ETSI TR 102 216 V5.1.0 (2024-05)

Smart Cards;
Vocabulary for Secure Element Technologies specifications

Reference
RTR/SET-00102216v510

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

Contents

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.

Foreword

This Technical Report (TR) 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:
  - 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.

Modal verbs terminology

In the present document "**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.

1 Scope

The purpose of the present document is to identify specialist technical terms used within the Secure Element Technologies (SET) project for the purposes of writing technical documents. The motivations for this are:

- to ensure that editors use terminology that is consistent across specifications;
- to provide a reader with convenient reference for technical terms that are used across multiple documents;
- to prevent inconsistent use of terminology across documents.

The present document is a collection of terms, definitions, abbreviations and acronyms related to the baseline documents defining SET objectives and systems framework. The present document provides a tool for further work on SET technical documentation and facilitates their understanding.

The terms, definitions and abbreviations as given in the present document are either imported from existing documentation (SET, 3GPP, ETSI, ISO/IEC or elsewhere) or newly created by smart card experts whenever the need for precise vocabulary was identified.

The following types of terms and acronyms are not included in the present document:

- terms and acronyms generally used in computer science, information technology and cryptography;
- terms and acronyms from specific application domains such as mobile telephony and banking;
- terms and acronyms defined and used solely within a specific SET specification to facilitate readability.

But such terms and acronyms may be included if they are frequently used in the SET specifications and a common, precise definition of the term or acronym would aid the interpretation and implementation of the specifications.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

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] Void.

[i.2] ETSI TS 102 221: "Smart Cards; UICC-Terminal interface; Physical and logical characteristics".

[i.3] Recommendation ITU-T E.212: "The international identification plan for public networks and subscriptions".

3 Definition of terms, symbols, equations and abbreviations

3.1 Terms

3.1.0 Introduction

The purpose of the present document is to provide the terms to be used in ETSI SET deliverables.

3.1.1 0-9

1,8 V technology Smart Card: *smart card* containing an integrated circuit designed to operate with supply voltages of 1,8 V ± 10 % and 3 V ± 10 %

3 V technology Smart Card: *smart card* containing an integrated circuit designed to operate with supply voltages of 3 V ± 10 % and 5 V ± 10 %

3.1.2 A

Access Mode (AM): one or more bytes encoding an operation that can be performed on a resource; e.g. read, write, delete, deactivate, etc.

access rule: ordered pair consisting of an *access mode* and a *security condition*

NOTE: The operation described by the *access mode* is allowed by the *UICC operating system* if and only if the security condition is satisfied with respect to the current security state of the *card*.

administrative command: *command* that creates or deletes a resource or modifies the *security attributes* of a resource

Answer To Reset (ATR): byte sequence issued on the communication line by a UICC immediately after a reset signal has been applied to the reset line

application: computer program that defines and implements a useful functionality on a smart *card*

NOTE: The term may apply to the functionality itself, to the representation of the functionality in a programming language, or to the realization of the functionality as *executable code*.

Application Dedicated File (ADF): *directory* on the UICC that is the *root* of a sub-hierarchy of *files* and sub-*directories* that contain data specific to a particular *application*

application executable: representation of an *application* as collection of *executable code*

application firewall: mechanism that prevents one *UICC application* from accessing the data or functionality of another *application*

NOTE: An application firewall can be implemented in hardware or in software.

Application Identifier (AID): data element that uniquely identifies an *application* in a *card*

NOTE: An application identifier is composed of a registered application provider identifier that identifies the entity providing the *application* and a proprietary application identifier extension that identifies the *application* within the set of applications provided by the *application provider* named by the registered application provider identifier.

application layer: layer above the transport layer on which the application messages are exchanged between the sending and receiving applications

application message: package of commands or data sent from the sending application to the receiving application, or vice versa, independently of the transport mechanism

NOTE: An application message is transformed with respect to a chosen transport layer and chosen level of security into one or more secured packets.

application program: representation of an *application* in a programming language such as assembly language, BASIC, C, Java™ SMIL, WML or XHTML

Application Programming Interface (API): collection of *entry points* and *data structures* that an *application program* can access when translated into an *application executable*

application protocol: set of procedures and message formats used to communicate with an *application*

application protocol data unit: synonym for *command*

Application Provider (AP): entity that provides the software components on a *card* required to perform an application

application session: related sequence of commands to and responses from a UICC application starting with application selection and ending either at application de-selection on logical channels or at the end of card session

