



**Smart Cards;
Remote APDU structure for UICC based applications
(Release 13)**

Reference

RTS/SCP-T02850vd00

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

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 only prevailing document is the print of the Portable Document Format (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

<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/CommitteeSupportStaff.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.

© European Telecommunications Standards Institute 2016.

All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE™** are Trade Marks of ETSI 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	5
Foreword.....	5
Modal verbs terminology.....	5
1 Scope	6
2 References	6
2.1 Normative references	6
2.2 Informative references.....	8
3 Definitions and abbreviations.....	8
3.1 Definitions.....	8
3.2 Abbreviations	8
4 Overview of remote management	9
5 Remote APDU format	10
5.1 Compact Remote Application data format	10
5.1.1 Compact Remote command structure	10
5.1.2 Compact Remote response structure.....	11
5.2 Expanded Remote Application data format.....	11
5.2.1 Expanded Remote command structure	11
5.2.1.0 Structure overview	11
5.2.1.1 C-APDU TLV	12
5.2.1.2 Immediate Action TLV	12
5.2.1.3 Error Action TLV.....	13
5.2.1.4 Script Chaining TLV	14
5.2.2 Expanded Remote response structure	14
5.3 Automatic application data format detection.....	17
6 Security parameters assigned to applications	18
6.1 Minimum Security Level (MSL).....	18
6.2 Access domain.....	18
7 Remote File Management (RFM)	18
7.0 RFM basic principles.....	18
7.1 Commands.....	19
7.2 UICC Shared File System Remote File Management	19
7.3 ADF Remote File Management.....	20
7.4 RFM implementation over HTTPS	20
8 Remote Application Management (RAM)	20
8.0 RAM basic principles	20
8.1 Remote application management application behaviour	21
8.2 Command coding and description	21
8.2.0 Basic rules.....	21
8.2.1 Commands	21
8.2.1.0 Application management commands overview.....	21
8.2.1.1 DELETE	22
8.2.1.2 SET STATUS	22
8.2.1.3 INSTALL	22
8.2.1.3.0 Basic requirements for INSTALL command.....	22
8.2.1.3.1 INSTALL [for load]	22
8.2.1.3.2 INSTALL [for install]	22
8.2.1.4 LOAD	30
8.2.1.5 PUT KEY	30
8.2.1.5.0 Generic rules for PUT KEY command.....	30
8.2.1.5.1 PUT KEY for AES	31
8.2.1.5.2 PUT KEY for triple DES.....	31
8.2.1.6 GET STATUS.....	31

8.2.1.6.0	Basic rules	31
8.2.1.6.1	Menu parameters	32
8.2.1.7	GET DATA.....	32
8.2.1.7.0	Basic rules	32
8.2.1.7.1	Void.....	33
8.2.1.7.2	Extended Card resources information	33
8.2.1.8	STORE DATA.....	33
8.3	RAM implementation over HTTPS.....	34
9	Additional command for push.....	34
9.0	Introduction	34
9.1	Push command behaviour	34
9.1.1	Request for open channel.....	34
9.1.2	Request for CAT_TP link establishment	34
9.1.3	Behaviour for responses.....	34
9.1.4	Request for TCP connection.....	34
9.1.5	Request for Identification Packet.....	34
9.2	Commands coding.....	35
9.2.0	Coding	35
9.2.1	Data for BIP channel opening.....	35
9.2.2	Data for CAT_TP link establishment.....	36
9.2.3	Data for TCP connection opening.....	36
9.2.4	Data for sending of Identification Packet	37
9.3	Closing of the BIP channel.....	37
10	Confidential application management.....	37
10.0	Overview and basic requirements.....	37
10.1	Confidential loading.....	38
10.2	Additional application provider security	38
10.3	Confidential setup of Security Domains.....	39
10.4	Application personalisation in an APSD	39
Annex A (normative):	BER-TLV tags.....	40
Annex B (informative):	RFM over HTTP Communication Flow	41
Annex C (informative):	Bibliography	43
Annex D (informative):	Change history	44
History		47

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 (<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.

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 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.
-

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.

1 Scope

The present document defines the remote management of the UICC based on any of the secured packet structures specified in ETSI 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 ETSI 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

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 reference 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.

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.

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

- [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 2.3".

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] Void.
- [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".