

ETSI TS 102 412 V9.0.0 (2009-01)

Technical Specification

Smart Cards; Smart Card Platform Requirements Stage 1 (Release 9)

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
<https://standards.iteh.ai/catalog/standards/sist/dc561213-7a97-4eb4-a7ce-4aa985da8e4e/etsi-ts-102-412-v9.0.0-2009-01>



Reference

RTS/SCP-R00002v900

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, please send your comment to one of the following services:
http://portal.etsi.org/chaicor/ETSI_support.asp

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 2009.
All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™**, **TIPHON™**, the TIPHON logo and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.

3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

LTE™ is a Trade Mark of ETSI currently being registered

for the benefit of its Members and of the 3GPP Organizational Partners.

GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	7
Foreword.....	7
Introduction	7
1 Scope	8
2 References	8
2.1 Normative references	8
2.2 Informative references.....	9
3 Definitions and abbreviations.....	9
3.1 Definitions	9
3.2 Abbreviations	11
4 Requirements.....	12
4.1 Run time environment timing constraints	13
4.1.1 Abstract (informative).....	13
4.1.2 Background (informative).....	13
4.1.2.1 Use case - Network authentication.....	13
4.1.3 Requirements	14
4.1.4 Interaction with existing features (informative).....	14
4.2 Launch Application feature	14
4.2.1 Abstract (informative).....	14
4.2.2 Background (informative).....	14
4.2.3 Requirements	15
4.2.4 Interaction with existing features (informative).....	15
4.3 Mapped file support on the UICC.....	15
4.3.1 Abstract (informative).....	15
4.3.2 Background (informative).....	16
4.3.3 Requirements	16
4.3.4 Interaction with existing features (informative).....	16
4.4 Extension of logical channels.....	16
4.4.1 Abstract (informative).....	16
4.4.2 Background (informative).....	16
4.4.2.1 Typical problem situation	16
4.4.2.2 Possible problem solution	17
4.4.2.3 Use cases	17
4.4.2.3.1 Use case - JSR 177 applications	17
4.4.2.3.2 Use case - PC connection	17
4.4.3 Requirements	17
4.4.3.1 General requirements	17
4.4.3.2 Backward compatibility requirements.....	17
4.4.4 Interaction with existing features (informative).....	17
4.5 Secure channel to secure local terminal interfaces	17
4.5.1 Abstract (informative).....	17
4.5.2 Background (informative).....	18
4.5.2.1 Use case - User interface.....	18
4.5.2.2 Use case - UICC as a control point for device management	19
4.5.2.3 Use case - DRM and distributed applications	20
4.5.3 Requirements	22
4.5.3.1 End point requirements	22
4.5.3.2 Integrity requirements	22
4.5.3.3 Confidentiality requirements	22
4.5.3.4 Authentication requirements	22
4.5.3.5 Audit/Compliance requirements	22
4.5.3.6 Policy requirements.....	23
4.5.3.7 Transport Protocol requirements	23
4.5.4 Interaction with existing features (informative).....	23

