3GPP TSG-T (Terminals) Meeting #18
New Orleans, USA, 4-6 December 2002

Tdoc TP-020284

Source: TSG-T3

Title: Change Requests to TS 23.048, TS 31.115 and TS 31.116 "Secure Messaging"

Document for: Approval

This document contains several change requests as follows:

Doc-1st-Level	Spec	CR	Phase	Subject	Cat	Vers. old	Vers. new	Doc-2nd-Level
TP-020284	23.048	027	Rel-5	Clarification of the Install(Install) command in case of installing a non Toolkit Applet	F	5.4.0	5.5.0	T3-020887
TP-020284	23.048	029	Rel-5	Mandatory/Optional/Conditional data in the Toolkit Applet Specific Parameters field	F	5.4.0	5.5.0	T3-020929
TP-020284	31.116	002	Rel-6	Alignment with TS 23.048 Release 5: Correction of the Specific behaviour for Response Packets (Using SMS-PP)	F	6.1.0	6.2.0	T3-020893

Doc-1st-Level	Spec	CR	Phase	Subject	Cat	Vers. old	Vers. new	Doc-2nd-Level
TP-020284	23.048	028	Rel-5	Clarification on the RC/CC/DS coding in SPI2	F	5.4.0	5.5.0	T3-020894
TP-020284	31.115	002	Rel-6	Clarification on the RC/CC/DS coding in SPI2	A	6.0.0	6.1.0	T3-020895

3GPP TSG-T3 Meeting #25
Maastricht, Netherlands, 5 – 8 November 2002

Tdoc ⌘T3-020887
Revised T3-020828

CR-Form-v7

CHANGE REQUEST

⌘	**23.048**	**CR**	**027**	**-**	⌘	Current version:	**5.4.0** ⌘

*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:	⌘	Clarification of the Install(Install) command in case of installing a non Toolkit Applet		
Source:	⌘	TSG T3		
Work item code:	⌘	TEI	***Date:*** ⌘	08/11/2002
Category:	⌘	**F**	***Release:*** ⌘	Rel-5

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 behaviour of the Remote Applet Management Application is not clear in the case of installing an Applet that does not implement the ToolkitInterface interface
Summary of change:	⌘	Specify the behavior of the Remote Application Management when a non toolkit applet is installed.
Consequences if not approved:	⌘	Unclear and unpredictable behaviour of Remote Application Management for the installation of a non toolkit applet.

Clauses affected:	⌘	Annex A § A.1.1.4.2: Applet Management Commands for TS 43.019 compliant cards.

		Y	N		
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	

Other comments:	⌘	

Annex A (normative): Applet Management Commands for TS 43.019 compliant cards

(…)

A.1.1.4.2 Install (Install)

Toolkit registration is only active if the toolkit applet is at the state selectable, for example if the applet is registered for the event Menu Selection it shall only appear in the menu if the applet is in the selectable state.

The Install Parameter Field of the Install (Install) command shall be coded as follows:

Presence	Length	Name
Mandatory	1	Tag of System Parameters constructed field 'EF'
	1	Length of System Parameters constructed field
	8 – n or 16~~15~~-n	System Parameters constructed value field.
Mandatory	1	Tag of Applet specific parameters field: 'C9'
	1	Length of Applet specific Parameters field
	0-n	Applet specific Parameters

The System Parameters value field of the Install (Install) command shall be coded as follows:

Presence	Length	Name
Mandatory	1	Tag of non volatile memory requirements for installation field: 'C8'
	1	Length of non volatile memory requirement for installation (see A.1.4.2.2)
	2	Non volatile memory required for installation in byte (see A.1.4.2.2)
Mandatory	1	Tag of volatile memory requirements for installation field: 'C7'
	1	Length of volatile memory requirement for installation (see A.1.4.2.2)
	2	Volatile memory required for installation in byte (see A.1.4.2.2)
Conditional (see Note)	1	Tag of toolkit applet specific parameters field: 'CA'
	1	Length of toolkit applet specific parameters field
	6-n	Toolkit Applet specific Parameters (see A.1.4.2.1)
Note: These parameters are mandatory for Applets implemeting the *ToolkitInterface* defined in TS 43.019 [15].		

Even if the length of the non volatile or volatile memory is present in the Install(Load) command, the card shall use the values indicated in the Install(Install) command at instantiation, should these values differ.

The format of the install method buffer provided by the Install (Install) command shall be the one specified in the Open Platform Card specification [14].