3.1.3 B

bearer: communication technology for transmitting information

Bearer Independent Protocol (BIP): mechanism by which the *terminal* provides access to the data *bearers* supported by the *terminal* and the network

binding: association of two objects, for example the binding of a *security attribute* to a *file*

NOTE: Also, the realization of an *application programming interface* with respect to a specific programming language or software technology.

byte code: processor independent representation of a primitive computer instruction of a hypothetical central processing unit

3.1.4 C

card: synonym for *smart card*

Card Application Toolkit (CAT): mechanism that allows applications existing in the UICC to issue commands, during a card session, to the terminal and receive responses, and to receive events from the terminal

card holder: person who is in possession of a *smart card* and has been authorized to use that *smart card* by the *card issuer*

card issuer: entity that provides a *smart card* to *card holder*

NOTE: The card issuer is typically responsible for the security of the data on the *card* and for the *applications* placed on the *card*.

card session: entire sequence of *commands* and *responses* between the UICC and the terminal starting with the *answer to reset* and ending with a subsequent reset of or removal of power from the UICC

card manager: *system application* that governs the flow of content on to and off of the UICC and dispatches *commands* to *applications* on the UICC

channel session: related sequence of *commands* and *responses* between the *card* and an external entity during a *card session* on a given *logical channel*, starting with the opening of the *logical channel* and ending with the closure of the *logical channel* or the termination of the *card session*

class A operating conditions: conditions existing when the supply voltage provided by the *terminal* to the UICC is 5 V ± 10 %

class B operating conditions: conditions existing when the supply voltage provided by the *terminal* to the UICC is 3 V ± 10 %

class C operating conditions: conditions existing when the supply voltage provided by the *terminal* to the UICC is 1,8 V ± 10 %

command: sequence of bytes sent to a UICC that the UICC *operating system* or a UICC *application* interprets as an instruction to execute function or perform a procedure

command header: security header of a command packet

NOTE: It includes all fields except the Secured Data.

command packet: secured packet transmitted by the Sending Entity to the Receiving Entity, containing a secured Application Message

Counter (CNTR): mechanism or data field used for keeping track of a message sequence

NOTE: A counter can be implemented as a sequence oriented or time stamp derived value maintaining a level of synchronization.

Cryptographic Checksum (CC): string of bits derived from the data with which the cryptographic checksum is associated and specific cryptographic material

current ADF: currently selected ADF on a *logical channel*

current directory: *directory* most recently selected on the UICC; part of the current state of the UICC

current elementary file: *elementary file* most recently selected on the UICC; part of the current state of the UICC

current file: *current directory* or the *current elementary file*

current record number: *record pointer* associated with a *file* that holds index of the most recently accessed *record*; part of the current state of the UICC

cyclic file: *fixed length record file* with the property that the *record* that logically follows the last *record* in the *file* is the first *record* in the *file* and the *record* that precedes the first *record* in the *file* is the last *record* in the *file*

3.1.5 D

data channel: communication channel between a *UICC application* and an entity external to the UICC

Data Object (DO): information coded as TLV object(s), i.e. consisting of a *Tag, a Length and a Value* syntax part

data structure: memory address that can be accessed by an *application executable* in order to read or write data

Dedicated File (DF): deprecated synonym for *directory*

Digital Signature (DS): string of bits derived from the data with which the digital signature is associated and the private key of an asymmetric key pair

directory: *file* in the UICC *file system* that contains only other *files*

3.1.6 E

Elementary File (EF): *file* in a UICC *file system* containing data but no other *files*

NOTE: An elementary file can be a *transparent file* or a *record file*.

embedded UICC: UICC which is not easily accessible or replaceable, that is not intended to be removed or replaced in the terminal, and enables the secure changing of subscriptions

end-user application: *application* whose functionality can be accessed via the terminal

entry point: name, for example a memory address, that can be used by an *application executable* in order to access functionality defined by an *application programming interface*

NOTE: Depending on the software technology, an entry point is also called a subroutine, a function or a method.

executable code: generic term for either *byte code* or *native code*

3.1.7 F

file: named set of bytes on the UICC

NOTE: A file can be either a *directory* or an *elementary file*.

File Identifier (FID): 2-byte name of a *file* in the UICC *file system*

file system: hierarchically-organized set of *files* on the UICC

fixed length record file: *record file* in which the *records* all contain the same number of bytes

framework: set of *application programming interfaces*

3.1.8 G

None.

