ETSI TS 103 666-1 V15.0.0 (2019-11)

TECHNICAL SPECIFICATION

Smart Secure Platform (SSP);
Part 1: General characteristics
(Release 15)

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/5be2afe5-3d2b-4e23-bec1-e8a21649a701/etsi-ts-103-666-1-v15.0.0-2019-11

Reference
DTS/SCP-00TSSPvf00-1

Keywords
M2M, MFF

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/3e14fe5-35b-4e21-bfb1-e8f216495230/etsi-ts-103-666-1-v15.0.0-2019-11

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 prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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.

© ETSI 2019.
All rights reserved.

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

Contents

Intellectual Property Rights 11
Foreword 11
Modal verbs terminology 12
1 Scope 13
2 References 13
2.1 Normative references 13
2.2 Informative references 15
3 Definition of terms, symbols and abbreviations 15
3.1 Terms 15
3.2 Symbols 16
3.3 Abbreviations 16
4 Introduction 18
4.1 Background 18
4.2 Document layout 18
4.3 References to UICC 18
4.4 ASN.1 syntax 18
4.4.1 Introduction 18
4.4.2 Start of ASN.1 18
5 SSP architecture 19
5.1 Overview 19
5.2 SSP software architecture 19
5.3 SSP hardware architecture 20
5.4 Protocol stacks 21
5.5 Execution frameworks 22
6 SSP characteristics 22
6.1 Form factors 22
6.2 Power 22
6.2.1 Power mode 22
6.2.2 Power sources 23
6.2.2.1 Types of power sources 23
6.2.2.2 Power source of type Interface 23
6.2.2.3 Power source of type Independent 23
6.2.3 Power consumption 24
6.3 Clock 24
6.4 SSP initialization 24
6.4.1 SSP interface session 24
6.4.2 Capability exchange 24
6.4.2.1 Overall description 24
6.4.2.2 SSP not supporting SCL 24
6.4.2.3 SSP supporting SCL 25
6.4.2.4 Capabilities of the terminal 25
6.4.2.5 Capabilities of the SSP 26
6.5 Storage 27
6.6 Data management 27
6.6.1 UICC file system 27
6.6.2 SSP file system 27
6.6.2.1 Overview 27
6.6.2.2 SSP file system structure 28
6.6.2.2.1 Layout 28
6.6.2.2.2 Node types 29
6.6.2.2.3 Node descriptor 29
6.6.2.2.4 Node identity 30
6.6.2.2.5 File handling 31

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/5be344e5-3d2b-4221-bec1-e8a216d0a701/etsi-ts-103-666-1-v15.0.0-2019-11

6.6.2.2.6 Administrative operations 32
6.6.2.2.7 SSP file system access rights 32
6.6.2.3 Primitives of the SSP file system 33
6.6.2.3.1 FS-ADMIN-GET-CAPABILITIES-Service-Command 33
6.6.2.3.2 FS-ADMIN-CREATE-NODE-Service-Command 34
6.6.2.3.3 FS-ADMIN-DELETE-NODE-Service-Command 35
6.6.2.3.4 FS-ADMIN-UPDATE-NODE-ATTRIBUTES-Service-Command 35
6.6.2.3.5 FS-OP-FILE-OPEN-Service-Command 36
6.6.2.3.6 FS-OP-FILE-CLOSE-Service-Command 37
6.6.2.3.7 FS-OP-NODE-GET-INFO-Service-Command 37
6.6.2.3.8 FS-OP-FILE-READ-Service-Command 38
6.6.2.3.9 FS-OP-FILE-WRITE-Service-Command 39
6.6.2.3.10 FS-OP-FILE-GET-POSITION-Service-Command 40
6.6.2.4 Response code 41
6.6.2.4.1 Overview 41
6.6.2.4.2 Response code to SSP file system primitives 42
6.7 SSP identification 42
6.8 Runtime environment 42
6.8.1 CAT Runtime Environment 42
6.9 SSP suspension 43
6.10 SSP Applications 43
6.10.1 Overview 43
6.10.2 Ownership and security considerations 44
6.10.3 Lifecycle management 44
6.10.4 Identification and discovery 44
6.11 SSP security 44
6.11.1 SSP security architecture 44
6.11.2 Mandatory requirements 45
6.11.2.1 Overview 45
6.11.2.2 Security of SSP code 45
6.11.2.3 Privacy of data 46
6.11.2.3.1 Secure storage 46
6.11.2.4 SSP transactions 46
6.11.2.5 Attack resistance 46
6.11.3 Optional requirements 46
6.11.3.1 Overview 46
6.11.3.2 Random number generator 46
6.11.3.3 Remote provisioning 46
6.11.3.4 Remote auditing 47
6.11.4 Security certification 47
6.11.4.1 Overview 47
6.12 User interface 47
6.12.1 Web-based user interface 47
6.12.1.1 Overview 47
6.12.1.2 Port values 48
6.12.1.3 Presentation of SSP user interface 48
6.13 Accessor authentication service 48
6.13.1 Overview 48
6.13.2 Access control 49
6.13.2.1 Overview 49
6.13.2.2 Description 49
6.13.2.3 Accessor rights to a resource 50
6.13.3 Access control list 51
6.13.4 Accessor 51
6.13.4.1 Overview 51
6.13.4.2 Anonymous accessor 52
6.13.4.3 Accessor identity 52
6.13.4.4 Accessor conditions 52
6.13.4.5 Access rights 54
6.13.4.6 Operations on an accessor 55
6.13.4.6.1 Creation 55

