GlobalPlatform Amendment C [22].</td></tr>
<tr><td>RQ05_2502</td><td>8.2.1.3.2.8</td><td>An application intended to operate in contactless reader mode as defined in ETSI TS 102 622 [23] shall be installed with parameters given below in clauses 8.2.1.3.2.8.1 and 8.2.1.3.2.8.2.</td></tr>
<tr><td>RQ05_2503</td><td>8.2.1.3.2.8</td><td>If present, the "Additional Contactless Parameters" TLV object (tag 'B0') shall be included in the "System Specific Parameters" (tag 'EF').</td></tr>
<tr><td>RQ05_2504</td><td>8.2.1.3.2.8</td><td>The value part of "Additional Contactless Parameters" shall be coded as follows:
<table>
<tr><th>Tag</th><th>Length</th><th>Value</th><th>Presence</th></tr>
<tr><td>'86'</td><td>1</td><td>Reader mode protocol data Type A</td><td>Optional</td></tr>
<tr><td>'87'</td><td>N+2</td><td>Reader mode protocol data Type B</td><td>Optional</td></tr>
</table></td></tr>
<tr><td>RQ05_2505</td><td>8.2.1.3.2.8</td><td>The presence of the TLVs "Reader mode protocol data Type" indicates the RF technology/technologies that will be active once the Application Availability State of the application as defined in GlobalPlatform Amendment C [22] changes to ACTIVATED.</td></tr>
<tr><td>RQ05_2506</td><td>8.2.1.3.2.8</td><td>To present a reader mode application to the user, user interaction parameters as specified in GlobalPlatform Amendment C [22] shall be included in the installation parameters. Applicable parameters for reader mode applications are Application Visibility and Application Family.</td></tr>
<tr><td colspan="3">NOTE: RQ05_2505 is for information only.</td></tr>
</table>

<table>
<tr><th>RQ number</th><th>Clause</th><th>Description</th></tr>
<tr><td>RQ05_2601</td><td>8.2.1.3.2.8.1</td><td>The value part of the Reader mode protocol data Type A has the following coding:
<table>
<tr><th>Parameter</th><th>Value</th><th>Length</th></tr>
<tr><td>DATARATE_MAX</td><td>Maximum data rate supported as defined in ETSI TS 102 622 [23]</td><td>1</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>RQ number</th><th>Clause</th><th>Description</th></tr>
<tr><td>RQ05_2701</td><td>8.2.1.3.2.8.2</td><td>The value part of the Reader mode protocol data Type B has the following coding:
<table>
<tr><th>Parameter</th><th>Value</th><th>Length</th></tr>
<tr><td>AFI</td><td>Application family identifier as defined in ETSI TS 102 622 [23]</td><td>1</td></tr>
<tr><td>HIGHER_LAYER_DATA_LENGTH</td><td>Length of HIGHER_LAYER_DATA</td><td>1</td></tr>
<tr><td>HIGHER_LAYER_DATA</td><td>Higher layer data as defined in ETSI TS 102 622 [23]</td><td>N</td></tr>
</table></td></tr>
</table>

RQ number	Clause	Description
RQ05_2801	8.2.1.4	A card supporting DAP verification shall support at least DES scheme for Load File Data Block Signature computation according to GlobalPlatform Card Specification [5].
RQ05_2802	8.2.1.4	When using the Compact Remote Application data format, the context established by INSTALL [for load] shall be saved across command sessions for the whole sequence until the last LOAD command.

RQ number	Clause	Description
RQ05_2901	8.2.1.5	Key version number and key identifiers of KIc, KID and DEK shall be defined according to ETSI TS 102 225 [2]. The key used for ciphering the key values (e.g. KIc, KID or DEK) of the PUT KEY command is the key with identifier 3 (i.e. DEK). It is a static key.
RQ05_2902	8.2.1.5	If a DES key is used to cipher a key value of the PUT KEY command, the ciphering mode shall be ECB as defined in NIST SP 800-38A [7].
RQ05_2903	8.2.1.5	When replacing or adding key(s) within the same key set, or when updating the key version number of a key set, the encrypting key to be used is the DEK of the same key version number as the changed key(s).

RQ number	Clause	Description
RQ05_2904	8.2.1.5	When creating keys or key set(s) or when replacing keys that do not belong to a keyset, the encrypting key to be used is the DEK of the same key version number as KIc and KID in the Command Packet containing the PUT KEY command.
RQ05_2905	8.2.1.5	The key version number of KIc and KID used to secure the Response Packet shall be the same as the key version number indicated in the Command Packet.
RQ05_2906	8.2.1.5	The transport security keys (i.e. KIc/KID) used to secure the Response Packet shall be the same as the ones of the Command Packet containing the PUT KEY command.

RQ number	Clause	Description
RQ05_3101	8.2.1.5.1	If the command PUT KEY as defined in [5] is used with an AES key as encryption key (DEK), the remote entity shall cipher key values of AES keys only with an AES key of the same or greater length, where AES is the algorithm defined in [13].
RQ05_3102	8.2.1.5.1	If the command PUT KEY as defined in [5] is used with an AES key as encryption key (DEK), the coding of the key type for AES keys shall be '88'.
RQ05_3103	8.2.1.5.1	If the command PUT KEY as defined in [5] is used with an AES key as encryption key (DEK), the definitions of the command PUT KEY as defined in [5] shall be extended as in RQ05_3103 to RQ05_3109.
RQ05_3104	8.2.1.5.1	The field "length of the key or key component data" defined in [5] shall be set to the length of the "key data value" defined in RQ05_3105 - RQ053107.
RQ05_3105	8.2.1.5.1	The "key data value" defined in [5] shall be constructed as follows: **Description** / **Length** / **Value** / **Presence** Length of the key in bytes / 1 / 16, 24 or 32 for AES 16 or 24 for triple DES / Mandatory Ciphered key / 16 or 32 / / Mandatory Length of the MAC in bytes / 1 / 4 or 8 / Conditional
RQ05_3106	8.2.1.5.1	The field "length of the key in bytes" shall be set to the length of the key contained in the field "ciphered key" (without padding).
RQ05_3107	8.2.1.5.1	The field "length of the MAC" shall be present if "ciphered key" contains an AES key with key identifier '02' and key version '01' to '0F' or '11' (see clause "Coding of the KID for Cryptographic Checksum" in ETSI TS 102 225 [2]).
RQ05_3108	8.2.1.5.1	Key ciphering in case of PUT KEY for AES shall use CBC mode as defined in [14] with initial chaining value set to zero.
RQ05_3109	8.2.1.5.1	Keys that do not fill whole blocks of the AES ciphering scheme (e.g. AES with a key length of 192 bits or triple DES using three different keys) shall be padded to the next block boundary. Padding octets may have any value.

RQ number	Clause	Description
RQ05_3201	8.2.1.6	In addition to the mandatory values of the P1 parameter defined in GlobalPlatform Card Specification [5], combinations of the P1 parameter, i.e. setting more than one bit of b5 to b8, may be supported for command GET STATUS.
RQ05_3202	8.2.1.6	The LOGICALLY_DELETED Life Cycle State may be returned as defined in Open Platform Card Specification 2.0.1 [8].
RQ05_3203	8.2.1.6	If bit 2 of the P2 parameter in GET STATUS is set, the returned GlobalPlatform Registry Data TLV shall include an SCP Registry Data TLV (see table below for coding) which includes a Menu Parameters TLV for Issuer Security Domain, Security Domains and Applications: **TAG** / **Length** / **Value** 'EA' / Variable / SCP Registry Data '80' / Variable / Menu parameters (see clause 8.2.1.6.1)
RQ05_3204	8.2.1.6	When using the Compact Remote Application data format, the context established by GET STATUS [get first or all occurrence(s)] shall be saved across command sessions as long as more output data related to the initial GET STATUS command is available on the UICC.

<table>
<tr><th>RQ number</th><th>Clause</th><th>Description</th></tr>
<tr><td>RQ05_3301</td><td>8.2.1.6.1</td><td>The format of Menu parameters of SCP Registry Data shall be as follow:
<table>
<tr><th>Description</th><th>Length</th></tr>
<tr><td>First menu entry position</td><td>1</td></tr>
<tr><td>First menu entry identifier</td><td>1</td></tr>
<tr><td>First menu entry state</td><td>1</td></tr>
<tr><td>…</td><td>…</td></tr>
<tr><td>Last menu entry position</td><td>1</td></tr>
<tr><td>Last menu entry identifier</td><td>1</td></tr>
<tr><td>Last menu entry state</td><td>1</td></tr>
</table></td></tr>
<tr><td>RQ05_3302</td><td>8.2.1.6.1</td><td>The menu entry identifiers and positions of SCP Registry Data shall be the ones provided in the Menu Entries list defined in ETSI TS 102 241 [7], and shall be returned regardless of the menu entry state as well as regardless of the Application life cycle state (e.g. Selectable/Locked, etc.).</td></tr>
<tr><td>RQ05_3303</td><td>8.2.1.6.1</td><td>The menu entry state of SCP Registry Data is defined as follows:
• '00': menu entry is disabled.
• '01': menu entry is enabled.
• other values: RFU.</td></tr>
</table>

RQ number	Clause	Description
RQ05_3401	8.2.1.7	For command GET DATA, the value '80' for the CLA byte shall be supported. The value '00' for the CLA byte is optional.
RQ05_3402	8.2.1.7	The Issuer Security Domain shall support at least the following data object tags in GET DATA: • Tag '66': Card Data. • Tag 'E0': Key Information Template.
RQ05_3403	8.2.1.7	If a UICC contains an Application Provider Security Domain with Delegated Management privilege, the tag values '42' and '45' shall be supported by the ISD as specified in the UICC Configuration for GET DATA [16].
RQ05_3404	8.2.1.7	An Application Provider Security Domain shall support at least the data object tags: Tag 'E0': Key Information Template in GET DATA.
RQ05_3405	8.2.1.7	The command Get Data is extended to retrieve specific card information with tag values in P1 and P2. The following values have been defined: • 'FF 1F': Reserved for ETSI TS 123 048 [10]. • 'FF 20': Reserved for ETSI TS 123 048 [10]. • 'FF 21': Extended Card Resources Tag, this retrieves information on the card resources used and available. • 'FF 22' to 'FF 3F': reserved for allocation in the present document.

<table>
<tr><th>RQ number</th><th>Clause</th><th>Description</th></tr>
<tr><td>RQ05_3501</td><td>8.2.1.7.2</td><td>The Extended Card resources information data object shall be supported by the ISD.</td></tr>
<tr><td>RQ05_3502</td><td>8.2.1.7.2</td><td>After the successful execution of the command, the GET DATA response data field shall be coded as defined in GlobalPlatform [5].</td></tr>
<tr><td>RQ05_3503</td><td>8.2.1.7.2</td><td>The value of the TLV coded data object referred to in reference control parameters P1 and P2 of the GET DATA command message is:
<table>
<tr><th>Length</th><th>Description</th><th>Value</th></tr>
<tr><td>1</td><td>Number of installed application tag</td><td>'81'</td></tr>
<tr><td>1</td><td>Number of installed application length</td><td>X</td></tr>
<tr><td>X</td><td>Number of installed application</td><td></td></tr>
<tr><td>1</td><td>Free non volatile memory tag</td><td>'82'</td></tr>
<tr><td>1</td><td>Free non volatile memory length</td><td>Y</td></tr>
<tr><td>Y</td><td>Free non volatile memory</td><td></td></tr>
<tr><td>1</td><td>Free volatile memory tag</td><td>'83'</td></tr>
<tr><td>1</td><td>Free volatile memory length</td><td>Z</td></tr>
<tr><td>Z</td><td>Free volatile memory</td><td></td></tr>
</table></td></tr>
<tr><td>RQ05_3504</td><td>8.2.1.7.2</td><td>The free memory indicated in GET DATA shall be at least available for applications to be loaded into the ISD.</td></tr>
</table>

<table>
<tr><th>RQ number</th><th>Clause</th><th>Description</th></tr>
<tr><td>RQ05_3601</td><td>8.2.1.8</td><td>A UICC supporting confidential application management as specified in clause 10 shall support the STORE DATA command as specified in the UICC Configuration [16].</td></tr>
<tr><td>RQ05_3602</td><td>8.2.1.8</td><td>Support of the STORE DATA command described in GlobalPlatform Card Specification [5] is optional, but if the Third Party Security Policy requires management of Executable Load Files access constraints, it shall be supported as specified in the following REQ_xx - REQ_YY.</td></tr>
<tr><td>RQ05_3603</td><td>8.2.1.8</td><td>When using the Compact Remote Application data format, the context established by INSTALL [for personalization] (if supported) shall be saved across command sessions until the STORE DATA command containing the last block.</td></tr>
<tr><td>RQ05_3604</td><td>8.2.1.8</td><td>The STORE DATA Command is sent to a Security Domain to specify access rights restrictions to its Executable Load Files for a specified Third Party Security Domain.</td></tr>
<tr><td>RQ05_3605</td><td>8.2.1.8</td><td>If the Forbidden Executable Load File List is present in the STORE DATA command, each Executable Load File specified in the list shall be considered as Forbidden for the indicated Third Party Security Domain. Any other Executable Load File not present in the list is allowed for the specified Third Party Security Domain.</td></tr>
<tr><td>RQ05_3606</td><td>8.2.1.8</td><td>Any subsequent loading of Load Files performed by the Third Party Security Domain shall fail if the Load File references one or more Forbidden Executable Load Files. Access rights of Executable Load Files already present on card are not affected by the command.</td></tr>
<tr><td>RQ05_3607</td><td>8.2.1.8</td><td>If a STORE DATA Command is resent to a Security Domain, specifying a Third Party Security Domain for which a Forbidden Executable Load File List has already been defined, the new Forbidden Executable Load File List replaces the previous list for this Third Party Security Domain. If the new Forbidden Executable Load File List is empty the access restrictions for this Third Party Security Domain are removed from the addressed Security Domain.</td></tr>
<tr><td>RQ05_3608</td><td>8.2.1.8</td><td>The UICC shall prevent an Executable Load File from being set as Forbidden for its associated Security Domain.</td></tr>
<tr><td>RQ05_3609</td><td>8.2.1.8</td><td>The STORE DATA command to load Forbidden Load File List shall support the chaining of multiple STORE DATA commands to transfer large amounts of data. Parameter P1 of the command shall indicate non encrypted data and BER-TLV format of the command data field.</td></tr>
<tr><td>RQ05_3610</td><td>8.2.1.8</td><td>TAG 'BE' is used to specify a Forbidden Load File List in STORE DATA; the Third Party Security Domain AID TLV object and the Forbidden Load Files AID TLV objects are included in the Store Data Command Message to define the list of Forbidden Load Files for the Third Party Security Domain.
<table>
<tr><th>Presence</th><th>Length</th><th>Name</th><th>Value</th></tr>
<tr><td>Mandatory</td><td>1</td><td>Tag of Forbidden Executable Load Files AIDs constructed field</td><td>'BE'</td></tr>
<tr><td>Mandatory</td><td>1 or 2</td><td>Length of Forbidden Executable Load Files AIDs constructed field</td><td></td></tr>
<tr><td>Mandatory</td><td></td><td>Third Party Security Domain AID TLV</td><td></td></tr>
<tr><td>Optional</td><td></td><td>Forbidden Executable Load File #1 AID TLV</td><td></td></tr>
<tr><td>Optional</td><td></td><td>Forbidden Executable Load File #2 AID TLV</td><td></td></tr>
<tr><td></td><td>…</td><td>…</td><td></td></tr>
<tr><td>Optional</td><td></td><td>Forbidden Load File #N AID TLV</td><td></td></tr>
</table></td></tr>
<tr><td>RQ05_3611</td><td>8.2.1.8</td><td>The Third Party Security Domain AID TLV and the Forbidden Load File AID TLVs are coded as BER-TLV as defined in ETSI TS 101 220 [6] using tag '4F'.</td></tr>
</table>

RQ number	Clause	Description
RQ05_3701	8.3	When using remote APDUs to perform RAM over HTTPS, the header values defined in Amendment B of the Global Platform Card Specification v 2.2 [19] apply.

5.6 Additional command for push

Reference: ETSI TS 102 226 [1], clause 9.

RQ number	Clause	Description
RQ06_0101	9	The PUSH command enables an application to open a BIP channel, to establish a CAT_TP link, to open a TCP connection and/or to send an identification packet on TCP upon a remote entity request.
NOTE: RQ06_0101 is a definition.		

RQ number	Clause	Description
RQ06_0201	9.1.1	The PUSH command shall be considered completed once the terminal response to the OPEN CHANNEL proactive command has been received by the application.
RQ06_0301	9.1.2	The PUSH command shall be considered completed once the link reaches the OPEN state in CAT_TP or the link establishment is terminated due to an error condition.

RQ number	Clause	Description
RQ06_0401	9.1.3	It is mandatory for applications that process PUSH commands to support additional response data management. The additional response data shall be coded as defined in clause 9.2 in ETSI TS 102 226 [1].

RQ number	Clause	Description
RQ06_0501	9.1.4	The request for a TCP connection allows a remote entity to ask an application on the UICC to establish a TCP connection as defined in ETSI TS 102 483 [20].
NOTE: RQ06_0501 is a definition.		

RQ number	Clause	Description
RQ06_0601	9.1.5	The request for an identification packet allows a remote entity to ask an application on the UICC to send a data packet containing identification information on a TCP connection.

RQ number	Clause	Description
RQ06_0701	9.2	Each command is coded as an APDU. The support of PUSH command shall be supported in addition to the command tables defined in clauses 7 and 8 of ETSI TS 102 226 [1] for applications supporting BIP and/or CAT_TP.
RQ06_0702	9.2	The PUSH command shall be coded as follows:

Code	Value
CLA	'80'
INS	'EC'
P1	'01' '80' reserved for application specific usage
P2	'01': Request for BIP channel opening '02': Request for CAT_TP link establishment '03': Request for TCP connection '04': Request for Identification Packet (see note)
Lc	Length of subsequent data field
Data	Described below
NOTE: These values only apply for P1 = '01'.	

RQ number	Clause	Description
RQ06_0801	9.2.1	For Command data BIP channel opening; any COMPREHENSION-TLV data objects as defined for OPEN CHANNEL in ETSI TS 102 223 [4] can be present in the data field of the PUSH command. In addition, the application may define default values for one or more of these data objects.
RQ06_0802	9.2.1	The application shall use the data objects provided by both means to construct the OPEN CHANNEL command, whereby the objects provided in the PUSH command take precedence.
RQ06_0803	9.2.1	For OPEN CHANNEL, related to packet data service bearer, in ETSI TS 102 223 [4] the "Other address (local address)" parameter shall not be included in the command.
RQ06_0804	9.2.1	For OPEN CHANNEL, related to packet data service bearer, in ETSI TS 102 223 [4] the "Login" parameter and "Password" parameter shall be both present or absent in the command.
RQ06_0805	9.2.1	If the rules in RQ06_0803 and RQ06_0804 are not satisfied the Push requesting BIP open channel is rejected with status word set to '6A 80'.
RQ06_0806	9.2.1	If the OPEN CHANNEL command was successful (general result < '10'), the status word of the PUSH command shall be set to '90 00'.

RQ number	Clause	Description
RQ06_0807	9.2.1	If the OPEN CHANNEL command fails (general result ≥ '10'), the status word of the PUSH command shall be set to '6F 00' and the Result TLV of the TERMINAL RESPONSE shall be used as response data in the additional response data.

RQ number	Clause	Description
RQ06_0901	9.2.2	Data of Commands for CAT_TP link establishment shall have the following format: **Description** / **Format from ETSI TS 102 223 [4]** / **M/O/C** CAT_TP Destination Port / UICC/terminal interface transport level / M Max SDU size / Buffer size / O Identification data / Channel data / O
RQ06_0902	9.2.2	For CAT_TP Destination Port the transport protocol type is insignificant and shall be set to zero. For the PUSH command, an allocable port number shall be used.
RQ06_0903	9.2.2	If the Max SDU size data object is present in the command data field of the PUSH command and is non null data object, and if the size is available on the UICC, then the UICC shall use the requested size.
RQ06_0904	9.2.2	If the Max SDU size data object is not present in the command data field of the PUSH command or is null data object, or if the UICC is not able to provide the requested size, then the UICC shall use another appropriate value.
RQ06_0905	9.2.2	The identification data object present in the command data field of the PUSH command shall be used as identification data in the SYN PDU sent from the UICC.
RQ06_0906	9.2.2	If the identification data object present in the command data field of the PUSH command is of zero length, the length of the identification data in the SYN PDU shall also be zero.
RQ06_0907	9.2.2	If identification data is not present in the command data field of the PUSH command, the ICCID shall be used as identification data in the SYN PDU.
RQ06_0908	9.2.2	The SYN/ACK PDU sent from the remote entity shall have a null identification data field.
RQ06_0909	9.2.2	If the link reaches the OPEN state in CAT_TP, the status word of the PUSH command shall be set to '90 00'.
RQ06_0910	9.2.2	If the CAT_TP OPEN state is not reached, the PUSH command shall be considered as failed and the status word of the PUSH command shall be set to '6F 00'.
RQ06_0911	9.2.2	The response data in the additional response data for CAT_TP link establishment shall be coded as follows: • '01': SYN sent failed. • '02': SYN/ACK not received. • '03': ACK sent failed (first ACK).

RQ number	Clause	Description
RQ06_1001	9.2.3	By TCP connection opening the PUSH command shall be sent to the Multiplexing application identified by its TAR as defined in ETSI TS 101 220 [6].
RQ06_1002	9.2.3	The data field of the PUSH command shall consist of the following COMPREHENSION-TLV data objects: **Data Object from ETSI TS 102 223 [4]** / **M/O/C** / **Comment** Bearer description / M / UICC/terminal interface transport level / M / Transport protocol type shall be set to "TCP, UICC in client mode, remote connection" Data destination address / M / Network Access Name / O / Text String (User login) / O / Text String (User password) / C / "Text String (User login)" and "Text String (User password)" shall both be present or both be absent
RQ06_1003	9.2.3	In case of errors in the command data, the PUSH command shall be rejected with status word set to '6A 80'.
RQ06_1004	9.2.3	If the TCP connection opening was successful, the status word of the PUSH command shall be set to '90 00'.

RQ number	Clause	Description
RQ06_1005	9.2.3	If the TCP connection opening failed, the status word of the PUSH command shall be set to '6F 00'.

RQ number	Clause	Description
RQ06_1101	9.2.4	Sending of Identification Packet, the data field of the PUSH command may consist of the following COMPREHENSION-TLV data objects: **Description** / **Format from ETSI TS 102 223 [4]** / **M/O/C** Identification data / Channel data / O
RQ06_1102	9.2.4	The identification data object present in the command data field of the PUSH command shall be used as identification data in the identification packet sent from the UICC.
RQ06_1103	9.2.4	If the identification data object present in the command data field of the PUSH command is of zero length, the length of the identification data in the identification packet shall also be zero.
RQ06_1104	9.2.4	If identification data is not present in the command data field of the PUSH command, the ICCID shall be used as identification data string in the identification packet.
RQ06_1105	9.2.4	If the identification packet was sent successfully, the status word of the PUSH command shall be set to '90 00'.
RQ06_1106	9.2.4	If sending of the identification packet failed, the status word of the PUSH command shall be set to '6F 00'.

