3GPP TSG SA WG3 Security — S3#33 **S3-040369**
10 - 14 May 2004
Beijing, China

3GPP TSG-T2 #25 ***T2-040230***
Edinburgh, UK
19 -23 April 2004

Title: LS on Potential Security issues relating to use of AT Commands to access UICC
Release: Rel-6

Source: T2
To: SA3
Cc: T3

Contact Person:
Name: Nicolas Chaumartin
Tel. Number: +33 1 46 00 74 71 / +33 6 25 07 19 21
E-mail Address: nchaumartin@axalto.com

Attachments: T2-040228

1. Overall Description:

T2 has discussed a CR to add a set of AT commands to introduce the Logical Channel mechanism for the UICC as described in TS 31.101, the CR is attached to this LS (T2-040228). This CR is not approved but still in discussion stage in T2

As T2 was discussing this document some T2 members expressed their concerns that security issues may exist related to USIM remote access using AT commands described in TS 27.007 and in the CR.

T2 kindly asks SA3 to review the specification from a security perspective and to send its feedback concerning the issues described above.

2. Actions:

T2 kindly asks SA3 to review the specification from a security perspective and to send its feedback concerning the issue described above.

3. Date of next T2 Meetings:

T2#26	23 – 27 Aug 2004	Montreal, Canada
T2#27	8 – 12 Nov 2004	tbd

3GPP TSG-T2 #25
Edinburgh, UK
19 -23 April 2004

T2-040228

CR-Form-v7

CHANGE REQUEST

⌘	**27.007**	**CR**	**CRNum**	⌘ **rev**	**-**	⌘	Current version:	**6.4.0**	⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ □ ME ☒ Radio Access Network □ Core Network □

Title:	⌘	Support of logical channels in AT commands		
Source:	⌘	Axalto		
Work item code:	⌘		***Date:*** ⌘	21/04/2004
Category:	⌘	B	***Release:*** ⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change: ⌘ The Rel-4 UICC, and also existing SIM/WIM cards, offer the ability to send commands on different logical channels. This means that a terminal application can communicate with a card application, other than the SIM, on a selected logical channel. It is necessary to provide AT commands for opening and closing logical channels and also for sending APDU commands on these logical channels.

Summary of change: ⌘ The UICC ATR (Answer to Reset) provides information if the card implements logical channels and also their number. The following new commands should enable the usage of this new functionality.

The new get ATR command will enable the terminal application to know if logical channels are implemented and how many can be opened.

The new Open and Close Channels AT commands will enable the opening and closing of logical channels.

The SIM +CSIM and SIM +CRSM existing AT commands are extended to allow communication with a UICC application on a logical channel and not only the SIM.

Consequences if not approved: ⌘ No means to communicate with a UICC application other than SIM. And misalignement between TS 27.007 and TS 31.101

Clauses affected: ⌘ 2, 3.2, 8.xx, 8.17, 8.18, 9.2.1

		Y	N			
Other specs affected:	⌘			Other core specifications	⌘	
				Test specifications		

	□ □	O&M Specifications	
Other comments: ⌘			

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. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TS 22.002: "3rd Generation Partnership Project; Bearer Services (BS) supported by a GSM Public Land Mobile Network (PLMN)".

[…]

[59] 3GPP TS 31.102: "3rd Generation Partnership Project; Technical Specification Group Terminals; Characteristics of the USIM Application".

[60] ETSI TS 102 221 "Smart Cards; UICC-Terminal interface; Physical and logical characteristics (Release 1999)".

[61] 3GPP TS 44.065: "3rd Generation Partnership Project; General Packet Radio Service (GPRS); Mobile Station (MS) – Serving GPRS Support Node (SGSN); Subnetwork Dependent Convergence Protocol (SNDCP)".

[62] 3GPP TS 25.323: "3rd Generation Partnership Project; Packet Data Convergence Protocol (PDCP)".

[63] 3GPP TS 23.101: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General UMTS Architecture "

[xx] 3GPP TS 31.101: "UICC-Terminal Interface; Physical and Logical Characteristics"

3.2 Abbreviations

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

AT	ATtention; this two-character abbreviation is always used to start a command line to be sent from TE to TA
ASCI	Advanced Speech Call Items, including VGCS, VBS and eMLPP
BCD	Binary Coded Decimal

[…]

8.17 Generic ~~SIM~~UICC access +CSIM

Table 77: +CSIM action command syntax

Command	Possible response(s)

`+CSIM=<length>,<command>`	`+CSIM: <length>,<response>`
	`+CME ERROR: <err>`

`+CSIM=?`	

Description

Set command transmits to the MT the `<command>` it then shall send as it is to the ~~SIM~~ active application in the UICC on its selected logical channel. In the same manner the ~~SIM~~UICC`<response>` shall be sent back by the MT to the TA as it is. Refer subclause 9.2 for `<err>` values.

This command allows a direct control of applications ~~the~~ on the UICC~~SIM~~ by a~~n~~ distant application on the TE. The TE shall then take care of processing ~~SIM~~UICC information within the frame specified by GSM/UMTS.

NOTE: Compared to Restricted ~~SIM~~UICC Access command `+CRSM`, the definition of `+CSIM` allows TE to take more control over the ~~SIM~~UICC-MT interface. The locking and unlocking of the interface may be done by a special `<command>` value or automatically by TA/MT (by interpreting `<command>` parameter). In case that TE application does not use the unlock command (or does not send a `<command>` causing automatic unlock) in a certain timeout value, MT may release the locking.