The applet may invoke the register(bArray, bOffset, bLength) or the register() method: the applet instance shall be registered with the instance AID present in the Install (Install) command.

If the register (bArray, bOffset, bLength) is invoked, the AID passed in the parameters shall be the instance AID provided in the install method buffer.

If the register() method is invoked the instance AID present in the Install(Install) command and the AID within the Load File, as specified in Open Platform Card specification [14], should be the same.

3GPP TSG-T3 Meeting #25
Maastricht, Netherlands, 5 – 8 November 2002

Tdoc ⌘T3-020894
revised T3-020859

CR-Form-v3

CHANGE REQUEST

⌘ **23.048 CR 028** ⌘ rev **-** ⌘ Current version: **5.4.0** ⌘

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

Proposed change affects: ⌘ (U)SIM ☒ ME/UE □ Radio Access Network □ Core Network □

Title: ⌘	Clarification on the RC/CC/DS coding in SPI2		
Source: ⌘	TSG-T3		
Work item code: ⌘	TEI	***Date:*** ⌘	06/11/2002
Category: ⌘	**F**	***Release:*** ⌘	*REL-5*

Use one of the following categories:
F *(essential 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)*

Reason for change: ⌘	A misunderstanding with the word “security” could lead to say that if b4b3 is set to 00, ciphering cannot be applied in the response packet.
Summary of change: ⌘	In SPI second byte, b4b3 description, replace “No security” by “No RC, CC or DS”
Consequences if not approved: ⌘	Some interpretations can forbid having an encrypted response packet without RC/CC/DS field.

Clauses affected: ⌘	
Other specs Affected: ⌘	□ Other core specifications ⌘ □ Test specifications □ O&M Specifications
Other comments: ⌘	

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at: http://www.3gpp.org/3G_Specs/CRs.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

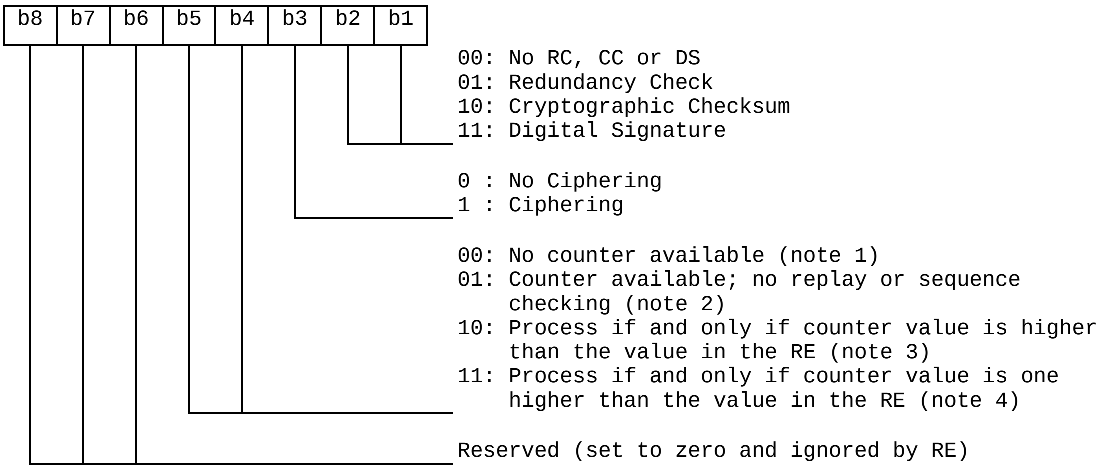
2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://www.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2000-09 contains the specifications resulting from the September 2000 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

5.1.1 Coding of the SPI

The SPI is coded as below.

First Octet:



```
00: No RC, CC or DS
01: Redundancy Check
10: Cryptographic Checksum
11: Digital Signature

0 : No Ciphering
1 : Ciphering

00: No counter available (note 1)
01: Counter available; no replay or sequence
    checking (note 2)
10: Process if and only if counter value is higher
    than the value in the RE (note 3)
11: Process if and only if counter value is one
    higher than the value in the RE (note 4)

Reserved (set to zero and ignored by RE)
```