RQ number	Clause	Description
RQ06_1201	9.3	The BIP channel shall be closed using the CLOSE CHANNEL proactive command specified in ETSI TS 102 223 [4] once the only or last link using the channel has been closed.

5.7 Confidential application management

Reference: ETSI TS 102 226 [1], clause 10.

RQ number	Clause	Description
RQ07_0201	10.1	If confidential loading of applications is supported, it shall be implemented as specified in the UICC Configuration [16] for the LOAD command using tag 'D4' for encrypted load files, for the key used for deciphering the load file, and for the Ciphered Load File Data Block privilege.

RQ number	Clause	Description
RQ07_0301	10.2	If an application provider wants to communicate confidentially with his security domain or an application in this security domain, and his security domain has no OTA capability, encapsulation of secured APDUs in secured packets shall be implemented as specified in RQ07_0302 to RQ07_0308.
RQ07_0302	10.2	The command string shall use the Expanded Remote Application data format.
RQ07_0303	10.2	The command string shall be secured using SCP02 with implementation option "i" = '55' according to GlobalPlatform Card Specification [5], i.e. the APDUs to be protected shall be included in a GlobalPlatform secure channel session starting with INITIALIZE UPDATE and EXTERNAL AUTHENTICATE, using the GlobalPlatform secure channel keys of a security domain that has no OTA capabilities.
RQ07_0304	10.2	If a script does not contain chaining information, the SCP02 secure channel session shall be terminated at the end of the command string.
RQ07_0305	10.2	If a script contains the chaining information "first script" or "subsequent script(s) will follow", the SCP02 secure channel session shall continue with the next script until the last script, unless one of the following conditions, which shall terminate the secure channel session, applies: • a new first script or a script without chaining information is received but no last script of the previous secure channel session has been received; • card reset.

RQ number	Clause	Description
RQ07_0306	10.2	The TAR of the command string shall represent the security domain that processes the SCP02 security or an application associated to this security domain. In the latter case, the GlobalPlatform API for the secure channel services, which is specified in Java Card API and Export File for Card Specification v2.2.1 (org.globalplatform) or Java Card, shall be available for the application.
RQ07_0307	10.2	The security domain that processes the SCP02 security shall be part of a hierarchy of security domains, where at least one ancestor has OTA capabilities.
RQ07_0308	10.2	The command string shall be contained in a secure packet that is unwrapped by the closest ascendant security domain with OTA capabilities as specified in UICC Configuration [16].
RQ07_0309	10.2	The support of the API related to Card Specification Version 2.2, Amendment A [18] is optional.
NOTE: Development of test cases for RQ07_0309 is out of scope for the present document.		

RQ number	Clause	Description
RQ07_0401	10.3	If confidential setup of security domains is supported, it shall be implemented as: Scenario #2.B (Push Model) as specified in the UICC Configuration [16] shall be supported.
RQ07_0402	10.3	If confidential setup of security domains is supported, it shall be implemented as: Scenario #1 (Pull Model) using the public key scheme as specified in the UICC Configuration [16] may be supported.
RQ07_0403	10.3	If confidential setup of security domains is supported, it shall be implemented as: Scenario #3 using ECKA-EG as specified in scenario #3 in Amendment E [24] may be supported.

RQ number	Clause	Description
RQ07_0501	10.4	The mechanism specified in the UICC Configuration [16] to personalize their associated applications, using INSTALL [for personalization] and STORE DATA, shall be supported by all security domains.

6 Test Cases

6.1 Overview of remote management

Test cases verifying the requirements from this clause are defined under clauses 6.2.1, 6.4.1 and 6.5.3 of the present document.

6.2 Remote APDU format

6.2.1 Compact Remote Application data format

Test cases verifying the requirements from this clause are defined under clause 6.4.1 of the present document.

6.2.2 Expanded Remote Application data format

6.2.2.1 Test case 1: A command session with C-APDU TLV Structure with definite length coding

6.2.2.1.1 Initial Conditions

- None.

6.2.2.1.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data coded as: [Expanded Remote command structure] to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} TLV Structure: C-APDU TLV Definite length coding	Secured Response Data is returned: 'AB 07 80 01 01 23 02 90 00'	RQ01_0001, RQ01_0002, RQ01_0003, RQ01_0005, RQ02_0301 RQ02_0302 RQ02_0303, RQ02_0401, RQ02_0801, RQ02_0801a, RQ02_0803, RQ02_0805, RQ02_0806, RQ02_0807, RQ04_0101, RQ04_0102
2	Send Command with Secured Data coded as: [Expanded Remote command structure] to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TARU} - READ BINARY coded with Le='00' TLV Structure: C-APDU TLV Definite length coding	Secured Response Data is returned: 'AB 7F 80 01 03 23 LEN [Data 90 00]' where the Data should be the content of EF_{TARU}	RQ01_0001, RQ01_0002, RQ01_0003, RQ01_0005 RQ02_0301, RQ02_0302, RQ02_0303, RQ02_0401, RQ02_0402, RQ02_0801, RQ02_0801a, RQ02_0803, RQ02_0805, RQ02_0806, RQ02_0807, RQ04_0101, RQ04_0102
3	Send Command with Secured Data coded as: [Expanded Remote command structure] to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TARU} - UPDATE BINARY (empty Le field) TLV Structure: C-APDU TLV Definite length coding	Secured Response Data is returned: 'AB 07 80 01 03 23 02 90 00'	RQ01_0001, RQ01_0002, RQ01_0003, RQ01_0005 RQ02_0301, RQ02_0302, RQ02_0303, RQ02_0401, RQ02_0405, RQ02_0801, RQ02_0801a, RQ02_0803, RQ02_0805, RQ02_0806, RQ02_0807, RQ04_0101, RQ04_0102

6.2.2.2 Test case 2: A command session containing multiple commands with C-APDU TLV Structure with definite length coding - Bad Format

6.2.2.2.1 Initial Conditions

- None.

6.2.2.2.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data coded as: [Expanded Remote command structure] to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TARU} - READ BINARY with wrong C-APDU Tag coded as: '23 05 00 B0 00 00 00' TLV Structure: C-APDU TLV Definite length coding	Secured Response Data is returned: 'AB 06 80 01 03 90 01 01'	RQ01_0001, RQ01_0002, RQ01_0003, RQ01_0005, RQ02_0301, RQ02_0302, RQ02_0303, RQ02_0401, RQ02_0801, RQ02_0801a, RQ02_0803, RQ02_0805, RQ02_0806, RQ02_0807, RQ02_0809, RQ02_0810, RQ02_0811, RQ02_0812 RQ04_0101, RQ04_0102
2	Send Command with Secured Data coded as: [Expanded Remote command structure] to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TARU} - READ BINARY with wrong C-APDU length coded as:'22 0F 00 B0 00 00 00' TLV Structure: C-APDU TLV Definite length coding	Secured Response Data is returned: 'AB 06 80 01 03 90 01 02'	RQ01_0001, RQ01_0002, RQ01_0003, RQ01_0005, RQ02_0301, RQ02_0302, RQ02_0303, RQ02_0401, RQ02_0801, RQ02_0801a, RQ02_0803, RQ02_0805, RQ02_0806, RQ02_0807, RQ02_0809, RQ02_0810, RQ02_0811, RQ02_0812 RQ04_0101, RQ04_0102

Step	Description	Expected Result	RQ
3	Send Command with Secured Data coded as: [Expanded Remote command structure] to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TARU} - READ BINARY with no length in C-APDU structure coded as: '22 00 B0 00 00 00' TLV Structure: C-APDU TLV Definite length coding	Secured Response Data is returned: 'AB 06 80 01 03 90 01 03'	RQ01_0001, RQ01_0002, RQ01_0003, RQ01_0005, RQ02_0301, RQ02_0302, RQ02_0303, RQ02_0401, RQ02_0801, RQ02_0801a, RQ02_0803, RQ02_0805, RQ02_0806, RQ02_0807, RQ02_0809, RQ02_0810, RQ02_0811, RQ02_0812 RQ04_0101, RQ04_0102

6.2.2.3 Test case 3: A command session with C-APDU TLV Structure with indefinite length coding

6.2.2.3.1 Initial Conditions

- None.

6.2.2.3.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data coded as: [Expanded Remote command structure] to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} TLV Structure: C-APDU TLV Indefinite length coding	Secured Response Data is returned: 'AF 80 23 02 90 00 00 00'	RQ01_0001, RQ01_0002, RQ01_0003, RQ01_0005 RQ02_0301a, RQ02_0302, RQ02_0303, RQ02_0401, RQ02_0802, RQ02_0802a, RQ02_0804 RQ04_0101, RQ04_0102

Step	Description	Expected Result	RQ
2	Send Command with Secured Data coded as: [Expanded Remote command structure] to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TARU} - UPDATE BINARY (empty Le field) TLV Structure: C-APDU TLV Indefinite length coding	Secured Response Data is returned: 'AF 80 23 02 90 00 23 02 90 00 23 02 90 00 00 00'	RQ01_0002, RQ01_0001, RQ01_0003, RQ02_0301a, RQ02_0302, RQ02_0303, RQ02_0401, RQ02_0402, RQ02_0802, RQ02_0802a, RQ02_0804 RQ04_0101, RQ04_0102
3	Send Command with Secured Data coded as: [Expanded Remote command structure] to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TARU} - READ BINARY coded with Le field set to '00' TLV Structure: C-APDU TLV Indefinite length coding	Secured Response Data is returned: 'AF 80 23 02 90 00 23 02 90 00 23 LEN [Data 90 00] 00 00' where the Data should be the content of EF_{TARU}	RQ01_0002, RQ01_0001, RQ01_0003, RQ01_0005, RQ02_0301a, RQ02_0302, RQ02_0303, RQ02_0401, RQ02_0802, RQ02_0802a, RQ02_0804 RQ04_0101, RQ04_0102

6.2.2.4 Test case 4: A command session with C-APDU TLV Structure with indefinite length coding - Bad Format

6.2.2.4.1 Initial Conditions

- None.

6.2.2.4.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data coded as: [Expanded Remote command structure] to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TARU} - READ BINARY with wrong C-APDU coded as ' 23 05 00 B0 00 00 00' TLV Structure: C-APDU TLV Indefinite length coding	Secured Response Data is returned: 'AF 80 23 02 90 00 23 02 90 00 90 01 01 00 00'	RQ01_0001, RQ01_0002, RQ01_0003, RQ01_0005 RQ02_0301a RQ02_0302, RQ02_0303, RQ02_0401, RQ02_0802, RQ02_0802a, RQ02_0804, RQ02_0806, RQ02_0807, RQ02_0809, RQ02_0811, RQ02_0812 RQ04_0101, RQ04_0102
2	Send Command with Secured Data coded as: [Expanded Remote command structure] to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TARU} - READ BINARY with wrong C-APDU length coded as:'22 0F 00 B0 00 00 00' TLV Structure: C-APDU TLV Indefinite length coding	Secured Response Data is returned: 'AF 80 23 02 90 00 23 02 90 00 90 01 02 00 00'	RQ01_0001, RQ01_0002, RQ01_0003, RQ01_0005 RQ02_0301a RQ02_0401, RQ02_0802, RQ02_0802a, RQ02_0804, RQ02_0806, RQ02_0807, RQ02_0809, RQ02_0811, RQ02_0812 RQ04_0101, RQ04_0102
3	Send Command with Secured Data coded as: [Expanded Remote command structure] to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TARU} - READ BINARY with no length in C-APDU structure as:'22 00 B0 00 00 00' TLV Structure: C-APDU TLV Indefinite length coding	Secured Response Data is returned: 'AF 80 23 02 90 00 23 02 90 00 90 01 03 00 00'	RQ01_0001, RQ01_0002, RQ01_0003, RQ01_0005 RQ02_0301a, RQ02_0401, RQ02_0802, RQ02_0802a, RQ02_0804, RQ02_0806, RQ02_0807, RQ02_0809, RQ02_0811, RQ02_0812 RQ04_0101, RQ04_0102

6.2.2.5 Test case 5: A command session with Immediate Action TLV Structure with definite length coding - Normal Format

6.2.2.5.1 Initial Conditions

- On the UICC-Terminal interface, prior to this test the Terminal shall have been powered on and performed the PROFILE DOWNLOAD procedure.
- Test application with AID30, AID31 and AID32 have been successfully installed.

6.2.2.5.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data coded as: [Expanded Remote command structure] to the Test application with AID30, which consist of proactive command: - DISPLAY TEXT TLV Structure: Immediate Action TLV using normal format Definite length coding	On the UICC-Terminal interface: The proactive session is performed successfully for DISPLAY TEXT.	RQ01_0001, RQ01_0002, RQ01_0003, RQ01_0005 RQ02_0301; RQ02_0302, RQ02_0304, RQ02_0501, RQ02_0504, RQ02_0509, RQ04_0101, RQ04_0102
2	Send Command with Secured Data coded as: [Expanded Remote command structure] to the Test application with AID31, which consist of proactive command: - PLAY TONE TLV Structure: Immediate Action TLV using normal format Definite length coding	On the UICC-Terminal interface: The proactive session is performed successfully for PLAY TONE.	RQ01_0001, RQ01_0002, RQ01_0003, RQ01_0005 RQ02_0301, RQ02_0302, RQ02_0304, RQ02_0501, RQ02_0504, RQ02_0509 RQ04_0101, RQ04_0102
3	Send Command with Secured Data coded as: [Expanded Remote command structure] to the Test application with AID32, which consist of proactive command: - REFRESH TLV Structure: Immediate Action TLV using normal format Definite length coding	On the UICC-Terminal interface: The proactive session is performed successfully for REFRESH.	RQ01_0001, RQ01_0002, RQ01_0003, RQ01_0005 RQ02_0301, RQ02_0302, RQ02_0304, RQ02_0501, RQ02_0504, RQ02_0509 RQ04_0101, RQ04_0102

6.2.2.6 Test case 6: A command session with Immediate Action TLV Structure with definite length coding - Referenced Format

6.2.2.6.1 Initial Conditions

- On the UICC-Terminal interface, prior to this test the Terminal shall have been powered on and performed the PROFILE DOWNLOAD procedure on the UICC/terminal interface.
- Test application with AID33 has been successfully installed.

6.2.2.6.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data coded as: [Expanded Remote command structure] to the Test application with AID33, consist of 2 Command TLV having the following TLV Structure in Definite length coding: 1st CMD: Immediate Action TLV - Referenced format indicating proactive session ('81') in the first command 2nd CMD: C-APDU TLV consist of DISPLAY TEXT	On the UICC-Terminal interface: The proactive session is performed successfully for DISPLAY TEXT.	RQ02_0301, RQ02_0302, RQ02_0304, RQ02_0502, RQ02_0509
2	Send Command with Secured Data coded as: [Expanded Remote command structure] to the Test application with AID33, consist of 3 Command TLV having the following TLV Structure in Definite length coding: 1st CMD: Immediate Action - Referenced format TLV indicating early response ('82') 2nd CMD: C-APDU TLV consist of DISPLAY TEXT 3rd CMD: Immediate Action - Referenced format TLV then to the second record in EF_{RMA} ('02') refers to REFRESH	Secure Response Data is returned to the sending entity, containing 'AB 07 80 01 01 23 02 90 00' On the UICC-Terminal interface: The proactive session is performed successfully for DISPLAY TEXT. The proactive session is performed successfully for REFRESH command.	RQ02_0301, RQ02_0302, RQ02_0304, RQ02_0502, RQ02_0503, RQ02_0504, RQ02_0509, RQ02_0508a, RQ02_0508b, RQ02_0508c RQ02_0801
3	Send Command with Secured Data coded as: [Expanded Remote command structure] to the Test application with AID33, which consist of 2 Command TLV having the following TLV Structure in Definite length coding: 1st CMD: Immediate Action - Referenced format to the first record in EF_{RMA} ('01') DISPLAY TEXT 2nd CMD: Immediate Action - Referenced format TLV to the second record in EF_{RMA} ('02') REFRESH	On the UICC-Terminal interface: The proactive session is performed successfully for DISPLAY TEXT. The proactive session is performed successfully for REFRESH command.	RQ02_0301, RQ02_0302, RQ02_0304, RQ02_0502, RQ02_0503, RQ02_0504, RQ02_0509,
4	Send Command with Secured Data coded as: [Expanded Remote command structure] to the Test application with AID33, consist of 3 Command TLV having the following TLV Structure in Definite length coding: 1st CMD: Immediate Action TLV - Referenced format indicating proactive session ('81') 2nd CMD: C-APDU TLV consist of DISPLAY TEXT 3rd CMD: C-APDU TLV - SELECT: DF_{TEST}	On the UICC-Terminal interface: The proactive session is performed successfully for DISPLAY TEXT. Secured Response Data is returned: 'AB 07 80 01 03 23 02 90 00'	RQ02_0301, RQ02_0302, RQ02_0304, RQ02_0502, RQ02_0504, RQ02_0509

6.2.2.7 Test case 7: A command session with Immediate Action TLV Structure with definite length coding - Immediate Action Error

6.2.2.7.1 Initial Conditions

- On the UICC-Terminal interface, prior to this test the Terminal shall have been powered on and performed the PROFILE DOWNLOAD procedure.
- Test application with AID34 has been successfully installed.

6.2.2.7.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data coded as: [Expanded Remote command structure] to the Test application with AID34, consist of 2 Command TLV having the following TLV Structure: Immediate Action TLV using referenced format indicating proactive session ('81') followed by a C-APDU TLV DISPLAY TEXT proactive command with wrong C-APDU length. Definite length coding.	Secured Response Data is returned: 'AB 06 80 01 01 81 01 01' On the UICC-Terminal interface: The proactive session is not performed for DISPLAY TEXT.	RQ02_0301, RQ02_0302, RQ02_0304, RQ02_0501, RQ02_0509, RQ02_0812a, RQ02_0813, RQ02_0814

6.2.2.8 Test case 8: A command session with Immediate Action TLV Structure with indefinite length coding - Normal Format

6.2.2.8.1 Initial Conditions

- On the UICC-Terminal interface, prior to this test the Terminal shall have been powered on and performed the PROFILE DOWNLOAD procedure.
- Test application with AID30, AID31 and AID32 have been successfully installed.

6.2.2.8.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data coded as: [Expanded Remote command structure] to the Test application with AID30, which consist of proactive command: - DISPLAY TEXT TLV Structure: Immediate Action TLV using normal format. Indefinite length coding.	On the UICC-Terminal interface: The proactive session is performed successfully for DISPLAY TEXT.	RQ02_0301a, RQ02_0302, RQ02_0304, RQ02_0501, RQ02_0504, RQ02_0509
2	Send Command with Secured Data coded as: [Expanded Remote command structure] to the Test application with AID31, which consist of proactive command: - PLAY TONE TLV Structure: Immediate Action TLV using normal format. Indefinite length coding.	On the UICC-Terminal interface: The proactive session is performed successfully for PLAY TONE.	RQ02_0301a, RQ02_0302, RQ02_0304, RQ02_0501, RQ02_0504, RQ02_0509
3	Send Command with Secured Data coded as: [Expanded Remote command structure] to the Test application with AID32, which consist of proactive command: - REFRESH TLV Structure: Immediate Action TLV using normal format. Indefinite length coding.	On the UICC-Terminal interface: The proactive session is performed successfully for REFRESH.	RQ01_0003, RQ02_0301a, RQ02_0302, RQ02_0304, RQ02_0501, RQ02_0504, RQ02_0509

6.2.2.9 Test case 9: A command session with Immediate Action TLV Structure with indefinite length coding - Referenced Format

6.2.2.9.1 Initial Conditions

- On the UICC-Terminal interface, prior to this test the Terminal shall have been powered on and performed the PROFILE DOWNLOAD procedure.
- Test application with AID33 has been successfully installed.

6.2.2.9.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data coded as: [Expanded Remote command structure] to the Test application with AID33, which consist of one Command TLV having the following TLV Structure: Immediate Action TLV using referenced format indicating proactive session ('81') followed by DISPLAY TEXT Indefinite length coding.	On the UICC-Terminal interface: The proactive session is performed successfully for DISPLAY TEXT.	RQ02_0301a, RQ02_0302, RQ02_0304, RQ02_0502, RQ02_0503, RQ02_0509
2	Send Command with Secured Data coded as: [Expanded Remote command structure] to the Test application with AID33, consist of 4 Command TLV having the following TLV Structure in Indefinite length coding: 1st CMD: Immediate Action TLV: - referenced format first record in EF_{RMA} ('03'), then 2nd CMD: Immediate Action TLV: - referenced format indicating early response ('82') 3rd CMD: C-APDU TLV consist of DISPLAY TEXT 4th CMD: Immediate Action TLV: - referenced format to the second record in EF_{RMA} ('02')	Secured Response Data is returned: 'AF 80 81 02 90 00 00 00' On the UICC-Terminal interface: The proactive session is performed successfully for the following proactive commands in the following order: - PLAY TONE - DISPLAY TEXT and - REFRESH.	RQ02_0301a, RQ02_0302, RQ02_0304, RQ02_0502, RQ02_0503, RQ02_0509, RQ02_0802, RQ02_0508a, RQ02_0508b, RQ02_0508c

6.2.2.10 Test case 10: A command session with Immediate Action TLV Structure with indefinite length coding - Immediate Action Error

6.2.2.10.1 Initial Conditions

- On the UICC-Terminal interface, prior to this test the Terminal shall have been powered on and performed the PROFILE DOWNLOAD procedure.
- Test application with AID34 has been successfully installed.

6.2.2.10.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data coded as: [Expanded Remote command structure] to the Test application with AID34, which consist of: - TLV Structure: Immediate Action TLV using referenced format indicating proactive session ('81') in the first command TLV followed by C-APDU TLV consist of DISPLAY TEXT with wrong C-APDU length Indefinite length coding.	Secured Response Data is returned: 'AF 80 81 01 01 00 00' On the UICC-Terminal interface: The proactive session is not performed for DISPLAY TEXT.	RQ02_0301a, RQ02_0302, RQ02_0304, RQ02_0501, RQ02_0509, RQ02_0812b, RQ02_0813, RQ02_0814

6.2.2.11 Test case 11: A command session with Error Action TLV Structure with definite length coding - normal format

6.2.2.11.1 Initial Conditions

- On the UICC-Terminal interface, prior to this test the Terminal shall have been powered on and performed the PROFILE DOWNLOAD procedure.
- Test application with AID1, AID35 has been successfully installed.