4.5.4.1	Logical Channels.....	23
4.6	Authenticate command longer than 255 bytes.....	23
4.6.1	Abstract (informative).....	23
4.6.2	Background (informative).....	23
4.6.2.1	Use case - EAP packet exchange	23
4.6.3	Requirements	23
4.6.3.1	General requirements	23
4.6.3.2	Backward compatibility requirements.....	24
4.6.4	Interaction with existing features (informative).....	24
4.7	CAT mechanisms to indicate the bearer connection status	24
4.7.1	Abstract (informative).....	24
4.7.2	Background (informative).....	24
4.7.2.1	Use case - Availability of network bearers	24
4.7.2.2	Use case - Network connection temporarily lost.....	24
4.7.2.3	Use case - Availability of local bearers.....	24
4.7.3	Requirements	24
4.7.3.1	Requirement 1 - Network bearer connection status	24
4.7.3.2	Requirement 2 - Local bearer connection status	25
4.7.4	Interaction with existing features (informative).....	25
4.8	New UICC-Terminal interface	25
4.8.1	Abstract (informative).....	25
4.8.2	Background (informative).....	25
4.8.2.1	Use case - multimedia file management.....	25
4.8.2.2	Use case - MMI on UICC	25
4.8.2.3	Use case - real-time multimedia data encryption/decryption	26
4.8.2.4	Use case - storage of terminal applications on the UICC	26
4.8.2.5	Use case - direct and indirect UICC connection to a PC.....	26
4.8.2.6	Use case - web server on Smart Card.....	26
4.8.2.7	Use case - antivirus on UICC	26
4.8.2.8	Use case - big phonebook management from the UICC	26
4.8.2.9	Use case - reduce personalization time	27
4.8.2.10	Use case - generic TCP/IP connectivity	27
4.8.3	Requirements	27
4.8.3.1	General requirements	27
4.8.3.2	Backward compatibility requirements.....	28
4.8.4	Interaction with existing features (informative).....	28
4.9	UICC based application acting as a server	28
4.9.1	Abstract (informative).....	28
4.9.2	Background (informative).....	28
4.9.3	Requirements	28
4.9.4	Interaction with existing features (informative).....	28
4.10	API for applications registered to a Smart Card Web Server	29
4.10.1	Abstract (informative).....	29
4.10.2	Background (informative).....	29
4.10.2.1	Registration of an application to the SCWS.....	29
4.10.2.2	Data exchange between SCWS and application.....	29
4.10.2.3	Issuing Proactive Commands	29
4.10.3	Requirements	30
4.10.4	Interaction with existing features (informative).....	30
4.11	Specific UICC environmental conditions	30
4.11.1	Abstract (informative).....	30
4.11.2	Background (informative).....	30
4.11.2.1	Use case - Automotive service	30
4.11.2.2	Use case - Remote monitoring camera.....	30
4.11.2.3	Use case - Remote stock monitoring for vending machines	31
4.11.2.4	Use case - Online electronic advertising board	31
4.11.3	Considerations (informative)	31
4.11.4	Requirements	31
4.11.4.1	Requirement 1: Temperature range	31
4.11.4.2	Requirement 2: Humidity.....	31
4.11.5	Interaction with existing features (informative).....	31
4.12	Introduction of high density memory technology in UICC.....	31

4.12.1	Abstract (informative).....	31
4.12.2	Background (informative).....	32
4.12.2.1	Use case - Enhanced UICC features.....	32
4.12.3	Requirements	32
4.12.4	Interaction with existing features (informative).....	32
4.13	Power supply indication mechanism	32
4.13.1	Abstract (informative).....	32
4.13.2	Background (informative).....	33
4.13.2.1	Use case - generic situation.....	33
4.13.2.2	Use case - USIM application with toolkit applications	33
4.13.3	Requirements	33
4.13.3.1	General Requirements.....	33
4.13.3.2	Backward compatibility requirements.....	33
4.13.4	Interaction with existing features (informative).....	34
4.14	Internet Connectivity up to UICC applications	34
4.14.1	Abstract (informative).....	34
4.14.2	Use Cases (informative).....	34
4.14.2.1	Use Case - Card OTA management	34
4.14.2.2	Use Case - User local access from the terminal to a card server.....	34
4.14.2.3	Use Case - Remote access to an identity server in the card	35
4.14.2.4	Use Case - User access from a locally connected device to a card service	35
4.14.3	Requirements	35
4.14.4	Interaction with existing features (informative).....	35
4.15	Contactless UICC services	36
4.15.1	Abstract (informative).....	36
4.15.2	Background (informative).....	36
4.15.2.1	Use case - Access.....	36
4.15.2.1.1	System aspects of use case.....	36
4.15.2.1.2	UICC role in use case	36
4.15.2.2	Use case - tickets.....	37
4.15.2.2.1	System aspects of throughput ticketing scenario.....	38
4.15.2.2.2	System aspects of high priced ticketing scenario	38
4.15.2.2.3	UICC role in use case	38
4.15.2.3	Use case - digital rights	39
4.15.2.3.1	System aspects of contactless digital rights.....	39
4.15.2.3.2	UICC role in use case	39
4.15.2.4	Use case - payment application.....	40
4.15.2.5	Use case - loyalty application.....	40
4.15.2.6	Use case - health care application	41
4.15.3	Requirements	41
4.15.3.1	Physical interface requirements	41
4.15.3.2	Multi-protocol concurrent operation requirements	41
4.15.3.3	Contactless communication modes requirements	41
4.15.3.4	Compatibility with existing contactless systems requirements	42
4.15.3.5	Parameters to be transported by the CLFIP requirements.....	42
4.15.3.6	Application integration requirements.....	42
4.15.3.7	Terminal and user interaction requirements	42
4.15.3.8	Interoperability requirements	42
4.15.4	Interaction with existing features (informative).....	42
4.16	Administration of the Smart Card Web Server.....	43
4.16.1	Abstract (informative).....	43
4.16.2	Background (informative).....	43
4.16.3	Requirements	43
4.16.4	Interaction with existing features (informative).....	43
4.17	Confidential Application Services.....	43
4.17.1	Abstract (informative).....	43
4.17.2	Background (informative).....	44
4.17.2.1	Use case 1: Mobile TV services.....	44
4.17.2.2	Use case 2: Banking Services.....	45
4.17.2.3	Use case 3: Contactless Applications.....	46
4.17.2.4	Use case 4: Mobile Virtual Network Operator services	47
4.17.3	Requirements (normative)	48

