ETSI TS 103 666-1 V15.9.0 (2022-08)

TECHNICAL SPECIFICATION

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ETSI TS 103 666-1 V15.9.0 (2022-08)
https://standards.iteh.ai/catalog/standards/sist/2fdd8ad9-63a3-4fff-8233-8df585eba064/etsi-ts-103-666-1-v15-9-0-2022-08

Reference

RTS/SET-T103666-1vf90

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

Important notice

The present document can be downloaded from:
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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

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

Copyright Notification

No part 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 2022.
All rights reserved.

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, abbreviations and coding conventions 15
3.1 Terms 15
3.2 Symbols 16
3.3 Abbreviations 16
3.4 Coding conventions 18

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 19

5 SSP architecture 19
5.1 Overview 19
5.2 SSP software architecture 20
5.3 SSP hardware architecture 20
5.4 Protocol stacks 21
5.5 Execution frameworks 22
5.6 Bundle Interoperability 22

6 SSP characteristics 23
6.1 Form factors 23
6.2 Power 23
6.2.1 Power mode 23
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 25
6.4.2.1 Overall description 25
6.4.2.2 SSP not supporting SCL 25
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 28
6.6.2.1 Overview 28
6.6.2.2 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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI TS 103 666-1 V15.9.0 (2022-08)
https://standards.iteh.ai/catalog/standards/sist/2fdd8ad9-63a3-4fff-8233-8df585eba064/etsi-ts-103-666-1-v15-9-0-2022-08

6.6.2.2.4 Node identity 30
6.6.2.2.5 File handling...31
6.6.2.2.6 Administrative operations...32
6.6.2.2.7 SSP file system access rights...32
6.6.2.3 Primitives 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...34
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 executable 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..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 53
6.13.4.5 Access rights 54
6.13.4.6 Operations on an accessor...55

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI TS 103 666-1 V15.9.0 (2022-08)
https://standards.iteh.ai/catalog/standards/sist/2fdd8ad9-63a3-4fff-8233-8df585eba064/etsi-ts-103-666-1-v15-9-0-2022-08

6.13.4.6.1 Creation 55
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 56
6.13.4.6.6 Update of the credential status and policy 56
6.13.4.7 Accessor credentials 56
6.13.4.8 Accessor credential policy 57
6.13.4.9 Accessor credential status 58
6.13.5 Primitives 59
6.13.5.1 AAS-OP-GET-CAPABILITIES-Service-Command 59
6.13.5.2 AAS-ADMIN-CREATE-ACCESSOR-Service-Command 60
6.13.5.3 AAS-ADMIN-UPDATE-ACCESSOR-Service-Command 61
6.13.5.4 AAS-ADMIN-DELETE-ACCESSOR-Service-Command 62
6.13.5.5 AAS-OP-AUTHENTICATE-ACCESSOR-Service-Command 62
6.13.5.6 AAS-OP-ACCESS-SERVICE-Service-Command 63
6.13.5.7 AAS-OP-GET-CHALLENGE-Service-Command 64
6.13.6 Response code 65
6.13.6.1 Overview 65
6.13.6.2 Response codes to accessor authentication service commands 65

7 Physical interfaces 66
7.1 Overview 66
7.2 Reset 66
7.3 ISO/IEC 7816 interface 67
7.3.1 Electrical specifications 67
7.3.1.1 Electrical specifications of the interface 67
7.3.1.2 Contacts 67
7.3.2 Initial communication establishment procedures 67
7.3.2.1 SSP interface activation and deactivation 67
7.3.2.2 Supply voltage switching 67
7.3.2.3 Answer To Reset content 67
7.3.2.4 PPS procedure 67
7.3.2.5 Reset procedure 67
7.3.2.6 Clock stop mode 68
7.3.2.7 Bit/character duration and sampling time 68
7.3.2.8 Error handling 68
7.3.3 Data link protocols 68
7.3.3.1 Overview 68
7.3.3.2 Character frame 68
7.3.3.3 Protocol T=1 68
7.4 SPI interface 68
7.5 I2C interface 68
7.6 SWP interface 68
7.7 USB interface 68
7.8 Proprietary interface 69

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI TS 103 666-1 V15.9.0 (2022-08)
https://standards.iteh.ai/catalog/standards/sist/2fdd8ad9-63a3-4fff-8233-8df585eba064/etsi-ts-103-666-1-v15-9-0-2022-08