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/5bc34fe5-3d2b-4e23-bec1-e8a21649a701/etsi-ts-103-666-1-v15.0.0-2019-11

6.13.4.6.2 Deletion 55
6.13.4.6.3 Update of the access control list 55
6.13.4.6.4 Update of the conditions and credentials 55
6.13.4.6.5 Update of the group list 55
6.13.4.7 Accessor credentials 55
6.13.4.8 Accessor credential policy 56
6.13.4.9 Accessor credential status 57
6.13.5 Primitives of the access control 58
6.13.5.1 AAS-OP-GET-CAPABILITIES-Service-Command 58
6.13.5.2 AAS-ADMIN-CREATE-ACCESSOR-Service-Command 59
6.13.5.3 AAS-ADMIN-UPDATE-ACCESSOR-Service-Command 60
6.13.5.4 AAS-ADMIN-DELETE-ACCESSOR-Service-Command 61
6.13.5.5 AAS-OP-AUTHENTICATE-ACCESSOR-Service-Command 61
6.13.5.6 AAS-OP-ACCESS-SERVICE-Service-Command 62
6.13.5.7 AAS-OP-GET-CHALLENGE-Service-Command 63
6.13.6 Response code 64
6.13.6.1 Overview 64
6.13.6.2 Response code to access control primitives 64

7 Physical interfaces 65
7.1 Overview 65
7.2 Reset 65
7.3 ISO/IEC 7816 interface 66
7.3.1 Electrical specifications 66
7.3.1.1 Electrical specifications of the interface 66
7.3.1.2 Contacts 66
7.3.2 Initial communication establishment procedures 66
7.3.2.1 SSP interface activation and deactivation 66
7.3.2.2 Supply voltage switching 66
7.3.2.3 Answer To Reset content 66
7.3.2.4 PPS procedure 66
7.3.2.5 Reset procedure 66
7.3.2.6 Clock stop mode 67
7.3.2.7 Bit/character duration and sampling time 67
7.3.2.8 Error handling 67
7.3.3 Data link protocols 67
7.3.3.1 Overview 67
7.3.3.2 Character frame 67
7.3.3.3 Protocol T=1 67
7.4 SPI interface 67
7.5 I2C interface 67
7.6 SWP interface 67
7.7 USB interface 67
7.8 Proprietary interface 67

8 SSP Common Layer (SCL) 68
8.1 Introduction 68
8.2 SCL network 68
8.3 Protocol layers 69
8.3.1 Overview 69
8.3.2 Network layer 69
8.3.3 Transport layer 69
8.3.4 Session layer 69
8.4 SCL core services 69
8.4.1 Overview 69
8.4.2 Common core features 69
8.4.3 Link gate 69
8.4.3.1 Link service gate 69
8.4.3.1.1 General description 69
8.4.3.1.2 Additional registry entries 69
8.4.3.1.3 SSP_MTU 70
8.4.3.2 Link application gate 70

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/5be34fe5-362b-4e23-bec1-e8a216d9a701/etsi-ts-103-666-1-v15.0.0-2019-11

8.4.4 Administration gate 70
8.4.4.1 Administration service gate 70
8.4.4.2 Administration application gate 70
8.4.5 Identity gate 70
8.4.5.1 Identity service gate 70
8.4.5.1.1 General description 70
8.4.5.1.2 Additional registry entries 70
8.4.5.1.3 CAPABILITY_EXCHANGE 71
8.4.5.1.4 GATE_URN_LIST 71
8.4.5.2 Identity application gate 71
8.4.6 Loopback gate 71
8.4.6.1 Loopback service gate 71
8.4.6.2 Loopback application gate 71
8.5 SCL procedures 72
8.5.1 Host registration 72
8.5.2 Host deregistration 72
8.5.3 Pipe management 72
8.5.4 Registry access 72
8.5.5 Hosts and gates discovery 72
8.5.6 Loopback testing 72