6.2.2.11.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data coded as: [Expanded Remote command structure] to test application with AID35, which consist of the following Command TLVs: - 1st CMD: Error Action TLV using normal format consist of DISPLAY TEXT - 2nd CMD: C-APDU TLV consist of SELECT: DF_{TEST} - 3rd CMD: C-APDU TLV consist of SELECT: EF_{TPRU} - 4th CMD: C-APDU TLV consist of READ BINARY Definite length coding.	On the UICC-Terminal interface: The proactive session is performed successfully for DISPLAY TEXT. Secured Response Data is returned: 'AB LEN 80 01 04 23 LENx [Data SW1 SW2]'	RQ02_0301, RQ02_0302, RQ02_0305, RQ02_0601, RQ02_0605, RQ02_0606
2	Send Command with Secured Data coded as: [Expanded Remote command structure] to Test application with AID1, which consist of the following Command TLVs: - 1st CMD: Error Action TLV with no action - 2nd CMD: C-APDU TLV consists of SELECT: DF_{TEST} as C-APDU TLV - 3rd CMD: C-APDU TLV consists of SELECT: EF_{TPRU} as C-APDU TLV - 4th CMD: C-APDU TLV consist of READ BINARY as C-APDU TLV Definite length coding.	Secured Response Data is returned: 'AB 07 80 01 04 23 02 69 82'	RQ02_0301, RQ02_0302, RQ02_0305, RQ02_0603, RQ02_0607

6.2.2.12 Test case 12: A command session with Error Action TLV Structure with definite length coding - Referenced format

6.2.2.12.1 Initial Conditions

- On the UICC-Terminal interface, prior to this test the Terminal shall have been powered on and performed the PROFILE DOWNLOAD procedure.
- Test application with AID36 has been successfully installed.

6.2.2.12.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data coded as: [Expanded Remote command structure] to Test application with AID 36, which consist of the following Commands TLV: - 1st CMD: Error Action TLV using referenced format to the third record in EF_{RMA} (' 03') to PLAY TONE - 2nd CMD: C-APDU TLV consist of SELECT: DF_{TEST} - 3rd CMD: C-APDU TLV consist of SELECT: EF_{TPRU} - 4th CMD: C-APDU TLV consist of READ BINARY as C-APDU TLV Definite length coding.	On the UICC-Terminal interface: The proactive session is performed successfully for PLAY TONE. Secured Response Data is returned: 'AB LEN 80 01 05 82 LENx [Data SW1 SW2]'	RQ02_0301, RQ02_0302, RQ02_0305, RQ02_0602, RQ02_0604, RQ02_0605, RQ02_0606

6.2.2.13 Test case 13: A command session with Error Action TLV Structure with indefinite length coding - Normal format

6.2.2.13.1 Initial Conditions

- On the UICC-Terminal interface, prior to this test the Terminal shall have been powered on and performed the PROFILE DOWNLOAD procedure.
- Test application with AID35, AID36 and AID1 has been successfully installed.

6.2.2.13.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Secured Data coded as: [Expanded Remote command structure] to the Test application with AID35, which consist of the following Commands TLV: - 1st CMD: Error Action TLV using normal format consist of DISPLAY TEXT - 2nd CMD: C-APDU TLV consist of SELECT: DF_{TEST} - 3rd CMD: C-APDU TLV consist of SELECT: EF_{TPRU} - 4th CMD: C-APDU TLV consist of READ BINARY Indefinite length coding.	Secured Response Data is returned: 'AF 80 23 02 90 00 23 02 90 00 82 LEN [Data SW1 SW2] 82 02 69 85' On the UICC-terminal interface: The proactive session is performed successfully for DISPLAY TEXT.	RQ02_0301a, RQ02_0302, RQ02_0305, RQ02_0601, RQ02_0605, RQ02_0606 RQ02_0802, RQ02_0802a, RQ02_0804
2	Send Secured Data coded as: [Expanded Remote command structure] to the Test application with AID1, which consist of the following Commands TLV: - 1st CMD: Error Action TLV with no action - 2nd CMD: C-APDU TLV consist of SELECT: DF_{TEST} - 3rd CMD: C-APDU TLV consist of SELECT: EF_{TPRU} - 4th CMD: C-APDU TLV consist of READ BINARY as C-APDU TLV Indefinite length coding.	Secured Response Data is returned: 'AF 80 23 02 90 00 23 02 90 00 82 02 69 85'	RQ02_0301a, RQ02_0302, RQ02_0305, RQ02_0603, RQ02_0607, RQ02_0802, RQ02_0802a, RQ02_0804

6.2.2.14 Test case 14: A command session with Error Action TLV Structure with indefinite length coding - Referenced format

6.2.2.14.1 Initial Conditions

- On the UICC-Terminal interface, prior to this test the Terminal shall have been powered on and performed the PROFILE DOWNLOAD procedure.
- Test application with AID35, AID36 and AID1 has been successfully installed.

6.2.2.14.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Secured Data coded as: [Expanded Remote command structure] to the Test application with AID36, which consist of the following Commands TLV: - 1st CMD: Error Action TLV using referenced format to the third record in EF_{RMA} ('03') for PLAY TONE - 2nd CMD: C-APDU TLV consist of SELECT: DF_{TEST} - 3rd CMD: C-APDU TLV consist of SELECT: EF_{TPRU} - 4th CMD: C-APDU TLV consist of READ BINARY Indefinite length coding.	Secured Response Data is returned: 'AF 80 23 02 90 00 23 02 90 00 82 LEN [Data SW1 SW2] 82 02 69 85' On the UICC-terminal interface: The proactive session is performed successfully for PLAY TONE.	RQ02_0301a, RQ02_0302, RQ02_0305, RQ02_0602, RQ02_0604, RQ02_0605, RQ02_0606, RQ02_0802, RQ02_0802a, RQ02_0804

6.2.2.15 Test case 15: A command session with Script Chaining TLV Structure with definite length coding

6.2.2.15.1 Initial Conditions

- None.

6.2.2.15.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Secured Data coded as: [Expanded Remote command structure] to the UICC Shared File System Remote File Management application, which contains: - Script Chaining TLV with the Script Chaining Value '01' as the first command TLV - SELECT: DF_{TEST} as C-APDU TLV - SELECT: EF_{TARU} as C-APDU TLV - UPDATE BINARY with data '01 01 … 01' (17 bytes) as C-APDU TLV Definite length coding.	'AB 07 80 01 04 83 02 90 00'	RQ02_0301, RQ02_0302, RQ02_0306, RQ02_0701, RQ02_0702, RQ02_0704, RQ04_0103 RQ04_0104
2	Send Secured Data coded as: [Expanded Remote command structure] to the UICC Shared File System Remote File Management application, which contains: - Script Chaining TLV with the Script Chaining Value '02' as the first command TLV - UPDATE BINARY with data '01 01 01' (100 bytes) as C-APDU TLV Definite length coding.	'AB 07 80 01 02 83 02 90 00'	RQ02_0301, RQ02_0302, RQ02_0306, RQ02_0701, RQ02_0702, RQ02_0704, RQ04_0103 RQ04_0104

Step	Description	Expected Result	RQ
3	Send Secured Data coded as: [Expanded Remote command structure] to the UICC Shared File System Remote File Management application, which contains: - Script Chaining TLV with the Script Chaining Value '03' as the first command TLV - UPDATE BINARY with data '01 01 01' as C-APDU TLV - READ BINARY as C-APDU TLV Definite length coding.	'AB 81 83 80 01 03 83 LEN [Data 90 00]' where the Data should be the content of EF_{TARU}.	RQ02_0301, RQ02_0302, RQ02_0306, RQ02_0701, RQ02_0702, RQ02_0704, RQ04_0103 RQ04_0104

6.2.2.16 Test case 16: A command session with Script Chaining TLV Structure with definite length coding (Script Chaining Error).

6.2.2.16.1 Initial Conditions

- None.

6.2.2.16.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Secured Data coded as: [Expanded Remote command structure] to the UICC Shared File System Remote File Management application, which contains: - Script Chaining TLV with the Script Chaining Value '02' as the first command TLV - SELECT: DF_{TEST} as C-APDU TLV - SELECT: EF_{TARU} as C-APDU TLV - UPDATE BINARY with data '01 01 01' as C-APDU TLV Definite length coding.	'AB 06 80 01 01 83 02 01'	RQ02_0301, RQ02_0302, RQ02_0306, RQ02_0817a

6.2.2.17 Test case 17: A command session with Script Chaining TLV Structure with indefinite length coding

6.2.2.17.1 Initial Conditions

- None.

6.2.2.17.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Secured Data coded as: [Expanded Remote command structure] to the UICC Shared File System Remote File Management application, which contains: - Script Chaining TLV with the Script Chaining Value '01' as the first command TLV - SELECT: DF_{TEST} as C-APDU TLV - SELECT: EF_{TARU} as C-APDU TLV - UPDATE BINARY with data '01 01 … 01' (17 Bytes) as C-APDU TLV Indefinite length coding.	'AF 80 83 02 90 00 83 02 90 00 83 02 90 00 00 00'	RQ02_0301a, RQ02_0302, RQ02_0306, RQ04_0103 RQ04_0104

Step	Description	Expected Result	RQ
2	Send Secured Data coded as: [Expanded Remote command structure] to the UICC Shared File System Remote File Management application, which contains: - Script Chaining TLV with the Script Chaining Value '02' as the first command TLV - UPDATE BINARY with data '01 01 01' (100 bytes) as C-APDU TLV Indefinite length coding.	'AF 80 83 02 90 00 83 02 90 00 83 02 90 00 00 00'	RQ02_0301a, RQ02_0302, RQ02_0306, RQ04_0103 RQ04_0104
3	Send Secured Data coded as: [Expanded Remote command structure] to the UICC Shared File System Remote File Management application, which contains: - Script Chaining TLV with the Script Chaining Value '03' as the first command TLV - UPDATE BINARY with data '01 01 01' as C-APDU TLV - READ BINARY as C-APDU TLV Indefinite length coding.	'AF 80 83 02 90 00 83 02 90 00 83 02 90 00 83 LEN [Data 90 00] 00 00' where the Data should be the content of EF_{TARU}.	RQ02_0301a, RQ02_0302, RQ02_0306, RQ04_0103 RQ04_0104

6.2.2.18 Test case 18: A command session with Script Chaining TLV Structure with indefinite length coding (Script Chaining Error)

6.2.2.18.1 Initial Conditions

- None.

6.2.2.18.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Secured Data coded as: [Expanded Remote command structure] to the UICC Shared File System Remote File Management application, which contains: - Script Chaining TLV with the Script Chaining Value '02' as the first command TLV - SELECT: DF_{TEST} as C-APDU TLV - SELECT: EF_{TARU} as C-APDU TLV - UPDATE BINARY with data '01 01 01' as C-APDU TLV Indefinite length coding.	'AF 80 83 02 01 00 00'	RQ02_0301a, RQ02_0302, RQ02_0306, RQ02_0817b, RQ02_0818, RQ02_0819

6.3 Security parameters assigned to applications

6.3.1 Minimum Security Level (MSL)

Test cases verifying the requirements from this clause are defined under clause 6.5.3 of the present document.

6.3.2 Access domain

Test cases verifying the requirements from this clause are defined under clause 6.5.3 of the present document.

6.4 Remote File Management (RFM)

6.4.1 UICC Shared File System Remote File Management

6.4.1.1 Test case 1: A command session with a single SELECT command. Check access to the file tree

6.4.1.1.1 Initial Conditions

- None.

6.4.1.1.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: SELECT: EF_{DIR} GET RESPONSE	Response with Secured Data is returned last or only additional data response shall be '02 90 00' and FCP data containing TLV '83 02 2F 00'	RQ04_0301, RQ04_0302, RQ04_0304 RQ01_0001, RQ01_0002, RQ01_0003, RQ02_0101, RQ02_0103 RQ02_0104 RQ02_0201
2	Send Command with Secured Data to the UICC Shared File System Remote File Management application which contains: SELECT: DF_{TEST}	Response with Secured Data is returned last or only additional data response shall be '01 90 00'	RQ04_0301, RQ04_0304 RQ01_0001, RQ01_0002, RQ01_0003, RQ02_0101, RQ02_0201
3	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: SELECT: DF_{TESTB}	Response with Secured Data is returned last or only additional data response shall be '01 69 85' or other error SW	RQ04_0303, RQ01_0001, RQ01_0002, RQ01_0003, RQ02_0101, RQ02_0201
4	Send Command with Secured Data to the UICC Shared File System Remote File Management application which contains: SELECT by DF name: ADF	Response with Secured Data is returned last or only additional data response shall be '01 69 85' or other error SW	RQ04_0201
5	Send Command with Secured Data to the UICC Shared File System Remote File Management application which contains: SELECT: DF_{TEST} SELECT: EF_{TARU} (see note)	Response with Secured Data is returned last or only additional data response shall be '02 90 00'	RQ04_0201
NOTE: SELECT command is executed as SELECT by FID.			

6.4.1.2 Test case 2: A command session with multiple commands (SELECT, UPDATE BINARY, READ BINARY).

6.4.1.2.1 Initial Conditions

- None.

6.4.1.2.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TARU} - UPDATE BINARY with data '01 01 01'	Response with Secured Data is returned last or only additional data response shall be '03 90 00'	RQ01_0001, RQ01_0002, RQ01_0003, RQ01_0005, RQ01_0007, RQ02_0101, RQ02_0201, RQ04_0101, RQ04_0304
2	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TARU} - READ BINARY with P3/Le = '00'	Response with Secured Data is returned last or only additional data response shall be '03 90 00' and contain all data of EF_{TARU} starting with '01 01 01' until the end of file	RQ01_0001, RQ01_0002, RQ01_0003, RQ01_0005, RQ01_0007, RQ02_0101, RQ02_0104, RQ02_0105, RQ02_0201, RQ04_0101, RQ04_0201, RQ04_0203, RQ04_0304
3	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - READ BINARY with P3/Le = '00'	Response with Secured Data is returned last or only additional data response shall be '01 69 86'	RQ01_0001, RQ01_0002, RQ01_0003, RQ01_0005, RQ01_0009, RQ04_0101

6.4.1.3 Test case 3: A command session with multiple commands (SEARCH RECORD, UPDATE RECORD, INCREASE, READ RECORD)

6.4.1.3.1 Initial Conditions

- None.

6.4.1.3.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{CY4R4b} - UPDATE RECORD with data '01 01 01 01' with P2 set to PREVIOUS mode	Response with Secured Data is returned last or only additional data response shall be '03 90 00'	RQ04_0101, RQ04_0201, RQ04_0304

Step	Description	Expected Result	RQ
2	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{CY4R4b} - SEARCH RECORD with data '01 01 01 01'	Response with Secured Data is returned last or only additional data response shall be '03 90 00' and contain '01' data byte	RQ04_0101, RQ04_0201, RQ04_0203, RQ04_0304
3	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{CY4R4b} - READ RECORD with P3/Le = '00'	Response with Secured Data is returned last or only additional data response shall be'03 90 00 ' and contain '01 01 01 01' data bytes	RQ04_0101, RQ04_0201, RQ04_0202, RQ04_0304
4	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{CY4R4b} - INCREASE with data '01 01 01 01' - GET RESPONSE	Response with Secured Data is returned last or only additional data response shall be '04 90 00' and contain '02 02 02 02 01 01 01 01' data bytes	RQ04_0101, RQ04_0201, RQ04_0304

6.4.1.4 Test case 4: A command session with multiple commands (SET DATA, RETRIEVE DATA).

6.4.1.4.1 Initial Conditions

- None.

6.4.1.4.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT by FID: DF_{TEST} - SELECT: $EF_{BER-TLV}$ - SET DATA with '81 02 01 01'	Response with Secured Data is returned last or only additional data response shall be '03 90 00'	RQ04_0101, RQ04_0201, RQ04_0304
2	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT by FID: DF_{TEST} - SELECT: $EF_{BER-TLV}$ - RETRIEVE DATA with P3/Le = '00'and Tag value '81' - GET RESPONSE	Response with Secured Data is returned last or only additional data response shall be'04 90 00' and contain '81 02 01 01' data bytes	RQ04_0101, RQ04_0201, RQ04_0204, RQ04_0304

6.4.1.5 Test case 5: A command session with multiple commands (ACTIVATE FILE, DEACTIVATE FILE)

6.4.1.5.1 Initial Conditions

- None.

6.4.1.5.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TARU} - ACTIVATE FILE	Response with Secured Data is returned last or only additional data response shall be '03 90 00'	RQ04_0101, RQ04_0201, RQ04_0304
2	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TARU} - DEACTIVATE FILE	Last or only additional data response shall be '03 90 00'	RQ04_0101, RQ04_0201, RQ04_0304
3	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TARU} - READ BINARY	Response with Secured Data is returned last or only additional data response shall be '03 69 85'	RQ01_0005, RQ04_0101, RQ04_0201, RQ04_0304

6.4.1.6 Test case 6: A command session with multiple commands (VERIFY PIN, CHANGE PIN)

6.4.1.6.1 Initial Conditions

- None.

6.4.1.6.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TUACP} - VERIFY PIN with PIN = '31 31 31 31 FF FF FF FF'	Response with Secured Data is returned last or only additional data response shall be '03 90 00'	RQ04_0101, RQ04_0201, RQ04_0304
	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TPRU} - VERIFY PIN with PIN = '31 31 31 31 FF FF FF FF' - READ BINARY	Response with Secured Data is returned last or only additional data response shall be '04 90 00', and contain all data of EF_{TPRU}	
2	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TUACP} - CHANGE PIN with data = '31 31 31 31 FF FF FF FF 32 32 32 32 FF FF FF FF' - VERIFY PIN with PIN = '32 32 32 32 FF FF FF FF'	Response with Secured Data is returned last or only additional data response shall be '04 90 00'	RQ04_0101, RQ04_0201, RQ04_0304

6.4.1.7 Test case 7: A command session with multiple commands (DISABLE PIN, ENABLE PIN)

6.4.1.7.1 Initial Conditions

- None.

6.4.1.7.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TUACP} - DISABLE PIN with PIN = ' 31 31 31 31 FF FF FF FF'	Response with Secured Data is returned last or only additional data response shall be '03 90 00'	RQ04_0101, RQ04_0201, RQ04_0304
2	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TUACP} - VERIFY PIN with PIN = '31 31 31 31 FF FF FF FF'	Response with Secured Data is returned last or only additional data response shall be '03 69 83' or any other security error SW	RQ04_0101, RQ04_0201, RQ04_0304
3	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TUACP} - ENABLE PIN with PIN = ' 31 31 31 31 FF FF FF FF'	Response with Secured Data is returned last or only additional data response shall be '03 90 00'	RQ04_0101, RQ04_0201, RQ04_0304
4	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TUACP} - VERIFY PIN with PIN = '31 31 31 31 FF FF FF FF'	Response with Secured Data is returned last or only additional data response shall be '03 90 00'	RQ04_0101, RQ04_0201, RQ04_0304

6.4.1.8 Test case 8: A command session with multiple commands (UNBLOCK PIN)

6.4.1.8.1 Initial Conditions

- None.

6.4.1.8.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TUACP} - VERIFY PIN with PIN = '30 30 30 30 FF FF FF FF'	Response with Secured Data is returned last or only additional data response shall be '03 63 C2'	RQ04_0101, RQ04_0201, RQ04_0304
2	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TUACP} - VERIFY PIN with PIN = '30 30 30 30 FF FF FF FF'	Response with Secured Data is returned last or only additional data response shall be '03 63 C1'	RQ04_0101, RQ04_0201, RQ04_0304

Step	Description	Expected Result	RQ
3	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TUACP} - VERIFY PIN with PIN = '30 30 30 30 FF FF FF FF'	Response with Secured Data is returned last or only additional data response shall be '03 63 C0'	RQ04_0101, RQ04_0201, RQ04_0304
4	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TUACP} - VERIFY PIN with PIN = '30 30 30 30 FF FF FF FF'	Response with Secured Data is returned last or only additional data response shall be '03 63 C0' or '03 69 83'	RQ04_0101, RQ04_0201, RQ04_0304
5	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TUACP} - UNBLOCK PIN with Data = '33 33 33 33 FF FF FF FF 34 34 34 34 FF FF FF FF'	Response with Secured Data is returned last or only additional data response shall be '03 90 00'	RQ04_0101, RQ04_0201, RQ04_0304
6	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TUACP} - VERIFY PIN with PIN = '34 34 34 34 FF FF FF FF'	Response with Secured Data is returned last or only additional data response shall be '03 90 00'	RQ04_0101, RQ04_0201, RQ04_0304

6.4.1.9 Test case 9: A command session with multiple commands (CREATE FILE, RESIZE FILE, DELETE FILE)

6.4.1.9.1 Initial Conditions

- None.

6.4.1.9.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - CREATE FILE: EF_{XX}	Response with Secured Data is returned last or only additional data response shall be '02 90 00'	RQ04_0101, RQ04_0201, RQ04_0304
2	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{XX} - READ BINARY	Response with Secured Data is returned last or only additional data response shall be '03 90 00' and contain all data of EF_{XX} starting with 'FF FF FF FF FF' data bytes	RQ04_0101, RQ04_0201, RQ04_0304
3	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - RESIZE FILE: EF_{XX} - SELECT: EF_{XX} - READ BINARY	Response with Secured Data is returned last or only additional data response shall be '04 90 00' and contain all data of EF_{TARU} starting with 'FF FF FF'	RQ04_0101, RQ04_0201, RQ04_0304
4	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - DELETE FILE: EF_{XX}	Response with Secured Data is returned last or only additional data response shall be '03 90 00'	RQ04_0101, RQ04_0201, RQ04_0304

Step	Description	Expected Result	RQ
5	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{XX}	Response with Secured Data is returned last or only additional data response shall be '02 6A 82'	RQ04_0101, RQ04_0201, RQ04_0304

6.4.2 ADF Remote File Management

6.4.2.1 Test case 1: A command session with a single SELECT command. Check access to the file tree

6.4.2.1.1 Initial Conditions

- None.

6.4.2.1.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ADF Remote File Management application which contains: - SELECT: DF_{TESTB} - SELECT: EF_{TARUB} (see note)	Response with Secured Data is returned last or only additional data response shall be '02 90 00'	RQ04_0406, RQ04_0407, RQ04_0409, RQ04_0410
2	Send Command with Secured Data to the ADF Remote File Management application, which contains: - SELECT by path from MF: EF_{TARU}	Response with Secured Data is returned last or only additional data response shall be '01 90 00'	RQ04_0408, RQ04_0409, RQ04_0410
NOTE: SELECT command is executed as SELECT by FID.			

6.4.2.2 Test case 2: A command session with multiple commands (SELECT, UPDATE BINARY, READ BINARY)

6.4.2.2.1 Initial Conditions

- None.

