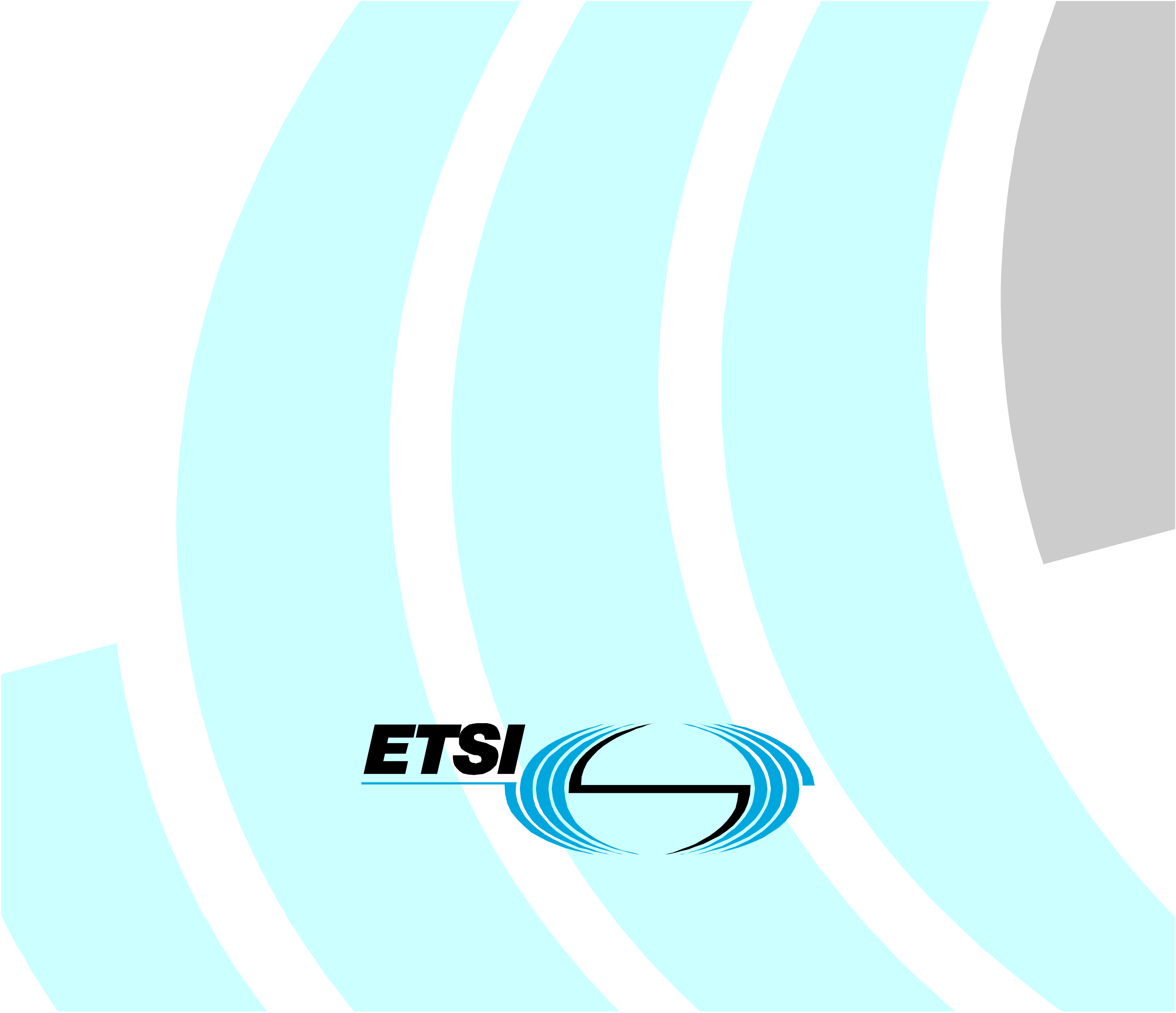
ETSI TR 102 216 V3.0.0 (2003-09)

Technical Report

Smart cards;
Vocabulary for Smart Card Platform specifications



Reference
DTR/SCP-010012

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

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

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

If you find errors in the present document, send your comment to:
editor@etsi.org

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2003.
All rights reserved.

