ETSI TS 103 481 V11.0.0 (2016-05)

TECHNICAL SPECIFICATION

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/ffc3a58c-ce60-4a04-a716-5f2a205ee0b7/etsi-ts-103-481-v11.0.0-2016-05

Reference

DTS/SCP-00RAMTESTV09000

Keywords

protocol, smart card

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/fc3a58c-ce00-4a0d-a716-5fea205eddb7/etsi-ts-103-481-v11.0.0-2016-05

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2016.
All rights reserved.

DECTTM, **PLUGTESTS**TM, **UMTS**TM and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPPTM and **LTE**™ are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights 10

Foreword 10

Modal verbs terminology 10

Introduction 10

1 Scope 11

2 References 11
2.1 Normative references 11
2.2 Informative references 13

3 Definitions, symbols and abbreviations 13
3.1 Definitions 13
3.2 Abbreviations 13
3.3 Formats 14
3.3.1 Format of the table of optional features 14
3.3.2 Format of the applicability table 14
3.3.3 Status and Notations 15

4 Test Environment 15
4.1 Test Applicability 15
4.1.1 Table of optional features 15
4.1.2 Applicability table 16
4.2 Test environment description 19
4.3 Tests format 20
4.3.1 Initial Conditions 20
4.3.2 Test procedure 20
4.4 General initial conditions 21
4.4.1 Common rules 21
4.4.2 File system and files content 21
4.4.3 AID and TAR coding 22
4.5 Test equipment / OTA server 23
4.5.1 Test equipment / OTA server requirements 23
4.5.2 Default conditions for DUT operation 23
4.5.3 Java Card™ Software Development Kit 23

5 Conformance Requirements 24
5.1 Overview of remote management 24
5.2 Remote APDU format 24
5.3 Security parameters assigned to applications 30
5.4 Remote File Management (RFM) 31
5.5 Remote Application Management (RAM) 33
5.6 Additional command for push 48
5.7 Confidential application management 51

6 Test Cases 52
6.1 Overview of remote management 52
6.2 Remote APDU format 53
6.2.1 Compact Remote Application data format 53
6.2.2 Expanded Remote Application data format 53
6.2.2.1 Test case 1: A command session with C-APDU TLV Structure with definite length coding 53
6.2.2.1.1 Initial Conditions 53
6.2.2.1.2 Test Procedure 53
6.2.2.2 Test case 2: A command session containing multiple commands with C-APDU TLV Structure with definite length coding - Bad Format 54
6.2.2.2.1 Initial Conditions 54
6.2.2.2.2 Test Procedure 54
6.2.2.3 Test case 3: A command session with C-APDU TLV Structure with indefinite length coding 55
6.2.2.3.1 Initial Conditions 55

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/ffc3a58c-ce60-4d0a-a716-5f2a205eddb7/etsi-ts-103-481-v11.0.0-2016-05