6.4.2.2.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ADF Remote File Management application, which contains: - SELECT: DF_{TESTB} - SELECT: EF_{TARUB} - UPDATE BINARY with data '01 01 01'	Response with Secured Data is returned last or only additional data response shall be '03 90 00'	RQ04_0409, RQ04_0410
2	Send Command with Secured Data to the ADF Remote File Management application, which contains: - SELECT: DF_{TESTB} - SELECT: EF_{TARUB} - READ BINARY with P3/Le = '00'	Response with Secured Data is returned last or only additional data response shall be '03 90 00' and contain all data of EF_{TARUB} starting with '01 01 01' until the end of file	RQ04_0403, RQ04_0409, RQ04_0410

6.4.2.3 Test case 3: A command session with multiple commands (SEARCH RECORD, UPDATE RECORD, INCREASE, READ RECORD)

6.4.2.3.1 Initial Conditions

- None.

6.4.2.3.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ADF Remote File Management application, which contains: - SELECT by path: EF_{CY4R4b} - UPDATE RECORD with data '01 01 01 01' with P2 set to PREVIOUS mode	Response with Secured Data is returned last or only additional data response shall be '02 90 00'	RQ04_0201, RQ04_0409, RQ04_0410
2	Send Command with Secured Data to the ADF Remote File Management application, which contains: - SELECT by path: EF_{CY4R4b} - SEARCH RECORD with data '01 01 01 01'	Response with Secured Data is returned last or only additional data response shall be '02 90 00' and contain '01' data byte	RQ04_0201, RQ04_0409, RQ04_0410
3	Send Command with Secured Data to the ADF Remote File Management application, which contains: - SELECT by path: EF_{CY4R4b} - READ RECORD with P3/Le = '00'	Response with Secured Data is returned last or only additional data response shall be'02 90 00 ' and contain '01 01 01 01' data bytes	RQ04_0201, RQ04_0202, RQ04_0409, RQ04_0410
4	Send Command with Secured Data to the ADF Remote File Management application, which contains: - SELECT by path: EF_{CY4R4b} - INCREASE with data '01 01 01 01' - GET RESPONSE	Response with Secured Data is returned last or only additional data response shall be '03 90 00' and contain '02 02 02 02 01 01 01 01' data bytes	RQ04_0409, RQ04_0410

6.4.2.4 Test case 4: A command session with multiple commands (SET DATA, RETRIEVE DATA)

6.4.2.4.1 Initial Conditions

- None.

6.4.2.4.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ADF Remote File Management application, which contains: - SELECT by path: $EF_{BER-TLV}$ - SET DATA with '81 02 01 01'	Response with Secured Data is returned last or only additional data response shall be '02 90 00'	RQ04_0101, RQ04_0201, RQ04_0409, RQ04_0410
2	Send Command with Secured Data to the ADF Remote File Management application, which contains: - SELECT by path: $EF_{BER-TLV}$ - RETRIEVE DATA with P3/Le = '00'and Tag value '81' - GET RESPONSE	Response with Secured Data is returned last or only additional data response shall be'03 90 00' and contain '81 02 01 01' data bytes	RQ04_0101, RQ04_0201, RQ04_0204, RQ04_0409, RQ04_0410

6.4.2.5 Test case 5: A command session with multiple commands (ACTIVATE FILE, DEACTIVATE FILE)

6.4.2.5.1 Initial Conditions

- None.

6.4.2.5.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ADF Remote File Management application, which contains: - SELECT: DF_{TESTB} - SELECT: EF_{TARUB} - ACTIVATE FILE	Response with Secured Data is returned last or only additional data response shall be '03 90 00'	RQ04_0101, RQ04_0409, RQ04_0410
2	Send Command with Secured Data to the ADF Remote File Management application, which contains: - SELECT: DF_{TESTB} - SELECT: EF_{TARUB} - DEACTIVATE FILE	Last or only additional data response shall be '03 90 00'	RQ04_0101, RQ04_0409, RQ04_0410
3	Send Command with Secured Data to the ADF Remote File Management application, which contains: - SELECT: DF_{TESTB} - SELECT: EF_{TARUB} - READ BINARY	Response with Secured Data is returned last or only additional data response shall be '03 69 85'	RQ04_0409, RQ04_0410

6.4.2.6 Test case 6: A command session with multiple commands (VERIFY PIN, CHANGE PIN)

6.4.2.6.1 Initial Conditions

- None.

6.4.2.6.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ADF Remote File Management application, which contains: - SELECT by path: EF_{TUACP} - VERIFY PIN with PIN = '31 31 31 31 FF FF FF FF'	Response with Secured Data is returned last or only additional data response shall be '02 90 00'	RQ04_0101, RQ04_0201, RQ04_0409, RQ04_0410
2	Send Command with Secured Data to the ADF Remote File Management application, which contains: - SELECT by path: EF_{TPRU} - VERIFY PIN with PIN = '31 31 31 31 FF FF FF FF' - READ BINARY	Response with Secured Data is returned last or only additional data response shall be '02 90 00', and contain all data of EF_{TPRU}	RQ04_0409, RQ04_0410
3	Send Command with Secured Data to the ADF Remote File Management application, which contains: - SELECT by path: EF_{TUACP} - CHANGE PIN with data = '31 31 31 31 FF FF FF FF 32 32 32 32 FF FF FF FF' - VERIFY PIN with PIN = '32 32 32 32 FF FF FF FF'	Response with Secured Data is returned last or only additional data response shall be '03 90 00'	RQ04_0101, RQ04_0201, RQ04_0409, RQ04_0410

6.4.2.7 Test case 7: A command session with multiple commands (DISABLE PIN, ENABLE PIN)

6.4.2.7.1 Initial Conditions

- None.

6.4.2.7.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ADF Remote File Management application, which contains: - SELECT by path: EF_{TUACP} - DISABLE PIN with PIN = ' 31 31 31 31 FF FF FF FF'	Response with Secured Data is returned last or only additional data response shall be '02 90 00'	RQ04_0101, RQ04_0201, RQ04_0409, RQ04_0410
2	Send Command with Secured Data to the ADF Remote File Management application, which contains: - SELECT by path: EF_{TUACP} - VERIFY PIN with PIN = '31 31 31 31 FF FF FF FF'	Response with Secured Data is returned last or only additional data response shall be '02 69 83' or any other security error SW	RQ04_0101, RQ04_0201, RQ04_0409, RQ04_0410
3	Send Command with Secured Data to the ADF Remote File Management application, which contains: - SELECT by path: EF_{TUACP} - ENABLE PIN with PIN = ' 31 31 31 31 FF FF FF FF'	Response with Secured Data is returned last or only additional data response shall be '02 90 00'	RQ04_0101, RQ04_0201, RQ04_0409, RQ04_0410
4	Send Command with Secured Data to the ADF Remote File Management application, which contains: - SELECT by path: EF_{TUACP} - VERIFY PIN with PIN = '31 31 31 31 FF FF FF FF'	Response with Secured Data is returned last or only additional data response shall be '02 90 00'	RQ04_0101, RQ04_0201, RQ04_0409, RQ04_0410

6.4.2.8 Test case 8: A command session with multiple commands (UNBLOCK PIN)

6.4.2.8.1 Initial Conditions

- None.

6.4.2.8.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ADF Remote File Management application, which contains: - SELECT by path: EF_{TUACP} - VERIFY PIN with PIN = '30 30 30 30 FF FF FF FF'	Response with Secured Data is returned last or only additional data response shall be '02 63 C2'	RQ04_0101, RQ04_0201, RQ04_0409, RQ04_0410
2	Send Command with Secured Data to the ADF Remote File Management application, which contains: - SELECT by path: EF_{TUACP} - VERIFY PIN with PIN = '30 30 30 30 FF FF FF FF'	Response with Secured Data is returned last or only additional data response shall be '02 63 C1'	RQ04_0101, RQ04_0201, RQ04_0409, RQ04_0410
3	Send Command with Secured Data to the ADF Remote File Management application, which contains: - SELECT by path: EF_{TUACP} - VERIFY PIN with PIN = '30 30 30 30 FF FF FF FF'	Response with Secured Data is returned last or only additional data response shall be '02 63 C0'	RQ04_0101, RQ04_0201, RQ04_0409, RQ04_0410

Step	Description	Expected Result	RQ
4	Send Command with Secured Data to the ADF Remote File Management application, which contains: - SELECT by path: EF_{TUACP} - VERIFY PIN with PIN = '30 30 30 30 FF FF FF FF'	Response with Secured Data is returned last or only additional data response shall be '02 63 C0' or '03 69 83'	RQ04_0101, RQ04_0201, RQ04_0409, RQ04_0410
5	Send Command with Secured Data to the ADF Remote File Management application, which contains: - SELECT by path: EF_{TUACP} - UNBLOCK PIN with Data = '33 33 33 33 FF FF FF FF 34 34 34 34 FF FF FF FF'	Response with Secured Data is returned last or only additional data response shall be '02 90 00'	RQ04_0101, RQ04_0201, RQ04_0409, RQ04_0410
6	Send Command with Secured Data to the ADF Remote File Management application, which contains: - SELECT by path: EF_{TUACP} - VERIFY PIN with PIN = '34 34 34 34 FF FF FF FF'	Response with Secured Data is returned last or only additional data response shall be '02 90 00'	RQ04_0101, RQ04_0201, RQ04_0409, RQ04_0410

6.4.2.9 Test case 9: A command session with multiple commands (CREATE FILE, RESIZE FILE, DELETE FILE)

6.4.2.9.1 Initial Conditions

- None.

6.4.2.9.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ADF Remote File Management application, which contains: - SELECT: DF_{TESTB} - CREATE FILE: EF_{XX}	Response with Secured Data is returned last or only additional data response shall be '02 90 00'	RQ04_0101, RQ04_0201, RQ04_0409
2	Send Command with Secured Data to the ADF Remote File Management application, which contains: - SELECT: DF_{TESTB} - SELECT: EF_{XX}. - READ BINARY	Response with Secured Data is returned last or only additional data response shall be '03 90 00' and contain all data of EF_{XX} starting with 'FF FF FF FF FF' data bytes	RQ04_0101, RQ04_0201, RQ04_0409
3	Send Command with Secured Data to the ADF Remote File Management application, which contains: - SELECT: DF_{TESTB} - RESIZE FILE: EF_{XX} - SELECT: EF_{XX}. - READ BINARY	Response with Secured Data is returned last or only additional data response shall be '04 90 00' and contain all data of EF_{XX} starting with 'FF FF FF' data bytes	RQ04_0101, RQ04_0201, RQ04_0409
4	Send Command with Secured Data to the ADF Remote File Management application, which contains: - SELECT: DF_{TESTB}. - DELETE FILE: EF_{XX}	Response with Secured Data is returned last or only additional data response shall be '3 90 00'	RQ04_0101, RQ04_0201, RQ04_0409
5	Send Command with Secured Data to the ADF Remote File Management application, which contains: - SELECT: DF_{TESTB} - SELECT: EF_{XX}	Response with Secured Data is returned last or only additional data response shall be '02 6A 82'	RQ04_0101, RQ04_0201, RQ04_0409

6.4.3 RFM implementation over HTTPS

The content of this clause is FFS.

6.5 Remote Application Management (RAM)

6.5.1 DELETE

6.5.1.1 Test case 1: DELETE command

6.5.1.1.1 Initial Conditions

- Test application with AID1 have been successfully installed.

6.5.1.1.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the Test Application with AID1 which contains a command: - '00 01 00 00'	Response with Secured Data is returned to the sending entity containing '01 90 00'	RQ01_0002, RQ01_0004, RQ01_0007, RQ02_0201
2	Send Command with Secured Data to the ISD which contains: - DELETE with AID1 - GET RESPONSE	Response with Secured Data is returned to the sending entity containing '02 90 00' and contain '00' data byte	RQ01_0002, RQ01_0004, RQ01_0007 RQ05_0109 RQ05_0301 RQ05_0401
3	Send Command with Secured Data to the Test Application with AID1 which contains a command: • '00 01 00 00'	Response with Secured Data is returned to the sending entity containing SW = '6X XX' with Response Status Code in the additional data expected = '09' TAR unknown	RQ05_0101 RQ05_0401 RQ05_0402

6.5.2 SET STATUS

6.5.2.1 Test case 1: SET STATUS command within a command session

6.5.2.1.1 Initial Conditions

- Prepare for install of the Test Application with AID1 using the load() and install(for load) methods.

6.5.2.1.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install and make selectable] the Test Application with AID1 - SET STATUS to lock the applet with AID1	Response with Secured Data is returned to the sending entity containing '02 90 00'	RQ01_0002, RQ01_0004, RQ01_0007, RQ02_0201 RQ05_0501RQ05_0109 RQ05_0301

Step	Description	Expected Result	RQ
2	Send Command with Secured Data to the Test Application with AID1, which contains: - '00 01 00 00'	Response with Secured Data is returned to the sending entity containing SW = '6X XX' with Response Status Code in the additional data expected = '09' TAR unknown (see note)	RQ01_0002, RQ01_0004, RQ01_0007, RQ02_0201 RQ05_0501 RQ05_0109 RQ05_0301
NOTE: In case of HTTPS the response is "unknown application".			

6.5.3 INSTALL

6.5.3.1 INSTALL [for load]

6.5.3.1.1 Test case 1: INSTALL [for load] as a single command in the session

6.5.3.1.1.1 Initial Conditions

- None.

6.5.3.1.1.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD which contains: - INSTALL (for load) command with Load File AID1	Response with Secured Data is returned, last or only additional data response shall be '01 90 00 00'	RQ01_0007, RQ05_0101 RQ05_0109, RQ05_0301 RQ05_0302 RQ05_0601

6.5.3.1.2 Test case 2: INSTALL[for load] with memory management parameters

6.5.3.1.2.1 Initial Conditions

- None.

6.5.3.1.2.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the TAR of the ISD which contains: - INSTALL [for load] with Load File AID1 The System Specific parameters "Non volatile code space limit" (Tag 'C6'), "Volatile data space limit" (Tag 'C7') and "Non volatile data space limit" (Tag 'C8') should be set Params = 'EF 0C C6 02 FF FF C7 02 FF FF C8 02 FF FF' - LOAD	Response with Secured Data is returned, last or only additional data response shall be '02 90 00 00'	RQ05_0101 RQ05_0601 RQ05_0701, RQ05_0702, RQ05_0703
2	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install and make selectable] with AID1	Response with Secured Data is returned, last or only additional data response shall be '02 90 00 00'	RQ05_0101 RQ05_0605

Step	Description	Expected Result	RQ
3	Send Command with Secured Data to the Test Application with AID1 which contains: - '00 01 00 00'	Response with Secured Data is returned, last or only additional data response shall be '01 90 00'	RQ05_0101 RQ05_0701

6.5.3.2 INSTALL [for install]

6.5.3.2.1 Test case 1: INSTALL[for install] with SIM File Access and Toolkit Application Specific Parameters

6.5.3.2.1.1 Initial Conditions

- Prepare for install of the 'Test Application AID2' using the load() and install(for load) methods.

6.5.3.2.1.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID2 The "SIM File Access and Toolkit Application Specific Parameters" TLV object (Tag 'CA') included in the "System Specific Parameters" (Tag 'EF') should be set. The MSL length should be set to '00'. Params = 'EF 1A C8 02 FF FF C7 02 FF FF CA 10 01 FF 01 00 10 02 01 01 03 02 00 00 03 TAR006' - INSTALL[for make selectable] with AID2	Response with Secured Data is returned, last or only additional data response shall be '02 90 00 00'	RQ01_0007, RQ05_0109, RQ05_0101 RQ05_0601 RQ05_0801 RQ05_0802 RQ05_0901 RQ05_0902 RQ05_0903
2	Send Command with Secured Data to the Test Application with AID2 which contains: - '00 01 00 00'	Response with Secured Data is returned, last or only additional data response shall be '01 90 00'	RQ05_0601 RQ05_0803 RQ05_0802 RQ05_0901

6.5.3.2.2 Test case 2: INSTALL[for install] with UICC System Specific Parameters and SIM File Access and Toolkit Application Specific Parameters

6.5.3.2.2.1 Initial Conditions

- Prepare for install of the 'Test Application AID4' using the load() and install(for load) methods.

6.5.3.2.2.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: INSTALL[for install] with AID4 The UICC System Specific Parameters (Tag 'EA') and the "SIM File Access and Toolkit Application Specific Parameters" TLV object (Tag 'CA') should be set: Params = 'EF 1A C8 02 FFFF C7 02 FFFF CA 10 01 FF 01 00 10 02 01 01 03 02 00 00 03 TAR010 EA 11 80 0F 01 00 10 02 0101 0302 00 00 03 TAR010 00' INSTALL[for make selectable] with AID20	Response with Secured Data is returned, last or only additional data response shall be '01 6A 80'	RQ05_0901 RQ05_0902 RQ05_0903 RQ05_1001 RQ05_1101 RQ05_1102 RQ05_1104
2	Send Command with Secured Data to the Test Application with AID4 which contains: - '00 01 00 00'	SW = '6X XX' with Response Status Code in the additional data expected = '09' TAR unknown (CAT-TP/SMS), or "unknown application" (HTTPS)	RQ05_1001

6.5.3.2.3 Test case 3: INSTALL[for install] with UICC System Specific Parameter "UICC Toolkit Application specific parameters field"

6.5.3.2.3.1 Initial Conditions

- Prepare for install of the 'Test Application AID3' using the load() and install(for load) methods.

6.5.3.2.3.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID3 The UICC System Specific Parameter "UICC Toolkit Application specific parameters field" (Tag '80') should be set. The MSL length should be set to '00': Params = 'EF 08 C8 02 FF FF C7 02 FF FF EA 11 80 0F 01 00 10 02 01 01 03 02 00 00 03 TAR008 00' - INSTALL[for make selectable] with AID3	Response with Secured Data is returned, last or only additional data response shall be '02 90 00 00'	RQ05_0801 RQ05_0802 RQ05_0807 RQ05_1002 RQ05_1101 RQ05_1102 RQ05_1104 RQ05_1601
2	Send Command with Secured Data to the Test Application with AID3 which contains: - '00 01 00 00'	Response with Secured Data is returned, last or only additional data response shall be '01 90 00'	RQ05_1101

6.5.3.2.4 Test case 4: INSTALL[for install] with UICC System Specific Parameter "UICC Access Application specific parameters field"

6.5.3.2.4.1 Initial Conditions

- Prepare for install of the 'Test Application AID8' using the load() and install(for load) methods.

6.5.3.2.4.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID8 The UICC System Specific Parameter "UICC Access Application specific parameters field" (Tag '81') should be set: Params = 'EA 13 80 0B 01 00 10 00 00 00 03 TAR014 00 81 04 00 01 FF 00' - INSTALL[for make selectable] with AID8	Response with Secured Data is returned, last or only additional data response shall be '02 90 00 00'	RQ05_1002 RQ05_1201 RQ05_1202
2	Send Command with Secured Data to the Test Application with AID8 which contains: - '00 01 00 00'	Response with Secured Data is returned, last or only additional data response shall be '01 90 00'	RQ05_1201

6.5.3.2.5 Test case 5: INSTALL[for install] with UICC System Specific Parameter "UICC Administrative Access Application specific parameters field"

6.5.3.2.5.1 Initial Conditions

- Prepare for install of the 'Test Application AID5' using the load() and install(for load) methods.

6.5.3.2.5.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data coded as Compact Remote command structure to the ISD, which contains: - INSTALL[for install] with AID5 The UICC System Specific Parameter "UICC Administrative Access Application specific parameters field" (Tag '82') should be set: Params = 'EA 13 80 0B 01 00 10 00 00 00 03 TAR011 00 82 04 00 01 FF 00' - INSTALL[for make selectable] with AID5	Response with Secured Data is returned, last or only additional data response shall be '02 90 00 00'	RQ05_1002 RQ05_1401 RQ05_1402
2	Send Command with Secured Data to the Test Application with AID5 which contains: - '00 01 00 00'	Response with Secured Data is returned, last or only additional data response shall be '01 90 00'	RQ05_1401

6.5.3.2.6 Test case 6: INSTALL[for install] with UICC System Specific Parameter "UICC Access Application specific parameters field" and "UICC Administrative Access Application specific parameters field" for the same ADF

6.5.3.2.6.1 Initial Conditions

- Prepare for install of the 'Test Application AID18' using the load() and install(for load) methods.

6.5.3.2.6.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID18 The UICC System Specific Parameter "UICC Access Application specific parameters field" (Tag '81') and "UICC Administrative Access Application specific parameters field" (Tag '82') should be set: Params = 'EA 34 80 0B 01 00 10 00 00 00 03 TAR022 00 81 13 10 A0000000090005FFFFFFFF89E0000002 01 00 00 82 13 10 A0000000090005FFFFFFFF89E0000002 01 00 00' - INSTALL[for make selectable] with AID18	Response with Secured Data is returned, last or only additional data response shall be '02 90 00 00'	RQ05_1003 RQ05_1201 RQ05_1202 RQ05_1401 RQ05_1402
2	Send Command with Secured Data to the Test Application with AID18 with: - '00 01 00 00'	Response with Secured Data is returned, last or only additional data response shall be '01 90 00'	RQ05_1003
3	Send Command with Secured Data coded as [Compact Remote command structure] to the ADF Remote File Management application, which contains: - SELECT: DF_{TESTB} - SELECT: EF_{TARUB} - UPDATE BINARY with data '01 01 01'	Response with Secured Data is returned, last or only additional data response shall be '03 90 00' with response data containing all data of EF_{TARUB} starting with '01 01 01' until the end of file	RQ05_1003

6.5.3.2.7 Test case 7: INSTALL[for install] with UICC System Specific Parameter "UICC Access Application specific parameters field" and "UICC Administrative Access Application specific parameters field" for the same UICC file system

6.5.3.2.7.1 Initial Conditions

- Prepare for install of the 'Test Application AID18' using the load() and install(for load) methods

6.5.3.2.7.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the TAR value of the ISD, which contains: - INSTALL[for install] with AID18 The UICC System Specific Parameter "UICC Access Application specific parameters field" (Tag '81') and "UICC Administrative Access Application specific parameters field" (Tag '82') should be set: Params = 'EA 19 80 0B 01 00 10 00 00 00 03 TAR022 00 81 04 00 01 00 00 82 04 00 01 00 00' - INSTALL[for make selectable] with AID18	Response with Secured Data is returned, last or only additional data response shall be '02 90 00 00'	RQ05_1004 RQ05_1201 RQ05_1202 RQ05_1401 RQ05_1402
2	Send Command with Secured Data to the Test Application with AID18 with: - '00 01 00 00'	Response with Secured Data is returned, last or only additional data response shall be '01 90 00'	RQ05_1004
3	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TARU} - READ BINARY with P3/Le = '00'	Response with Secured Data is returned, last or only additional data response shall be '03 90 00' with response data containing all data of EF_{TARU} starting with '01 01 01' until the end of file.	RQ05_1004

6.5.3.2.8 Test case 8: INSTALL[for install] with the maximum number of timers required for SIM Toolkit Application Specific Parameters set too high ('09')

6.5.3.2.8.1 Initial Conditions

- Prepare for install of the 'Test Application AID2' using the load() and install(for load) methods.