9 Secure SCL 72
9.1 Protocol stack 72
9.2 Secure datagram 73
9.3 Security protocol 74
9.3.1 Overview 74
9.3.2 Shared secret initialization 74
9.3.3 Secure SCL shared keys generation 75
9.4 Accessor authentication service procedure 75
9.4.1 Initialization 75

10 Communication layers above SCL 76
10.1 Overview 76
10.2 APDU protocol 76
10.2.1 Introduction 76
10.2.2 Command-response pairs 76
10.2.2.1 General definition 76
10.2.2.2 CLA byte 76
10.2.2.3 INS byte 76
10.2.2.4 Coding of SW1 and SW2 77
10.2.3 SSP commands 77
10.2.3.1 Overview 77
10.2.3.2 EXCHANGE CAPABILITIES 77
10.2.3.2.1 Description 77
10.2.3.2.2 Command parameters 77
10.2.3.2.3 Command data 78
10.2.3.2.4 Command response 78
10.2.3.3 SELECT 78
10.2.4 Logical channels 78
10.2.4.1 Overview 78
10.2.4.2 MANAGE CHANNEL 78
10.2.5 UICC file system commands 79
10.2.5.1 Overview 79
10.2.5.2 Methods for selecting a file 79
10.2.5.3 Reservation of file IDs 79
10.2.5.4 Security features 79
10.2.5.5 Additional commands 79
10.2.6 Card Application Toolkit 79
10.2.6.1 Overview 79
10.2.6.2 Terminal profile 80
10.2.6.3 Proactive polling 80
10.2.6.4 Additional commands 80

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/5be34fe5-362b-4e23-bec1-e8a2fc49a701/etsi-ts-103-666-1-v15.0.0-2019-11

10.2.7 SSP suspension 80
10.2.8 APDU transfer over SCL 80
10.2.8.1 Overview 80
10.2.8.2 UICC APDU gate 81
10.2.8.2.1 UICC APDU overview 81
10.2.8.2.2 UICC APDU service gate 81
10.2.8.2.3 UICC APDU application gate 81
10.2.8.2.4 State diagram for the UICC APDU gate 82
10.3 File system protocol 82
10.3.1 Overview 82
10.3.2 Presentation layer 83
10.3.3 File system control service gate 83
10.3.3.1 Overview 83
10.3.3.2 Commands 84
10.3.3.3 Responses 84
10.3.3.4 Events 84
10.3.4 File system control application gate 84
10.3.4.1 Overview 84
10.3.4.2 Commands 84
10.3.4.3 Responses 85
10.3.4.4 Events 85
10.3.5 File system data service gate 85
10.3.5.1 Overview 85
10.3.5.2 Commands 85
10.3.5.3 Responses 85
10.3.5.4 Events 85
10.3.6 File system data application gate 85
10.3.6.1 Overview 85
10.3.6.2 Commands 85
10.3.6.3 Responses 85
10.3.6.4 Events 85
10.4 Transmission Control Protocol support 86
10.4.1 Overview 86
10.4.2 Management of TCP connections 87
10.4.2.1 TCP connection request 87
10.4.2.1.1 TCP active connection request (client mode) 87
10.4.2.1.2 TCP passive connection request (server mode) 87
10.4.2.2 TCP connection established 87
10.4.2.3 TCP end of connection 87
10.4.3 Presentation layer 87
10.4.4 TCP control service gate 88
10.4.4.1 Overview 88
10.4.4.2 Commands 88
10.4.4.2.1 List of commands 88
10.4.4.2.2 TCP-REQUEST-CONNECTION-Service-Command 88
10.4.4.2.3 TCP-CLOSE-CONNECTION-Service-Command 89
10.4.4.2.4 TCP-GET-STATUS-CONNECTION-Service-Command 90
10.4.4.3 Responses 91
10.4.4.4 Events 92
10.4.5 TCP control application gate 92
10.4.5.1 Overview 92
10.4.5.2 Commands 92
10.4.5.2.1 List of commands 92
10.4.5.2.2 TCP-ACCEPT-CONNECTION-Application-Command 92
10.4.5.3 Responses 93
10.4.5.4 Events 93
10.4.5.4.1 List of events 93
10.4.5.4.2 EVT-TCP-ERROR-Application-Event 94
10.4.6 TCP data service gate 95
10.4.6.1 Overview 95
10.4.6.2 Commands 95