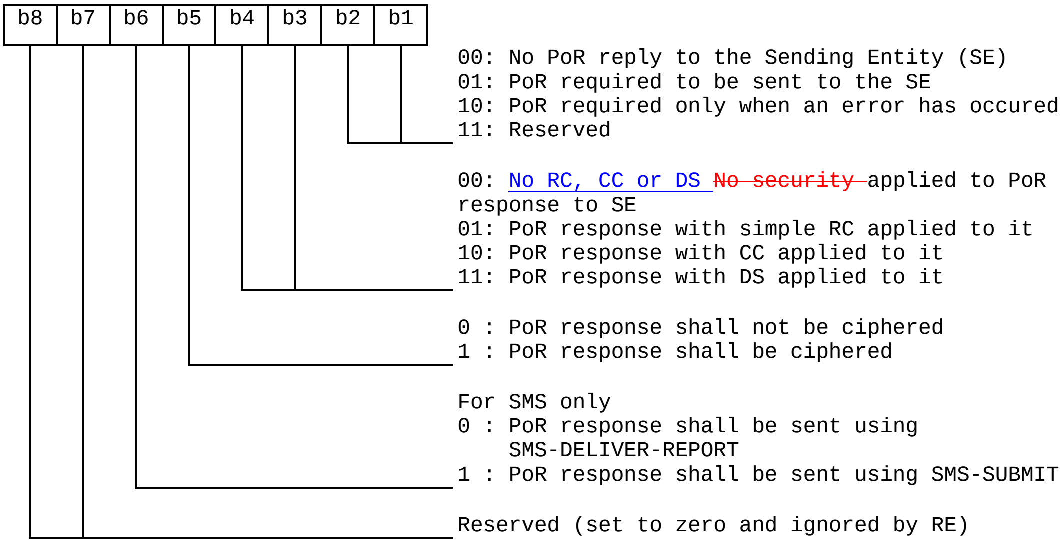
NOTE 1: In this case the counter field is present in the message.

NOTE 2: In this case the counter value is used for information purposes only, (e.g. date or time stamp). If the Command Packet was successfully unpacked, the counter value can be forwarded from the Receiving Entity to the Receiving Application. This depends on proprietary implementations and happens in an application dependent way.

NOTE 3: The counter value is compared with the counter value of the last received Command Packet. This is tolerant to failures on the transport level (i.e. losses of Command Packets). A possible scenario is a global update.

NOTE 4: This provides strict control in addition to security indicated in note 3.

Second Octet:



00: No PoR reply to the Sending Entity (SE)
01: PoR required to be sent to the SE
10: PoR required only when an error has occured
11: Reserved

00: No RC, CC or DS ~~No security~~ applied to PoR response to SE
01: PoR response with simple RC applied to it
10: PoR response with CC applied to it
11: PoR response with DS applied to it

0 : PoR response shall not be ciphered
1 : PoR response shall be ciphered

For SMS only
0 : PoR response shall be sent using SMS-DELIVER-REPORT
1 : PoR response shall be sent using SMS-SUBMIT

Reserved (set to zero and ignored by RE)

3GPP TSG-T3 Meeting #25
Maastricht, Netherlands, 5 – 8 November 2002

Tdoc ⌘ T3-020929

CR-Form-v7

CHANGE REQUEST

⌘ **23.048 CR** 029 ⌘ **rev** **-** ⌘ Current version: **5.4.0** ⌘

*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:	⌘	Mandatory/Optional/Conditional data in the Toolkit Applet Specific Parameters field			
Source:	⌘	TSG-T3			
Work item code:	⌘	TEI	***Date:***	⌘	06/11/2002
Category:	⌘	**F**	***Release:***	⌘	Rel-5

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:	⌘	To ensure backward compatibility with existing infrastructures between Rel-4 and Rel-5 of TS 23.048, it is necessary to specify whether a parameter in the Toolkit Applet Specific Parameters field is mandatory, optional or conditional.
Summary of change:	⌘	For each parameter of the Toolkit Applet Specific Parameters field it is defined whether it is mandatory, optional or conditional to include them in the install(install) command data. Editorial changes
Consequences if not approved:	⌘	Backward compatibility issue and interoperability problem

