ETSI TS 103 481 V16.1.0 (2023-01)

Smart Cards;
Test specification for the Remote APDU structure for UICC based applications;
UICC features
(Release 16)

Reference
RTS/SET-00103481vg10

Keywords
management, remote, smart card, testing

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

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

Version x.y.z

where:

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

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

The present document defines test cases for the UICC relating to Remote APDU structure for UICC based applications as specified in ETSI TS 102 226 [1].

1 Scope

The present document covers the minimum characteristics considered necessary for the UICC in order to provide compliance to ETSI TS 102 226 [1].

It specifies conformance test cases for the UICC relating to Remote APDU structure for UICC based applications as specified in ETSI TS 102 226 [1].

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

- In the case of a reference to a TC SET document, a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.

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

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

The following referenced documents are necessary for the application of the present document.

[1] ETSI TS 102 226: "Smart Cards; Remote APDU structure for UICC based applications".

[2] ETSI TS 102 225: "Smart Cards; Secured packet structure for UICC based applications".

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

[4] ETSI TS 102 223: "Smart Cards; Card Application Toolkit (CAT) (Release 9)".

[5] GlobalPlatform: "GlobalPlatform Card Specification Version 2.3".

NOTE 1: Available at http://www.globalplatform.org/.

NOTE 2: Rel-12 and earlier versions of the present document reference Version 2.2.1.

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

[7] ETSI TS 102 241: "Smart Cards; UICC Application Programming Interface (UICC API) for Java Card ™".

[8] GlobalPlatform: "GlobalPlatform Card Specification Version 2.0.1".

NOTE 1: Available at http://www.globalplatform.org/.

NOTE 2: This reference is retained only because some requirements from older versions of the present document reference it.

[9] ETSI TS 102 222: "Integrated Circuit Cards (ICC); Administrative commands for telecommunications applications".

[10] ETSI TS 123 048: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Security mechanisms for the (U)SIM application toolkit; Stage 2 (3GPP TS 23.048)".

[11] ETSI TS 102 127: "Smart Cards; Transport protocol for CAT applications; Stage 2".

[12] ETSI TS 143 019: "Digital cellular telecommunications system (Phase 2+); Subscriber Identity Module Application Programming Interface (SIM API) for Java Card; Stage 2 (3GPP TS 43.019)".

[13] FIPS-197 (2001): "Advanced Encryption Standard (AES)".

NOTE: Available at http://csrc.nist.gov/publications/fips/index.html.

[14] NIST Special Publication 800-38A (2001): "Recommendation for Block Cipher Modes of Operation - Methods and Techniques".

NOTE: Available at http://csrc.nist.gov/publications/nistpubs/.

[15] NIST Special Publication 800-38B (2001): "Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication".

NOTE: Available at http://csrc.nist.gov/publications/nistpubs/.

[16] GlobalPlatform: "GlobalPlatform Card, UICC Configuration", Version 2.0.

NOTE 1: Available at http://www.globalplatform.org/.

NOTE 2: Rel-15 and earlier versions of the present document reference Version 1.0.1.

[17] ETSI TS 102 588: "Smart Cards; Application invocation Application Programming Interface (API) by a UICC webserver for Java Card™ platform".

[18] GlobalPlatform: "GlobalPlatform Card, Confidential Card Content Management Card Specification v2.3 - Amendment A", Version 1.1.

NOTE 1: Available at http://www.globalplatform.org/.

NOTE 2: Rel-12 and earlier versions of the present document reference Version 1.0.1.

[19] GlobalPlatform: "Card Specification Version v2.2 Amendment B", Version 1.1.3.

NOTE 1: Available at http://www.globalplatform.org/.

NOTE 2: The Rel-11 version of the present document references Version 1.1.

NOTE 3: The Rel-12 version of the present document references Version 1.1.1.

[20] ETSI TS 102 483: "Smart cards; UICC-Terminal interface; Internet Protocol connectivity between UICC and terminal".

[21] ISO/IEC 8825-1: "Information technology -- ASN.1 encoding rules -- Part 1: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)".