6.2.2.3.2 Test Procedure ... 56
6.2.2.4 Test case 4: A command session with C-APDU TLV Structure with indefinite length coding - Bad Format ... 56
6.2.2.4.1 Initial Conditions ... 56
6.2.2.4.2 Test Procedure ... 57
6.2.2.5 Test case 5: A command session with Immediate Action TLV Structure with definite length coding - Normal Format ... 58
6.2.2.5.1 Initial Conditions ... 58
6.2.2.5.2 Test Procedure ... 58
6.2.2.6 Test case 6: A command session with Immediate Action TLV Structure with definite length coding - Referenced Format ... 59
6.2.2.6.1 Initial Conditions ... 59
6.2.2.6.2 Test Procedure ... 59
6.2.2.7 Test case 7: A command session with Immediate Action TLV Structure with definite length coding - Immediate Action Error ... 60
6.2.2.7.1 Initial Conditions ... 60
6.2.2.7.2 Test Procedure ... 60
6.2.2.8 Test case 8: A command session with Immediate Action TLV Structure with indefinite length coding - Normal Format ... 60
6.2.2.8.1 Initial Conditions ... 60
6.2.2.8.2 Test Procedure ... 60
6.2.2.9 Test case 9: A command session with Immediate Action TLV Structure with indefinite length coding - Referenced Format ... 61
6.2.2.9.1 Initial Conditions ... 61
6.2.2.9.2 Test Procedure ... 61
6.2.2.10 Test case 10: A command session with Immediate Action TLV Structure with indefinite length coding - Immediate Action Error ... 61
6.2.2.10.1 Initial Conditions ... 61
6.2.2.10.2 Test Procedure ... 61
6.2.2.11 Test case 11: A command session with Error Action TLV Structure with definite length coding - normal format ... 62
6.2.2.11.1 Initial Conditions ... 62
6.2.2.11.2 Test Procedure ... 62
6.2.2.12 Test case 12: A command session with Error Action TLV Structure with definite length coding - Referenced format ... 62
6.2.2.12.1 Initial Conditions ... 62
6.2.2.12.2 Test Procedure ... 63
6.2.2.13 Test case 13: A command session with Error Action TLV Structure with indefinite length coding - Normal format ... 63
6.2.2.13.1 Initial Conditions ... 63
6.2.2.13.2 Test Procedure ... 63
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 ... 64
6.2.2.15 Test case 15: A command session with Script Chaining TLV Structure with definite length coding ... 64
6.2.2.15.1 Initial Conditions ... 64
6.2.2.15.2 Test Procedure ... 64
6.2.2.16 Test case 16: A command session with Script Chaining TLV Structure with definite length coding (Script Chaining Error) ... 65
6.2.2.16.1 Initial Conditions ... 65
6.2.2.16.2 Test Procedure ... 65
6.2.2.17 Test case 17: A command session with Script Chaining TLV Structure with indefinite length coding ... 65
6.2.2.17.1 Initial Conditions ... 65
6.2.2.17.2 Test Procedure ... 65
6.2.2.18 Test case 18: A command session with Script Chaining TLV Structure with indefinite length coding (Script Chaining Error) ... 66
6.2.2.18.1 Initial Conditions ... 66
6.2.2.18.2 Test Procedure ... 66
6.3 Security parameters assigned to applications ... 66

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/ffe3a58c-ce604a04-a716-5f2a205eddb7/etsi-ts-103-481-v11.0.0-2016-05

6.3.1 Minimum Security Level (MSL) 66
6.3.2 Access domain 66
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). 68
6.4.1.3.1 Initial Conditions 68
6.4.1.3.2 Test Procedure 68
6.4.1.4 Test case 4: A command session with multiple commands (SET DATA, RETRIEVE DATA). 69
6.4.1.4.1 Initial Conditions 69
6.4.1.4.2 Test Procedure 69
6.4.1.5 Test case 5: A command session with multiple commands (ACTIVATE FILE, DEACTIVATE FILE) 69
6.4.1.5.1 Initial Conditions 69
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) 70
6.4.1.6.1 Initial Conditions 70
6.4.1.6.2 Test Procedure 70
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) 71
6.4.1.8.1 Initial Conditions 71
6.4.1.8.2 Test Procedure 71
6.4.1.9 Test case 9: A command session with multiple commands (CREATE FILE, RESIZE FILE, DELETE FILE) 72
6.4.1.9.1 Initial Conditions 72
6.4.1.9.2 Test Procedure 72
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 73
6.4.2.2 Test case 2: A command session with multiple commands (SELECT, UPDATE BINARY, READ BINARY) 73
6.4.2.2.1 Initial Conditions 73
6.4.2.2.2 Test Procedure 73
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) 74
6.4.2.4.1 Initial Conditions 74
6.4.2.4.2 Test Procedure 74
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) 75
6.4.2.6.1 Initial Conditions 75
6.4.2.6.2 Test Procedure 75
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 76
6.4.2.8 Test case 8: A command session with multiple commands (UNBLOCK PIN) 76
6.4.2.8.1 Initial Conditions 76