6.5.3.2.8.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID2 The maximum number of timers required for Toolkit Application Specific Parameters should be set to '09': Params = 'EF 12 CA 10 01 FF 01 09 10 02 01 01 03 02 00 00 03 TAR006' - INSTALL[for make selectable] with AID2	Response with Secured Data is returned, last or only additional data response shall be '01 6A 80'	RQ05_0901 RQ05_0902 RQ05_0903 RQ05_1501
2	Send Command with Secured Data to the Test Application with AID2 which contains: - '00 01 00 00'	Response with Secured Data is returned: SW = '6X XX' with Response Status Code in the additional data expected = '09' TAR unknown (CAT-TP/SMS), or "unknown application" (HTTPS)	RQ05_1501

6.5.3.2.9 Test case 9: INSTALL[for install] with the maximum number of timers required for UICC Toolkit Application Specific Parameters set too high ('09')

6.5.3.2.9.1 Initial Conditions

- Prepare for install of the 'Test Application AID3' using the load() and install(for load) methods.

6.5.3.2.9.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID3 The maximum number of timers required for Toolkit Application Specific Parameters should be set to '09': Params = 'EA 11 80 0F 01 09 10 02 0101 0302 00 00 03 TAR008 00' - INSTALL[for make selectable] with AID3	Response with Secured Data is returned, last or only additional data response shall be '01 6A 80'	RQ05_1101 RQ05_1102 RQ05_1104 RQ05_1501
2	Send Command with Secured Data to the Test Application with AID3 which contains: - '00 01 00 00'	Response with Secured Data is returned: SW = '6X XX' with Response Status Code in the additional data expected = '09' TAR unknown (CAT-TP/SMS), or "unknown application" (HTTPS)	RQ05_1501

6.5.3.2.10 Test case 10: INSTALL[for install] with the maximum number of channels required for SIM Toolkit Application Specific Parameters set too high ('08')

6.5.3.2.10.1 Initial Conditions

- Prepare for install of the 'Test Application AID2' using the load() and install(for load) methods.

6.5.3.2.10.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID2 The maximum number of channels required for Toolkit Application Specific Parameters should be set to '08': Params = 'EF 12 CA 10 01 FF 01 00 10 02 01 01 03 02 00 08 03 TAR006' - INSTALL[for make selectable] with AID2	Response with Secured Data is returned, last or only additional data response shall be '01 6A 80'	RQ05_0901 RQ05_0902 RQ05_0903 RQ05_1502
2	Send Command with Secured Data to the Test Application with AID2 which contains: - '00 01 00 00'	Response with Secured Data is returned: SW = '6X XX' with Response Status Code in the additional data expected = '09' TAR unknown (CAT-TP/SMS), or "unknown application" (HTTPS)	RQ05_1502

6.5.3.2.11 Test case 11: INSTALL[for install] with the maximum number of channels required for UICC Toolkit Application Specific Parameters set too high ('08')

6.5.3.2.11.1 Initial Conditions

- Prepare for install of the 'Test Application AID3' using the load() and install(for load) methods.

6.5.3.2.11.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID3 The maximum number of channels required for Toolkit Application Specific Parameters should be set to '08': Params = 'EA 11 80 0F 01 00 10 02 0101 0302 08 00 03 TAR008 00' - INSTALL[for make selectable] with AID3	Response with Secured Data is returned, last or only additional data response shall be '01 6A 80'	RQ05_1101 RQ05_1102 RQ05_1104 RQ05_1502
2	Send Command with Secured Data to the Test Application with AID3 which contains: - '00 01 00 00'	Response with Secured Data is returned: SW = '6X XX' with Response Status Code in the additional data expected = '09' TAR unknown (CAT-TP/SMS), or "unknown application" (HTTPS)	RQ05_1502

6.5.3.2.12 Test case 12: INSTALL[for install] with the maximum number of services required for UICC Toolkit Application Specific Parameters set too high ('09')

6.5.3.2.12.1 Initial Conditions

- Prepare for install of the 'Test Application AID3' using the load() and install(for load) methods.

6.5.3.2.12.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID3 The maximum number of services required for Toolkit Application Specific Parameters should be set to '09': Params = 'EA 11 80 0F 01 00 10 02 0101 0302 08 00 03 TAR008 09' - INSTALL[for make selectable] with AID3	Response with Secured Data is returned, last or only additional data response shall be '01 6A 80'	RQ05_1101 RQ05_1102 RQ05_1104 RQ05_1503
2	Send Command with Secured Data to the Test Application with AID3 which contains: - '00 01 00 00'	Response with Secured Data is returned: SW = '6X XX' with Response Status Code in the additional data expected = '09' TAR unknown (CAT-TP/SMS), or "unknown application" (HTTPS)	RQ05_1503

6.5.3.2.13 Test case 13: INSTALL[for install] with requested item identifier for SIM Toolkit Application Specific Parameters set to '128'

6.5.3.2.13.1 Initial Conditions

- Prepare for install of the 'Test Application AID2' using the load() and install(for load) methods.

6.5.3.2.13.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID2 The requested item identifier for Toolkit Application Specific Parameters should be set to '128': Params = 'EF 1A C8 02 FFFF C7 02 FFFF CA 10 01 FF 01 00 10 02 01 01 03 80 00 00 03 TAR006' - INSTALL[for make selectable] with AID2	Response with Secured Data is returned, last or only additional data response shall be '01 6X XX' (6X XX is error SW)	RQ05_0901 RQ05_0902 RQ05_0903 RQ05_1506
2	Send Command with Secured Data to the Test Application with AID2which contains: - '00 01 00 00'	Response with Secured Data is returned: SW = '6X XX' with Response Status Code in the additional data expected = '09' TAR unknown (CAT-TP/SMS), or "unknown application" (HTTPS)	RQ05_1506

6.5.3.2.14 Test case 14: INSTALL[for install] with requested item identifier for UICC Toolkit Application Specific Parameters set to '128'

6.5.3.2.14.1 Initial Conditions

- Prepare for install of the 'Test Application AID3' using the load() and install(for load) methods.

6.5.3.2.14.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID3 The requested item identifier for Toolkit Application Specific Parameters should be set to '128': Params = 'EA 11 80 0F 01 00 10 02 0101 03 80 00 00 03 TAR008 00' - INSTALL[for make selectable] with AID3	Response with Secured Data is returned, last or only additional data response shall be '01 6X XX' (6X XX is error SW)	RQ05_1101 RQ05_1102 RQ05_1104 RQ05_1506
2	Send Command with Secured Data to the Test Application with AID3which contains: - '00 01 00 00'	Response with Secured Data is returned: SW = '6X XX' with Response Status Code in the additional data expected = '09' TAR unknown (CAT-TP/SMS), or "unknown application" (HTTPS)	RQ05_1506

6.5.3.2.15 Test case 15: INSTALL[for install] with Minimum Security Level field of SIM Toolkit Application different from zero

6.5.3.2.15.1 Initial Conditions

- Prepare for install of the 'Test Application AID2' using the load() and install(for load) methods.

6.5.3.2.15.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID2 MSL field should be set to '0102': Params = 'EF 1C C8 02 FFFF C7 02 FFFF CA 12 01 FF 01 00 10 02 01 01 03 02 00 02 0101 03 TAR006' - INSTALL[for make selectable] with AID2	Response with Secured Data is returned, last or only additional data response shall be '02 90 00 00'	RQ05_1602 RQ05_1701 RQ05_1801 RQ05_1802
2	Send Command with Secured Data with SPI1 set to '02' to the Test Application with AID2 with: - '00 01 00 00'	Response with Secured Data is returned, last or only additional data response shall be '01 90 00'	RQ05_1802 RQ03_0104

6.5.3.2.16 Test case 16: INSTALL[for install] with Minimum Security Level field of UICC Toolkit Application different from zero

6.5.3.2.16.1 Initial Conditions

- Prepare for install of the 'Test Application AID3' using the load() and install(for load) methods.

6.5.3.2.16.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID3 MSL field should be set to '0102': Params = 'EA 11 80 0F 01 00 10 02 0101 0302 00 02 0101 03 TAR008 00' - INSTALL[for make selectable] with AID3	Response with Secured Data is returned, last or only additional data response shall be '02 90 00 00'	RQ05_1602 RQ05_1701 RQ05_1801 RQ05_1802
2	Send Command with Secured Data with SPI1 set to '02' to the Test Application with AID3 with: - '00 01 00 00'	Response with Secured Data is returned, last or only additional data response shall be '01 90 00'	RQ05_1802 RQ03_0104

6.5.3.2.17 Test case 17: INSTALL[for install] with Minimum Security Level field of SIM Toolkit Application different from SPI1

6.5.3.2.17.1 Initial Conditions

- Prepare for install of the 'Test Application AID2' using the load() and install(for load) methods.

6.5.3.2.17.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID2 MSL field should be set to '0106': Params = 'EF 1C C8 02 FF FF C7 02 FF FF CA 12 01 FF 01 00 10 02 01 01 03 02 00 02 0101 03 TAR006' - INSTALL[for make selectable] with AID2	Response with Secured Data is returned, last or only additional data response shall be '02 90 00 00'	RQ05_1602 RQ05_1701 RQ05_1801 RQ05_1802
2	Send Command with Secured Data with SPI1 set to '02' to the Test Application with AID2 with: - '00 01 00 00'	Response with Secured Data is returned: SW = '6X XX' with Response Status Code in the additional data expected = '0A' 'Insufficient Security Level'	RQ05_1802 RQ03_0102

6.5.3.2.18 Test case 18: INSTALL[for install] with Minimum Security Level field of UICC Toolkit Application different from SPI1

6.5.3.2.18.1 Initial Conditions

- Prepare for install of the 'Test Application AID3' using the load() and install(for load) methods.

6.5.3.2.18.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID3 MSL field should be set to '0106': Params = 'EA 11 80 0F 01 00 10 02 0101 0302 00 02 0101 03 TAR008 00' - INSTALL[for make selectable] with AID3	Response with Secured Data is returned, last or only additional data response shall be '02 90 00 00'	RQ05_1602 RQ05_1701 RQ05_1801 RQ05_1802

Step	Description	Expected Result	RQ
2	Send Command with Secured Data with SPI1 set to '02' to the Test Application with AID3 with: - '00 01 00 00'	Response with Secured Data is returned: SW = '6X XX' with Response Status Code in the additional data expected = '0A' 'Insufficient Security Level'	RQ05_1802 RQ03_0102

6.5.3.2.19 Test case 19: INSTALL[for install] SIM Toolkit Applications with Access Domain Parameter equal to '00' and 'FF'

6.5.3.2.19.1 Initial Conditions

- Prepare for install of the 'Test Application AID6' and 'Test Application AID7' using the load() and install(for load) methods.

6.5.3.2.19.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID6 The Access Domain Parameter should be set to '00': Params = 'EF 15 C8 02 FF FF C7 02 FF FF CA 0B 01 00 01 00 10 00 00 03 TAR012' - INSTALL[for make selectable] with AID6	Response with Secured Data is returned, last or only additional data response shall be '02 90 00 00'	RQ05_0901 RQ05_0903 RQ05_1901 RQ05_2001 RQ05_2004
2	Send Command with Secured Data to the Test Application with AID6 with: - '00 01 00 00'	Response with Secured Data is returned, last or only additional data response shall be '01 90 00'	RQ05_2001
3	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TARU} - READ BINARY with P3/Le = '00'	Response with Secured Data is returned, last or only additional data response shall be '03 90 00' with response data containing all data of EF_{TARU} starting with '01 01 01' until the end of file	RQ05_2001
4	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID7 The Access Domain Parameter should be set to 'FF': Params = 'EF 15 C8 02 FF FF C7 02 FF FF CA 0B 01 FF 01 00 10 00 00 03 TAR013' - INSTALL[for make selectable] with AID7	Response with Secured Data is returned, last or only additional data response shall be '02 90 00 00'	RQ05_2004
5	Send Command with Secured Data to the Test Application with AID7 with: - '00 02 00 00'	Response with Secured Data is returned, last or only additional data response shall be '01 90 00'	RQ05_2004
6	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TARU} - READ BINARY with P3/Le = '00'	Response with Secured Data is returned, last or only additional data response shall be '03 90 00' with response data containing all data of EF_{TARU} starting with '01 01 01' until the end of file	RQ05_2004 RQ03_0202

6.5.3.2.20 Test case 20: INSTALL[for install] UICC Toolkit Applications with Access Domain Parameter equal to '00' and 'FF'

6.5.3.2.20.1 Initial Conditions

- Prepare for install of the 'Test Application AID8' and 'Test Application AID9' using the load() and install(for load) methods.

6.5.3.2.20.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID8 The Access Domain Parameter should be set to '00': Params = 'EA 13 80 0B 01 00 10 00 00 00 03 TAR014 00 81 04 00 01 00 00' - INSTALL[for make selectable] with AID8	Response with Secured Data is returned, last or only additional data response shall be '02 90 00 00'	RQ05_1201 RQ05_1202 RQ05_1901 RQ05_2001 RQ05_2004
2	Send Command with Secured Data to the Test Application with AID8 with: • - '00 01 00 00'	Response with Secured Data is returned, last or only additional data response shall be '01 90 00'	RQ05_2001
3	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: • - SELECT: DF_{TEST} • - SELECT: EF_{TARU} • - READ BINARY with P3/Le = '00'	Response with Secured Data is returned, last or only additional data response shall be '03 90 00' with response data containing all data of EF_{TARU} starting with '01 01 01' until the end of file	RQ05_2001
4	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID9 **The Access Domain Parameter should be set to 'FF':** **Params = 'EA 13** **80 0B 01 00 10 00 00 00 03 TAR015 00** **81 04 00 01 FF 00'** - INSTALL[for make selectable] with AID9	Response with Secured Data is returned, last or only additional data response shall be '02 90 00 00'	RQ05_2004
5	Send Command with Secured Data to the Test Application with AID9 with: • - '00 02 00 00'	Response with Secured Data is returned, last or only additional data response shall be '01 90 00'	RQ05_2004
6	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: • - SELECT: DF_{TEST} • - SELECT: EF_{TARU} • - READ BINARY with P3/Le = '00'	Response with Secured Data is returned, last or only additional data response shall be '03 90 00' with response data containing all data of EF_{TARU} starting with '01 01 01' until the end of file.	RQ05_2004 RQ03_0202

6.5.3.2.21 Test case 21: INSTALL[for install] SIM Toolkit Application with Access Domain Parameter equal to '00' and access condition set to 'NEVER'

6.5.3.2.21.1 Initial Conditions

- Prepare for install of the 'Test Application AID6' using the load() and install(for load) methods.

6.5.3.2.21.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID6 The Access Domain Parameter should be set to '00': Params = 'EF 15 C8 02 FF FF C7 02 FF FF CA 0B 01 00 01 00 10 00 00 03 TAR012' - INSTALL[for make selectable] with AID6	Response with Secured Data is returned, last or only additional data response shall be '02 90 00 00'	RQ05_0901 RQ05_0903 RQ05_1901 RQ05_2002 RQ05_2003 RQ05_2005
2	Send Command with Secured Data to the Test Application with AID6 with: - '00 03 00 00'	Response with Secured Data is returned, last or only additional data response shall be '01 90 00'	RQ05_2005
3	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: EF_{TNU} - READ BINARY with P3/Le = '00'	Response with Secured Data is returned, last or only additional data response shall be '03 90 00 55 55 55' containing all data of EF_{TNU}	RQ05_2005 RQ03_0202

6.5.3.2.22 Test case 22: INSTALL[for install] UICC Toolkit Application with Access Domain Parameter equal to '00' and access condition set to 'NEVER'

6.5.3.2.22.1 Initial Conditions

- Prepare for install of the 'Test Application AID8' using the load() and install(for load) methods.

6.5.3.2.22.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID8 The Access Domain Parameter should be set to '00': Params = 'EA 13 80 0B 01 00 10 00 00 00 03 TAR014 00 81 04 00 01 00 00' - INSTALL[for make selectable] with AID8	Response with Secured Data is returned, last or only additional data response shall be '02 90 00 00'	RQ05_1201 RQ05_1202 RQ05_2002 RQ05_2003 RQ05_2005
2	Send Command with Secured Data to the Test Application with AID8 with: - '00 03 00 00'	Response with Secured Data is returned, last or only additional data response shall be '01 90 00'	RQ05_2005
3	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TNU} - READ BINARY with P3/Le = '00'	Response with Secured Data is returned, last or only additional data response shall be '03 90 00 55 55 55' containing all data of EF_{TNU}	RQ05_2005 RQ03_0202

6.5.3.2.23 Test case 23: INSTALL[for install] SIM Toolkit Application with Access Domain Parameter not supported

6.5.3.2.23.1 Initial Conditions

- Prepare for install of the 'Test Application AID2' using the load() and install(for load) methods.

6.5.3.2.23.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID2 The Access Domain Parameter should be set to '02' and the Access Domain Data should be set to '0000F4': Params = 'EF 18 C8 02 FF FF C7 02 FF FF CA 0E 04 02 00 00 F4 01 00 10 00 00 03 TAR012' - INSTALL[for make selectable] with AID6	Response with Secured Data is returned, last or only additional data response shall be '01 6A 80'	RQ05_0901 RQ05_0903 RQ05_2006
2	Send Command with Secured Data to the Test Application with AID2 which contains: - '00 01 00 00'	Response with Secured Data is returned: SW = '6X XX' with Response Status Code in the additional data expected = '09' TAR unknown (CAT-TP/SMS), or "unknown application" (HTTPS)	RQ05_2006 RQ03_0202

6.5.3.2.24 Test case 24: INSTALL[for install] UICC Toolkit Application with Access Domain Parameter not supported

6.5.3.2.24.1 Initial Conditions

- Prepare for install of the 'Test Application AID8' using the load() and install(for load) methods.

6.5.3.2.24.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID8 The Access Domain Parameter should be set to '01': Params = 'EA 13 80 0B 01 00 10 00 00 00 03 TAR014 00 81 04 00 01 01 00' - INSTALL[for make selectable] with AID8	Response with Secured Data is returned, last or only additional data response shall be '01 6A 80'	RQ05_1201 RQ05_1202 RQ05_2006
2	Send Command with Secured Data to the Test Application with AID8 which contains: - '00 01 00 00'	SW = '6X XX' with Response Status Code in the additional data expected = '09' TAR unknown (CAT-TP/SMS), or "unknown application" (HTTPS)	RQ05_2006 RQ03_0202

6.5.3.2.25 Test case 25: INSTALL[for install] UICC Toolkit Application with Access Domain Parameter equal to '02'

6.5.3.2.25.1 Initial Conditions

- Prepare for install of the 'Test Application AID8' using the load() and install(for load) methods.

6.5.3.2.25.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID8 The Access Domain Parameter should be set to '02' , the Access Domain Data should be set to '0000F4': Params = 'EA 16 80 0B 01 00 10 00 00 00 03 TAR014 00 81 07 00 04 02 00 00 F4 00' - INSTALL[for make selectable] with AID8	Response with Secured Data is returned, last or only additional data response shall be '02 90 00 00'	RQ05_1201 RQ05_1202 RQ05_2101
2	Send Command with Secured Data to the Test Application with AID8 with: - '00 01 00 00'	Response with Secured Data is returned, last or only additional data response shall be '01 90 00'	RQ05_2101
3	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TARU} - READ BINARY with P3/Le = '00'	Response with Secured Data is returned, last or only additional data response shall be '03 90 00' with response data containing all data of EF_{TARU} starting with '01 01 01' until the end of file	RQ05_2101 RQ03_0202

6.5.3.2.26 Test case 26: INSTALL[for install] SIM Toolkit Applications with Access Domain Parameter equal to '00' - independency from the PIN status at UICC-Terminal interface

6.5.3.2.26.1 Initial Conditions

- Prepare for install of the 'Test Application AID6' using the load() and install(for load) methods.

6.5.3.2.26.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID6 The Access Domain Parameter should be set to '00': Params = 'EF 15 C8 02 FF FF C7 02 FF FF CA 0B 01 00 01 00 10 00 00 03 TAR012' - INSTALL[for make selectable] with AID6	Response with Secured Data is returned, last or only additional data response shall be '02 90 00 00'	RQ05_0901 RQ05_0903 RQ05_2002 RQ05_2003
2	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TUACP} - VERIFY PIN with PIN = '30 30 30 30 FF FF FF FF'	Response with Secured Data is returned, last or only additional data response shall be '03 63 C2'	RQ05_2002 RQ05_2003
3	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TUACP} - VERIFY PIN with PIN = '30 30 30 30 FF FF FF FF'	Response with Secured Data is returned, last or only additional data response shall be '03 63 C1'	RQ05_2002 RQ05_2003
4	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TUACP} - VERIFY PIN with PIN = '30 30 30 30 FF FF FF FF'	Response with Secured Data is returned, last or only additional data response shall be '03 63 C0'	RQ05_2002 RQ05_2003

Step	Description	Expected Result	RQ
5	Send Command with Secured Data to the Test Application with AID6 with: - '00 04 00 00'	Response with Secured Data is returned, last or only additional data response shall be '01 90 00'	RQ05_2002 RQ05_2003
6	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TUACP} - READ BINARY with P3/Le = '00'	Response with Secured Data is returned, last or only additional data response shall be '03 90 00' with response data containing all data of EF_{TUACP} starting with '01 01 01' until the end of file	RQ05_2002 RQ05_2003 RQ03_0201 RQ03_0202

6.5.3.2.27 Test case 27: INSTALL[for install] UICC Toolkit Applications with Access Domain Parameter equal to '00' - independency from the PIN status at UICC-Terminal interface

6.5.3.2.27.1 Initial Conditions

- Prepare for install of the 'Test Application AID8' using the load() and install(for load) methods.