[22] GlobalPlatform: "Card Specification Version 2.3, Amendment C: Contactless Services" Version 1.2.

NOTE 1: Available at http://www.globalplatform.org/.

NOTE 2: The Rel-11 version of the present document references Version 1.0.1.

NOTE 3: The Rel-12 version of the present document references Version 1.1.

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

[24] GlobalPlatform: "Security Upgrade for Card Content Management - GlobalPlatform Card Specification v2.2 - Amendment E", Version 1.0.

NOTE: Available at http://www.globalplatform.org/.

[25] GlobalPlatform: "Java Card API and Export File for Card Specification v2.2.1 (org.globalplatform) Version 1.6".

NOTE 1: Available at http://www.globalplatform.org/.

NOTE 2: Rel-12 and earlier versions of the present document reference Version 1.5.

[26] Oracle: "Application Programming Interface, Java Card™ Platform, 3.0.1 Classic Edition".

[27] Oracle: "Runtime Environment Specification, Java Card™ Platform, 3.0.1 Classic Edition".

[28] Oracle: "Virtual Machine Specification Java Card™ Platform, 3.0.1 Classic Edition".

NOTE: Oracle Java Card™ Specifications can be downloaded at https://docs.oracle.com/en/java/javacard/3.1/index.html.

[29] ISO/IEC 9646-7:1995: "Information technology -- Open Systems Interconnection -- Conformance testing methodology and framework -- Part 7: Implementation Conformance Statements".

[30] ETSI TS 102 230-2: "Smart Cards; UICC-Terminal interface; Physical, electrical and logical test specification; Part 2: UICC features (Release 9)".

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

[32] GlobalPlatform: "GlobalPlatform Card, Common Implementation Configuration", Version 2.0.

NOTE: Available at http://www.globalplatform.org/.

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.

Not applicable.

3 Definition of terms, symbols, abbreviations and formats

3.1 Terms

For the purposes of the present document, the terms given in ETSI TS 102 226 [1], ETSI TS 102 127 [11] and the following apply:

Controlling Authority Security Domain (CASD): on-card controlling entity representing an off card trusted third party

NOTE: It provides services to confidentially load or generate Secure Channel keys of the APSD.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TS 102 226 [1], ETSI TS 102 127 [11] and the following apply:

ACK	ACKnowledge
ADD	Access Domain Data
ADF	Application Data File
ADP	Access Domain Parameter
AES	Advanced Encryption Standard
AID	Application IDentifier
APDU	Application Protocol Data Unit
API	Application Programming Interface
APSD	Application Provider Security Domain
BER-TLV	Basic Encoding Rules - Tag, Length, Value
BIP	Bearer Independent Protocol
C-APDU	Command - Application Protocol Data Unit
CASD	Controlling Authority Security Domain
CBC	Cell Broadcast Centre
CLA	CLAss
CMAC	Cipher-based Message Authentication Code
DAP	Data Authentication Pattern
DEK	Data Encryption Key
DES	Data Encryption Standard
DF	Directory File
ECB	Electronic Code Book
ECKA	Elliptic Curve Key Agreement algorithm
EF	Elementary File
FFS	For Further Study
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ICCID	Integrated Circuit Card IDentification
INS	INStruction
ISD	Issuer Security Domain
KIc	Key and algorithm Identifier for ciphering
KID	Key and algorithm IDentifier for RC/CC/DS
MAC	Message Authentication Code
MF	Management Field
MSL	Minimum Security Level
MSLD	Minimum Security Level Data
OTA	Over The Air
PDU	Packet Data Unit
RAM	Remote Application Management
R-APDU	Response - Application Protocol Data Unit
RF	Radio Frequency
RFM	Remote File Management
RFU	Reserved for Future Use
SCP02	Secure Channel Protocol 02
SD	Security Domain
SDU	Service Data Unit
SSD	Supplementary Security Domain
TAR	Toolkit Application Reference
TCP	Transmission Control Protocol
TLV	Tag Length Value