Clauses affected:	⌘	§ 3.2, § 9, Annex A.1

Other specs affected: ⌘

Y	N		
		Other core specifications	⌘
		Test specifications	
		O&M Specifications	

Other comments:	⌘	EP SCP TS 102 226 is impacted

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

3.2 Abbreviations

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

ADD	Access Domain Data
ADP	Access Domain Parameter
CBC	Cipher Block Chaining
CBS	Cell Broadcast Service
CC	Cryptographic Checksum
CNTR	Counter
CHI	Command Header Identifier
CHL	Command Header Length
CPI	Command Packet Identifier
CPL	Command Packet Length
DAP	Data Authentication Pattern
DES	Data Encryption Standard
DCS	Data Coding Scheme
DS	Digital Signature
ECB	Electronic codebook
IEI	Information Element Identifier
IEIDL	Information Element Identifier Data Length
IED	Information Element Data
KIc	Key and algorithm Identifier for ciphering
KID	Key and algorithm Identifier for RC/CC/DS
KIK	Key Identifier for protecting KIc and KID
MID	Message IDentifier
MO-SMS	Mobile Originated Short Message
MT-SMS	Mobile Terminated Short Message
MSL	Minimum Security Level
MSLD	Minimum Security Level Data
OP	Open Platform
PCNTR	Padding Counter
PLMN	Public Land Mobile Network
PoR	Proof of Receipt
PP	Page Parameter
RA	Receiving Application
RC	Redundancy Check
RE	Receiving Entity
RHI	Response Header Identifier
RHL	Response Header Length
RPI	Response Packet Identifier
RPL	Response Packet Length
SA	Sending Application
SE	Sending Entity
SIM	Subscriber Identity Module
SM	Short Message
SMS	Short Message Service
SMS-PP	Short Message Service – Point to Point
SMS-CB	Short Message Service – Cell Broadcast
SMS-SC	Short Message Service - Service Centre
SN	Serial Number
SPI	Security Parameters Indication
TAR	Toolkit Application Reference
TLV	Tag – Length – Value (data structure)
UDH	User Data Header
UDHI	User Data Header Indicator
UDHL	User Data Header Length
UDL	User Data Length
USIM	Universal Subscriber Identity Module
USSD	Unstructured Supplementary Services Data

9 Open Platform commands for Remote Applet Management

Remote Applet Management on a UICC card includes the ability to load, install, and remove applets. This management is under the responsibility of the Network Operator or Service Provider owning the UICC. The described procedure is mandatory for 3GPP TS 43.019 compliant cards. Other technologies may either use this procedure or use their own mechanisms. The concept of embedding APDUs in a short message is as defined in clause ~~7~~8 "Remote File management" in the present document.

Annex A (normative): Remote Management Applications Implementation for TS 43.019 compliant cards

A.1 Applet Management Commands for TS 43.019 compliant cards

(…)

A.1.1.4.2 Install (Install)

Toolkit registration is only active if the toolkit applet is at the state selectable, for example if the applet is registered for the event Menu Selection it shall only appear in the menu if the applet is in the selectable state.

The Install Parameter Field of the Install (Install) command shall be coded as follows:

Presence	Length	Name
Mandatory	1	Tag of System Parameters constructed field 'EF'
	1	Length of System Parameters constructed field
	16~~5~~-n	System Parameters constructed value field.
Mandatory	1	Tag of Applet specific parameters field: 'C9'
	1	Length of Applet specific Parameters field
	0-n	Applet specific Parameters

The System Parameters value field of the Install (Install) command shall be coded as follows:

Presence	Length	Name
Mandatory	1	Tag of non volatile memory requirements for installation field: 'C8'
	1	Length of non volatile memory requirement for installation (see A.1.1.4.2.2)
	2	Non volatile memory required for installation in byte (see A.1.1.4.2.2)
Mandatory	1	Tag of volatile memory requirements for installation field: 'C7'
	1	Length of volatile memory requirement for installation (see A.1.1.4.2.2)
	2	Volatile memory required for installation in byte (see A.1.1.4.2.2)
Mandatory	1	Tag of toolkit applet specific parameters field: 'CA'
	1	Length of toolkit applet specific parameters field
	6-n	Toolkit Applet specific Parameters (see A.1.1.4.2.1)

Even if the length of the non volatile or volatile memory is present in the Install(Load) command, the card shall use the values indicated in the Install(Install) command at instantiation, should these values differ.

The format of the install method buffer provided by the Install (Install) command shall be the one specified in the Open Platform Card specification [14].

The applet may invoke the register(bArray, bOffset, bLength) or the register() method: the applet instance shall be registered with the instance AID present in the Install (Install) command.

If the register (bArray, bOffset, bLength) is invoked, the AID passed in the parameters shall be the instance AID provided in the install method buffer.

If the register() method is invoked the instance AID present in the Install(Install) command and the AID within the Load File, as specified in Open Platform Card specification [14], should be the same.

