

Source: T3

Title: Draft TS 31.116 V1.0.0: Remote APDU Structure for (U)SIM Toolkit Applications

Document for: Information

DRAFT 3GPP TS 31.116 V1.0.0 (2002-03)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Terminals; Remote APDU Structure for (U)SIM Toolkit applications (Release 5)



Keywords

SIM, USIM, SMS, Smart card, security

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

<http://www.3gpp.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.

© 2001, 3GPP Organizational Partners (ARIB, CWTS, ETSI, T1, TTA, TTC).
All rights reserved.

Contents

Foreword.....	5
Introduction	5
1 Scope	6
2 References	6
2.1 Normative references.....	6
3 Definitions and abbreviations	6
4 Introduction	6
5 Remote APDU Format	7
5.1 Remote command coding	7
5.2 Response coding.....	7
5.2.1 SIM specific behaviour for Response Packets (Using SMS-PP)	7
5.2.1 USIM specific behaviour for Response Packets (Using SMS-PP).....	7
6 Remote File Management	7
6.1 SIM Remote File Management.....	7
6.1.1 SIM Input Commands.....	8
6.1.2 SIM Output Commands	8
6.2 USIM Remote File Management	8
7 Remote Applet Management.....	8
7.1 Access Domain Parameter.....	8
7.1.1 SIM Access Mechanism.....	9
7.1.2 USIM Access Mechanism.....	10
Change History	11
Foreword.....	4
Introduction	4
1 Scope	5
2 References	5
2.1 Normative references	5
3 Definitions and abbreviations	5
4 Introduction	5
5 Remote APDU Format	6
5.1 Remote command coding.....	6
5.2 SIM specific behaviour for Response Packets (Using SMS-PP).....	6
6 Remote File Management	6
6.1 SIM Remote File Management.....	6
6.1.1 Input Commands.....	6
6.1.2 Output Commands.....	7
6.2 USIM Remote File Management.....	7
7 Remote Applet Management.....	7
7.1 Access Domain Parameter.....	7
7.2 APDU Access Mechanism	7
7.3 3GPP Access Mechanism.....	8
Change History	9

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG 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 TSG for information;
 - 2 presented to TSG for approval;
 - 3 or greater indicates TSG 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

This specification is the result of a split of TS 23.048 REL-5 between the generic part and the bearers specific application. The generic part has been transferred to SCP. This specification is the bearers specific part.

1 Scope

The present document defines the remote management of files and applets on the SIM/USIM.

It describes the APDU format for remote management.

Furthermore the document specifies:

- a set of commands coded according to this APDU structure and used in the remote file management on the SIM/USIM specified in 3GPP TS 51.011 [1], 3GPP TS 31.101 [2] and 3GPP TS 31.102 [3].
- a set of commands coded according to this APDU structure and used in the remote applet management on the SIM/USIM. This is based on TS 102 226 ~~the Open Platform Card Specification~~ [4].

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

2.1 Normative references

- [1] 3GPP TS 51.011: "Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".
- [2] 3GPP TS 31.101: "UICC-Terminal Interface; Physical and Logical Characteristics".
- [3] 3GPP TS 31.102: "3rd Generation Partnership Project (3GPP); Characteristics of the NAA application".
- [4] ~~Open Platform Card Specification version 2.0.1 (see <http://www.globalplatform.org/>)~~
- [45] ETSI TS 102 226: "Remote APDU structure for UICC based applications".
- [56] ISO/IEC 7816-4 (1995): "Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 4: Interindustry commands for interchange".

3 Definitions and abbreviations

All definitions and abbreviations applicable to this document are specified in TS 102 226 [5].

4 Introduction

The remote APDU structure for SIM/USIM applications shall comply with the one defined in TS 102 226 [5]. This specification only contains additional requirements or explicit limitations for SIM/USIM applications.

5 Remote APDU Format

5.1 Remote command coding

The SIM/USIM Remote command coding shall comply with the ~~clause Remote command coding 5.1~~ of TS 102 226 [5].

5.2 Response coding

~~5.2 SIM specific behaviour for Response Packets (Using SMS-PP)~~

The SIM/USIM Response coding shall comply with the Response coding ~~clause 5.2~~ of TS 102.226 [5], added features are defined below.

5.2.1 SIM specific behaviour for Response Packets (Using SMS-PP)

Table 1 summarises the behaviour of the SIM's RE/RA with regard to PoR.

Table 1: SIM specific behaviour

PoR	successful case	Unsuccessful cases (see table 5)
No	'90 00' or '91 XX', null RP-ACK	'90 00' or '91 XX', null RP-ACK
Yes	'9F XX' (PoR OK, status code '00').	'9E XX' (security error of some kind).

NOTE: in the case where no proof of Receipt is required by the sending entity, it is however permissible for the SIM to send back data using '9F XX' in the successful case or '9E XX' in the unsuccessful case.

If the SIM responds with the '90 00' or '91 XX' code, then there is no User Data to be included in an SMS-DELIVER-REPORT; the ME sends a "null" RP-ACK, with no User Data attached.

In the case of a '9F XX' or '9E XX' response from the SIM, 'XX' indicates the length of the response data to be obtained from the SIM using a later GET RESPONSE command. The response obtained from the SIM is the complete Response Packet to be included in the User Data part of the SMS-DELIVER-REPORT which will be returned to the Sending Entity as the TP part of the RP-ACK in the '9F XX' case, or as the TP part of the RP-ERROR in the '9E XX' case. In the case of a '9E XX' response from the SIM, the value of the TP-FCS element of the RP-ERROR shall be 'SIM data download error'. Because the SIM is unable to indicate to the ME that the TP-UDHI bit is to be set, the Sending Entity receiving the Response Packet shall expect the UDH structure in any event. See 3GPP TS 24.011 [4] for more detail of the structure of the RP-ACK and RP-ERROR protocol element, and 3GPP TS 23.040 [3] for more detail of the SMS-DELIVER-REPORT 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 102.226 [5].