Defined values

`<length>` : integer type; length of the characters that are sent to TE in `<command>` or `<response>` (two times the actual length of the command or response)

`<command>` : command passed on by the MT to the ~~SIM~~UICC in the format as described in ~~GSM 51.011 [28]~~ 3GPP TS 31.101 [xx] (hexadecimal character format; refer `+CSCS`)

`<response>` : response to the command passed on by the ~~SIM~~UICC to the MT in the format as described in ~~GSM 51.011 [28~~ 3GPP TS 31.101 [xx] (hexadecimal character format; refer `+CSCS`)

Implementation

Optional.

8.18 Restricted ~~SIM~~UICC access +CRSM

Table 78: +CRSM action command syntax

Command	Possible response(s)

`+CRSM=<command>[,<fileid>`
`[,<P1>,<P2>,<P3>[,<data>]]]`
	`+CRSM: <sw1>,<sw2>[,<response>]`
	`+CME ERROR: <err>`

`+CRSM=?`	

Description

By using this command instead of Generic ~~SIM~~UICC Access +CSIM TE application has easier but more limited access to the ~~SIM~~UICC database. Set command transmits to the MT the ~~SIM~~UICC <command> and its required parameters. MT handles internally all UICC~~SIM~~-MT interface locking and file selection routines. As response to the command, MT sends the actual ~~SIM~~UICC information parameters and response data. MT error result code +CME ERROR may be returned when the command cannot be passed to the ~~SIM~~UICC, but failure in the execution of the command in the ~~SIM~~UICC is reported in <sw1> and <sw2> parameters. Refer to subclause 9.2 for <err> values.

Coordination of command requests to ~~SIM~~UICC and the ones issued by GSM/UMTS application inside the MT is implementation dependent. However the TE should be aware of the precedence of the GSM/UMTS application commands to the TE commands.

Defined values

<command> (command passed on by the MT to the ~~SIM~~UICC; refer ~~GSM 51.011 [28]~~ 3GPP TS 31.101 [xx]):

164	SELECT
176	READ BINARY
178	READ RECORD
192	GET RESPONSE
214	UPDATE BINARY
220	UPDATE RECORD
242	STATUS

all other values are reserved

NOTE 1: The MT internally executes all commands necessary for selecting the desired file, before performing the actual command.

<fileid>: integer type; this is the identifier of a elementary datafile on ~~SIM~~UICC. Mandatory for every command except STATUS and SELECT.

NOTE 2: The range of valid file identifiers depends on the actual ~~SIM~~UICC and is defined in ~~GSM 51.011 [28]~~ 3GPP TS 31.101 [xx]. Optional files may not be present at all.

<P1>, <P2>, <P3>: integer type; parameters passed on by the MT to the ~~SIM~~UICC. These parameters are mandatory for every command, except GET RESPONSE and STATUS. The values are described in ~~GSM 51.011 [28]~~3GPP TS 31.101 [xx]

<data>: information which shall be written to the SIM (hexadecimal character format; refer +CSCS)

<sw1>, <sw2>: integer type; information from the ~~SIM~~UICC about the execution of the actual command. These parameters are delivered to the TE in both cases, on successful or failed execution of the command

<response>: response of a successful completion of the command previously issued (hexadecimal character format; refer +CSCS). STATUS and GET RESPONSE return data, which gives information about the current elementary datafield. This information includes the type of file and its size (refer ~~GSM 51.011 [28]~~3GPP TS 31.101 [xx]). After READ BINARY or READ RECORD command the requested data will be returned. <response> is not returned after a successful UPDATE BINARY or UPDATE RECORD command

Implementation

Optional.

[…]

8.x Request UICC ATR +CATR

Table x: +CATR action command syntax

Command	Possible response(s)

`+CATR`	`+CATR: <ATR>`
	`+CME ERROR: <err>`

`+CATR=?`	

Description

Execution of the command causes the TA to return `<ATR>,` which is intended to permit the TE to identify the individual ATR (Answer to Reset) of the UICC, which is attached to ME. Refer subclause 9.2 for possible `<err>` values.

Defined values

<ATR>: Answer to Reset (string without double quotes that consists only of hexadecimal numbers from 00 to FF)

See 3GPP TS 31.101 [xx] for more information about ATR~~.~~

Implementation

Optional.

8.y Open Logical Channel +CCHO

Table xx: +CCHO action command syntax

Command	Possible response(s)

`+CCHO`	`<Logical Channel>`
	`+CME ERROR: <err>`

`+CCHO=?`	

Description

Execution of the command causes the TA to return `<logical channel number>` to allow the TE to identify a logical channel that is being allocated by the UICC, which is attached to ME. The UICC will open a new logical channel when receiving this command and return the newly opened logical channel number as the response.

Note that the logical channel number is contained in the CLASS byte of an APDU command, thus implicitly contained in all APDU commands sent to a UICC. See 3GPP TS 31.101 [xx] for further information on logical channels in APDU commands protocol.

Refer subclause 9.2 for possible `<err>` values.

Defined values

`<Logical Channel>`: A logical channel number (string without double quotes that represents a decimal value)

See 3GPP TS 31.101 [xx] for more information about defined values.

Implementation

Optional.

8.w Close Logical Channel +CCHC

Table xx: +CCHC parameter command syntax

Command	Possible response(s)
`+CCHC=<logical channel number>`	*+CCHC ERROR: <err>*
`+CCHC=?`	

Description

This command sends to the ME a logical channel number that the UICC should close. The TE will no longer be able to send commands on this logical channel. The UICC will close the logical channel when receiving this command. Refer subclause 9.2 for possible `<err>` values.

Defined values

`<logical channel number>`: A logical channel number (string without double quotes that represents a decimal value)

Implementation

Optional.