8.4.3.1.3 SSP_MTU 71
8.4.3.2 Link application gate 71
8.4.4 Administration gate 71
8.4.4.1 Administration service gate 71
8.4.4.2 Administration application gate 71
8.4.5 Identity gate 71
8.4.5.1 Identity service gate 71
8.4.5.1.1 General description 71
8.4.5.1.2 Additional registry entries 71
8.4.5.1.3 CAPABILITY_EXCHANGE 72
8.4.5.1.4 GATE_URN_LIST 72
8.4.5.2 Identity application gate 72
8.4.6 Loopback gate 72
8.4.6.1 Loopback service gate 72
8.4.6.2 Loopback application gate 72
8.4.6.3 Registry 73
8.5 SCL procedures 73
8.5.1 Host registration 73
8.5.2 Host deregistration 73
8.5.3 Pipe management 73
8.5.4 Registry access 74
8.5.5 Hosts and gates discovery 74
8.5.6 Loopback testing 74

9 Secure SCL 74
9.1 Protocol stack 74
9.2 Structure of secure SCL message 74
9.3 Security protocol 76
9.3.1 Overview 76
9.3.2 Shared secret initialization 76
9.3.3 Secure SCL shared keys generation 77
9.4 Accessor authentication service procedure 77
9.4.1 Initialization 77

10 Communication layers above SCL 78
10.1 Overview 78
10.2 APDU protocol 78
10.2.1 Introduction 78
10.2.2 Command-response pairs 78
10.2.2.1 General definition 78
10.2.2.2 CLA byte 78
10.2.2.3 INS byte 78
10.2.2.4 Coding of SW1 and SW2 79
10.2.3 SSP commands 79
10.2.3.1 Overview 79
10.2.3.2 EXCHANGE CAPABILITIES 79
10.2.3.2.1 Description 79
10.2.3.2.2 Command parameters 80
10.2.3.2.3 Command data 80
10.2.3.2.4 Command response 80
10.2.3.3 SELECT 80
10.2.4 Logical channels 80
10.2.4.1 Overview 80
10.2.4.2 MANAGE CHANNEL 81
10.2.5 UICC file system commands 81
10.2.5.1 Overview 81
10.2.5.2 Methods for selecting a file 81
10.2.5.3 Reservation of file IDs 81
10.2.5.4 Additional commands 81
10.2.5.5 Security features 81
10.2.6 Card Application Toolkit 81
10.2.6.1 Overview 81

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI TS 103 666-1 V15.9.0 (2022-08)
https://standards.iteh.ai/catalog/standards/sist/2fdd8ad9-63a3-4fff-8233-8df585eba064/etsi-ts-103-666-1-v15-9-0-2022-08

10.2.6.2 Terminal profile 82
10.2.6.3 Proactive polling 82
10.2.6.4 Additional commands 82
10.2.7 SSP suspension 82
10.2.8 APDU transfer over SCL 83
10.2.8.1 Overview 83
10.2.8.2 UICC APDU gate 83
10.2.8.2.1 UICC APDU overview 83
10.2.8.2.2 UICC APDU service gate 83
10.2.8.2.3 UICC APDU application gate 83
10.2.8.2.4 State diagram for the UICC APDU gate 84
10.3 File system protocol 84
10.3.1 Overview 84
10.3.2 Presentation layer 85
10.3.3 File system control service gate 85
10.3.3.1 Overview 85
10.3.3.2 Commands 86
10.3.3.3 Responses 86
10.3.3.4 Events 86
10.3.4 File system control application gate 86
10.3.4.1 Overview 86
10.3.4.2 Commands 86
10.3.4.3 Responses 87
10.3.4.4 Events 87
10.3.5 File system data service gate 87
10.3.5.1 Overview 87
10.3.5.2 Commands 87
10.3.5.3 Responses 87
10.3.5.4 Events 87
10.3.6 File system data application gate 87
10.3.6.1 Overview 87
10.3.6.2 Commands 87
10.3.6.3 Responses 87
10.3.6.4 Events 87
10.4 Transmission Control Protocol support 88
10.4.1 Overview 88
10.4.2 Management of TCP connections 89
10.4.2.1 TCP connection request 89
10.4.2.1.1 TCP active connection request (client mode) 89
10.4.2.1.2 TCP passive connection request (server mode) 89
10.4.2.2 TCP connection established 89
10.4.2.3 TCP end of connection 89
10.4.3 Presentation layer 89
10.4.4 TCP control service gate 90
10.4.4.1 Overview 90
10.4.4.2 Commands 90
10.4.4.2.1 List of commands 90
10.4.4.2.2 TCP-REQUEST-CONNECTION-Service-Command 90
10.4.4.2.3 TCP-CLOSE-CONNECTION-Service-Command 91
10.4.4.2.4 TCP-GET-STATUS-CONNECTION-Service-Command 92
10.4.4.3 Responses 93
10.4.4.4 Events 94
10.4.5 TCP control application gate 94
10.4.5.1 Overview 94
10.4.5.2 Commands 94
10.4.5.2.1 List of commands 94
10.4.5.2.2 TCP-ACCEPT-CONNECTION-Application-Command 94
10.4.5.3 Responses 95
10.4.5.4 Events 95
10.4.5.4.1 List of events 95
10.4.5.4.2 EVT-TCP-ERROR-Application-Event 96
10.4.6 TCP data service gate 97