6.5.3.2.27.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID8 The Access Domain Parameter should be set to '00': Params = 'EA 13 80 0B 01 00 10 00 00 00 03 TAR014 00 81 04 00 01 00 00' - INSTALL[for make selectable] with AID8	Response with Secured Data is returned, last or only additional data response shall be '02 90 00 00'	RQ05_1201 RQ05_1202 RQ05_2002 RQ05_2003
2	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TUACP} - VERIFY PIN with PIN = '30 30 30 30 FF FF FF FF'	Response with Secured Data is returned, last or only additional data response shall be '03 63 C2'	RQ05_2002 RQ05_2003
3	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TUACP} - VERIFY PIN with PIN = '30 30 30 30 FF FF FF FF'	Response with Secured Data is returned, last or only additional data response shall be '03 63 C1'	RQ05_2002 RQ05_2003
4	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TUACP} - VERIFY PIN with PIN = '30 30 30 30 FF FF FF FF'	Response with Secured Data is returned, last or only additional data response shall be '03 63 C0'	RQ05_2002 RQ05_2003
5	Send Command with Secured Data to the Test Application with AID8 with: - '00 04 00 00'	Response with Secured Data is returned, last or only additional data response shall be '01 90 00'	RQ05_2002 RQ05_2003
6	Send Command with Secured Data to the UICC Shared File System Remote File Management application, which contains: - SELECT: DF_{TEST} - SELECT: EF_{TUACP} - READ BINARY with P3/Le = '00'	Response with Secured Data is returned, last or only additional data response shall be '03 90 00' with response data containing all data of EF_{TUACP} starting with '01 01 01' until the end of file	RQ05_2002 RQ05_2003 RQ03_0201 RQ03_0202

6.5.3.2.28 Test case 28: INSTALL[for install] of SIM Toolkit Applications with different Priority levels

6.5.3.2.28.1 Initial Conditions

- Prepare for install of the 'Test Application AID10' using the load() and install(for load) methods.

6.5.3.2.28.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID10 The Priority level should be set to '01': Params = 'EF 15 C8 02 FF FF C7 02 FF FF CA 0B 01 FF 01 00 10 00 00 03 TAR016' - INSTALL[for make selectable] with AID10	Response with Secured Data is returned, last or only additional data response shall be '02 90 00 00'	RQ05_0901 RQ05_0903 RQ05_2301 RQ05_2303
2	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID11 The Priority level should be set to 'FF': Params = 'EF 15 C8 02 FF FF C7 02 FF FF CA 0B 01 FF FF 00 10 00 00 03 TAR017' - INSTALL[for make selectable] with AID11	Response with Secured Data is returned, last or only additional data response shall be '02 90 00 00'	RQ05_2301
3	Start Proactive Session: Check Activation Priority	AID10 is triggered before AID11	RQ05_2301

6.5.3.2.29 Test case 29: INSTALL[for install] of UICC Toolkit Applications with different Priority levels

6.5.3.2.29.1 Initial Conditions

- install(for load) method for 'Test Application AID12' and 'Test Application AID13' is performed successfully.

6.5.3.2.29.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID12 The Priority level should be set to '01': Params = 'EA 0D 80 0B 01 00 10 00 00 00 03 TAR018 00' - INSTALL[for make selectable] with AID12	Response with Secured Data is returned, last or only additional data response shall be '02 90 00 00'	RQ05_1101 RQ05_1102 RQ05_1104 RQ05_2301 RQ05_2303
2	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID13 The Priority level should be set to 'FF': Params = 'EA 0D 80 0B FF 00 10 00 00 00 03 TAR019 00' - INSTALL[for make selectable] with AID13	Response with Secured Data is returned, last or only additional data response shall be '02 90 00 00'	RQ05_2301
3	Start Proactive Session: Check Activation Priority	AID12 is triggered before AID13	RQ05_2301

6.5.3.2.30 Test case 30: INSTALL[for install] SIM Toolkit Applets with same Priority levels

6.5.3.2.30.1 Initial Conditions

- Prepare for install of the 'Test Application AID10' and 'Test Application AID11' using the load() and install(for load) methods.

6.5.3.2.30.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID10 The Priority level should be set to '01': Params = 'EF 15 C8 02 FF FF C7 02 FF FF CA 0B 01 FF 01 00 10 00 00 03 TAR016' - INSTALL[for make selectable] with AID10	Response with Secured Data is returned, last or only additional data response shall be '02 90 00 00'	RQ05_0901 RQ05_0903 RQ05_2302
2	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID11 The Priority level should be set to '01': Params = 'EF 15 C8 02 FF FF C7 02 FF FF CA 0B 01 FF 01 00 10 00 00 03 TAR017' - INSTALL[for make selectable] with AID11	Response with Secured Data is returned, last or only additional data response shall be '02 90 00 00'	RQ05_2302
3	Start Proactive Session: Check Activation Priority	AID10 is triggered before AID11	RQ05_2302

6.5.3.2.31 Test case 31: INSTALL[for install] UICC Toolkit Applets with same Priority levels

6.5.3.2.31.1 Initial Conditions

- Prepare for install of the 'Test Application AID12' and 'Test Application AID13' using the load() and install(for load) methods.

6.5.3.2.31.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID12 The Priority level should be set to '01': Params = 'EA 0D 80 0B 01 00 10 00 00 00 03 TAR018 00' - INSTALL[for make selectable] with AID12	Response with Secured Data is returned, last or only additional data response shall be '02 90 00 00'	RQ05_1101 RQ05_1102 RQ05_1104 RQ05_2302
2	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID13 The Priority level should be set to '01': Params = 'EA 0D 80 0B 01 00 10 00 00 00 03 TAR019 00' - INSTALL[for make selectable] with AID13	Response with Secured Data is returned, last or only additional data response shall be '02 90 00 00'	RQ05_2302
3	Start Proactive Session: Check Activation Priority	AID12 is triggered before AID13	RQ05_2302

6.5.3.2.32 Test case 32: INSTALL[for install] two SIM Toolkit Applications with identical TAR value

6.5.3.2.32.1 Initial Conditions

- Prepare for install of the 'Test Application AID2' and 'Test Application AID14' using the load() and install(for load) methods.

6.5.3.2.32.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID2 TAR026 value should be set: Params = 'EF 1A C8 02 FF FF C7 02 FF FF CA 10 01 FF 01 00 10 02 0101 0302 00 00 03 TAR026' - INSTALL[for make selectable] with AID2	Response with Secured Data is returned, last or only additional data response shall be '02 90 00 00'	RQ05_0901 RQ05_0902 RQ05_0903 RQ05_2401 RQ05_2405
2	Send Command with Secured Data to the Test Application with TAR006 , with: - '00 01 00 00'	Response with Secured Data is returned: SW = '6X XX' with Response Status Code in the additional data expected = '09' TAR unknown (CAT-TP/SMS) or "unknown application" (HTTPS)	RQ05_2405
3	Send Command with Secured Data to the Test Application with TAR026 , with: - '00 01 00 00'	Response with Secured Data is returned, last or only additional data response shall be '01 90 00'	RQ05_2405
4	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID14 TAR026 value should be set: Params = 'EF 1A C8 02 FF FF C7 02 FF FF CA 10 01 FF 01 00 10 02 0101 0302 00 00 03 TAR026' - INSTALL[for make selectable] with AID14	Response with Secured Data is returned, last or only additional data response shall be '01 6A 80'	RQ05_2406
5	Send Command with Secured Data to the Test Application with AID14 which contains: - '00 01 00 00'	Response with Secured Data is returned: SW = '6X XX' with Response Status Code in the additional data expected = '09' TAR unknown (CAT-TP/SMS), or "unknown application" (HTTPS)	RQ05_2406

6.5.3.2.33 Test case 33: INSTALL[for install] two UICC Toolkit Application with identical TAR value

6.5.3.2.33.1 Initial Conditions

- Prepare for install of the 'Test Application AID3' and 'Test Application AID15' using the load() and install(for load) methods.

6.5.3.2.33.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID3 TAR028 value should be set: Params = 'EA 11 80 0F 01 00 10 02 0101 0302 00 00 03 TAR028 00' - INSTALL[for make selectable] with AID3	Response with Secured Data is returned, last or only additional data response shall be '02 90 00 00'	RQ05_1101 RQ05_1102 RQ05_1104 RQ05_2401 RQ05_2403 RQ05_2405

Step	Description	Expected Result	RQ
2	Send Command with Secured Data to the Test Application with TAR008 , with: - '00 01 00 00'	Response with Secured Data is returned: SW = '6X XX' with Response Status Code in the additional data expected = '09' TAR unknown (CAT-TP/SMS) or "unknown application" (HTTPS)	RQ05_2405
3	Send Command with Secured Data to the TAR028 value, with: - '00 01 00 00'	Response with Secured Data is returned, last or only additional data response shall be '01 90 00'	RQ05_2405
4	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID15 TAR028 value should be set: Params = 'EA 11 80 0F 01 00 10 02 0101 0302 00 00 03 TAR028 00' - INSTALL[for make selectable] with AID15	Response with Secured Data is returned, last or only additional data response shall be '01 6A 80'	RQ05_2406
5	Send Command with Secured Data to the Test Application with AID15 which contains: - '00 01 00 00'	Response with Secured Data is returned: SW = '6X XX' with Response Status Code in the additional data expected = '09' TAR unknown (CAT-TP/SMS) or "unknown application" (HTTPS)	RQ05_2406

6.5.3.2.34 Test case 34: INSTALL[for install] SIM Toolkit Application with multiple TAR values

6.5.3.2.34.1 Initial Conditions

- Prepare for install of the 'Test Application AID2' using the load() and install(for load) methods.

6.5.3.2.34.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID2 TAR006 and TAR007values should be set: Params = 'EF 1D C8 02 FF FF C7 02 FF FF CA 13 01 FF 01 00 10 02 01 01 03 02 00 00 06 TAR006 TAR007' - INSTALL[for make selectable] with AID2	Response with Secured Data is returned, last or only additional data response shall be '02 90 00 00'	RQ05_0901 RQ05_0902 RQ05_0903 RQ05_2402 RQ05_2403
2	Send Command with Secured Data to the Test Application with TAR006 value, which contains: - '00 01 00 00'	Response with Secured Data is returned, last or only additional data response shall be '01 90 00'	RQ05_2402
3	Send Command with Secured Data to the Test Application with TAR007 value, which contains: - '00 01 00 00'	Response with Secured Data is returned, last or only additional data response shall be '01 90 00'	RQ05_2402

6.5.3.2.35 Test case 35: INSTALL[for install] UICC Toolkit Application with multiple TAR values

6.5.3.2.35.1 Initial Conditions

- Prepare for install of the 'Test Application AID3' using the load() and install(for load) methods.

6.5.3.2.35.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID3 TAR008 and TAR009values should be set: Params = 'EA 14 80 12 01 00 10 02 0101 0302 00 00 06 TAR008 TAR009 00' - INSTALL[for make selectable] with AID3	Response with Secured Data is returned, last or only additional data response shall be '02 90 00 00'	RQ05_1101 RQ05_1102 RQ05_1104 RQ05_2402 RQ05_2403
2	Send Command with Secured Data to the Test Application with TAR008 value, which contains: - '00 01 00 00'	Response with Secured Data is returned, last or only additional data response shall be '01 90 00'	RQ05_2402
3	Send Command with Secured Data to the Test Application with TAR009 value, which contains: - '00 01 00 00'	Response with Secured Data is returned, last or only additional data response shall be '01 90 00'	RQ05_2402

6.5.3.2.36 Test case 36: INSTALL[for install] SIM Toolkit Application without TAR value in the Install parameters, the AID contains TAR value

6.5.3.2.36.1 Initial Conditions

- Prepare for install of the 'Test Application AID16' using the load() and install(for load) methods.

6.5.3.2.36.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID16 (AID16 contains TAR020 value) The TAR value length in install parameters should be set to '00': Params = 'EF 17 C8 02 FF FF C7 02 FF FF CA 0D 01 FF 01 00 10 02 01 01 03 02 00 00 00' - INSTALL[for make selectable] with AID16	Response with Secured Data is returned, last or only additional data response shall be '02 90 00 00'	RQ05_0901 RQ05_0902 RQ05_0903 RQ05_2404
2	Send Command with Secured Data to the Test Application with TAR010 value, which contains: - '00 01 00 00'	Response with Secured Data is returned, last or only additional data response shall be '01 90 00'	RQ05_2404

6.5.3.2.37 Test case 37: INSTALL[for install] UICC Toolkit Application without TAR value in the Install parameters, the AID contains TAR value

6.5.3.2.37.1 Initial Conditions

- Prepare for install of the 'Test Application AID17' using the load() and install(for load) methods.

6.5.3.2.37.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID17 (AID17 contains TAR021 value) The TAR value length in install parameters should be set to '00': Params = 'EA 0E 80 0C 01 00 10 02 0101 0302 00 00 00 00' - INSTALL[for make selectable] with AID17	Response with Secured Data is returned, last or only additional data response shall be '02 90 00 00'	RQ05_1101 RQ05_1102 RQ05_1104 RQ05_2404
2	Send Command with Secured Data to the Test Application with TAR021 value, which contains: - '00 01 00 00'	Response with Secured Data is returned, last or only additional data response shall be '01 90 00'	RQ05_2404

6.5.3.2.38 Test case 38: INSTALL[for install] for contactless application with Reader mode protocol data type A

6.5.3.2.38.1 Initial Conditions

- Prepare for install of the 'Test Application AID19' using the load() and install(for load) methods.

6.5.3.2.38.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID19 The "Reader mode protocol data Type A" TLV object (tag '86') should be set. Params= EF 0F C7 02 FF FF C8 02 FF FF B0 05 86 01 03 00' - INSTALL[for make selectable] with AID19	Response with Secured Data is returned, last or only additional data response shall be '02 90 00 00'	RQ05_2502 RQ05_2504 RQ05_2506 RQ05_2601 RQ05_2503
2	Activate the SWP interface and perform HCI initialization	During the HCI initialization the UICC shall set DATARATE_MAX to '03'	RQ05_2601

6.5.3.2.39 Test case 39: INSTALL[for install] for contactless application with Reader mode protocol data type B

6.5.3.2.39.1 Initial Conditions

- Prepare for install of the 'Test Application AID20' using the load() and install(for load) methods.

6.5.3.2.39.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID20 The "Reader mode protocol data Type B" TLV object (tag '87') should be set. Params= 'EF 0F C7 02 FF FF C8 02 FF FF B0 05 87 03 03 03 00 00' - INSTALL[for make selectable] with AID20	Response with Secured Data is returned, last or only additional data response shall be '02 90 00 00'	RQ05_2502 RQ05_2504 RQ05_2506 RQ05_2503
2	Activate the SWP interface and perform HCI initialization	During the HCI initialization the UICC shall set the parameters to the values specified in step 1	RQ05_2701

6.5.3.2.40 Test case 40: INSTALL[for install] for contactless application with Card Emulation mode

6.5.3.2.40.1 Initial Conditions

- Prepare for install of the 'Test Application AID21' using the load() and install(for load) methods.

6.5.3.2.40.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data to the ISD, which contains: - INSTALL[for install] with AID21 Params= 'EF 11 C7 02 FF FF C8 02 FF FF A0 07 80 00 A5 03 82 01 C0 00' - INSTALL[for make selectable] with AID21	Response with Secured Data is returned, last or only additional data response shall be '02 90 00 00'	RQ05_2501

6.5.4 LOAD

6.5.4.1 Test case 1: LOAD with DES for DAP verification

6.5.4.1.1 Initial Conditions

- The key and algorithm to be used for DAP Verification or Mandated DAP Verification are implicitly known by the corresponding Security Domain.

6.5.4.1.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Secured Data to the ISD which contains: INSTALL[for load] command with Load File AID1 LOAD command with DES DAP GET RESPONSE	Response with Secured Data is returned, last or only additional data response shall be '03 90 00' and contain '00' data byte	RQ05_0109 RQ05_0301, RQ05_0606, RQ05_2801, RQ05_2802

Step	Description	Expected Result	RQ
2	Send Secured Data to the ISD, which contains: - INSTALL[for install and make selectable] the applet with AID1 GET RESPONSE	Response with Secured Data is returned, last or only additional data response shall be '02 90 00' and contain '00' data byte	RQ02_0104 RQ05_0109 RQ05_0301 RQ05_0605
3	Send Secured Data to the Test Application with AID1,which contains: - '00 01 00 00'	Response with Secured Data is returned, last or only additional data response shall be '01 90 00'	RQ05_0109 RQ05_0301

6.5.5 PUT KEY

6.5.5.1 Test case 1: PUT KEY - create new 3DES 2 keys

6.5.5.1.1 Initial Conditions

- Install the 'Test Application with AID4'.

6.5.5.1.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Secured Data to create new key set, with Key Version Number (KVN) and key identifiers of KIc, KID and DEK as defined in ETSI TS 102 225 [2], to the Test Application with AID40 which contains: - PUT KEY command with new 3DES 2 keys - GET RESPONSE The encrypting key to be used is the DEK of the same Key Version Number (KVN) as the KIc and KID in the Command Packet containing the PUT KEY command	Response with Secured Data is returned, last or only additional data response shall be '02 90 00' and contain 'KVN KeyCheckValue1 KeyCheckValue2 KeyCheckValue3', secured using keys as indicated in the Command Packet	RQ05_0109 RQ05_0301, RQ05_0110 RQ05_2901, RQ05_2904, RQ05_2905, RQ05_2906, RQ05_3105

6.5.5.2 Test case 2: PUT KEY - create new 3DES 3 keys

6.5.5.2.1 Initial Conditions

- Install the 'Test Application with AID4'.

6.5.5.2.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Secured Data to create new key set, with Key Version Number (KVN) and key identifiers of KIc, KID and DEK as defined in ETSI TS 102 225 [2], to the Test Application with AID4 which contains: - PUT KEY command with new 3DES 3 keys - GET RESPONSE The encrypting key to be used is the DEK of the same key version number (KVN) as the KIc and KID in the Command Packet containing the PUT KEY command	Response with Secured Data is returned, last or only additional data response shall be '02 90 00' and contain 'KVN KeyCheckValue1 KeyCheckValue2 KeyCheckValue3', secured using keys as indicated in the Command Packet	RQ05_0110, RQ05_2901, RQ05_2904, RQ05_2905, RQ05_2906, RQ05_3105

6.5.5.3 Test case 3: PUT KEY - add and replace DES keys

6.5.5.3.1 Initial Conditions

- Install the 'Test Application with AID4'.

6.5.5.3.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Secured Data to create new key set, with key version number (KVN) and key identifiers of KIc, KID and DEK as defined in ETSI TS 102 225 [2], to the Test Application with AID4 which contains: - PUT KEY command with new DES keys - GET RESPONSE The encrypting key to be used is the DEK of the same key version number (KVN) as the KIc and KID in the Command Packet containing the PUT KEY command	Response with Secured Data is returned, last or only additional data response shall be '02 90 00' and contain 'KVN KeyCheckValue1 KeyCheckValue2 KeyCheckValue3', secured using keys as indicated in the Command Packet	RQ05_2901, RQ05_2902, RQ05_2904, RQ05_2905, RQ05_2906
2	Send Secured Data to change KIc with key version number (KVN) defined in step 1, to the Test Application with AID4 which contains: - PUT KEY command with existing DES keys - GET RESPONSE Use DES key for DEK (key id 3) in ECB mode of the same key version number as the changed keys	Response with Secured Data is returned, last or only additional data response shall be '02 90 00' and contain 'KVN KeyCheckValue1', secured using keys as indicated in the Command Packet	RQ05_2901, RQ05_2902, RQ05_2903, RQ05_2905, RQ05_2906

6.5.5.4 Test case 4: PUT KEY - create new 16 bytes AES keys

6.5.5.4.1 Initial Conditions

- Install the 'Test Application with AID4'.

6.5.5.4.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Secured Data to create new key set with key version number and key identifiers of KIc, KID and DEK as defined in ETSI TS 102 225 [2], to the Test Application with AID4 which contains: - PUT KEY command with new 16 bytes AES keys - GET RESPONSE Use AES key for DEK (key id 3) of the same length with key type '88' in CBC mode with initial chaining value set to zero	Response with Secured Data is returned, last or only additional data response shall be '02 90 00' and contain 'KVN KeyCheckValue1 KeyCheckValue2 KeyCheckValue3', secured using keys as indicated in the Command Packet	RQ05_2901, RQ05_2904, RQ05_2905, RQ05_2906, RQ05_3101, RQ05_3102, RQ05_3103

6.5.5.5 Test case 5: PUT KEY - create new 24 bytes AES keys

6.5.5.5.1 Initial Conditions

- Install the 'Test Application with AID4'.

6.5.5.5.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Secured Data with key version number and key identifiers of KIc, KID and DEK as defined in ETSI TS 102 225 [2], to the Test Application with AID4 which contains: - PUT KEY command with new 24 bytes AES keys - GET RESPONSE Use AES key for DEK (key id 3) of the greater length with key type '88' in CBC mode with initial chaining value set to zero. Use padding with any value.	Response with Secured Data is returned, last or only additional data response shall be '02 90 00' and contain 'KVN KeyCheckValue1 KeyCheckValue2 KeyCheckValue3', secured using keys as indicated in the Command Packet	RQ05_2901, RQ05_2904, RQ05_2905, RQ05_2906, RQ05_3101, RQ05_3102, RQ05_3103, RQ05_3104, RQ05_3105, RQ05_3106, RQ05_3107, RQ05_3108, RQ05_3109
2	Send Secured Data with key version number and key identifiers of KIc, KID and DEK as defined in ETSI TS 102 225 [2], to the Test Application with AID4 which contains: PUT KEY command with 24 bytes AES (error) Use AES key for DEK (key id 3) of the shorter length (16 bytes).	Response with Secured Data is returned, last or only additional data response shall be '01 69 85' or other error SW	RQ05_3101, RQ05_3103

6.5.5.6 Test case 6: PUT KEY - create new 32 bytes AES keys

6.5.5.6.1 Initial Conditions

- Install the 'Test Application with AID4'.

6.5.5.6.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Secured Data with key version number and key identifiers of KIc, KID and DEK as defined in ETSI TS 102 225 [2] 2to the Test Application with AID4 which contains: - PUT KEY command with new 32 bytes AES keys - GET RESPONSE Use AES key for DEK (key id 3) of the same length with key type '88' in CBC mode with initial chaining value set to zero	Response with Secured Data is returned, last or only additional data response shall be '02 90 00' and contain 'KVN KeyCheckValue1 KeyCheckValue2 KeyCheckValue3', secured using keys as indicated in the Command Packet	RQ05_2901, RQ05_2904, RQ05_2905, RQ05_2906 RQ05_3101, RQ05_3102, RQ05_3103, RQ05_3104, RQ05_3105, RQ05_3106, RQ05_3107, RQ05_3108
2	Send Secured Data with key version number and key identifiers of KIc, KID and DEK as defined in ETSI TS 102 225 [2], to the Test Application with AID4 which contains: - PUT KEY command with 32 bytes AES keys (error) Use AES key for DEK (key id 3) of the shorter length (16 bytes)	Response with Secured Data is returned last or only additional data response shall be '01 69 85' or other error SW	RQ05_3101, RQ05_3103

6.5.6 GET STATUS

6.5.6.1 Test case 1: GET STATUS with different P1 values

6.5.6.1.1 Initial Conditions

- Install Test Application with AID1 with predefined menu entries Toolkit Application specific parameters.