3.1.9 H

None.

3.1.10 I

ID-000: physical form factor for a UICC; commonly called the plug-in form factor

ID-1: physical form factor for a UICC; commonly called the credit card form factor

interpreter: software program that simulates a hypothetical central processing unit

3.1.11 J

None.

3.1.12 K

keystore: file or a collection of files that contain cryptographic key material such as PINs or other authentication material

3.1.13 L

logical channel: one of one or more *command*/*response* communication contexts multiplexed on the physical channel between the terminal and the UICC

Logical Secure Element (LSE): secure element functionalities, applications and files grouped together to act like a secure element (e.g. UICC) when multiple logical secure element interfaces are supported

Logical Secure element Interface (LSI): logical connection between an endpoint in the terminal and one logical secure element

logical UICC: upper layers of the UICC which implement the logic for handling the commands, files and protocols

LSE base: lower layers of the UICC which are common for all LSEs

3.1.14 M

Master File (MF): directory file representing the root in the card using a hierarchy of DFs

Mobile Network Operator (MNO): entity providing communication services to its customers through mobile networks

multi-application UICC: contain more than one *application*

multi-session UICC: supports more than one concurrent *application session* during a *card session*

multi-verification capable UICC: *multi-application UICC* that supports separate authentication requirements for each *application*

3.1.15 N

native code: processor-dependent representation of a basic computer operation such as "increment by one" that is executed by the hardware circuitry of a computer

Network Access Application (NAA): application residing on an eUICC or UICC that provides authorization to access a Recommendation ITU-T E.212 network [i.3]

EXAMPLE: A USIM application.

Network Access Credentials: data required to authenticate to a Recommendation ITU-T E.212 [i.3] Network

NOTE: Network Access Credentials may include data such as Ki/K, and IMSI stored within a NAA.

3.1.16 O

None.

3.1.17 P

plug-in UICC: UICC in an *ID-000* physical form factor

proactive UICC: UICC which is capable of issuing commands to the *terminal*

proactive UICC session: sequence of related commands and responses which starts with the status response '91 XX' (proactive command pending) and ends with a status response of '90 00' (normal ending of command) after Terminal Response

3.1.18 Q

None.

3.1.19 R

receiving application: entity to which the application message is destined

receiving entity: entity where the secured packet is received (e.g. SMS-SC, UICC, USSD entry point, or dedicated toolkit server) and where the security mechanisms are utilized

NOTE: The receiving entity processes the secured packets.

record: sequence of bytes of data in a *record file* that is regarded as a single block of data and can be referenced as a unit using a *record number*

record file: *elementary file* in a UICC *file system* that consists of a sequence of *records*

NOTE: A record file can be a fixed length record file, a variable length record file or a cyclic file.

record length: number of bytes in a record

record number: sequential number that uniquely identifies each *record* within a *record file*

record pointer: UICC state variable that holds a *record number* associated with a *record file*

Redundancy Check (RC): string of bits derived from the data with which the redundancy check is associated for the purpose of detecting accidental changes to the message without the use of any secret information

response: portion of the consequence of executing a *command* on the UICC that is communicated back to the entity issuing the *command*

response header: security header of a response packet

response packet: secured packet transmitted by the Receiving Entity to the Sending Entity, containing a secured response and possibly application data

root directory: synonym for *Master File*

3.1.20 S

security attribute: set of *access rules* associated with a resource on the UICC

Security Condition (SC): sequence of one or more bytes that encodes a Boolean expression over variables whose value depends on the current state of the UICC

NOTE: If the Boolean expression evaluates to TRUE the security condition is said to be satisfied. One such variable could be "The password associated with key number 1 has been successfully entered".

Secure Element: tamper-resistant dedicated platform, consisting of hardware and software, capable of securely hosting applications and their confidential and cryptographic data and providing a secure application execution environment, e.g. the UICC

security header: that part of the secured packet which consists of all security information

EXAMPLE: Counter, key identification, indication of security level, checksum or digital signature.

secured packet: information flow on top of which the level of required security has been applied

NOTE: An application message is transformed with respect to a chosen Transport Layer and chosen level of security into one or more secured packets.

sender identification: simple verification of the identity of the sending entity by the receiving entity comparing the sender identity with an a priori stored identity of the sender at the receiving entity

sending application: entity generating an application message to be sent

sending entity: entity from which the secured packet originates (e.g. SMS-SC, UICC, USSD entry point, or dedicated toolkit server) and where the security mechanisms are invoked

NOTE: The sending entity generates the secured packets to be sent.