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/5be34fe5-3d2b-4e23-bec1-e8f21649a701/etsi-ts-103-666-1-v15.0.0-2019-11

10.4.6.3 Responses 95
10.4.6.4 Events 95
10.4.7 TCP data application gate 95
10.4.7.1 Overview 95
10.4.7.2 Commands 95
10.4.7.3 Responses 95
10.4.7.4 Events 95
10.4.8 Application protocols 95
10.4.8.1 HTTP(S) protocol 95
10.4.8.2 TLS protocol 96
10.5 User Datagram Protocol support 96
10.5.1 Overview 96
10.5.2 Presentation layer 97
10.5.3 UDP service gate 97
10.5.3.1 Overview 97
10.5.3.2 Commands 97
10.5.3.2.1 List of commands 97
10.5.3.2.2 UDP-REQUEST-SOCKET-Command 97
10.5.3.2.3 UDP-CLOSE-SOCKET-Command 98
10.5.3.3 Responses 99
10.5.3.4 Events 99
10.5.3.4.1 List of events 99
10.5.3.4.2 EVT-UDP-DATAGRAM-OUT-Service-Event 100
10.5.4 UDP application gate 100
10.5.4.1 Overview 100
10.5.4.2 Commands 100
10.5.4.3 Responses 100
10.5.4.4 Events 100
10.5.4.4.1 List of events 100
10.5.4.4.2 EVT-UDP-DATAGRAM-IN-Application-Event 101
10.5.4.4.3 EVT-UDP-ERROR-Application-Event 101
10.5.5 Application protocols 102
10.5.5.1 CoAP over UDP Protocol 102
10.6 CRON service support 102
10.6.1 Overview 102
10.6.2 Presentation layer 102
10.6.3 CRON service gate 103
10.6.3.1 Overview 103
10.6.3.2 Commands 103
10.6.3.2.1 List of commands 103
10.6.3.2.2 CRON-REQUEST-TIMER-Command 103
10.6.3.2.3 CRON-READ-DATE-TIME-Command 104
10.6.3.2.4 CRON-KILL-TIMER-Command 105
10.6.3.2.5 CRON-KILL-ALL-TIMERS-Command 105
10.6.3.3 Responses 105
10.6.3.4 Events 106
10.6.4 CRON application gate 106
10.6.4.1 Commands 106
10.6.4.2 Responses 106
10.6.4.3 Events 107
10.6.4.3.1 List of events 107
10.6.4.3.2 CRON-ELAPSED-TIMER-Event 107
10.7 Contactless related applications support 107
10.7.1 Introduction 107
10.7.2 HCP tunneling over SCL 107
10.7.2.1 Overview 107
10.7.2.2 SCL HCI service gate 108
10.7.2.3 SCL HCI application gate 108
10.8 Card Application Toolkit (CAT) over SCL 108
10.8.1 Overview 108
10.8.2 Structure of Card Application Toolkit (CAT) communications 109

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/5bc34fe5-3d2b-4e23-bec1-e8a21649a701/etsi-ts-103-666-1-v15.0.0-2019-11

10.8.3 CAT application gate 110
10.8.3.1 Overview 110
10.8.3.2 Commands 110
10.8.3.3 Responses 110
10.8.3.4 Events 110
10.8.3.4.1 Supported events 110
10.8.3.4.2 EVT_ENVELOPE_CMD 110
10.8.3.4.3 EVT_TERMINAL_RESPONSE 110
10.8.3.5 Registry 111
10.8.4 CAT service gate 111
10.8.4.1 Overview 111
10.8.4.2 Commands 111
10.8.4.3 Responses 111
10.8.4.4 Events 111
10.8.4.4.1 Supported events 111
10.8.4.4.2 EVT_PROACTIVE_CMD 111
10.8.4.4.3 EVT_ENVELOPE_RSP 112
10.8.4.5 Registry 112
10.8.5 State diagram for the CAT application gate 112
10.9 Access control protocol 113
10.9.1 Introduction 113
10.9.2 Presentation layer 114
10.9.3 Accessor authentication service gate 114
10.9.3.1 Overview 114
10.9.3.2 Commands 115
10.9.3.3 Responses 115
10.9.3.4 Events 115
10.9.4 Accessor authentication application gate 115
10.9.4.1 Overview 115
10.9.4.2 Commands 115
10.9.4.3 Responses 115
10.9.4.4 Events 115