6.5.6.1.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Secured Data to the ISD, which contains: - GET STATUS with P1='80' - GET RESPONSE	Response with Secured Data is returned, last or only additional data response shall be '02 90 00', containing 'EA LEN 80 LEN MP ID 00/01' (see note)	RQ05_0109 RQ05_0301 RQ05_3201, RQ05_3203, RQ05_3301, RQ05_3302, RQ05_3303
2	Send Secured Data with the AID of the Test Application to the ISD, which contains: - GET STATUS with P1= '40' with AID1 - GET RESPONSE	Response with Secured Data is returned, last or only additional data response shall be '02 90 00'(see note), containing 'EA LEN 80 LEN MP ID 00/01'(see note)	RQ05_0109 RQ05_0301 RQ05_3201, RQ05_3203,
3	Send Secured Data with the AID of the Test Application to the ISD, which contains: - GET STATUS with P1= '20' with package AID1 - GET RESPONSE	Response with Secured Data is returned, last or only additional data response shall be '02 90 00'(see note), containing 'EA LEN 80 LEN MP ID 00/01' (see note)	RQ05_0109 RQ05_0301 RQ05_3201, RQ05_3203,
4	Send Secured Data with the AID of the Test Application to the ISD, which contains: - GET STATUS with P1= '10' with package AID - GET RESPONSE	Response with Secured Data is returned, last or only additional data response shall be '02 90 00'(see note), containing 'EA LEN 80 LEN MP ID 00/01' (see note)	RQ05_0109 RQ05_0301 RQ05_3201, RQ05_3203,
NOTE: Values of MP (menu entry position) or ID (menu entry identifier) should not be checked.			

6.5.6.2 Test case 2: GET STATUS with optional P1 values

6.5.6.2.1 Initial Conditions

- Install Test Application with AID1 with predefined menu entries Toolkit Application specific parameters.

6.5.6.2.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Secured Data to the Test Application with AID1, which contains: - GET STATUS with P1= 'D0' - GET RESPONSE	Response with Secured Data is returned, last or only additional data response shall be '02 90 00', containing 'EA LEN 80 LEN MP ID 00/01'(see note)	RQ05_0109 RQ05_0301 RQ05_3201, RQ05_3203,
NOTE: Values of MP (menu entry position) or ID (menu entry identifier) should not be checked.			

6.5.6.3 Test case 3: GET STATUS returns Menu Entries in the LOCKED state

6.5.6.3.1 Initial Conditions

- Install Test Application with AID1 with predefined menu entries Toolkit Application specific parameters.

6.5.6.3.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Secured Data to the ISD, which contains: - SET STATUS to lock the applet with AID1	Response with Secured Data is returned, last or only additional data response shall be '01 90 00'	RQ01_0002, RQ05_0501
2	Send Secured Data coded to the ISD, which contains: - GET STATUS of the applet with AID1, i.e. '80 F2 P1 02 02 4F LEN AID1 00' - GET RESPONSE	Response with Secured Data is returned, last or only additional data response shall be '02 90 00', containing 'EA LEN 80 LEN MP ID 00/01' (see note)	RQ05_3201, RQ05_3203, RQ05_3301, RQ05_3302, RQ05_3303
NOTE: Values of MP (menu entry position) or ID (menu entry identifier) should not be checked.			

6.5.7 GET DATA

6.5.7.1 Test case 1: GET DATA with different P1 values

6.5.7.1.1 Initial Conditions

- All necessary information (i.e. Card Data, Key Information, Extended Card Resources Information) is made available on the card.

6.5.7.1.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Secured Data to the ISD, which contains: - GET DATA with P1P2 = '0066' (Card Data) - GET RESPONSE	Response with Secured Data is returned, last or only additional data includes tag '66' and ends with '02 90 00'	RQ05_0109, RQ05_0301, RQ05_3401, RQ05_3402
2	Send Secured Data to the ISD, which contains: - GET DATA with P1P2 = '00E0' (Key Information Template) - GET RESPONSE	Response with Secured Data is returned, last or only additional data includes tag 'E0' and ends with '02 90 00'	RQ05_0109, RQ05_0301, RQ05_3401, RQ05_3402
3	Send Secured Data to the Application Provider SD with AID40, which contains: - GET DATA with P1P2 = '00E0' (Key Information Template) - GET RESPONSE	Response with Secured Data is returned, last or only additional data includes tag 'E0' and ends with '02 90 00'	RQ05_0109, RQ05_0301, RQ05_3401, RQ05_3404
4	Send Secured Data to the ISD, which contains: - GET DATA with P1P2 = 'FF21' (Extended Card resources information) - GET RESPONSE	Response with Secured Data is returned, last or only additional data includes '81 LEN NN 82 LEN NVM 83 LEN VM' and end with '02 90 00' (see note)	RQ05_0109, RQ05_0301, RQ05_3405 RQ05_3501, RQ05_3503, RQ05_3504
NOTE: Values and length of NN (number of installed applications), NVM (Non Volatile Memory) and VM (Volatile Memory) should not be checked.			

6.5.8 STORE DATA

6.5.8.1 Test case 1: STORE DATA

6.5.8.1.1 Initial Conditions

- Install Test Application with AID1.

6.5.8.1.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Secured Data to the Test Application with AID1, which contains: - STORE DATA	Response with Secured Data is returned, last or only additional data ends with '01 90 00'	RQ05_0109, RQ05_3601

6.5.8.2 Test case 2: STORE DATA with a Forbidden Load File List

6.5.8.2.1 Initial Conditions

- Install Test Application with AID1.

6.5.8.2.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Secured Data to the Test Application with AID1, which contains: - STORE DATA with Forbidden Load File List	Response with Secured Data is returned, last or only additional data ends with '01 90 00'	RQ05_3602-11

6.5.9 RAM implementation over HTTPS

The content of this clause is FFS.

6.6 Additional command for push

6.6.1 BIP

See test case definition in clause 6.6.2.

6.6.2 CAT_TP

6.6.2.1 Test case 1: Send Secured Data (READ BINARY) using Expanded and Compact format with the different TAR value

6.6.2.1.1 Initial Conditions

- None.

6.6.2.1.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data coded as: [Compact Remote command structure] to the UICC Shared File System Remote File Management application [TAR value for Compact format], which contains: - SELECT: $DF_{SIMTEST}$ - SELECT: EF_{TARU} - READ BINARY with P3/Le = '00'	Response with Secured Data is returned last or only additional data response shall be '03 90 00' and contain all data of EF_{TARU} until the end of file	RQ02_0901, RQ05_0107, RQ05_0108

Step	Description	Expected Result	RQ
2	Send Command with Secured Data coded as: [Expanded Remote command structure] to the UICC Shared File System Remote File Management application [TAR value for Expanded format], which contains: - SELECT: $DF_{SIMTEST}$ - SELECT: EF_{TARU} - READ BINARY TLV Structure: C-APDU TLV Definite length coding	Secured Response Data is returned: 'AB 7F 80 01 03 23 LEN [Data 90 00]' where the Data should be the content of EF_{TARU}	RQ02_0902, RQ05_0107, RQ05_0108

6.6.2.2 Test case 2: Send Secured Data (READ BINARY) using Expanded and Compact format with the same TAR value

6.6.2.2.1 Initial Conditions

- None.

6.6.2.2.2 Test Procedure

Step	Description	Expected Result	RQ
1	Send Command with Secured Data coded as: [Expanded Remote command structure] to the UICC Shared File System Remote File Management application [TAR value for Compact format], which contains: - SELECT: $DF_{SIMTEST}$ - SELECT: EF_{TARU} - READ BINARY TLV Structure: C-APDU TLV Definite length coding	SW = '6X XX' with Error Response Status Code in the additional data expected = '09' TAR unknown or other error	RQ04_0102, RQ05_0108
2	Send Command with Secured Data coded as: [Compact Remote command structure] to the UICC Shared File System Remote File Management application [TAR value for Expanded format], which contains: - SELECT: $DF_{SIMTEST}$ - SELECT: EF_{TARU} - READ BINARY	SW = '6X XX' with Error Response Status Code in the additional data expected = '09' TAR unknown or other error	RQ04_0102, RQ05_0108

6.6.2.3 Test case 3: PUSH Command, PoR required - No Error

6.6.2.3.1 Initial Conditions

- None.

6.6.2.3.2 Test Procedure

Step	Description	Expected result	RQ
1	Send ENVELOPE_SMS_PP to the ISD with SPI = '02 21', and Secured Data which contains: - PUSH command for BIP channel opening - PUSH command for CAT_TP link establishment i.e. Data = '80 EC 01 01 25 35 07 02 00 00 03 00 00 02 3C 03 01 1F 40 39 02 05 78 47 0A 09 47 53 4D 41 65 55 49 43 43 3E 05 21 7F 00 00 01 80 EC 01 02 05 3C 03 01 02 02'	SW = '91 XX'	RQ06_0101, RQ06_0701, RQ06_0702, RQ06_0806, RQ06_0901

Step	Description	Expected result	RQ
2	Send FETCH	OPEN CHANNEL with response data 'D0 27 81 03 01 40 01 82 02 81 82 35 07 02 00 00 03 00 00 02 39 02 05 78 47 0A 09 47 53 4D 41 65 55 49 43 43 3C 03 01 30 50 3E 05 21 7F 00 00 01 90 00'	RQ06_0201, RQ06_0801, RQ06_0802
3	Send TERMINAL RESPONSE (OPEN CHANNEL)	SW = '91 XX'	RQ06_0201
4	Send FETCH	PROACTIVE COMMAND: SEND DATA (SYN PDU)	
5	Send TERMINAL RESPONSE (SEND DATA)	SW = '91 XX'	RQ06_0201
6	Send ENVELOPE(EVENT DOWNLOAD - Data available)	SW = '91 XX'	
7	Send FETCH	PROACTIVE COMMAND: RECEIVE DATA (SYN/ACK PDU)	
8	Send TERMINAL RESPONSE (RECEIVE DATA)	SW = '91 XX'	RQ06_0201
9	Send FETCH	PROACTIVE COMMAND: SEND DATA (ACK PDU)	
10	Send TERMINAL RESPONSE (SEND DATA)	SW = '91 XX'	RQ06_0201
11	Send FETCH	PROACTIVE COMMAND: SEND SHORT MESSAGE (PoR)	RQ06_0401
12	Send TERMINAL RESPONSE (SEND SHORT MESSAGE)	SW = '90 00'	RQ06_0301

6.7 Confidential application management

FFS

Annex A (normative): BER-TLV tags

A.1 BER-TLV tags

Table A.1: BER-TLV tags

Description	Length of tag	Value
Command Scripting template tag for definite length coding	1	Defined in ETSI TS 101 220 [6]
Response Scripting template tag for definite length coding	1	Defined in ETSI TS 101 220 [6]
Command Scripting template tag for indefinite length coding	1	Defined in ETSI TS 101 220 [6]
Response Scripting template tag for indefinite length coding	1	Defined in ETSI TS 101 220 [6]
Number of executed command TLV objects tag	1	Defined in ETSI TS 101 220 [6]
Bad format TLV tag	1	Defined in ETSI TS 101 220 [6]
Immediate Action tag	1	Defined in ETSI TS 101 220 [6]
Immediate Action Response tag	1	Defined in ETSI TS 101 220 [6]
Error Action tag	1	Defined in ETSI TS 101 220 [6]
Script Chaining tag	1	Defined in ETSI TS 101 220 [6]
Script Chaining Response tag	1	Defined in ETSI TS 101 220 [6]

Annex B (normative): Default file system and files content

B.1 DF_{TEST} (UICC Access Tests DF)

B.1.1 DF identifier

A file identifier not allocated to ensure that the File ID is not used by any other DF defined in any of the applications listed in clause 4.4.3. The suggestion is to use '7F4A'.

B.1.2 EF_{TNU} (Transparent Never Update)

This is a 3 byte transparent EF for testing purposes with fixed contents.

A file identifier not allocated to ensure that the File ID is not used by any other EF defined in any of the applications listed in clause 4.4.3. The suggestion is to use '6F 02'.

Identifier: '6FXX'		Structure: transparent
File size: 3 bytes		Update activity: low
Access Conditions: READ ALWAYS UPDATE NEVER ACTIVATE ALWAYS DEACTIVATE ALWAYS		
Bytes	Description	Length
1 - 3	55 55 55	3 bytes

B.1.3 EF_{TARU} (Transparent Always Read and Update)

This is a 120 byte transparent EF for testing purposes with predefined contents.

A file identifier not allocated to ensure that the File ID is not used by any other EF defined in any of the applications listed in clause 4.4.3. The suggestion is to use '6F 03'.

Identifier: '6FXX '		Structure: transparent
File size: 120 bytes		Update activity: low
Access Conditions: READ ALWAYS UPDATE ALWAYS ACTIVATE ALWAYS DEACTIVATE ALWAYS		
Bytes	Description	Length
1 - 120	FF ... FF	120 bytes

B.1.4 EF_{TUACP} (Transparent Update Access Condition PIN)

This is a 120 byte transparent EF for testing purposes with predefined contents.

A file identifier not allocated to ensure that the File ID is not used by any other EF defined in any of the applications listed in clause 4.4.3. The suggestion is to use '6F 05'.

Identifier: '6FXX'		Structure: transparent
File size: 120 bytes		Update activity: low
Access Conditions: READ ALWAYS UPDATE PIN ACTIVATE ALWAYS DEACTIVATE ALWAYS		
Bytes	Description	Length
1 - 120	FF ... FF	120 bytes

B.1.5 EF_{TPRU} (Transparent PIN Read and Update)

This is a 120 byte transparent EF for testing purposes with predefined contents.

A file identifier not allocated to ensure that the File ID is not used by any other EF defined in any of the applications listed in clause 4.4.3. The suggestion is to use '6F 06'.

Identifier: '6FXX'		Structure: transparent
File size: 120 bytes		Update activity: low
Access Conditions: READ PIN UPDATE PIN ACTIVATE ALWAYS DEACTIVATE ALWAYS		
Bytes	Description	Length
1 - 120	FF ... FF	120 bytes

B.1.6 EF_{LF4R4b}

This is a linear fixed EF for testing purposes with 4 records and 4 bytes/record with predefined contents located under DF_{TEST}

A file identifier is not allocated in order to ensure that the File ID is not used by any other EF defined in any of the applications listed in clause 4.4.3. The suggestion is to use '6F FC'.

Identifier: '6F XX'		Structure: linear fixed
Record length: 4 bytes		Update activity: low
Access Conditions: READ ALWAYS UPDATE ALWAYS DEACTIVATE ALWAYS ACTIVATE ALWAYS		
Bytes	Description	Length
1 to 4	LF4R4b test contents	4 bytes

Coding:

1st record:	A0	A1	A2	B0
2nd record:	B0	B1	B2	A0
3rd record:	B0	B1	B2	A0
4th record:	A0	A1	A2	B0

B.1.7 $EF_{BER-TLV}$

This is a 120 byte BER-TLV EF for testing purposes with predefined contents.

A file identifier not allocated to ensure that the File ID is not used by any other EF defined in any of the applications listed in clause 4.4.3. The suggestion is to use '6F 09'.

Identifier: '6F XX'	Structure: BER-TLV
File size: 10 bytes	Update activity: low
Access Conditions: READ ALWAYS UPDATE ALWAYS DEACTIVATE ALWAYS ACTIVATE ALWAYS INCREASE ALWAYS	

Bytes	Description	Length
1 to 10	Test contents: ‚FF ... FF'	10 bytes

B.1.8 EF_{CY4R4b}

This is a cyclic EF for testing purposes with 4 records and 4 bytes/record with predefined contents located under DF_{TEST}

A file identifier is not allocated in order to ensure that the File ID is not used by any other EF defined in any of the applications listed in clause 4.4.3. The suggestion is to use '6F FD'.

Identifier: '6F XX'	Structure: cyclic
Record length: 4 bytes	Update activity: low
Access Conditions: READ ALWAYS UPDATE ALWAYS DEACTIVATE ALWAYS ACTIVATE ALWAYS INCREASE ALWAYS	

Bytes	Description	Length
1 to 4	CY4R10b test contents	4 bytes

Coding:

1st record:	A0	A1	A2	B0
2nd record:	B0	B1	B2	A0
3rd record:	B0	B1	B2	A0
4th record:	A0	A1	A2	B0

B.2 DF_{TESTB} (Tests DF under ADF_1)

B.2.1 DF identifier

A file identifier not allocated to ensure that the File ID is not used by any other DF defined in any of the applications listed in clause 4.4.3. The suggestion is to use '7F4B'.

B.2.2 EF_{TARUB} (Transparent Always Read and Update B)

This is a 120 byte transparent EF for testing purposes with predefined contents.

A file identifier not allocated to ensure that the File ID is not used by any other EF defined in any of the applications listed in clause 4.4.3. The suggestion is to use '6F 04'.

Identifier: '6FXX'		Structure: transparent	
File size: 120 bytes		Update activity: low	
Access Conditions: READ UPDATE ACTIVATE DEACTIVATE	ALWAYS ALWAYS ALWAYS ALWAYS		
Bytes	Description		Length
1 - 120	FF ... FF		120 bytes

B.3 $DF_{TELECOM}$

B.3.1 EF_{RMA} (Remote Management Actions)

This is a linear fixed EF for testing purposes with is a 36 byte with predefined contents.

This file is located under $DF_{TELECOM}$ ('7F10') as defined in ETSI TS 102 222 [9].

Identifier: '6F53'		Structure: linear fixed	
Record length: 36 bytes		Update activity: low	
Access Conditions: READ UPDATE ACTIVATE DEACTIVATE	ADM ADM ADM ADM		
Bytes	Description		Length
1 to 36	Test content as defined below		36 bytes

1st record:	DISPLAY TEXT	1A 81 03 01 21 80 82 02 81 02 8D 0F 04 54 6F 6F 6C 6B 69 74 20 54 65 73 74 20 31 FF FF FF FF FF FF FF FF FF
2nd record:	REFRESH	10 81 03 01 01 01 82 02 81 82 92 05 01 3F 00 2F E2 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
3rd record:	PLAY TONE	1B 81 03 01 20 00 82 02 81 03 85 09 44 69 61 6C 20 54 6F 6E 65 8E 01 01 84 02 01 05 FF FF FF FF FF FF FF FF

Annex C (normative): Secure data coding and command structure

C.1 Commands

Table C.1

<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td rowspan="8">SELECT</td><td>SELECT DF <Text> with FID 'd1 d2': '00 A4 00 0C 02 d1 d2' (no response data)</td></tr>
<tr><td>SELECT EF <Text> with FID 'e1 e2': '00 A4 00 04 02 e1 e2' (return FCP template) - for T=0 (Compact format)</td></tr>
<tr><td>SELECT EF <Text> with FID 'e1 e2': '00 A4 00 04 02 e1 e2 00' (return FCP template) for T=1 (Expanded Format)</td></tr>
<tr><td>SELECT EF <Text> with FID 'e1 e2': '00 A4 00 04 02 e1 e2'</td></tr>
<tr><td>SELECT EF <Text> with FID 'e1 e2' as case 4: '00 A4 00 04 02 e1 e2 00'</td></tr>
<tr><td>Select Applet with AID '00 A4 04 00 LC AID' (SELECT by DF name)</td></tr>
<tr><td>SELECT by path: '00 A4 09 00 LC File_path'</td></tr>
<tr><td>SELECT by path from MF: '00 A4 08 0C LC File_path'</td></tr>
<tr><td>UPDATE BINARY</td><td>UPDATE BINARY with data 'XX XX XX': '00 D6 00 00 03 XX XX XX'</td></tr>
<tr><td>TERMINAL PROFILE</td><td>TERMINAL PROFILE should indicate support of following features:
<table>
<tr><td>Item</td><td>Byte.bit</td><td>Terminal Profile</td></tr>
<tr><td>1</td><td>1.1</td><td>Profile Download</td></tr>
<tr><td>17</td><td>3.1</td><td>DISPLAY TEXT</td></tr>
<tr><td>21</td><td>3.5</td><td>PLAY TONE</td></tr>
<tr><td>24</td><td>3.8</td><td>REFRESH</td></tr>
<tr><td>30</td><td>4.6</td><td>SET UP MENU</td></tr>
</table></td></tr>
<tr><td>SET STATUS</td><td>Set Status to lock the applet with the AID: '80 F0 40 FF Len AID' -</td></tr>
<tr><td>ENVELOPE_SMS_PP</td><td>'80 C2 00 00 Lc
D1 XX
82 02 82 81
86 02 80 01
8B YY
40 05 81 12 50 F3 96 F6 22 22 22 22 22 22 22 len ZZ…ZZ Secure Packet Header Data',
where the Data is the Secured Data as defined in the test case and the header contains SPI2 = '21'</td></tr>
<tr><td>PROACTIVE COMMAND: DISPLAY TEXT</td><td>BER-TLV: D0 1A 81 03 01 21 80 82 02 81 02 8D
0F 04 54 6F 6F 6C 6B 69 74 20 54 65
73 74 20 31</td></tr>
<tr><td>TERMINAL RESPONSE: DISPLAY TEXT</td><td>BER-TLV: 81 03 01 21 80 82 02 82 81 83 01 00</td></tr>
<tr><td>PROACTIVE COMMAND: PLAY TONE</td><td>BER-TLV: D0 1B 81 03 01 20 00 82 02 81 03 85
09 44 69 61 6C 20 54 6F 6E 65 8E 01
01 84 02 01 05</td></tr>
<tr><td>TERMINAL RESPONSE: PLAY TONE</td><td>BER-TLV: 81 03 01 20 00 82 02 82 81 83 01 00</td></tr>
<tr><td>PROACTIVE COMMAND: REFRESH</td><td>BER-TLV: D0 10 81 03 01 01 01 82 02 81 82 92
05 01 3F 00 2F E2</td></tr>
<tr><td>TERMINAL RESPONSE: REFRESH</td><td></td></tr>
<tr><td>READ BINARY</td><td>'00 B0 00 00 00'</td></tr>
<tr><td>READ RECORD</td><td>'00 B2 01 04 00'</td></tr>
<tr><td>UPDATE RECORD</td><td>'00 DC 00 04 LC Data' (current mode)
’00 DC 00 03 LC Data’ (PREVIOUS mode)</td></tr>
</table>