DECTTM, **PLUGTESTS**TM and **UMTS**TM are Trade Marks of ETSI registered for the benefit of its Members.
TIPHONTM and the **TIPHON logo** are Trade Marks currently being registered by ETSI for the benefit of its Members.
3GPPTM is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

Contents

Intellectual Property Rights

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

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

Foreword

This Technical Report (TR) has been produced by ETSI Project 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.

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

For the purposes of this Technical Report (TR) the following references apply:

[1] ETSI TR 121 905: "Universal Mobile Telecommunications System (UMTS); Vocabulary for 3GPP Specifications (3GPP TR 21.905)".

3 Definitions

For the purposes of the present document, the following terms and definitions apply.

3.1 0-9

1.8V technology Smart Card: *smart card* containing an integrated circuit designed to operate with supply voltages of 1.8V ± 10% and 3V ± 10%

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

3.2 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

3.3 B

bearer: communication technology for transmitting information

Bearer Independent Protocol (BIP): *application programming interface* by a *UICC operating system* that provides *applications* with access to the *bearers* supported by the *terminal*

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

NOTE: Also, the realization of a *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

3.4 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

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

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*

3.5 D

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

Data Object (DO): information coded in the *Tag-Length-Value* syntax

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*

3.6 E

Elementary File (EF): *file* in a UICC *file system* containing data but not 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*

3.7 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*

3.8 G

None.

3.9 H

None.

3.10 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

3.11 J

None.

3.12 K

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

3.13 L

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

3.14 M

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

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*

3.15 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 a UICC provides authorization to access a network

EXAMPLE: A USIM application.

3.16 O

None.

3.17 P

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

proactive UICC: UICC that provides the *Card Application Toolkit application programming interface* to *applications*

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

3.18 Q

None.

3.19 R

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*

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

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*

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

root directory: synonym for *Master File*

3.20 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".

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

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*

smart card: physically secure computing device in one of the physical formats defined in TS 102 221

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

3.21 T

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

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

3.22 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

3.23 V

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

virtual machine: synonym for *interpreter*

3.24 W

None.

3.25 X

None.

3.26 Y

None.

3.27 Z

None.

4 Abbreviations

For the purposes of the present document, the following abbreviations apply.

4.1 0-9

None.

4.2 A

AC	Access Condition
ACK	ACKnowledge
ADD	Access Domain Data
ADF	Application Dedicated File
ADM	ADMinistrative
ADP	Access Domain Parameter
AID	Application IDentifier
ALW	ALWays
AM	Access Mode

AM_DO	Access Mode - Data Object
AP	Application Provider
APDU	Application Protocol Data Unit
API	Application Programming Interface
ARR	Access Rule Reference
AT	Authentication Template
ATR	Answer To Reset
AVN	Applet Version Number

4.3 B

BCD	Binary Coded Decimal
BER	Basic Encoding Rules
BGT	Block Guard Time
BIP	Bearer Independent Protocol
BWI	Block Waiting Integer
BWT	Block Waiting Time

4.4 C

C-APDU	Command - APDU
C-TPDU	Command - TPDU
CAD	Card Acceptance Device
CAT	Card Application Toolkit
CBC	Cipher Block Chaining
CC	Cryptographic Checksum
CCT	Cryptographic Checksum Template
CHI	Command Header Identifier
CHL	Command Header Length
CHV	Card Holder Verification information
CLA	CLAss
CLK	ClocK
CNTR	CouNTeR
CPI	Command Packet Identifier
CPL	Command Packet Length
CRC	Cyclic Redundancy Check
CRT	Control Reference Template
CT	Confidentiality Template
CWI	Character Waiting Integer
CWT	Character Waiting Time