Short File Identifier (SFI): 5-bit value associated with an *elementary file* in the UICC *file system* that can be used to specify the target *elementary file* of a *command*

single verification capable UICC: UICC that supports only one authentication requirement that is used by all *applications*

smart card: physically secure computing device in one of the physical formats defined in ETSI TS 102 221 [i.2]

status code: indication that a message has been received (correctly or incorrectly, indicating reason for failure)

system application: *UICC application* whose functionality can be accessed by other applications running on the same UICC

System on Chip (SoC): integrated circuit that contains all the required circuitry and components of an electronic system on a single chip

3.1.21 T

telecommunications Service Provider: MNO, or party trusted by the MNO acting on behalf of the MNO, which provides services to the subscriber

terminal: device that can send *commands* to and interpret *responses* from a UICC

toolkit application: *application* on the UICC that calls or is called by the *Card Application Toolkit application programming interface*

Toolkit Application Reference (TAR): unique identifier associated with a *Toolkit Application*

transparent file: *elementary file* in a UICC *file system* consisting of a sequence of bytes without any further structure from the *UICC operating system* point of view

transport layer: layer responsible for transporting secured packets through the network

NOTE: The transport layer implements one or more transport mechanisms, (e.g. SMS or USSD).

type 1 UICC: UICC that enters a negotiable communication mode after a warm reset

type 2 UICC: UICC that enters a specific communication mode after a warm reset

3.1.22 U

UICC: *smart card* that conforms to the specifications written and maintained by the ETSI Smart Card Platform project

NOTE: UICC is neither an abbreviation nor an acronym.

UICC application: *application* residing on a UICC

UICC application session: synonym for *application session*

UICC operating system: *executable codes* stored in a UICC that manages the logical resources of the UICC, including external and inter-*application* communication, process scheduling, *file system* management and resource access control

unsecured acknowledgement: status code included in a response message

3.1.23 V

variable length record file: *record file* in which different *records* may have different *record lengths*

virtual machine: synonym for *interpreter*

3.1.24 W

None.

3.1.25 X

None.

3.1.26 Y

None.

3.1.27 Z

None.

3.2 Symbols and equations

The purpose of the present document is to provide the symbols and equations to be used in ETSI SET deliverables.

'0' - '9' 'A' - 'F'	Typographic representation of the sixteen hexadecimal digits used in SET specifications
b8 ... b1	Bits of one byte. b8 is the most significant and b1 is the least significant when the byte is interpreted as an integer value
etu	elementary time unit
f	frequency
Fi	clock rate conversion factor
Gnd	Ground
I_{cc}	Supply current
Kc	Ciphering key
Ki	Individual subscriber authentication key
KIc	Key and algorithm Identifier for ciphering
Lc	Number of bytes in the data field of a C-APDU
Le	Maximum number of bytes of data expected in the data field of an R-APDU
Luicc	Number of bytes of data in an R-APDU
tf	Fall time
tr	Rise time
V_{cc}	Supply Voltage (also Vcc)
V_{pp}	Programming Voltage (also Vpp)
V_{IH}	Input Voltage (high)
V_{IL}	Input Voltage (low)
V_{OH}	Output Voltage (high)
V_{OL}	Output Voltage (low)

3.3 Abbreviations

3.3.0 Introduction

The purpose of the present document is to provide the abbreviations to be used in ETSI SET deliverables.

3.3.1 0-9

None.

3.3.2 A

AC	Access Condition
ACK	ACKnowledge
ADD	Access Domain Data
ADF	Application Dedicated File
ADM	ADMinistrative
ADP	Access Domain Parameter
AFI	Application Family Identifier
AID	Application Identifier
AKA	Authentication and Key Agreement
ALW	ALWays
AM	Access Mode
AM_DO	Access Mode - Data Object
AP	Application Provider
APDU	Application Protocol Data Unit

API	Application Programming Interface
APN	Access Point Name
APSD	Application Provider Security Domain
ARD	Additional Response Data
ARR	Access Rule Reference
ASN	Abstract Syntax Notation
AT	Authentication Template
ATR	Answer To Reset
AVN	Applet Version Number

3.3.3 B

BCD	Binary Coded Decimal
BER	Basic Encoding Rules
BER-TLV	Basic Encoding Rules - Tag, Length, Value
BGT	Block Guard Time
BIP	Bearer Independent Protocol
BWI	Block Waiting Integer
BWT	Block Waiting Time

