ETSI TS 102 226 V9.0.0 (2009-06)

Technical Specification

Smart Cards;
Remote APDU structure for UICC based applications
(Release 9)

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/79e2d982-1222-4bec-a9b2-0926288ffdf9/etsi-ts-102-226-v9.0.0-2009-06

Reference
RTS/SCP-T02850v900

Keywords
protocol, 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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/79e2d982-
2222-4bce-9b22-e26288ffdf9/etsi-ts-102-226-v9.0.0-
2009-06

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/chaircor/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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/79e2d982-122d-0bec-a9b2-0926288ffdf0/etsi-ts-102-226-v9.0.0-2009-06

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/79e2d982-1222-4bec-a9b2-0926288ffdf9/etsi-ts-102-226-v9.0.0-2009-06

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).

It is based on work originally done in the 3GPP in TSG-terminals WG3 and ETSI SMG.

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 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 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.

iTeh STANDARD PREVIEW (standards.iteh.ai) Full standard: https://standards.iteh.ai/catalog/standards/sist/79e20882-f322-40ec-a9b2-0926288ffdf9/etsi-ts-102-226-v9.0.0-2009-06

1 Scope

The present document defines the remote management of the UICC based on the secured packet structure specified in TS 102 225 [1].

It specifies the APDU format for remote management.

- Furthermore the present document specifies: a set of commands coded according to this APDU structure and used in the remote file management on the UICC. This is based on TS 102 221 [2].
- A set of commands coded according to this APDU structure and used in the remote application management on the UICC. This is based on the GlobalPlatform Card Specifications.

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.

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/79...2d982-1222-4aec-a9b2-0926288ffdf9/etsi-ts-102-226-v9.0.0-2009-06

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 102 225: "Smart Cards; Secured packet structure for UICC based applications".

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

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

[4] GlobalPlatform: "GlobalPlatform Card Specification, Version 2.2" including "Errata and precision list" Version 0.2.

NOTE: See http://www.globalplatform.org/.

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

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

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

NOTE: See http://www.globalplatform.org/.

[8] Void.

[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, Release 5)".

[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 Release 5)".

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

NOTE: See 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: See 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: See http://csrc.nist.gov/publications/nistpubs/.

[16] "GlobalPlatform Card UICC Configuration", Version 1.0.

NOTE: See http://www.globalplatform.org/.

[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 Specification Version 2.2, Amendment A" Version 1.0 including "Errata and Precisions" Version 1.0.

NOTE: See http://www.globalplatform.org/.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/79e2d982-1224dbec-4912-09262881c109/etsi-ts-102-226-v9.0.0-2009-06

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.

Not applicable.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TS 102 225 [1] and TS 101 220 [5] apply.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TS 102 225 [1] 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
EF	Elementary File
ICCID	Integrated Circuit Card IDentification
INS	INStruction
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
RFM	Remote File Management
RFU	Reserved for Future Use
SCP02	Secure Channel Protocol 02
SDU	Service Data Unit
TAR	Toolkit Application Reference
TLV	Tag Length Value

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/79e2d982-122f-4bec-a9b2-0926288ffdf9/etsi-ts-102-226-v9.0.0-2009-06

4 Overview of remote management

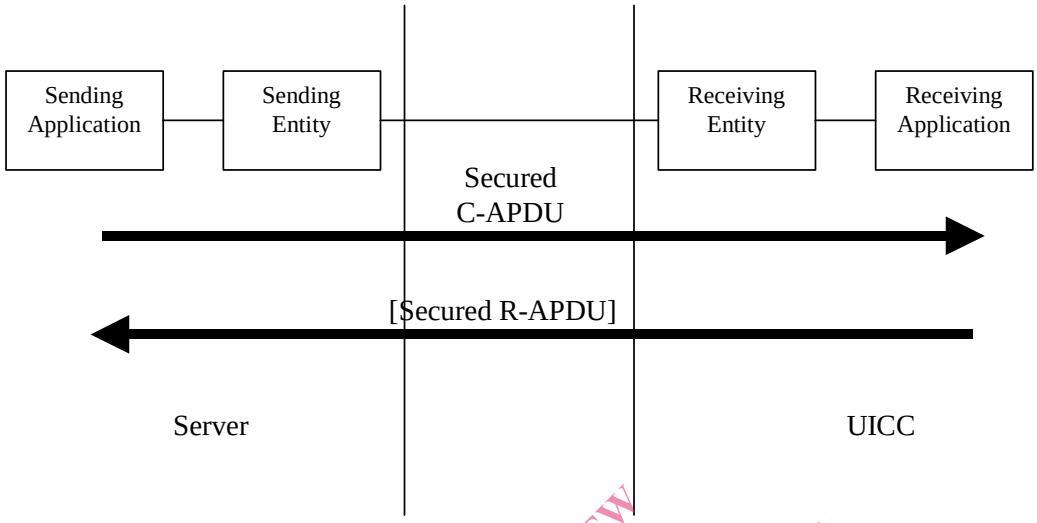

Figure 4.1: Remote management

ETSI STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/79e2d982-1213-abec-a9b2-095b628b8ff9/etsi-ts-102-226-v9.0.0-2009-06

All data exchanged between the Sending Entity and Receiving Entity shall be formatted as "Secured data" according to TS 102 225 [1]:

1) The parameter(s) in the "Secured data" is either a single command, or a list of commands, which shall be processed sequentially.

2) The Remote Management application shall take parameters from the "Secured data" and shall act upon the files or applications or perform other actions according to these parameters. A Remote Management application is the on-card Receiving Application that performs either Remote File Management (RFM) or Remote Application Management (RAM) as defined in the following clauses.