4.17.3.1	Confidential application environment	48
4.17.3.2	Administration by Card issuer.....	48
4.17.3.2.1	Third party area environment administration	48
4.17.3.2.2	Third party area creation.....	49
4.17.3.2.3	Third party area policy definition	49
4.17.3.3	Administration by Third party.....	49
4.17.3.4	Service Operator specific requirements	50
4.17.4	Interaction with existing features (informative).....	50
4.18	UICC for Machine-to-Machine (M2M) applications	50
4.18.1	Abstract (informative).....	50
4.18.2	Use Cases (informative).....	51
4.18.2.1	Use case – Track and Trace.....	51
4.18.2.1.1	Use case – Emergency Call	51
4.18.2.1.2	Use case - Fleet Management	51
4.18.2.1.3	Use case – Theft Tracking	52
4.18.2.2	Use case – Monitoring	53
4.18.2.2.1	Use case – Metering / Prepaid delivery of utilities (water, gas, electricity)	53
4.18.2.2.2	Use case – Person / Animal protection	53
4.18.2.2.3	Use case – Object protection	54
4.18.2.3	Use case – Transaction.....	55
4.18.2.3.1	Use case – PoS Terminals (Point of Sale Terminals)	55
4.18.2.4	Use case – Control	55
4.18.2.4.1	Use case – Controlling vending machines	55
4.18.2.4.2	Use case – Controlling production machines	56
4.18.3	Requirements	56
4.18.3.1	General M2M UICC Requirements	56
4.18.3.1.1	Specific requirements related to definition of classes	56
4.18.3.1.2	Example for a possible class system (informative).....	57
4.18.3.2	MFF Requirements	57
4.18.4	Interaction with existing features (informative).....	57
4.19	Location based services for broadcast technology	57
4.19.1	Abstract (informative).....	57
4.19.2	Use Cases (informative).....	58
4.19.3	Requirement for retrieving location information for broadcast technology.....	58
4.19.4	Interaction with existing features (informative).....	58
4.20	Terminals with reduced functionality.....	58
4.20.1	Abstract (informative).....	58
4.20.2	Use case (informative).....	58
4.20.2.1	Use case – Data card	58
4.20.3	Requirements	58
4.20.4	Interaction with existing features (informative).....	59
4.21	Digital Rights Management.....	59
4.21.1	Abstract (informative).....	59
4.21.2	Use cases (informative)	59
4.21.2.1	Use case - Transfer of protected contents and rights by using a UICC	59
4.21.2.2	Use case - Provisioning of rights in the UICC	59
4.21.2.3	Use case - Direct rendering of DRM-protected content by using the UICC	59
4.21.2.4	Use case - Pre-loading of rights by using the UICC	60
4.21.3	Requirements	60
4.21.4	Interaction with existing features (informative).....	60
4.22	Multicast dataflow in UICC	60
4.22.1	Abstract (informative).....	60
4.22.2	Use cases (informative)	60
4.22.2.1	Use case – Broadcast data services	60
4.22.2.2	Use case – Mobile TV related services	61
4.22.3	Requirement for multicast dataflow (subscription and dataflow reception)	61
4.22.4	Interaction with existing features (informative).....	61
Annex A (informative):	Requirement numbering scheme.....	62
Annex B (informative):	Change history	63
History		64

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 Specification (TS) has been produced by ETSI Technical Committee Smart Card Platform (SCP).