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI TS 103 666-1 V15.9.0 (2022-08)
https://standards.iteh.ai/catalog/standards/sist/2fdd8ad9-63a3-4fff-8233-8df585eba064/etsi-ts-103-666-1-v15-9-0-2022-08

10.4.6.1 Overview 97
10.4.6.2 Commands 97
10.4.6.3 Responses 97
10.4.6.4 Events 97
10.4.7 TCP data application gate 97
10.4.7.1 Overview 97
10.4.7.2 Commands 97
10.4.7.3 Responses 97
10.4.7.4 Events 97
10.4.8 Application protocols 97
10.4.8.1 HTTP(S) protocol 97
10.4.8.2 TLS protocol 98
10.5 User Datagram Protocol support 98
10.5.1 Overview 98
10.5.2 Presentation layer 99
10.5.3 UDP service gate 99
10.5.3.1 Overview 99
10.5.3.2 Commands 99
10.5.3.2.1 List of commands 99
10.5.3.2.2 UDP-REQUEST-SOCKET-Command 99
10.5.3.2.3 UDP-CLOSE-SOCKET-Command 100
10.5.3.3 Responses 101
10.5.3.4 Events 101
10.5.3.4.1 List of events 101
10.5.3.4.2 EVT-UDP-DATAGRAM-OUT-Service-Event 102
10.5.4 UDP application gate 102
10.5.4.1 Overview 102
10.5.4.2 Commands 102
10.5.4.3 Responses 102
10.5.4.4 Events 102
10.5.4.4.1 List of events 102
10.5.4.4.2 EVT-UDP-DATAGRAM-IN-Application-Event 103
10.5.4.4.3 EVT-UDP-ERROR-Application-Event 103
10.5.5 Application protocols 104
10.5.5.1 CoAP over UDP Protocol 104
10.6 CRON service support 104
10.6.1 Overview 104
10.6.2 Presentation layer 105
10.6.3 CRON service gate 105
10.6.3.1 Overview 105
10.6.3.2 Commands 105
10.6.3.2.1 List of commands 105
10.6.3.2.2 CRON-REQUEST-TIMER-Command 106
10.6.3.2.3 CRON-READ-DATE-TIME-Command 107
10.6.3.2.4 CRON-KILL-TIMER-Command 107
10.6.3.2.5 CRON-KILL-ALL-TIMERS-Command 108
10.6.3.3 Responses 108
10.6.3.4 Events 109
10.6.4 CRON application gate 109
10.6.4.1 Commands 109
10.6.4.2 Responses 109
10.6.4.3 Events 109
10.6.4.3.1 List of events 109
10.6.4.3.2 CRON-ELAPSED-TIMER-Event 109
10.7 Contactless related applications support 110
10.7.1 Introduction 110
10.7.2 HCP tunnelling over SCL 110
10.7.2.1 Overview 110
10.7.2.2 SCL HCI service gate 110
10.7.2.3 SCL HCI application gate 110
10.8 Card Application Toolkit (CAT) over SCL 111
10.8.1 Overview 111

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI TS 103 666-1 V15.9.0 (2022-08)
https://standards.iteh.ai/catalog/standards/sist/2fdd8ad9-63a3-4fff-8233-8df585eba064/etsi-ts-103-666-1-v15-9-0-2022-08