11 SSP classes 116
11.1 Overview 116

Annex A (informative): Example of SCL flow 117

Annex B (informative): Support for UICC applications over SCL 118

B.1 UICC APDU service gate 118

Annex C (normative): SCL secure pipe 119

C.1 Overview 119

C.2 Authentication tokens 119
C.2.1 Description 119
C.2.2 Format 119

C.3 Certification paths 120
C.3.1 Description 120
C.3.2 Format 120
C.3.3 Identifiers and value used by certificate management 120
C.3.3.1 ECC domain parameters 120
C.3.3.2 Algorithm identifiers and parameters 121
C.3.3.3 Certificate policy OID 121
C.3.3.4 Certificate revocation 121
C.3.4 Long term keys 122
C.3.5 Functions 122

C.4 Datagram encryption 122
C.4.1 Principle 122
C.4.2 SharedInfo 122

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/5bc34fe5-3d2b-4e23-bcc1-ca216d9a701/etsi-ts-103-666-1-v15.0.0-2019-11

C.4.3 Encryption/decryption 123

Annex D (informative): TCP service procedures 124

D.1 Connection request in active mode 124

D.2 Connection request in passive mode 125

D.3 Connection request failure 126

D.4 Connection closing 127

Annex E (informative): UDP service procedures 128

E.1 UDP socket request 128

E.2 Socket closing 129

Annex F (informative): CRON service procedures 130

F.1 CRON timer request 130

F.2 CRON timer killing 131

F.3 CRON read date command 132

Annex G (informative): File system protocol service procedures 133

G.1 File reading 133

G.2 File writing 134

G.3 File writing from data stream 135

G.4 File reading from data stream 136

G.5 File reading and get the position 137

Annex H (informative): Example of access control 139

Annex J (informative): Accessor authentication service procedures 140

J.1 Accessor creation 140

J.2 Accessor deletion 140

J.3 Accessor update 141

J.4 Accessor authentication session opening 142

Annex K (informative): UML code of figures 143

Annex L (normative): ASN.1 definitions 144

L.1 End of ASN.1 144

L.2 Complete ASN.1 file 144

Annex M (informative): Change history 145

History 146

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/5be34fe5-3d2b-4e23-bec1-e8a21649a701/etsi-ts-103-666-1-v15.0.0-2019-11

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.

The present document is part 1 of a multi-part deliverable covering Smart Secure Platform (SSP), as identified below:

Part 1: "General characteristics";

Part 2: "Integrated SSP (iSSP) characteristics".

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/be34fe5-3d2b-6c23-bec1-e8a21649a701/etsi-ts-103-666-1-v15.0.0-2019-11

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/5be34fe5-3d2b-4e23-bec1-e8a21649a701/etsi-ts-103-666-1-v15.0.0-2019-11

1 Scope

The present document is part of a serie of documents that specify the technical solution for the Smart Secure Platform (SSP), according to the requirements listed in ETSI TS 103 465 [2].

The present document contains generic technical solutions for different aspects of SSP functionality. It does not specify any specific type of SSP.

The types of SSP are referred to as classes. The class specifications (for example the integrated SSP technical specification in ETSI TS 103 666-2 [8]) refer to the present document for common SSP functionality.

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 102 221: "Smart Cards; UICC-Terminal interface; Physical and logical characteristics".

[2] ETSI TS 103 465: "Smart Cards; Smart Secure Platform (SSP); Requirements Specification".

[3] ISO/IEC 7816-3: "Identification cards -- Integrated circuit cards -- Part 3: Cards with contacts -- Electrical interface and transmission protocols".

[4] ISO/IEC 7816-4: "Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange".

[5] ETSI TS 102 613: "Smart Cards; UICC - Contactless Front-end (CLF) Interface; Physical and data link layer characteristics".

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

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

[8] ETSI TS 103 666-2: "Smart Secure Platform (SSP); Part 2: Integrated SSP (iSSP) characteristics".

[9] ORACLE: "Application Programming Interface, Java Card™ Platform, 3.0.5 Classic Edition".

[10] ORACLE: "Runtime Environment Specification, Java Card™ Platform, 3.0.5 Classic Edition".

[11] ORACLE: "Virtual Machine Specification Java Card™ Platform, 3.0.5 Classic Edition".

NOTE: ORACLE Java Card™ Specifications can be downloaded at https://docs.oracle.com/javacard/3.0.5/index.html.

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

iTeh STANDARD PREVIEW (standards.iteh.ai) Full standard: https://standards.iteh.ai/catalog/standards/sist/5bc34fe5-3d2e-4e23-bec1-e8a21e49a70c/etsi-ts-103-666-1-v15.0.0-2019-11