The contents of the present document are subject to continuing work within TC SCP and may change following formal TC SCP approval. If TC SCP modifies the contents of the present document, it will then be republished by ETSI with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
 - 0 early working draft;
 - 1 presented to TC SCP for information;
 - 2 presented to TC SCP for approval;
 - 3 or greater indicates TC SCP approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

The present document specifies the requirements for Release 7 onwards of the TC SCP.

1 Scope

The present document specifies the additional requirements for Release 7 onwards of the TC SCP with respect to earlier releases.

The present document covers all the Stage 1 requirements which are not covered by other TC SCP stage 1 documents.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- 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.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
 - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
 - for informative references.

Referenced documents which are not found to be publicly available in the expected location might be found at <http://docbox.etsi.org/Reference>.

For online referenced documents, information sufficient to identify and locate the source shall be provided. Preferably, the primary source of the referenced document should be cited, in order to ensure traceability. Furthermore, the reference should, as far as possible, remain valid for the expected life of the document. The reference shall include the method of access to the referenced document and the full network address, with the same punctuation and use of upper case and lower case letters.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

- [1] ETSI TS 102 221: "Smart Cards; UICC-Terminal interface; Physical and logical characteristics (Release 7)".
- [2] ETSI TS 102 223: "Smart cards; Card Application Toolkit (CAT) (Release 6)".
- [3] ETSI TS 122 038: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); USIM Application Toolkit (USAT/SAT); Service description; Stage 1 (3GPP TS 22.038 Release 7)".
- [4] ETSI TS 151 011: "Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface (3GPP TS 51.011)".
- [5] ETSI TS 131 102: "Universal Mobile Telecommunications System (UMTS); Characteristics of the USIM application (3GPP TS 31.102 Release 6)".
- [6] ISO/IEC 7816-4: "Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange".

- [7] Trusted Computing Group (2003): "TPM Main - Part 1 Design Principles - Specification version 1.2".
- NOTE: Available at
https://www.trustedcomputinggroup.org/downloads/tpm-wg-mainrev62_Part1_Design_Principles.pdf.
- [8] ISO/IEC 14443: "Identification cards - Contactless integrated circuit(s) cards - Proximity cards".
- [9] ISO/IEC 18092: "Information technology - Telecommunications and information exchange between systems - Near Field Communication - Interface and Protocol (NFCIP-1)".
- [10] ISO/IEC 15693: "Identification cards - Contactless integrated circuit(s) cards - Vicinity cards".
- [11] ETSI EN 300 468: "Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems".
- [12] ETSI EN 302 304: "Digital Video Broadcasting (DVB); Transmission System for Handheld Terminals (DVB-H)".
- [13] OMA-TS-SRM-V1-0-20080128-C "OMA Secure Removable Media Specification".
- [14] OMA-AD-SRM-V1-0-0-20080128-C "OMA Secure Removable Media Architecture".
- [15] OMA-RD-SRM-V1-0-20080128-C "OMA Secure Removable Media Requirements".

2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area. For non-specific references, the latest version of the referenced document (including any amendments) applies.

- [i.1] GSMA Pay Buy Mobile, Business Opportunity Analysis, Public White Paper, version 1.0, November 2007.
- [i.2] ISO/IEC 16750-3: "Road vehicles - Environmental conditions and testing for electrical and electronic equipment -- Part 3: Mechanical loads".
- [i.3] AEC-Q100: "Stress Test Qualification for Integrated Circuits".
- [i.4] OMA-TS-BCAST-SvcCntProtection-V1.0 : "Service and Content Protection for Mobile Broadcast Services".