3) Remote Management commands shall be executed by the dedicated Remote Management Application (RAM). A Command "session" is defined as starting upon receipt of the parameter/command list, and ends when the parameter list in the "Secured data" is completed, or when an error (i.e. SW1 of the command indicates an error condition) is detected which shall halt further processing of the command list. Warnings or procedure bytes do not halt processing of the command list.

4) At the beginning and end of a Command "session" the logical state of the UICC as seen from the terminal shall not be changed to an extent sufficient to disrupt the behaviour of the terminal. If changes in the logical state have occurred that the terminal needs to be aware of, the application on the UICC may issue a REFRESH command according to TS 102 223 [3].

5 Remote APDU format

5.1 Compact Remote Application data format

5.1.1 Compact Remote command structure

A command string may contain a single command or a sequence of commands. The structure of each command shall be according to the generalized structure defined below; each element other than the Data field is a single octet (see TS 102 221 [2]).

The format of the commands is the same as the one defined in TS 102 221 [2] for T = 0 TPDU commands.

Class byte (CLA)	Instruction code (INS)	P1	P2	P3	Data

If the sending application needs to retrieve the Response parameters/data of a case 4 command, then a GET RESPONSE command shall follow this command in the command string.

The GET RESPONSE and any case 2 command (i.e. READ BINARY, READ RECORD) shall only occur once in a command string and, if present, shall be the last command in the string.

For all case 2 commands and for the GET RESPONSE command, if P3 = '00', then the UICC shall send back all available response parameters/data e.g. if a READ RECORD command has P3='00' the whole record shall be returned. The limitation of 256 bytes does not apply for the length of the response data. In case the data is truncated in the response, the remaining bytes are lost and the status words shall be set to '62 F1'.

5.1.2 Compact Remote response structure

If a proof of Receipt is required by the sending entity, the Additional Response Data sent by the Remote Management Application shall be formatted according to table 5.1.

Table 5.1: Format of additional response data

Length	Name
1	Number of commands executed within the command script (see note)
2	Status bytes or '61 xx' procedure bytes of last executed command / GET RESPONSE
X	Response data of last executed command / GET RESPONSE if available (i.e. if the last command was a case 2 command or a GET RESPONSE)
NOTE:	This field shall be set to '01' if one command was executed within the command script, '02' if two commands were executed, etc.

iTeh STANDARD PREVIEW (standards.iteh.ai)

5.2 Expanded Remote Application data format

5.2.1 Expanded Remote command structure

The "Secured data" sent to a Remote Management Application shall be a BER-TLV data object formatted according to table 5.2.

Table 5.2: Expanded format of Remote Management application command "secured data"

Length in bytes	Name
1	Command Scripting template tag
L	Length of Command Scripting template= A+B+…C
A	Command TLV
B	Command TLV
	…
C	Command TLV

The Command Scripting template is a BER-TLV data object as defined in TS 101 220 [5] and the tag of this TLV is defined in annex A.

A Remote Management application command string may contain a single or several Command TLVs.

A Command TLV can be one of the following:

- A C-APDU, containing a remote management command.
- An Immediate Action TLV, containing a proactive command or another action to be performed when it is encountered while processing the sequence of Command TLVs.
- An Error Action TLV, containing a proactive command to be performed only if an error is encountered in a C-APDU following this TLV.
- A script Chaining TLV as first Command TLV.

5.2.1.1 C-APDU TLV

The structure of each C-APDU shall be a TLV structure coded according to the C-APDU COMPREHENSION-TLV data object coding defined in TS 102 223 [3]. The restriction on the length of the C-APDU mentioned in the note in TS 102 223 [3] shall not apply.

For all case 2 and case 4 C-APDUs, if Le='00' in the C-APDU, then the UICC shall send back all available response parameters/data in the R-APDU e.g. if a READ RECORD command has Le='00' the whole record shall be returned. The limitation of 256 bytes does not apply for the length of the response data.

In case the data is truncated in the response of a C-APDU, the status words for this C-APDU shall be set to '62 F1' in the corresponding R-APDU. This shall terminate the processing of the command list.

If a R-APDU fills the response buffer so that no further R-APDU can be included in the response scripting template, this shall terminate the processing of the command list.

If Le field is empty in the C-APDU, then no response data is expected in the R-APDU. In that case, no R-APDU shall be returned by the UICC in the application additional response data except if the corresponding C-APDU is the last command executed in the script.

NOTE: In this expanded format the GET RESPONSE command is not used.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/79e20987-1222-4f8c-a9b2-092628bfdfd9/etsi-ts-102-226-v9.0.0-2009-06

5.2.1.2 Immediate Action TLV

The Immediate Action TLV is a BER TLV data object that allows the Remote Management Application to issue a proactive command during the execution or that allows to abort the execution if a proactive session is ongoing. It shall be formatted as shown in table 5.3 or table 5.4.

Table 5.3: Immediate Action TLV - normal format

Length in bytes	Name
1	Immediate Action tag (see annex A)
L	Length of Immediate Action = A > 1
A	Set of COMPREHENSION-TLV data objects

Table 5.4: Immediate Action TLV - referenced format

Length in bytes	Name
1	Immediate Action tag (see annex A)
1	Length of Immediate Action = 1
1	'01' to '7F': Reference to a record in EF_{RMA} '81': Proactive session indication '82': Early response other values: RFU

In case of reference to a record in EF_{RMA}, the referenced record shall contain the set of COMPREHENSION-TLV data objects preceded by a length value as defined for a BER TLV, see [10].