A.1.1.4.2.1 Toolkit Applet Specific Parameters

The toolkit applet specific parameters field is used to specify the ME and UICC resources the applet instance can use. These resources include the timers, the Bearer Independent protocol channels, menu items for the Set Up Menu and the Minimum Security Level. The Network Operator or Service Provider can also define the menu position and the menu identifier of the menus activating the applet. The following format is used to code the applet parameters:

<table>
<tr><th>Presence</th><th>Length</th><th>Name</th><th>Value</th></tr>
<tr><td>Mandatory</td><td>1</td><td>Length of Access Domain field</td><td></td></tr>
<tr><td>Mandatory</td><td>1-p</td><td>Access Domain (see A.1.1.4.2.3)</td><td></td></tr>
<tr><td>Mandatory</td><td>1</td><td>Priority level of the Toolkit applet instance (see A.1.1.4.2.4)</td><td></td></tr>
<tr><td>Mandatory</td><td>1</td><td>Maximum number of timers allowed for this applet instance</td><td></td></tr>
<tr><td>Mandatory</td><td>1</td><td>Maximum text length for a menu entry</td><td></td></tr>
<tr><td>Mandatory</td><td>1</td><td>Maximum number of menu entries allowed for this applet instance</td><td>= m</td></tr>
<tr><td>Conditional
See Note 1</td><td>/</td><td>Position of the first menu entry ('00' means last position)</td><td>~~\~~</td></tr>
<tr><td>Conditional
See Note 1</td><td>|</td><td>Identifier of the first menu entry ('00' means don't care)</td><td>~~|~~</td></tr>
<tr><td>Conditional
See Note 1</td><td>2*m bytes |</td><td>….</td><td>~~| = 2*m bytes~~</td></tr>
<tr><td>Conditional
See Note 1</td><td>|</td><td>Position of the last menu entry ('00' means last position)</td><td>~~|~~</td></tr>
<tr><td>Conditional
See Note 1</td><td>\</td><td>Identifier of the last menu entry ('00' means don't care)</td><td>~~/~~</td></tr>
<tr><td>Optional</td><td>1</td><td>Maximum number of channels for this applet instance</td><td></td></tr>
<tr><td>Optional</td><td>1</td><td>Length of Minimum Security Level field</td><td></td></tr>
<tr><td>Conditional
See Note 2</td><td>0-q</td><td>Minimum Security Level (MSL) (see A.1.1.4.2.5)</td><td></td></tr>
<tr><td colspan="4">The Presence column specifies whether it is mandatory or optional or conditional to include the corresponding parameter in the command data. If an optional parameter is included, then all the previous parameters in the above table shall be included also.
Note 1: The Position and the Identifier of a menu entry are mandatory if m is greater than 0.
Note 2: The MSL shall be included in the Toolkit Applet Specific Parameters if the length of MSL field is greater than 0.</td></tr>
</table>

If the Maximum number of channels field is included in the command data then the Length of Minimum Security Level field shall also be included.

If the maximum number of timers required is greater than '08' (maximum numbers of timers specified in TS 31.111 [6]), the card shall return the Status Word '6A80', incorrect parameters in data field, to the Install(Install) command.

If the maximum number of channels required is greater than '07' (maximum numbers of channels specified in TS 31.111 [6]), the card shall return the Status Word '6A80', incorrect parameters in data field, to the Install(Install) command.

The position of the new menu entries is an absolute position among the existing ones.

A part of the item identifier shall be under the control of the card system and the other part under the control of the card issuer. Item identifiers are split in two ranges:

- [1,127] under control of the card issuer;
- [128,255] under the control of the toolkit framework.

If the requested item identifier is already allocated, or in the range [128,255], then the card shall reject the install command. If the requested item identifier is '00', the card shall take the first free value in the range [128,255].

A.1.1.4.2.2 Memory space

The memory space required indicates the minimum size that shall be available on the card to download the application. The UICC shall reject the applet downloading if the required size is not available on the card.

A.1.1.4.2.3 Access domain

The access domain is used to specify the UICC files that may be accessed by the applet and the operations allowed on these files. The Access Domain field is formatted as follows:

Length	Name
1	Access Domain Parameter (ADP) (see A.1.1.4.2.3.1)
p-1	Access Domain Data (ADD)

The Access Domain Data coding and length is defined for each Access Domain Parameter.

A.1.1.4.2.3.1 Access Domain Parameter

This parameter indicates the mechanism used to control the applet instance access to the GSM file System.