4.5 D

DAD	Destination ADdress
DAP	Digital Authentication Pattern
DCS	Data Coding Scheme
DES	Data Encryption Standard
DF	Dedicated File
DO	Data Object
DS	Digital Signature
DST	Digital Signature Template
DTMF	Dual Tone Multiple Frequency
DUUP	Do not Use Universal PIN

4.6 E

ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography

EDC	Error Detection Code byte
EF	Elementary File

4.7 F

FCI	File Control Information
FCP	File Control Parameter
FID	File IDentifier

4.8 G

GP	Global Platform

4.9 H

HT	Hash code Template

4.10 I

I/O	Input/Output
I-Block	Information Block
IC	Integrated Circuit
ICC	Integrated Circuit Card
ICCID	Integrated Circuit Card IDentification
ID	IDentifier
IFD	InterFace Device
IFS	Information Field Size
IFSC	Information Field Size for the UICC
IFSD	Information Field Size for the terminal
IMS	IP Multimedia Services
INF	INFormation field
INS	INStruction
IOP	InterOPerability
IP	Internet Protocol
ISIM	IMS SIM

4.11 J

None.

4.12 K

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

4.13 L

LCSI	Life Cycle Status Information
LCSI_DO	Life Cycle Status Information - Data Object
LEN	LENgth
LRC	Longitudinal Redundancy Check
LSB	Least Significant Bit

4.14 M

M	Mandatory
MAC	Message Authentication Code
MF	Master File
MSB	Most Significant Bit
MSL	Minimum Security Level
MSLD	Minimum Security Level Data

4.15 N

NAA	Network Access Application
NACK	Negative ACKnowledgement
NAI	Next Action Indicator
NAD	Node Address byte
NEV	NEVer

4.16 O

O	Optional

4.17 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
PoR	Proof of Receipt
PPS	Protocol and Parameter Selection
PS	PIN Status
PS_DO	PIN Status - Data Object

4.18 Q

None.

4.19 R

R-APDU	Response - APDU
R-Block	Receive-Ready block
R-TPDU	Response - TPDU
RC	Redundancy Check
RFU	Reserved for Future Use
RHI	Response Header Identifier
RHL	Response Header Length
RID	Registered application provider IDentifier
RPC	Remote Procedure Call
RPI	Response Packet Identifier
RPL	Response Packet Length
RST	ReSeT

4.20 S

S-Block	Supervisory - Block
SAD	Source ADdress
SAT	SIM Application Toolkit
SC	Security Condition
SC_DO	Security Condition - Data Object
SDU	Service Data Unit
SE	Security Environment
SEID	Security Environment IDentifier
SFI	Short elementary File Identifier
SIM	Subscriber Identity Module
SM	Secure Message
SPI	Security Parameters Indication
SW	Status Word
SW1/SW2	Status Word 1/Status Word 2

4.21 T

TAR	Toolkit Application Reference
TLV	Tag Length Value
TPDU	Transfer Protocol Data Unit

4.22 U

UCS2	Universal Character Set 2
USAT	USIM Application Toolkit
USIM	Universal Subscriber Identity Module
UUP	Use Universal PIN

4.23 V

None.

4.24 W

WI	Waiting time Integer
WTX	Waiting Time eXtension
WWT	Work Waiting Time

4.25 X

None.

4.26 Y

None.

4.27 Z

None.

5 Symbols and equations

For the purposes of the present document, the following symbols and equations apply:

'0' - '9' 'A' - 'F'	Typographic representation of the sixteen hexadecimal digits used in SCP 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)

Annex A (informative): Change history

Change history								
	SCP Doc.	**WG1 Doc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**Old**	**New**
SCP-13	SCP-030161	-	-	-	-	Presented to SCP #13 for information	-	1.0.0
-	-	SCP1-030146	-	-	-	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

History

Document history		
V3.0.0	September 2003	Publication