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/ffc3a78c-ce60-4a04-a716-5f2a205dddb7/etsi-ts-103-481-v11.0.0-2016-05

6.4.2.8.2 Test Procedure 76
6.4.2.9 Test case 9: A command session with multiple commands (CREATE FILE, RESIZE FILE, DELETE FILE)..77
6.4.2.9.1 Initial Conditions 77
6.4.2.9.2 Test Procedure 77
6.4.3 RFM implementation over HTTPS...77
6.5 Remote Application Management (RAM) 78
6.5.1 DELETE 78
6.5.1.1 Test case 1: DELETE command 78
6.5.1.1.1 Initial Conditions 78
6.5.1.1.2 Test Procedure 78
6.5.2 SET STATUS 78
6.5.2.1 Test case 1: SET STATUS command within a command session 78
6.5.2.1.1 Initial Conditions 78
6.5.2.1.2 Test Procedure 78
6.5.3 INSTALL..79
6.5.3.1 INSTALL [for load]..79
6.5.3.1.1 Test case 1: INSTALL [for load] as a single command in the session 79
6.5.3.1.2 Test case 2: INSTALL[for load] with memory management parameters.......................................79
6.5.3.2 INSTALL [for install] 80
6.5.3.2.1 Test case 1: INSTALL[for install] with SIM File Access and Toolkit Application Specific Parameters 80
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...80
6.5.3.2.3 Test case 3: INSTALL[for install] with UICC System Specific Parameter "UICC Toolkit Application specific parameters field" 81
6.5.3.2.4 Test case 4: INSTALL[for install] with UICC System Specific Parameter "UICC Access Application specific parameters field" 81
6.5.3.2.5 Test case 5: INSTALL[for install] with UICC System Specific Parameter "UICC Administrative Access Application specific parameters field" 82
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...82
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 83
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') 84
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') 85
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')..85
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') 86
6.5.3.2.13 Test case 13: INSTALL[for install] with requested item identifier for SIM Toolkit Application Specific Parameters set to '128'...87
6.5.3.2.14 Test case 14: INSTALL[for install] with requested item identifier for UICC Toolkit Application Specific Parameters set to '128'...87
6.5.3.2.15 Test case 15: INSTALL[for install] with Minimum Security Level field of SIM Toolkit Application different from zero 88
6.5.3.2.16 Test case 16: INSTALL[for install] with Minimum Security Level field of UICC Toolkit Application different from zero 88
6.5.3.2.17 Test case 17: INSTALL[for install] with Minimum Security Level field of SIM Toolkit Application different from SPI1 88
6.5.3.2.18 Test case 18: INSTALL[for install] with Minimum Security Level field of UICC Toolkit Application different from SPI1 89
6.5.3.2.19 Test case 19: INSTALL[for install] SIM Toolkit Applications with Access Domain Parameter equal to '00' and 'FF' 89
6.5.3.2.20 Test case 20: INSTALL[for install] UICC Toolkit Applications with Access Domain Parameter equal to '00' and 'FF' 90

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/ffc3a58c-ce60-4a04-a71f-52a2052ddb07/etsi-ts-103-481-v11.0.0-2016-05