Value	Name	Support	ADD length
'00'	Full access to the File System	Mandatory	0
'01'	APDU access mechanism (see A.1.1.4.2.3.2)	Optional	2
'02'	3GPP access mechanism (see A.1.1.4.2.3.3)	Optional	[To be defined]
'03' to '7F'	RFU	RFU	RFU
'80' to 'FE'	Proprietary mechanism	-	-
'FF'	No access to the File System	Mandatory	0

The access rights granted to an applet and defined in the access domain parameter shall be independent from the access rights granted at the (U)SIM/ME interface.

NOTE: This implies in particular that the status of a secret code (e.g. disabled CHV1, blocked CHV2, etc.) at the (U)SIM/ME interface does not affect the access rights granted to an application.

If an applet with Access Domain Parameter 'FF' (i.e. No Access to the File System) tries to access a file the framework shall throw an exception.

If an applet has Access Domain Parameter ‘00’ (i.e. Full Access to the File System), all actions can be performed on a file except the ones with NEVER access condition.

If the Access Domain Parameter requested is not supported, the card shall return the Status Word '6A80', incorrect parameters in data field, to the Install(Install) command.

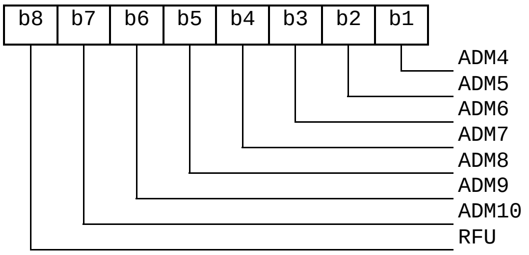
A.1.1.4.2.3.2 APDU access mechanism

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.

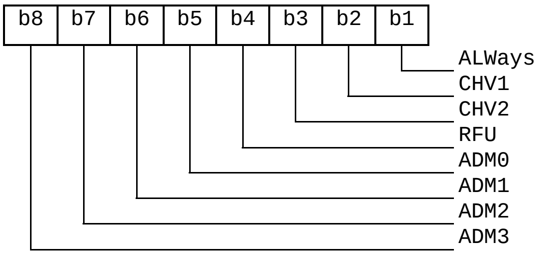
The APDU Access Domain Data is a bit map combination of the file access condition levels described in 3GPP TS 51.011. When the bit is set the associated Access Condition is granted.

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
:	:

A.1.1.4.2.3 3GPP Access Mechanism

TBD

A.1.1.4.2.4 Priority level of the Toolkit applet

The priority specifies the order of activation of an applet compared to the other applet registered to, the same event. If two or more applets are registered to the same event and have the same priority level, the applets are activated according to their installation date (i.e. the most recent applet is activated first). The following values are defined for priority:

- '00' : RFU

- '01' : Highest priority level
- ...
- 'FF' : Lowest priority level

A.1.1.4.2.5 Coding of the Minimum Security Level

The Minimum Security Level (MSL) is used to specify the minimum level of security to be applied to Secured Packets sent to the application. The Receiving Entity shall check the Minimum Security Level before processing the security of the Command Packet. If the check fails, the Receiving Entity shall reject the messages and a Response Packet with the 'Insufficient Security Level' Response Status Code (see Table 5) shall be sent if required.

If the length of the Minimum Security Level field is zero, no minimum security level check shall be performed by the receiving entity.

If the length of the Minimum Security Level field is greater than zero, the Minimum Security Level field shall be coded according to the following table:

Length	Name
1	MSL Parameter (see A.1.1.4.2.5.1)
q-1	MSL Data

The MSL Data coding and length is defined for each MSL Parameter.

A.1.1.4.2.5.1 MSL Parameter

The possible values for the MSL Parameter are:

Value	Name	Support	MSL Data length
'00'	RFU	RFU	N/A
'01'	Minimum SPI1 (see A.1.1.4.2.5.2)	Optional	1
'02' to '7F'	RFU	RFU	N/A
'80' to 'FE'	Reserved for Proprietary Mechanisms	Optional	N/A
'FF'	RFU	RFU	N/A

A.1.1.4.2.5.2 Minimum SPI1

The Minimum Security Level Data for the Minimum SPI1 MSL parameter shall use the same coding as the first octet of the SPI of a command packet (see clause 5.1.1).

The first octet of the SPI field in the incoming message Command Packet (SPI1) shall be checked against the Minimum Security Level Data (MSLD) byte by the receiving entity according to the following rules:

- if SPI1.b2b1 is equal to or greater than MSLD.b2b1 and
- if SPI1.b3 is equal to or greater than MSLD.b3 and
- if SPI1.b5b4 is equal to or greater than MSLD.b5b4

then the Message Security Level is sufficient and the check is successful, otherwise the check is failed.