5.2.1 USIM specific behaviour for Response Packets (Using SMS-PP)

[TBD]

6 Remote File Management

6.1 SIM Remote File Management

Command and Response formats are defined in TS 102 226 [5]. Nevertheless, the list of commands defined in TS 102 226 [5] for Remote File Management does not apply for SIM application. All the SIM Remote File Management commands are defined below.

6.1.1 SIM Input Commands

The standardised commands are listed in table 2. The commands are as defined in 3GPP TS 51.011 [1], except that the SELECT command is extended from the one in 3GPP TS 51.011 [1] to include "SELECT by path" as defined in ISO/IEC 7816-4 [6].

Table 2: Input Commands

Operational command
SELECT
UPDATE BINARY
UPDATE RECORD
SEEK
INCREASE
VERIFY CHV
CHANGE CHV
DISABLE CHV
ENABLE CHV
UNBLOCK CHV
INVALIDATE
REHABILITATE

6.1.2 SIM Output Commands

The commands listed in table 3 are defined in 3GPP TS 51.011[1]. These commands shall only occur once in a command string and, if present, shall be the last command in the string. The Response Data shall be placed in the Additional Response Data element of the Response Packet. If SMS is being used, these should result in the generation of a single SM by the UICC.

Table 3: Output commands

Operational command
READ BINARY
READ RECORD
GET RESPONSE

6.2 USIM Remote File Management

All USIM Remote File Management shall comply with TS 102 226 [5].

7 Remote Applet Management

All SIM/USIM Remote Applet Management shall comply with TS 102 226 [5], added features are defined below.

7.1 Access Domain Parameter

This parameter indicates the mechanism used to control the applet instance access to the File System. It is a parameter of the `INSTALL` (Install) command described in TS 102 226 [5].

Value	Name	Support	ADD length
'00'	Full access to the File System (see TS 102 226 [5])	Mandatory	0
'01'	SIM access mechanism	Optional	2
'02'	USIM access mechanism	Optional	-
'03' to '7F'	RFU	RFU	RFU
'80' to 'FE'	Proprietary mechanism	-	-
'FF'	No access to the File System	Mandatory	0

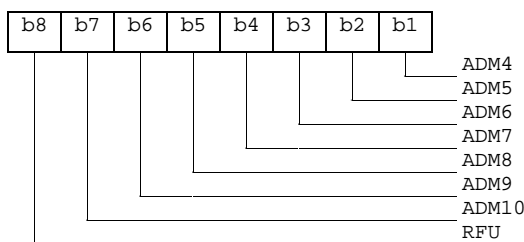
7.21.1 SIM Access Mechanism

This mechanism shall be used, if supported, by the framework if the Access Domain Parameter value is '01'. It shall use the Access Domain Data passed at applet instantiation to define the access conditions fulfilled while the toolkit applet is running.

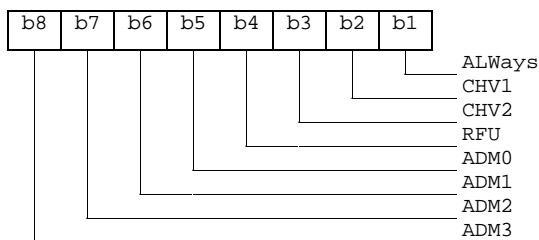
The APDU Access Domain Data is a bit map combination of the file access condition levels described in 3GPP TS 51.011 [1]. When the bit is set the associated Access Condition is granted.

The APDU Access Domain Data is coded as follows:

Byte 1:



Byte 2:



EXAMPLE:

Possible combinations of fulfilled Access Conditions are shown below:

ADD value	Applet access condition fulfilled
'00 00'	No access
'00 01'	ALWays
'00 02'	CHV1
'00 03'	ALWays and CHV1
'00 04'	CHV2
'00 05'	ALWays and CHV2
'00 06'	CHV1 and CHV2
:	:
'00 10'	ADM0
:	:
'00 20'	ADM1
:	:
'00 22'	ADM1 and CHV1
:	:
'01 00'	ADM4
:	:
'40 00'	ADM10
:	:
'41 37'	ADM10 and ADM4 and ADM1 and ADM0 and CHV2 and CHV1 and ALWays
:	:

7.1.23 USIM Access Mechanism

[TBD]

Change History

This annex lists all changes made to the present document.

History Table					
Date	Meeting	Tdoc	Changes	Old	New
2001-10	T3 API #9	T3a010198	Initial version is based on 3GPP TS 23.048 V5.1.0	-	0.0.0
2001-11	T3#21	T3-010672	Submitted to 3GPP T3#21. Editorial changes.	0.0.0	0.0.1
2002-01	T3#22	T3-010123050	Submitted to 3GPP T3#22. Updated to include the results of TSG-T#14 and editorial changes.	0.0.1	0.1.0
2002-03	T#15	TP-020076	Submitted to 3GPP TSG-T#15 for information.	0.1.0	1.0.0

Rapporteurs: Sophie Viallet (sophie.viallet@gemplus.com) and Florence Martin (flmartin@montrouge.sema.slb.com)