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' 91
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' 92
6.5.3.2.23 Test case 23: INSTALL[for install] SIM Toolkit Application with Access Domain Parameter not supported 93
6.5.3.2.24 Test case 24: INSTALL[for install] UICC Toolkit Application with Access Domain Parameter not supported 93
6.5.3.2.25 Test case 25: INSTALL[for install] UICC Toolkit Application with Access Domain Parameter equal to '02' 94
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 95
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 96
6.5.3.2.28 Test case 28: INSTALL[for install] of SIM Toolkit Applications with different Priority levels 97
6.5.3.2.29 Test case 29: INSTALL[for install] of UICC Toolkit Applications with different Priority levels 97
6.5.3.2.30 Test case 30: INSTALL[for install] SIM Toolkit Applets with same Priority levels 98
6.5.3.2.31 Test case 31: INSTALL[for install] UICC Toolkit Applets with same Priority levels 98
6.5.3.2.32 Test case 32: INSTALL[for install] two SIM Toolkit Applications with identical TAR value 99
6.5.3.2.33 Test case 33: INSTALL[for install] two UICC Toolkit Application with identical TAR value 100
6.5.3.2.34 Test case 34: INSTALL[for install] SIM Toolkit Application with multiple TAR values 101
6.5.3.2.35 Test case 35: INSTALL[for install] UICC Toolkit Application with multiple TAR values 101
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 102
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 102
6.5.3.2.38 Test case 38: INSTALL[for install] for contactless application with Reader mode protocol data type A 103
6.5.3.2.39 Test case 39: INSTALL[for install] for contactless application with Reader mode protocol data type B 103
6.5.3.2.40 Test case 40: INSTALL[for install] for contactless application with Card Emulation mode 104
6.5.4 LOAD 104
6.5.4.1 Test case 1: LOAD with DES for DAP verification 104
6.5.4.1.2 Test Procedure 104
6.5.5 PUT KEY 105
6.5.5.1 Test case 1: PUT KEY - create new 3DES 2 keys 105
6.5.5.1.1 Initial Conditions 105
6.5.5.1.2 Test Procedure 105
6.5.5.2 Test case 2: PUT KEY - create new 3DES 3 keys 105
6.5.5.2.1 Initial Conditions 105
6.5.5.2.2 Test Procedure 106
6.5.5.3 Test case 3: PUT KEY - add and replace DES keys 106
6.5.5.3.1 Initial Conditions 106
6.5.5.3.2 Test Procedure 106
6.5.5.4 Test case 4: PUT KEY - create new 16 bytes AES keys 106
6.5.5.4.1 Initial Conditions 106
6.5.5.4.2 Test Procedure 107
6.5.5.5 Test case 5: PUT KEY - create new 24 bytes AES keys 107
6.5.5.5.1 Initial Conditions 107
6.5.5.5.2 Test Procedure 107
6.5.5.6 Test case 6: PUT KEY - create new 32 bytes AES keys 107
6.5.5.6.1 Initial Conditions 107
6.5.5.6.2 Test Procedure 108
6.5.6 GET STATUS 108
6.5.6.1 Test case 1: GET STATUS with different P1 values 108
6.5.6.1.1 Initial Conditions 108
6.5.6.1.2 Test Procedure 108
6.5.6.2 Test case 2: GET STATUS with optional P1 values 109
6.5.6.2.1 Initial Conditions 109
6.5.6.2.2 Test Procedure 109
6.5.6.3 Test case 3: GET STATUS returns Menu Entries in the LOCKED state 109

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/ff3a58c-ce60-4a04-a716-52a205ddb7/etsi-ts-103-481-v11.0.0-2016-05

6.5.6.3.1 Initial Conditions 109
6.5.6.3.2 Test Procedure 109
6.5.7 GET DATA 110
6.5.7.1 Test case 1: GET DATA with different P1 values 110
6.5.7.1.1 Initial Conditions 110
6.5.7.1.2 Test Procedure 110
6.5.8 STORE DATA 111
6.5.8.1 Test case 1: STORE DATA 111
6.5.8.1.1 Initial Conditions 111
6.5.8.1.2 Test Procedure 111
6.5.8.2 Test case 2: STORE DATA with a Forbidden Load File List 111
6.5.8.2.1 Initial Conditions 111
6.5.8.2.2 Test Procedure 111
6.5.9 RAM implementation over HTTPS 111
6.6 Additional command for push 111
6.6.1 BIP 111
6.6.2 CAT_TP 111
6.6.2.1 Test case 1: Send Secured Data (READ BINARY) using Expanded and Compact format with the different TAR value. 111
6.6.2.1.1 Initial Conditions 111
6.6.2.1.2 Test Procedure 112
6.6.2.2 Test case 2: Send Secured Data (READ BINARY) using Expanded and Compact format with the same TAR value. 112
6.6.2.2.1 Initial Conditions 112
6.6.2.2.2 Test Procedure 112
6.6.2.3 Test case 3: PUSH Command, PoR required - No Error 112
6.6.2.3.1 Initial Conditions 112
6.6.2.3.2 Test Procedure 113
6.7 Confidential application management 113