3GPP TSG-T3 Meeting #25
Maastricht, Netherlands, 5 – 8 November 2002

Tdoc ⌘T3-020895
revised T3-020860

CR-Form-v3

CHANGE REQUEST

⌘ **31.115 CR 002** ⌘ rev **-** ⌘ Current version: **6.0.0** ⌘

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

Proposed change affects: ⌘ (U)SIM ☒ ME/UE □ Radio Access Network □ Core Network □

Title:	⌘	Clarification on the RC/CC/DS coding in SPI2			
Source:	⌘	TSG-T3			
Work item code:	⌘	TEI	***Date:***	⌘	06/11/2002
Category:	⌘	**A**	***Release:***	⌘	*REL-6*

Use one of the following categories:
F *(essential 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)*

Reason for change:	⌘	A misunderstanding with the word “security” could lead to say that if b4b3 is set to 00, ciphering cannot be applied in the response packet. Corresponds to a correction on earlier release of the same specification, the Rel-5 specification reference is TS 23.048
Summary of change:	⌘	In SPI second byte, b4b3 description, replace “No security” by “No RC, CC or DS”
Consequences if not approved:	⌘	Some interpretations can forbid having an encrypted response packet without RC/CC/DS field.

Clauses affected:	⌘		
Other specs Affected:	⌘	□ Other core specifications □ Test specifications □ O&M Specifications	⌘
Other comments:	⌘		

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at: http://www.3gpp.org/3G_Specs/CRs.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://www.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2000-09 contains the specifications resulting from the September 2000 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

4.2 A Command Packet contained in a Single Short Message Point to Point

The relationship between the Command Packet and its inclusion in the UDH structure of a single Short Message with no other UDH elements is indicated in table 1.

Table 1: Relationship of Command Packet in UDH for single Short Message Point to Point

SMS specific elements	Generalised Command Packet Elements	Comments
UDL		Indicates the length of the entire SM.
UDHL	='02'	The first octet of the content or User Data part of the Short Message itself. Length of the total User Data Header, in this case, includes the length of IEIa + IEIDLa + IEDa (see figure 1), and is '02' in this case.
IEIa	CPI= '70'	Identifies this element of the UDH as the Command Packet Identifier. This value is reserved in 3GPP TS 23.040 [3].
IEIDLa	='00'	Length of this object, in this case the length of IEDa, which is zero, indicating that IEDa is a null field..
IEDa		Null field.
SM (8 bit data)	Length of Command Packet (2 octets)(note)	Length of the Command Packet (CPL), coded over 2 octets, and shall not be coded according to ISO/IEC 7816-6 [5].
	Command Header Identifier	(CHI) Null field.
	Length of the Command Header	Length of the Command Header (CHL), coded over one octet, and shall not be coded according to ISO/IEC 7816-6 [5].
	SPI to RC/CC/DS in the Command Header	The remainder of the Command Header.
	Secured Data	Application Message, including possible padding octets.

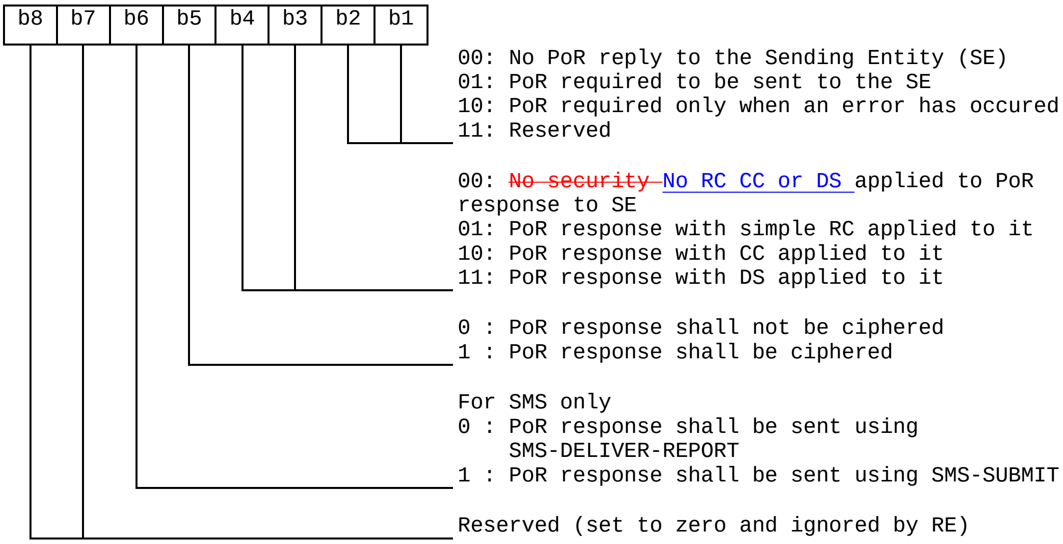
NOTE: Whilst not absolutely necessary in this particular instance, this field is necessary for the case where concatenated Short Message is employed (see subclause 4.3).