10.8.2 Structure of Card Application Toolkit (CAT) communications 111
10.8.3 CAT application gate 112
10.8.3.1 Overview 112
10.8.3.2 Commands 112
10.8.3.3 Responses 112
10.8.3.4 Events 112
10.8.3.4.1 Supported events 112
10.8.3.4.2 EVT_ENVELOPE_CMD 112
10.8.3.4.3 EVT_TERMINAL_RESPONSE 113
10.8.3.5 Registry 113
10.8.4 CAT service gate 113
10.8.4.1 Overview 113
10.8.4.2 Commands 113
10.8.4.3 Responses 113
10.8.4.4 Events 113
10.8.4.4.1 Supported events 113
10.8.4.4.2 EVT_PROACTIVE_CMD 114
10.8.4.4.3 EVT_ENVELOPE_RSP 114
10.8.4.5 Registry 114
10.8.5 State diagram for the CAT application gate 114
10.9 Access control protocol 115
10.9.1 Introduction 115
10.9.2 Presentation layer 116
10.9.3 Accessor authentication service gate 116
10.9.3.1 Overview 116
10.9.3.2 Commands 117
10.9.3.3 Responses 117
10.9.3.4 Events 117
10.9.4 Accessor authentication application gate 117
10.9.4.1 Overview 117
10.9.4.2 Commands 117
10.9.4.3 Responses 117
10.9.4.4 Events 117
11 SSP classes 118
11.1 Overview 118
Annex A (informative): Example of SCL flow 119
Annex B (informative): Support for UICC applications over SCL 120
B.1 UICC APDU service gate 120
Annex C (normative): SCL secure pipe 121
C.1 Overview 121
C.2 Authentication tokens 121
C.2.1 Description 121
C.2.2 Format 121
C.3 Certification paths 122
C.3.1 Description 122
C.3.2 Format 122
C.3.3 Identifiers and value used by certificate management 122
C.3.3.1 ECC domain parameters 122
C.3.3.2 Algorithm identifiers and parameters 123
C.3.3.3 Certificate policy OID 123
C.3.3.4 Certificate revocation 123
C.3.4 Long term keys 124
C.3.5 Functions 124
C.4 Datagram encryption 124
C.4.1 Principle 124

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI TS 103 666-1 V15.9.0 (2022-08)
https://standards.iteh.ai/catalog/standards/sist/2fdd8ad9-63a3-4fff-8233-8df585eba064/etsi-ts-103-666-1-v15-9-0-2022-08

C.4.2 SharedInfo ...124
C.4.3 Encryption/decryption ...125

Annex D (informative): TCP service procedures ...126

D.1 Connection request in active mode ...126

D.2 Connection request in passive mode ...127

D.3 Connection request failure...128

D.4 Connection closing ...129

Annex E (informative): UDP service procedures ...130

E.1 UDP socket request ...130

E.2 Socket closing ...131

Annex F (informative): CRON service procedures ...132

F.1 CRON timer request ...132

F.2 CRON timer killing ...133

F.3 CRON read date command...134

Annex G (informative): File system protocol service procedures ...135

G.1 File reading...135

G.2 File writing ...136

G.3 File writing from data stream ...137

G.4 File reading from data stream...138

G.5 File reading and get the position ...139

Annex H (informative): Example of access control ...141

Annex I: Void ...142

Annex J (informative): Accessor authentication service procedures ...143

J.1 Accessor creation ...143

J.2 Accessor deletion ...143

J.3 Accessor update...144

J.4 Accessor authentication session opening ...145

Annex K (informative): UML code of figures ...147

Annex L (normative): ASN.1 definitions ...148

L.1 End of ASN.1 ...148

L.2 Complete ASN.1 file ...148

Annex M (informative): Change history ...149

History ...150

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI TS 103 666-1 V15.9.0 (2022-08)
https://standards.iteh.ai/catalog/standards/sist/77d8ad9-63a3-4fff-8233-8df585eba064/etsi-ts-103-666-1-v15-9-0-2022-08

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

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

Trademarks

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

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI TS 103 666-1 V15.9.0 (2022-08)
https://standards.iteh.ai/catalog/standards/sist/2fdd8ad9-63a3-4fff-8233-8df585eba064/etsi-ts-103-666-1-v15-9-0-2022-08

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Secure Element Technologies (SET).

The contents of the present document are subject to continuing work within TC SET and may change following formal TC SET approval. If TC SET 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 SET for information;

2 presented to TC SET for approval;

3 or greater indicates TC SET 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";

Part 3: "Embedded SSP (eSSP) Type 1 characteristics";

Part 4: "Embedded SSP (eSSP) Type 2 characteristics".

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)
ETSI TS 103 666-1 V15.9.0 (2022-08)
https://standards.iteh.ai/catalog/standards/sist/2fdd8ad9-63a3-4fff-8233-8df585eba064/etsi-ts-103-666-1-v15-9-0-2022-08

1 Scope

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

[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, Classic Edition 3.0.5".