3 Definitions and abbreviations

3.1 Definitions

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

central repository: a repository of registered applications residing in the UICC

CLF: ContactLess Front-end, circuitry in the terminal which:

- Handles the analog part of the contactless communication.
- May handle some layers of the contactless protocol.
- May exchange data with the terminal and the UICC.

CLFI (CLF Interface): physical interface between the UICC and the CLF

CLFIP (CLFI Protocol): communication protocol between the UICC and the CLF carried over the CLFI

DRM Agent: Entity in the Device that manages Permissions for Media Objects on the Device, as described in OMA SRM technical specification [13]

DRM Agent-SRM Agent Mutual Authentication: DRM Agent and the SRM Agent can authenticate each other based on credentials that are securely provisioned in each. The result of this mutual authentication allows the DRM Agent and SRM Agent to establish a secure communication for the exchange and sharing of secret elements as described in the OMA SRM architecture specification [14]

HSP: high speed protocol running on top of the NUT interface

M2M communication module: electronics system including all necessary components to establish wireless communications between machines. M2M communication modules are usually integrated directly into target devices, such as automated meter readers (AMRs), vending machines, alarm systems, cars equipments or others.

M2M UICC: UICC with specific properties for use in M2M environments, this includes existing form factors and an optional new form factor

Machine to Machine (Communication): Communication between remotely deployed devices with specific responsibilities and requiring little or no human intervention, which are all connected to a dedicated management server via the mobile network data communications

ME/TE owner: entity having the right to configure or administrate a CAD and/or remote terminal

MFF (M2M Form Factor): new form factor dedicated to M2M applications

Packaging: process to mount an integrated circuit device (e.g. UICC) into a package, which provides physical contacts for electric interconnection, protects the device in harsh environments and prevents the device from mechanical damage, vibration, chemistry attack and high temperatures, etc.

Rights: Collection of permissions and constraints defining under which circumstances access is granted to DRM Content as described in the OMA SRM technical specification [13].

Secure Removable Media (SRM): Removable media that implements means to protect against unauthorized access to its internal data and includes an SRM Agent. (e.g. secure memory card, smart card) as described in the OMA SRM technical specification [13]

Service Operator: third party that is able to manage sub-third party areas.

terminal: entity with which the Smart Card can establish a secure channel

EXAMPLE 1: Card Acceptance Device such as a mobile handset i.e. in the case of a wired Smart Card to terminal (such as PDA or handset) communication.

EXAMPLE 2: A Remote Terminal is a terminal communicating to a CAD, which can access the UICC resources, for example a PC connect over a local link to handset.

NOTE: In the present document a distinction will be made between a CAD and a Remote Terminal only where applicable, in case this distinction is not relevant the generic term terminal will be used.

terminal end point: point for terminating the secure channel from the UICC point of view, which could be a Mobile Terminal or a Remote Terminal

EXAMPLE: A remote terminal can be a Set-top box, a PC, or even a Bluetooth earpiece connected to a Mobile Terminal.

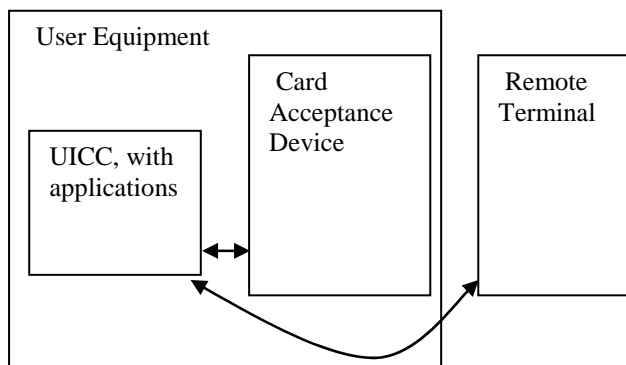


Figure 1: Possible secure channels with a UICC

third party application: an application developed and installed on the card by a player different from the card issuer

third party area: an area of the UICC (memory and resources) allocated to accommodate one (or several) third party application

third party policy: a set of policies which define some characteristics and restrictions for the third party applications allocated into the corresponding third party areas

trusted device: device which is not infected by malevolent code, whether because it is compliant to the requirements defined in TCG [7] or because the user/owner/administrator guarantees device integrity by giving verifiable evidence

NOTE: A more exact definition is out of scope of SCP.