IEIa identifies the Command Packet and indicates that the first portion of the SM contains the Command Packet Length, the Command Header length followed by the remainder of the Command Header: the Secured Data follows on immediately as the remainder of the SM element. The UDHL field indicates the length of the IEIa and IEIDLa octets only ('02' in this case).

It is recognised that most checksum algorithms require input data in modulo 8 length. In order to achieve a modulo 8 length of the data before the RC/CC/DS field in the Command Header the Length of the Command Packet and the Length of the Command Header shall be included in the calculation of RC/CC/DS if used. These fields shall not be ciphered.

The SPI shall be coded as specified in TS 102 225 [9]. The b6 of the second octet is used for SMS only and shall be coded as followed:

Second Octet:



```
00: No PoR reply to the Sending Entity (SE)
01: PoR required to be sent to the SE
10: PoR required only when an error has occured
11: Reserved
```

00: ~~No security~~ No RC CC or DS applied to PoR response to SE
01: PoR response with simple RC applied to it
10: PoR response with CC applied to it
11: PoR response with DS applied to it

0 : PoR response shall not be ciphered
1 : PoR response shall be ciphered

For SMS only
0 : PoR response shall be sent using SMS-DELIVER-REPORT
1 : PoR response shall be sent using SMS-SUBMIT

Reserved (set to zero and ignored by RE)

3GPP TSG-T3 Meeting #25
Maastricht, Netherlands, 5 – 8 November 2002

Tdoc ⌘ T3-020893

CR-Form-v7

CHANGE REQUEST

⌘	**31.116**	**CR**	**002**	⌘**rev**	**-**	⌘	Current version:	**6.1.0** ⌘

*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⌘	X	ME		Radio Access Network		Core Network	

Title: ⌘	Alignment with TS 23.048 Release 5: Correction of the Specific behaviour for Response Packets (Using SMS-PP)			
Source: ⌘	TSG T3			
Work item code:⌘	TEI		***Date:*** ⌘	05/11/2002
Category: ⌘	**F**		***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: ⌘	A previous CR (CR001) to TS 31.116 Rel-6 introducing the "USIM Specific behaviour for Response Packets (Using SMS-PP)" to align with TS 23.048 Rel-5 was not correct.
Summary of change:⌘	Remove the § 4.2.2 and merge the description of the SIM Specific behaviour for Response Packets (Using SMS-PP) with the one of the USIM.
Consequences if not approved: ⌘	TS 23.048 Rel-5 and TS 31.116 Rel-6 are not aligned.

Clauses affected: ⌘	§ 4.2.1, § 4.2.2				
	Y	N			
Other specs affected: ⌘		X	Other core specifications	⌘	
		X	Test specifications		
		X	O&M Specifications		
Other comments: ⌘					

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

4 Remote APDU Format

4.1 Remote command coding

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

4.2 Response coding

The SIM/USIM Response coding shall comply with the Response coding of TS 102 226 [5], added features are defined below.

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

If PoR is not requested, no data shall be returned by the (U)SIM's RE/RA and the (U)SIM's RE/RA shall indicate to the terminal to issue a RP-ACK.

If PoR is requested, data shall be returned by the (U)SIM's RE/RA. The (U)SIM's RE/RA shall indicate to the terminal to issue:

a RP-ACK if the response status code octet is '00' or,

a RP-ERROR if there is a security error of some kind (see table 5).

The data returned by the (U)SIM is the complete Response Packet to be included in the User Data part of the SMS-DELIVER-REPORT.

NOTE: if no PoR is requested, it is however permissible for the (U)SIM to send back data.

Because the (U)SIM is unable to indicate to the Terminal that the TP-UDHI bit is to be set, the Sending Entity receiving the Response Packet shall expect the UDH structure in any event.

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 TS 102 226 [5].

~~4.2.2 USIM specific behaviour for Response Packets (Using SMS-PP)~~

4.2.2 Void