



Smart Cards; Vocabulary for Smart Card Platform specifications

STANDARDS PREVIEW
(standards.itih.ai)
Full standard:
<https://standards.itih.ai/catalog/standards/sct/607aa760-a625-4452-a186-fcd08998a12c/etsi-tr-102-216-v5.0.0-2019-11>

Reference

RTR/SCP-000014

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

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	5
Foreword.....	5
Modal verbs terminology.....	5
1 Scope	6
2 References	6
2.1 Normative references	6
2.2 Informative references.....	6
3 Definition of terms, symbols, equations and abbreviations.....	7
3.1 Terms.....	7
3.1.0 Introduction.....	7
3.1.1 0-9.....	7
3.1.2 A.....	7
3.1.3 B.....	8
3.1.4 C.....	8
3.1.5 D.....	9
3.1.6 E.....	9
3.1.7 F.....	9
3.1.8 G.....	9
3.1.9 H.....	10
3.1.10 I.....	10
3.1.11 J.....	10
3.1.12 K.....	10
3.1.13 L.....	10
3.1.14 M.....	10
3.1.15 N.....	10
3.1.16 O.....	10
3.1.17 P.....	10
3.1.18 Q.....	11
3.1.19 R.....	11
3.1.20 S.....	11
3.1.21 T.....	11
3.1.22 U.....	12
3.1.23 V.....	12
3.1.24 W.....	12
3.1.25 X.....	12
3.1.26 Y.....	12
3.1.27 Z.....	12
3.2 Symbols and equations.....	12
3.3 Abbreviations	13
3.3.0 Introduction.....	13
3.3.1 0-9.....	13
3.3.2 A.....	13
3.3.3 B.....	13
3.3.4 C.....	13
3.3.5 D.....	14
3.3.6 E.....	14
3.3.7 F.....	14
3.3.8 G.....	14
3.3.9 H.....	14
3.3.10 I.....	14
3.3.11 J.....	15
3.3.12 K.....	15
3.3.13 L.....	15
3.3.14 M.....	15
3.3.15 N.....	15

3.3.16	O	15
3.3.17	P	15
3.3.18	Q	16
3.3.19	R	16
3.3.20	S	16
3.3.21	T	16
3.3.22	U	16
3.3.23	V	16
3.3.24	W	16
3.3.25	X	17
3.3.26	Y	17
3.3.27	Z	17
Annex A:	Change history	18
History		19

iTeh STANDARD PREVIEW
 (standards.iteh.ai)
 Full standard:
<https://standards.iteh.ai/catalog/standards/sist/607aa760-a625-4452-a186-fcd08998a12c/etsi-tr-102-216-v5.0.0-2019-11>

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 Report (TR) has been produced by ETSI Technical Committee Smart Card Platform (SCP).

The contents of the present document are subject to continuing work within EP SCP and may change following formal EP SCP approval. If EP SCP decide to modify the contents of the present document, it will be re-released by EP SPC 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 EP SCP for information;
 - 2 presented to EP SCP for approval;
 - 3 or greater indicates EP SCP approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

Modal verbs terminology

In the present document "**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 Smart Card Platform (SCP) 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 SCP objectives and systems framework. The present document provides a tool for further work on SCP technical documentation and facilitates their understanding.

The terms, definitions and abbreviations as given in the present document are either imported from existing documentation (SCP, 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 SCP specification to facilitate readability.

But such terms and acronyms may be included if they are frequently used in the SCP 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 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.

- [i.1] Void.
- [i.2] ETSI TS 102 221: "Smart Cards; UICC-Terminal interface; Physical and logical characteristics".

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 SCP 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 $1,8\text{ V} \pm 10\%$ and $3\text{ V} \pm 10\%$

3 V technology Smart Card: *smart card* containing an integrated circuit designed to operate with supply voltages of $3\text{ V} \pm 10\%$ and $5\text{ V} \pm 10\%$

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 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 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 \pm 10 %

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

class C operating conditions: conditions existing when the supply voltage provided by the *terminal* to the UICC is 1.8 V \pm 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

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*.

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.