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

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

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)
ETSI TS 103 666-1 V15.9.0 (2022-08)
https://standards.iteh.ai/catalog/standards/sist/2fdd8ad9-65a5-4ff1-8233-8d1585eba064/etsi-ts-103-666-1-v15-9-0-2022-08

[13] GlobalPlatform: "Virtual Primary Platform - Network Protocol", Version 1.0.1.

NOTE: Available at https://globalplatform.org/specs-library/globalplatform-technology-virtual-primary-platform-v1-0-1/.

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

[15] Recommendation ITU-T X.680 (08/2015): "Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation".

[16] Recommendation ITU-T X.690 (08/2015): "Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)".

[17] ETSI TS 102 671: "Smart Cards; Machine to Machine UICC; Physical and logical characteristics".

[18] IETF RFC 7230: "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing".

[19] IETF RFC 2818: "HTTP Over TLS".

[20] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[21] IETF RFC 793: "Transmission Control Protocol".

[22] GlobalPlatform: "Card Specification", Version 2.3.1.

NOTE: Available at https://globalplatform.org/specs-library/card-specification-v2-3-1/.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[23] IETF RFC 768 (August 1980): "User Datagram Protocol".

[24] IETF RFC 7252: "The Constrained Application Protocol (CoAP)".

[25] GlobalPlatform: "UICC Configuration", Version 2.0.

NOTE: Available at https://globalplatform.org/specs-library/uicc-configuration-v2/.

https://standards.iteh.ai/catalog/standards/sist/2fdd8ad9-63a3-4fff-8233-8df585eba064/etsi-ts-103-666-1-v15-9-0-2022-08

[26] IETF RFC 792: "Internet Control Message Protocol".

[27] IETF RFC 6895: "Domain Name System (DNS) IANA Considerations".

[28] IETF RFC 4122: "A Universally Unique IDentifier (UUID) URN Namespace".

[29] IETF RFC 8141: "Uniform Resource Names (URNs)".

[30] IETF RFC 8615: "Well-Known Uniform Resource Identifiers (URIs)".

[31] IETF RFC 3629: "UTF-8, a transformation format of ISO 10646".

[32] ETSI TS 103 713: "Smart Secure Platform (SSP); SPI interface".

[33] ETSI TS 102 705: "Smart Cards; UICC Application Programming Interface for Java Card™ for Contactless Applications".

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

[35] ANSI X9.63:2011: "Public Key Cryptography for the Financial Services Industry - Key Agreement and Key Transport Using Elliptic Curve Cryptography".

[36] BSI Technical Guideline TR-03111: "Elliptic Curve Cryptography", Version 2.0.

[37] FIPS PUB 180-4:2015: "Secure Hash Standard (SHS)".

[38] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[39] IETF RFC 5480: "Elliptic Curve Cryptography Subject Public Key Information".

[40] NIST SP 800-56A: "Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography" (Revision 3), April 2018.

[41] IETF RFC 5639: "Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation".

[42] IETF RFC 6960: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

[43] IETF RFC 5758: "Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA".

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 SET 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.

[i.1] ETSI TR 102 216: "Smart Cards; Vocabulary for Smart Card Platform specifications".

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

iTeh STANDARD PREVIEW (standards.iteh.ai) ETSI TS 103 666-1 V15.9.0 (2022-08) https://standards.iteh.ai/catalog/standards/sist/2fdd8ad9-63a3-4fff-8233-8df585eba064/etsi-ts-103-666-1-v15-9-0-2022-08

3 Definition of terms, symbols, abbreviations and coding conventions

3.1 Terms

For the purposes of the present document, the terms given in ETSI TR 102 216 [i.1] and the following apply:

access control: metadata defining access rights of an accessor or a group of accessors

NOTE: It is an element of the access control list.

access control list: list of access controls attached to the resource

accessor: application which is acting on behalf of an entity, e.g. user or modem

NOTE: The accessor claims an identity when accessing a resource.

accessor authentication: procedure for authentication of an accessor against its credential

accessor credential: means to prove the identity of the accessor, e.g. PIN, fingerprint/minutia, token, signature, etc.

group of accessors: set of accessors

NOTE: A group may be empty.

MBM host domain: SCL host domain residing inside the modem, equivalent to "MBM Host Domain" in GlobalPlatform VPP - Network Protocol [13]

resource: service or information on which access is controlled