3.3.4 C

C-APDU	Command - Application Protocol Data Unit
C-TPDU	Command - Transmission Protocol Data Unit
CA	Certificate Authority
CAD	Card Acceptance Device
CAT	Card Application Toolkit
CAT_TP	Card Application Toolkit Transport Protocol
CBC	Cipher Block Chaining
CC	Cryptographic Checksum
CCT	Cryptographic Checksum Template
CHI	Command Header Identifier
CHL	Command Header Length
CHV	Card Holder Verification information
CL	ContactLess
CLA	CLAss
CLK	ClocK
CLT	ContactLess Tunnelling
CMAC	Cipher-based Message Authentication Code
CNTR	CouNTeR
CPI	Command Packet Identifier
CPL	Command Packet Length
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CRT	Control Reference Template
CS	Circuit Switched
CSIM	CDMA Subscriber Identity Module
CT	Confidentiality Template
CWI	Character Waiting Integer
CWT	Character Waiting Time

3.3.5 D

DAD	Destination ADdress
DAP	Digital Authentication Pattern
DEA	Data Encryption Algorithm
DEK	Data Encryption Key
DCS	Data Coding Scheme
DES	Data Encryption Standard
DF	Dedicated File

DM	Delegated Management
DNS	Domain Name System
DO	Data Object
DPA	Differential Power Analysis
DS	Digital Signature
DST	Digital Signature Template
DTLS	Datagram Transport Layer Security
DTMF	Dual Tone Multiple Frequency
DUUP	Do not Use Universal PIN

3.3.6 E

EAP	Extensible Authentication Protocol
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECKA	Elliptic Curve Key Agreement algorithm
ECKA-EG	ElGamal ECKA
EDC	Error Detection Code byte
EF	Elementary File
EID	eUICC IDentifier
EMA	ElectroMagnetic Attacks
EPC	Evolved Packet Core
eUICC	embedded UICC

3.3.7 F

FCI	File Control Information
FCP	File Control Parameter
FFS	For Further Study
FID	File IDentifier

3.3.8 G

GP	GlobalPlatform
GSMA	GSM Association

3.3.9 H

HCI	Host Controller Interface
HCP	Host Controller Protocol
HSM	Hardware Security Module
HT	Hash code Template
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure

3.3.10 I

I/O	Input/Output
I-Block	Information Block
IC	Integrated Circuit
ICC	Integrated Circuit Card
ICCID	Integrated Circuit Card Identification
ICV	Integrity Check Value
ID	IDentifier
IFD	InterFace Device
IFS	Information Field Size
IFSC	Information Field Size for the UICC
IFSD	Information Field Size for the terminal
IMEI	International Mobile Equipment Identity

IMS IP Multimedia Services
IMSI International Mobile Subscriber Identity
INF INFormation field
INS INStruction
IOP InterOPerability
IP Internet Protocol
ISD Issuer Security Domain
ISIM IMS SIM
ISO International Organization for Standardization

3.3.11 J

JIL Joint Interpretation Library

3.3.12 K

KIc Key and algorithm Identifier for ciphering
KID Key and algorithm IDentifier for RC/CC/DS
KIK Key Identifier for protecting Kic and KID

3.3.13 L

LCSI Life Cycle Status Information
LCSI_DO Life Cycle Status Information - Data Object
LEN LENgth
LRC Longitudinal Redundancy Check
LSE Logical Secure Element
LSI Logical Secure element Interface
LSB Least Significant Bit

3.3.14 M

M Mandatory
MAC Message Authentication Code
ME Mobile Equipment
MF Master File
MNO Mobile Network Operator
MSB Most Significant Bit
MSISDN Mobile Subscriber Integrated Services Digital Network Number
MSL Minimum Security Level
MSLD Minimum Security Level Data
MTC Machine-Type Communication
MTU Maximum Transport Unit

3.3.15 N

NAA Network Access Application
NAC Network Access Credentials
NACK Negative ACKnowledgement
NAI Next Action Indicator
NAD Node Address byte
NAS Non Access Stratum
NEV NEVer
NIST National Institute of Standards and Technology

3.3.16 O

O	Optional
OFL	Open Firmware Loader
OFLA	Open Firmware Loader Agent
OS	Operating System
OSI	Open Systems Interconnection
OTA	Over The Air

3.3.17 P

P1	Parameter 1
P2	Parameter 2
P3	Parameter 3
PCB	Protocol Control Byte
PCI	Protocol Control Information
PCNTR	Padding CouNTeR
PDU	Protocol Data Unit
PIN	Personal Identification Number
PIX	Proprietary application Identifier eXtension
PKI	Public Key Infrastructure
PoR	Proof of Receipt
PPS	Protocol and Parameter Selection
PS	PIN Status
PS_DO	PIN Status - Data Object
PUK	PIN Unblocking Key

3.3.18 Q

None.