UICC powering modes:

- Battery powered:
 - Mode where the UICC and the CLF are powered from the battery of the terminal.
- Not Battery powered:
 - Mode where the UICC and the CLF are not powered from the battery of the terminal.

3.2 Abbreviations

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

ADF	Application Dedicated File
API	Application Programming Interface
CAD	Card Acceptance Device
CAS	Conditional Access System
CAT	Card Application Toolkit
CAT-TP	Card Application Toolkit - Transport Protocol
CEK	Content Encryption Key
CPU	Central Processing Unit
DF	Dedicated File
DM	Device Management
DRM	Digital Rights Management
DRM-UA	Digital Rights Management User Agent
DVB	Digital Video Broadcasting
DVB-H	DVB-Hand held
DVB-SH	Digital Video Broadcasting - Satellite services to Handhelds

DVB-T	Digital Video Broadcasting - Terrestrial
EAP	Extensible Authentication Protocol
EF	Elementary File
FLO	Forward Link Only
GPRS	General Packet Radio Service
HTTP	HyperText Transfer Protocol
HTTPS	Secure HyperText Transfer Protocol
IMS	IP Multimedia Services
IP	Internet Protocol
ISIM	IMS SIM
JSR	Java Specification Request
M2M	Machine to Machine (communication)
MBMS	Multimedia Broadcast/Multicast Service
ME	Mobile Equipment
MFF	Machine to Machine Form Factor
MNO	Mobile Network Operator
MO	(Device) Management Object
MT	Mobile Termination
MVNO	Mobile Virtual Network Operator
NUT	New UICC-Terminal
OMA	Open Mobile Alliance
OTA	Over The Air
PDA	Personal Digital Assistance
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POP	Post Office Protocol
POS	Point Of Sale
RFID	Radio Frequency Identification
RO	Rights Object
SC	Smart Card
SCWS	Smart Card Web Server
SMTP	Simple Mail Transfer Protocol
SRM	Secure Removable Media
T-DMB	Terrestrial – Digital Multimedia Broadcasting
TCG	Trusted Computing Group
TLS	Transport Layer Security
TMP	Trusted Media Player
TSM	Trusted Service Manager
UA	(Digital Rights Management) User Agent
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
URL	Uniform Resource Locator
USIM	Universal Subscriber Identity Module
USSM	UICC Security Service Module
WIM	Wireless Identity Module

4 Requirements

The present document specifies:

- run time environment timing constraints;
- launch application command;
- mapped file support on the UICC;
- extension of logical channels;
- secure channel to secure local terminal interfaces;
- authenticate command longer than 255 bytes;

- CAT mechanisms to indicate the bearer connection status;
- New UICC-Terminal (NUT) interface;
- Smart Card Web Server running in UICC;
- API for applications registered to a Smart Card Web Server;
- specific UICC environmental conditions;
- introduction of high density memory technology in UICC;
- power supply indication mechanism;
- Internet Connectivity up to UICC applications;
- contactless UICC services;
- administration of the Smart Card Web Server;
- confidential application services;
- UICC for Machine-to-Machine (M2M) applications;
- Location based services for broadcast technology;
- terminals with reduced functionality;
- OMA Secure Removable Media capability for the UICC;
- Multicast dataflow in UICC.

4.1 Run time environment timing constraints

4.1.1 Abstract (informative)

SCP specifications up to Release 6 do not put any restrictions to the run time behaviour of Smart Card applications on the CAT layer and on the application layer. However, an example for a situation which requires a defined runtime behaviour of the UICC is given in a note in Release 6 of TS 102 223 [2]: The maximum work time of applications before sending a MORE TIME proactive command to the terminal should not exceed a certain amount of time. This remark is made in the context of the network authentication command and it is not normative. To avoid future problems due to this undefined behaviour, the requirements in this clause aim at providing the infrastructure needed to achieve standardized behaviour in situations like those described above from Release 7 onwards.

4.1.2 Background (informative)

4.1.2.1 Use case - Network authentication

An application may not block a UICC with a USIM application longer than a well defined period of time in order to be able to process network authentication commands within a time limit which is a network parameter (TS 102 223 [2]).