Command	Description
SEARCH RECORD	'00 A2 01 04 LC Data'
INCREASE	'80 32 00 00 LC Data 00' (without the last '00' byte for T=0 (Compact Format))
SET DATA	'00 DB 00 80 LC Data'
RETRIEVE DATA	'00 CB 00 P2 01 XX 00'with XX= Tag value
ACTIVATE FILE	'00 44 00 00 00' (activating current file)
DEACTIVATE FILE	'00 04 00 00 00' deactivating current file
VERIFY PIN	'00 20 00 01 08 PIN'
CHANGE PIN	'00 24 00 01 10 Data' with Data = PINold||PINnew
ENABLE PIN	'00 28 00 01 08 PIN'
DISABLE PIN	'00 26 00 01 08 PIN'
UNBLOCK PIN	'00 2C 00 01 10 Data' with Data = PINtoUnblock||PINnew
DELETE	'80 E4 00 00 12 4F 10 AID'
CREATE FILE	CREAT FILE EF_{XX}: '0X E0 00 00 14 62 13 82 02 41 21 83 02 EF1 EF2 8A 01 05 8C 03 03 00 00 80 01 05' where EF1 EF2 is the FID
DELETE FILE	DELETE FILE EF_{XX}: 0X E4 00 00 02 EF1 EF2 where EF1 EF2 is the FID
RESIZE FILE	RESIZE FILE EF_{XX}: '8X D4 00 00 09 62 07 83 02 EF1 EF2 80 01 03'where EF1 EF2 is the FID
INSTALL	INSTALL[for load]: '80 E6 02 00 LC Data' with Data = '10 AID 00 00 XX Params 00' where XX = length of Params field ('00' if no Params) and Params are the Systems Specific Parameters as defined in the test case
	INSTALL[for install]: '80 E6 04 00 LC 10 ELF AID 10 EM AID 10 Application AID 03 XX XX XX (privileges) length [C9 0A 81 02 02 55 82 01 C8 83 01 F8 Params] 00' where Params are the parameters as defined in the test
	INSTALL[for install and make selctable]: FFS
LOAD	LOAD: '80 E6 P1 P2 LC C4 Len Data, where Len is the length of Data and the Data is the Load File Data Block
	LOAD with DES DAP: '80 E6 P1 P2 LC E2 YY 4F XX AID C3 08 Sign C4 Len Data, where Sign is the Load File Data Block DES Signature, XX is the length of the AID of the Security Domain with DAP verification privilege, YY is the length of DAP block, i.e. YY=08+XX, Len is the length of Data, Data is the Load File Data Block
GET RESPONSE	'00 C0 00 00 Len' where Len is the length of data available
GET STATUS	'80 F2 P1 02 02 4F 00 00'
GET DATA	'80 CA P1 P2 00'
STORE DATA	STORE DATA with arbitrary value (DGI format): '80/84 E2 88 00 13 00 70 10 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F '
	STORE DATA with Forbidden Load File List: '80/84 E2 80 00 LC BE XX 4F Len 3rdSD-AID 4F Len FLF-AID', 3rdSD is Third Party Security Domain AID and FLF-AID is Forbidden Executable Load File #1 AID
PUT KEY	PUT KEY command with new 3DES 3 keys: '84 D8 00 81 Len KVN FF 82 18 XX…XX 03 YY YY YY 01 18 01 00 FF 82 18 XX…XX 03 YY YY YY 01 14 01 00 FF 82 18 XX…XX 03 YY YY YY 01 48 01 00 MAC 00', where XX…XX is the coded key value, YY YY YY is the key check value and the KVN (key version number) should be chosen from the set of possible version numbers that are not already in use.
	PUT KEY command with new 3DES 2 keys: '84 D8 00 81 Len KVN FF 82 10 XX…XX 03 YY YY YY 01 18 01 00 FF 82 10 XX…XX 03 YY YY YY 01 14 01 00 FF 82 10 XX…XX 03 YY YY YY 01 48 01 00 MAC 00', where XX…XX is the coded key value, YY YY YY is the key check value and the KVN (key version number) should be chosen from the set of possible version numbers that are not already in use.
	PUT KEY command with new DES keys: '84 D8 00 81 Len KVN FF 83 08 XX…XX 03 YY YY YY 01 18 01 00 FF 83 08 XX…XX 03 YY YY YY 01 14 01 00 FF 83 08 XX…XX 03 YY YY YY 01 48 01 00 MAC 00', where XX…XX is the coded key value, YY YY YY is the key check value and the KVN (key version number) should be chosen from the set of possible version numbers that are not already in use
	PUT KEY command with existing DES keys '84 D8 KVN 01 Len FF 83 08 X…XX 03 YY YY Y 01 18 01 00 MAC 00', where XX…XX is the coded key value, YY YY YY is the key check value and the KVN (key version number) should be the one that already exists.
	PUT KEY command with new 16 bytes AES key: '84 D8 00 81 Len KVN FF 88 10 XX…XX 03 YY YY YY 01 18 01 00 FF 88 10 XX…XX 03 YY YY YY

Command	Description
	01 14 01 00 FF 88 10 XX…XX 03 YY YY YY 01 48 01 00 MAC 00', where XX…XX is the coded key value, YY YY YY is the key check value and the KVN (key version number) should be chosen from the set of possible version numbers that are not already in use
	PUT KEY command with new 24 bytes AES key '84 D8 00 81 Len KVN FF 88 18 XX…XX 03 YY YY YY 01 18 01 00 FF 88 18 XX…XX 03 YY YY YY 01 14 01 00 FF 88 18 XX…XX 03 YY YY YY 01 48 01 00 MAC 00', where XX…XX is the coded key value, YY YY YY is the key check value and the KVN (key version number) should be chosen from the set of possible version numbers that are not already in use
	PUT KEY command with new 32 bytes AES key '84 D8 00 81 Len KVN FF 88 20 XX…XX 03 YY YY YY 01 18 01 00 FF 88 20 XX…XX 03 YY YY YY 01 14 01 00 FF 88 20 XX…XX 03 YY YY YY 01 48 01 00 MAC 00', where XX…XX is the coded key value, YY YY YY is the key check value and the KVN (key version number) should be chosen from the set of possible version numbers that are not already in use
	PUT KEY command with 24 bytes AES (error) '84 D8 00 81 Len KVN FF 88 18 XX…XX 03 YY YY YY 01 18 01 00 FF 88 18 XX…XX 03 YY YY YY 01 14 01 00 FF 88 10 XX…XX 03 YY YY YY 01 48 01 00 MAC 00', where XX…XX is the coded key value, YY YY YY is the key check value and the KVN (key version number) should be chosen from the set of possible version numbers that are not already in use
	PUT KEY command with 32 bytes AES (error) '84 D8 00 81 Len KVN FF 88 20 XX…XX 03 YY YY YY 01 18 01 00 FF 88 20 XX…XX 03 YY YY YY 01 14 01 00 FF 88 10 XX…XX 03 YY YY YY 01 48 01 00 MAC 00', where XX…XX is the coded key value, YY YY YY is the key check value and the KVN (key version number) should be chosen from the set of possible version numbers that are not already in use.

C.2 Remote APDU Format

C.2.1 Compact Remote Application Data Format

FFS

C.2.2 Expanded Remote Application Data Format

C.2.2.1 C-APDU TLV

Definite length coding

'AA LEN
22 LEN APDU1
...
22 LEN APDUx'

Indefinite length coding

'AE 80
22 LEN APDU1
...
22 LEN APDUx
00 00'

C.2.2.2 Immediate Action TLV

Definite length coding

- Normal format

'AA LEN
81 LEN PRO_CMD1

…

81 LEN PRO_CMDx'

- Referenced format

'AA LEN

81 01 81

22 LEN PRO_CMD1,

Or

81 01 82

22 LEN PRO_CMD2

Or

81 01 YX (see note2)'

Indefinite length coding

- Normal format

'AE 80

81 LEN PRO_CMD1

.....

81 LEN PRO_CMDx

00 00'

- Referenced format

'AE 80

81 01 81

22 LEN PRO_CMD1,

81 01 82

22 LEN PRO_CMD2,

81 01 YX (see note 2)

00 00'

PRO_CMDx shall be a set of COMPREHENSION-TLV data objects constituting one of the allowed proactive commands specified for immediate action; i.e. DISPLAY TEXT, PLAY TONE or REFRESH.

NOTE 1: Void.

NOTE 2: This byte has value between '01' to '7F': Reference to a record in EF_{RMA}.

C.2.2.3 Error Action TLV

Definite length coding:

- Normal format

'AA LEN

82 LEN PRO_CMD1'

- Referenced format

'AA LEN

82 01 YX (see note 2)'

- No Action

'AA 02

82 00'

Indefinite length coding:

- Normal format

'AE 80
82 LEN PRO_CMD1

00 00'

- Referenced format

'AE 80

82 01 YX (see note 2)

00 00'

- No Action

'AE 02

82 00

00 00'

NOTE 1: PRO CMDx should be one of the allowed proactive commands specified for immediate action; i.e. DISPLAY TEXT or PLAY TONE.

NOTE 2: This byte has value between '01' to '7F': Reference to a record in EF_{RMA}.

C.2.2.4 Script Chaining TLV

- Definite length coding

'AA len 83 01 XX CMD TLV1 …. CMD TLVx' with 'XX'=Script Chaining Value

- Indefinite length coding

'AE 80 83 01 XX 00 00' with 'XX'=Script Chaining Value

Annex D (informative): Full command structure sample

D.1 Formatted SMS with PoR required - default

FFS

D.2 CAT-TP - default

FFS

D.3 HTTPS - default

FFS

Annex E (normative): AID and TAR values

E.1 UICC shared file system remote file management application

Description	TAR
Compact Format as defined in ETSI TS 101 220 [6]	TAR1: 'B0 00 00'
Expanded Format or automatic data format detection as defined in ETSI TS 101 220 [6]	TAR3: 'B0 01 20'

E.2 ADF remote file management application

Description	TAR
Compact Format as defined in ETSI TS 101 220 [6]	TAR2: 'B0 00 01'
For Expanded Format or automatic data format detection as defined in ETSI TS 101 220 [6]	TAR4: 'B0 01 40'

E.3 AID and TAR

Applet AID	AID	TAR	Description
AID1	FFS	FFS	Toolkit Test Applet
AID2	FFS	FFS	SIM Toolkit application with menu
AID3	FFS	FFS	UICC Toolkit application with menu
AID4	FFS	FFS	SIM Toolkit application with menu and UICC Toolkit application with menu combined
AID5	FFS	FFS	UICC Toolkit Admin Access application
AID6	FFS	FFS	SIM Toolkit Access application to update EF_TARU, EF_TNU, EF_TUACP
AID7	FFS	FFS	SIM Toolkit Access application to update EF_TARU
AID8	FFS	FFS	UICC Toolkit Access application to update EF_TARU, EF_TNU, EF_TUACP
AID9	FFS	FFS	UICC Toolkit Access application to update EF_TARU
AID10	FFS	FFS	SIM Toolkit application with Proactive Session: Check Application Priority
AID11	FFS	FFS	SIM Toolkit application with Proactive Session: Check Application Priority
AID12	FFS	FFS	UICC Toolkit application with Proactive Session: Check Application Priority
AID13	FFS	FFS	UICC Toolkit application with Proactive Session: Check Application Priority
AID14	FFS	FFS	SIM Toolkit application with menu
AID15	FFS	FFS	UICC Toolkit application with menu
AID16	FFS	FFS	SIM Toolkit application with menu
AID17	FFS	FFS	UICC Toolkit application with menu
AID18	FFS	FFS	UICC Toolkit Access and Admin Access application with menu to update EF_TARUB
AID19	FFS	FFS	Contactless application - Reader mode typeA
AID20	FFS	FFS	Contactless application - Reader mode typeB
AID21	FFS	FFS	Contactless application - Card Emulation
AID30	FFS	FFS	UICC Toolkit application, sends proactive command for DISPLAY TEXT
AID31	FFS	FFS	UICC Toolkit application, sends proactive command to PLAY TONE
AID32	FFS	FFS	UICC Toolkit application, sends proactive command to REFRESH
AID33	FFS	FFS	UICC Toolkit application, starts proactive session with data defined in EFRMA
AID34	FFS	FFS	UICC Toolkit application, sends Immediate Action Error upon DISPLAY TEXT
AID35	FFS	FFS	UICC Toolkit application, starts proactive session with DISPLAY TEXT on error
AID36	FFS	FFS	UICC Toolkit application, starts proactive session with PLAY TONE on error
AID40	FFS	FFS	Application Provider SD

Annex F (informative): FFS requirements

RQ No.	Clause	Description
RQ01_0006	4	Warnings or procedure bytes do not halt processing of the command list.
RQ01_0011	4	If changes in the logical state have occurred that the terminal needs to be aware of, the application on the UICC may issue a REFRESH command according to ETSI TS 102 223 [4].
RQ02_0106	5.1.1	In case the data is truncated in the response, the remaining bytes are lost and the status words shall be set to '62 F1'.
RQ02_0107	5.1.1	The limitation of 256 bytes does not apply for the length of the response data.
RQ02_0403	5.2.1.1	In case the data is truncated in the response of a C-APDU, the status words for this C-APDU shall be set to '62 F1' in the corresponding R-APDU. This shall terminate the processing of the command list.
RQ02_0404	5.2.1.1	If a R-APDU fills the response buffer so that no further R-APDU can be included in the response scripting template, this shall terminate the processing of the command list.
RQ02_0505	5.2.1.2	In case of "proactive session indication", execution of the remaining script shall be suspended if a proactive session is ongoing.
RQ02_0506	5.2.1.2	In case of "proactive session indication", execution of the remaining script shall be suspended if a proactive session is ongoing. Script processing shall be resumed after the end of the proactive session. If the UICC cannot suspend the script execution, e.g. because there is not enough internal resources available, the UICC shall terminate the processing of the script and return a "suspension error" in the response data.
RQ02_0507	5.2.1.2	If no "proactive session indication" is present as first Command TLV and another proactive session is ongoing, proactive commands in the script shall be silently ignored.
RQ04_0106	7	If a non-shareable file is selected by the remembered file context, the mechanisms defined in ETSI TS 102 221 [3] limiting the access to non-shareable files shall apply.
RQ05_0303	8.2	if additional application provider security as defined in clause 10.2 is applied, the secure messaging as defined in GlobalPlatform Card Specification [5] shall not apply to RAM APDU commands and responses (e.g. MAC shall not be present in the command data field).
RQ05_0304	8.2	if additional application provider security as defined in clause 10.2 is applied, the class byte shall indicate that an APDU command includes no secure messaging.
RQ05_0303	8.2.1	Script chaining may be used for confidential application management as specified in clause 10 or to chain a sequence of STORE DATA commands. It has no effect for other commands.
RQ05_0304	8.2.1	Whenever Script chaining is present for RAM, it shall be processed as defined in the present document.
RQ05_0305	8.2.1	When using the Compact Remote Application data format and if an application session is saved beyond a command session as defined below, this session context shall be deleted upon card reset.
RQ05_0602	8.2.1.3	INSTALL [for personalization] and Install [for extradition] command described in GlobalPlatform Card Specification [5] are optional.
RQ05_0603	8.2.1.3	A UICC supporting confidential application management as specified in clause 10 [1] shall support INSTALL [for personalization].
RQ05_0604	8.2.1.3	If INSTALL [for personalization] and Install [for extradition] implemented, both commands shall follow the specification in the UICC Configuration [16].
RQ05_0607	8.2.1.3	When using the Compact Remote Application data format, the context established by INSTALL [for personalization] (if supported) shall be saved across command sessions until the STORE DATA command containing the last block.
RQ05_0806	8.2.1.3.2	In case of JavaCardTM applications, If the register() method is invoked the instance AID present in the INSTALL [for install] command and the AID within the Load File, as specified in GlobalPlatform Card Specification [5], should be the same.
RQ05_1103	8.2.1.3.2.2.1	None of the toolkit resources will be accessible if the UICC Toolkit Application specific parameters are missing.
RQ05_1105	8.2.1.3.2.2.1	Any additional parameters to RQ05_1104 shall be ignored by the card.
RQ05_1301	8.2.1.3.2.2.3	The UICC toolkit parameters DAP is an optional signature. The card issuer's security policy may require the presence of this DAP.

<table>
<tr><th>RQ No.</th><th>Clause</th><th>Description</th></tr>
<tr><td>RQ05_1302</td><td>8.2.1.3.2.2.3</td><td>The input data used to compute UICC toolkit parameters DAP is the concatenation of the following data:
<table>
<tr><th>Description</th><th>Length</th></tr>
<tr><td>Length of instance AID</td><td>1</td></tr>
<tr><td>Instance AID</td><td>5 to 16</td></tr>
<tr><td>Length of UICC Toolkit parameters</td><td>1</td></tr>
<tr><td>UICC Toolkit parameters</td><td>n</td></tr>
</table>
The key used to compute this DAP is: Key identifier '02' of Key Version number '11' in the Issuer Security Domain.</td></tr>
<tr><td>RQ05_1303</td><td>8.2.1.3.2.2.3</td><td>Depending on the key type for DAP, if padding is required by the algorithm, the data is appended by '80' and filled up with zero or more '00'.</td></tr>
<tr><td>RQ05_1304</td><td>8.2.1.3.2.2.3</td><td>Depending on the key type for DAP, if DES is used, MAC in CBC mode with initial chaining value set to zero shall be used.</td></tr>
<tr><td>RQ05_1305</td><td>8.2.1.3.2.2.3</td><td>Depending on the key type for DAP, if AES [13] is used, CMAC mode [15] shall be used. The length of the MAC shall be associated with the key.</td></tr>
<tr><td>RQ05_1504</td><td>8.2.1.3.2.3</td><td>The mechanism to manage the position of the Menu Entries for Toolkit Application Specific Parameters is defined in ETSI TS 102 241 [7].</td></tr>
<tr><td>RQ05_1507</td><td>8.2.1.3.2.3</td><td>If the requested item identifier for Toolkit Application Specific Parameters is '00', the card shall take the first free value in the range [128...255].</td></tr>
<tr><td>RQ05_2102</td><td>8.2.1.3.2.5.2</td><td>The Access Domain Data for UICC access mechanism shall be checked against SE ID 01 access rules as defined in ETSI TS 102 221 [3].</td></tr>
<tr><td>RQ05_2201</td><td>8.2.1.3.2.5.3</td><td>The Access Domain DAP is an optional signature. The security policy of the provider of the application to which the file system belongs may require the presence of this DAP.</td></tr>
<tr><td>RQ05_2202</td><td>8.2.1.3.2.5.3</td><td>The input data used to compute the Access Domain DAP is the concatenation of the following data:
<table>
<tr><th>Description</th><th>Length</th></tr>
<tr><td>Length of instance AID</td><td>1</td></tr>
<tr><td>Instance AID</td><td>5 to 16</td></tr>
<tr><td>Length of File System AID</td><td>1</td></tr>
<tr><td>File System AID</td><td>0 or n</td></tr>
<tr><td>Length of Access Domain</td><td>1</td></tr>
<tr><td>Access Domain</td><td>n</td></tr>
</table></td></tr>
<tr><td>RQ05_2203</td><td>8.2.1.3.2.5.3</td><td>In case of UICC shared File system, the Length of File System AID is 0 and the File System AID is not present in the Access Domain DAP.</td></tr>
<tr><td>RQ05_2204</td><td>8.2.1.3.2.5.3</td><td>The key used to compute the Access Domain DAP is: Key identifier '02' of Key Version number '11' in the Security Domain associated to the application to which the File System belongs. In case of UICC shared file system, the associated Security Domain may be the Issuer Security Domain or another Security Domain, depending on the card issuer's security policy.</td></tr>
<tr><td>RQ05_2205</td><td>8.2.1.3.2.5.3</td><td>Depending on the key type for the Access Domain DAP, if padding is required by the algorithm, the data is appended by '80' and filled up with zero or more '00'.</td></tr>
<tr><td>RQ05_2206</td><td>8.2.1.3.2.5.3</td><td>Depending on the key type for the Access Domain DAP, if DES is used, MAC in CBC mode with initial value set to zero shall be used.</td></tr>
<tr><td>RQ05_2207</td><td>8.2.1.3.2.5.3</td><td>Depending on the key type for the Access Domain DAP, if AES [13] is used, CMAC mode [15] shall be used. The length of the MAC shall be associated with the key.</td></tr>
<tr><td>RQ05_3202</td><td>8.2.1.6</td><td>The LOGICALLY_DELETED Life Cycle State may be returned as defined in Open Platform Card Specification 2.0.1 [8].</td></tr>
<tr><td>RQ05_3204</td><td>8.2.1.6</td><td>When using the Compact Remote Application data format, the context established by GET STATUS [get first or all occurrence(s)] shall be saved across command sessions as long as more output data related to the initial GET STATUS command is available on the UICC.</td></tr>
<tr><td>RQ05_3403</td><td>8.2.1.7</td><td>If a UICC contains an Application Provider Security Domain with Delegated Management privilege, the tag values '42' and '45' shall be supported by the ISD as specified in the UICC Configuration for GET DATA [16].</td></tr>
</table>

Annex G (informative): Core specification version information

Unless otherwise specified, the versions of ETSI TS 102 226 [1] from which conformance requirements have been extracted are as follows.

Release	Latest version from which conformance requirements have been extracted
11.1	V11.2.0

Annex H (informative): Change History

Change history								
Date	**Meeting**	**Plenary Doc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**Old**	**New**
2018	SCP-84	SCP(18)000153r1	6	1	F	Correction of the length in the expected Response Scripting Template	11.0.0	11.1.0
2018	SCP-84	SCP(18)000154	7		F	Correction of the number of executed command and response TAG in the expected response	11.0.0	11.1.0
2018	SCP-84	SCP(18)000155	8		F	Correction of increase and install [for install] commands	11.0.0	11.1.0
2018	SCP-84	SCP(18)000156	9		F	Correction of the SW for missing verify pin	11.0.0	11.1.0
2018	SCP-84	SCP(18)000157	10		F	Remove Select as case 4	11.0.0	11.1.0
2018	SCP-84	SCP(18)000158r1	11	1	F	Correction of wrong definition of EF_{LF4R4b}	11.0.0	11.1.0
2018	SCP-84	SCP(18)000160	13		F	Correction for Search Record command with wrong P1	11.0.0	11.1.0
2018	SCP-84	SCP(18)000161	14		F	Correction of wrong number of executed commands	11.0.0	11.1.0
2018	SCP-84	SCP(18)000162	15		F	Add select by path from MF	11.0.0	11.1.0
2018	SCP-84	SCP(18)000163	16		F	Addition of missing additional data for Delete command	11.0.0	11.1.0
2018	SCP-84	SCP(18)000164	17		F	Addition of "unknown application" missing in case of HTTPS	11.0.0	11.1.0
2018	SCP-84	SCP(18)000165	18		F	Send the put key command to SD	11.0.0	11.1.0
2018	SCP-84	SCP(18)000166r1	19	1	F	GET STATUS command sent to SD	11.0.0	11.1.0
2018	SCP-84	SCP(18)000167r1	20	1	F	Add Cyclic file for Increase command tests	11.0.0	11.1.0
2018	SCP-84	SCP(18)000168	21		F	Correction of wrong number of expected commands	11.0.0	11.1.0
2018	SCP-85	SCP(18)000223	22		F	Clarification on Note about HTTP protocol	11.0.0	11.1.0
2018	SCP-85	SCP(18)000224r1	23		F	Correction of length in the expected response AB tag	11.0.0	11.1.0
2018	SCP-85	SCP(18)000225	24		F	Correction of EF RMA	11.0.0	11.1.0

History

Document history		
V11.0.0	May 2016	Publication
V11.1.0	March 2019	Publication