3.3.19 R

RAM	Remote Application Management
R-APDU	Response - Application Protocol Data Unit
R-Block	Receive-Ready block
R-TPDU	Response - Transmission Protocol Data Unit
RC	Redundancy Check
RE	Receiving Entity
RF	Radio Frequency
RFM	Remote File Management
RFU	Reserved for Future Use
RHI	Response Header Identifier
RHL	Response Header Length
RPI	Response Packet Identifier
RPL	Response Packet Length
RID	Registered application provider IDentifier
RPC	Remote Procedure Call
RPI	Response Packet Identifier
RPL	Response Packet Length
RSC	Response Status Code
RST	ReSeT

3.3.20 S

S-Block	Supervisory - Block
SAD	Source ADdress
SAT	SIM Application Toolkit
SC	Security Condition
SC_DO	Security Condition - Data Object

SCP02	Secure Channel Protocol 02
SCP03	Secure Channel Protocol 03
SD	Security Domain
SDU	Service Data Unit
SE	Security Environment
SEID	Security Environment IDentifier
SFI	Short elementary File Identifier
SIM	Subscriber Identity Module
SM	Secure Message
SMG	Special Mobile Group
SMS	Short Message Service
SMS-CB	Short Message Service - Cell Broadcast
SMS-SC	Short Message Service - Service Centre
SoC	System on Chip
SP	Special Publication
SPA	Simple Power Analysis
SPI	Security Parameters Indication
SW	Status Word
SW1/SW2	Status Word 1/Status Word 2
SWP	Single Wire Protocol

3.3.21 T

TAR	Toolkit Application Reference
TBD	To Be Defined
TC	Technical Committee
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TLV	Tag Length Value
TPDU	Transfer Protocol Data Unit

3.3.22 U

UCS2	Universal Character Set 2
UE	User Equipment
UI	User Interface
URN	Uniform Resource Name
USAT	USIM Application Toolkit
USB	Universal Serial Bus
USIM	Universal Subscriber Identity Module
USSD	Unstructured Supplementary Services Data
UUID	Universally Unique IDentifier
UUP	Use Universal PIN

3.3.23 V

VPN	Virtual Private Network

3.3.24 W

WI	Waiting time Integer
WLAN	Wireless Local Area Network
WTX	Waiting Time eXtension
WWT	Work Waiting Time

3.3.25 X

XML	eXtensible Markup Language

3.3.26 Y

None.

3.3.27 Z

None.

Annex A:
Change history

The table below indicates all changes that have been incorporated into the present document since it was placed under change control.

Change history								
Date	**Meeting**	**Plenary Doc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**Old**	**New**
	SCP-13	SCP-030161	-		-	Presented to SCP #13 for information	-	1.0.0
	-	-	-		-	Presented to SCP WG1 #7	1.0.0	1.1.0
	SCP-14	SCP-030217	-		-	Approved at SCP plenary meeting 14	2.0.0	3.0.0
	SCP#88	-	-		-	Approved at SCP plenary meeting 88	3.0.0	4.0.0
	SCP#89	SCP(19)000172	-		F	Alignment of CAT definitions and abbreviations with ETSI TS 102 223	4.0.0	5.0.0
2019-12	SCP#90	SCP(19)000269r1	1		D	Alignment of definitions and abbreviations with TS°102°225, TS°102°224 and TR°102°224	5.0.0	5.1.0
2019-12	SCP#90	SCP(19)000262r1	1		F	ETSI TR 102 216 synchronization with ETSI TS 103 465	5.0.0	5.1.0
2024-03	SET#113	SET(24)000030	-		B	MLI terms and abbreviations adding	5.0.0	5.1.0

History

Document history		
V3.0.0	September 2003	Publication
V4.0.0	May 2019	Publication
V5.0.0	November 2019	Publication
V5.1.0	May 2024	Publication