Annex A (normative): BER-TLV tags 114
A.1 BER-TLV tags 114

Annex B (normative): Default file system and files content 115

B.1 DF$_{TEST}$ (UICC Access Tests DF) 115
B.1.1 DF identifier 115
B.1.2 EF$_{TNU}$ (Transparent Never Update) 115
B.1.3 EF$_{TARU}$ (Transparent Always Read and Update) 115
B.1.4 EF$_{TUACP}$ (Transparent Update Access Condition PIN) 115
B.1.5 EF$_{TPRU}$ (Transparent PIN Read and Update) 116
B.1.6 EF$_{LF4R4b}$ 116
B.1.7 EF$_{BER-TLV}$ 116

B.2 DF$_{TESTB}$ (Tests DF under ADF_1) 117
B.2.1 DF identifier 117
B.2.2 EF$_{TARUB}$ (Transparent Always Read and Update B) 117

B.3 DF$_{TELECOM}$ 117
B.3.1 EF$_{RMA}$ (Remote Management Actions) 117

Annex C (normative): Secure data coding and command structure 119

C.1 Commands 119

C.2 Remote APDU Format 121
C.2.1 Compact Remote Application Data Format 121
C.2.2 Expanded Remote Application Data Format 121
C.2.2.1 C-APDU TLV 121
C.2.2.2 Immediate Action TLV 122
C.2.2.3 Error Action TLV 123
C.2.2.4 Script Chaining TLV 124

Annex D (informative): Full command structure sample 125

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/ffc3a58c-ee60-4a04-a716-5ba205edd6b7/etsi-ts-103-481-v11.0.0-2016-05

D.1 Formatted SMS with PoR required - default 125
D.2 CAT-TP - default 125
D.3 HTTPS - default 125

Annex E (normative): AID and TAR values....126
E.1 UICC shared file system remote file management application 126
E.2 ADF remote file management application 126
E.3 AID and TAR....126

Annex F (informative): FFS requirements 127

Annex G (informative): Core specification version information....129

Annex H (informative): Change History 130

History 131

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/ffc3a58c-ce60-4a04-a716-5f2a205eddb7/etsi-ts-103-481-v11.0.0-2016-05

Intellectual Property Rights

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

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/ffc3a58c-ce60-4a04-a71e-5f2a05eddb7/etsi-ts-103-481-v11.0.0-2016-05

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 http://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: See 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: See 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: See http://csrc.nist.gov/publications/fips/index.html.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/ffc3a58c-ce60-4a04-a716-5f2a25edd677/etsi-ts-103-481-v11.0.0-2016-05

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

NOTE: See 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: See http://csrc.nist.gov/publications/nistpubs/.

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

NOTE: See 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: See http://www.globalplatform.org/.

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

NOTE: See 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: See 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: See http://www.globalplatform.org/.

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

NOTE: See 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://www.oracle.com/technetwork/java/javame/javacard/download/overview/index.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)".

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/ffc3a58c-ee09-4a04-a816-5f2a205ed0b7/etsi-ts-103-481-v11.0.0-2016-05

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 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI TS 102 226 [1] 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 Abbreviations

For the purposes of the present document, the following abbreviations given in ETSI TS 102 226 [1] 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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/ffc3a8c-ce69-4a04-a716-5f2a25eddb7/etsi-ts-103-481-v11.0.0-2016-05