3GPP TSG-T (Terminals) Meeting #17
Biarritz, France 4 – 6 September 2002

Tdoc TP-020209

Source: T3

Title: Change Requests to TS 23.048, TS 31.115 and 31.116

Document for: Approval

This document contains several change requests as follows:

T3 Doc	Spec	CR	Rv	Rel	Cat	Subject
T3-020676	23.048	023	-	Rel-5	F	USIM specific behaviour for Response Packets (Using SMS_PP)
T3-020678	31.116	001	-	Rel-6	F	USIM specific behaviour for Response Packets (Using SMS_PP)
T3-020672	23.048	021	-	Rel-5	A	Clarification on computation of DES in CBC mode
T3-020673	23.048	022	-	Rel-5	F	Clarification on Put Key command
T3-020638	23.048	025	-	Rel-5	F	Clarification on letter “n” describing the length of parameters of the Install(Install) command
T3-020675	23.048	024	-	Rel-5	F	Toolkit Access with modified secret code status
T3-020674	23.048	026	-	Rel-5	F	Minimum Security Level for the Remote Management Applications and Access conditions for Remote File Management Application.
T3-020661	23.048	020	-	Rel-5	F	Maximum number of channels allowed for this applet instance
T3-020671	31.115	001		Rel-6	D	Editorial corrections to remove some duplicate specification work

TSG-T3 Meeting #24
Seattle, United States, 19 –22 August 2002

Tdoc ⌘ T3-020661
Updated T3-020565

CR-Form-v7

CHANGE REQUEST

⌘ **23.048** **CR** **020** ⌘ **rev** **-** ⌘ Current version: **5.3.0** ⌘

*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:	⌘	Maximum number of channels allowed for this applet instance
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	20/08/2002
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:	⌘	Clarify the behaviour of the card when more than the maximum number of channels allowed by the card is allocated to an applet.
Summary of change:	⌘	If the maximum number of channels indicated in the Toolkit Applet Specific Parameters is greater than '07' (maximum number of channels specified in 3GPP TS 31.111), the card shall return the Status Word '6A80', incorrect parameters in data field, to the Install(Install) command.
Consequences if not approved:	⌘	No clear way to process an invalid maximum number of channels. Can lead to different behaviours.

Clauses affected:	⌘	§ A.1.4.2.1

Other specs affected:	⌘	Y	N		⌘	
		X		Other core specifications		TS 102 226
				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/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.

A.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 defines the menu position and the menu identifier of the menus activating the applet. The following format is used to code the applet parameters:

Length	Name	Value
1	Length of Access Domain field	
1-n	Access Domain (see A.1.4.2.3)	
1	Priority level of the Toolkit applet instance (see A.1.4.2.4)	
1	Maximum number of timers allowed for this applet instance	
1	Maximum text length for a menu entry	
1	Maximum number of menu entries allowed for this applet instance	= m
1	Position of the first menu entry ('00' means last position)	\
1	Identifier of the first menu entry ('00' means don't care)	|
	….	| = 2*m bytes
1	Position of the last menu entry ('00' means last position)	|
1	Identifier of the last menu entry ('00' means don't care)	/
1	Maximum number of channels for this applet instance	
1	Length of Minimum Security Level field	
0-n	Minimum Security Level (MSL) (see A.1.4.2.5)	

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].

3GPP TSG-T3 #24
Seattle, United States, 19 –22 August 2002

Tdoc T3-020672
Updated T3-020537

CR-Form-v4

CHANGE REQUEST

⌘ **23.048** **CR** **021** ⌘ ev **-** ⌘ Current version: **5.3.0** ⌘

*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 [X] ME/UE [ ] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Clarification on computation of DES in CBC mode
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	21/08/2002
Category:	⌘	**A**
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)

Reason for change:	⌘	Reintroduction of CR T3-010784, approved for v5.2.0 and inadvertently withdrawn from v5.3.0.
Summary of change:	⌘	Deletion of the sentence “For the CBC modes the counter (CNTR) shall be used” for the computation of DES in CBC mode.
Consequences if not approved:	⌘	Risk of different interpretations leading to interoperability problems

Clauses affected:	⌘	§ 5.1.2
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:

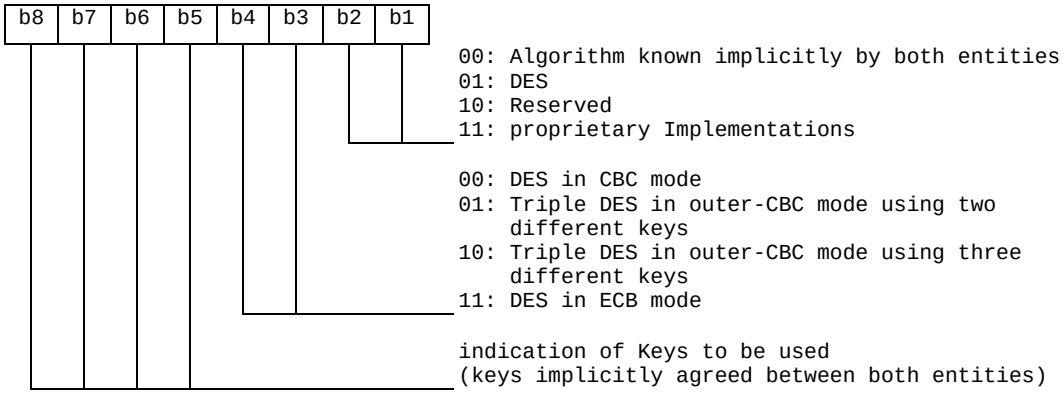
1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

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://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.

5.1.2 Coding of the KIc

The KIc is coded as below.



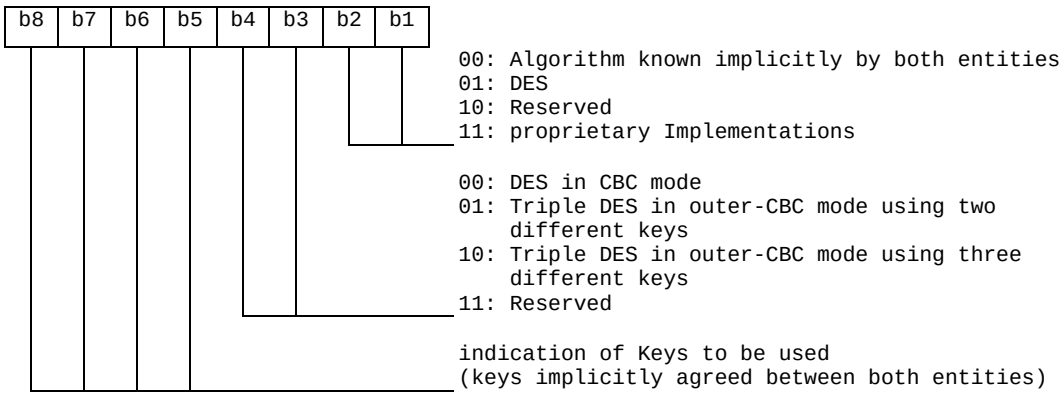
DES is the algorithm specified as DEA in ISO 8731-1 [9]. DES in CBC mode is described in ISO/IEC 10116 [10]. Triple DES in outer-CBC mode is described in section 15.2 of [17]. DES in ECB mode is described in ISO/IEC 10116 [10].

The initial chaining value for CBC modes shall be zero. ~~For the CBC modes the counter (CNTR) shall be used.~~

For Open Platform security architecture compliant cards see Annex B.

5.1.3 Coding of the KID

The KID is coded as below.



DES is the algorithm specified as DEA in ISO 8731-1 [9]. DES in CBC mode is described in ISO/IEC 10116 [10]. Triple DES in outer-CBC mode is described in section 15.2 of [17].

The initial chaining value for CBC modes shall be zero. If padding is required, the padding octets shall be coded hexadecimal '00'. These octets shall not be included in the secured data.

For Open Platform security architecture compliant cards see Annex B.

3GPP TSG-T3 #24
Seattle, United States, 19 –22 August 2002

Tdoc T3-020673
Updated T3-020538

CR-Form-v4

CHANGE REQUEST

⌘ **23.048** **CR** **022** ⌘ ev **-** ⌘ Current version: **5.3.0** ⌘

*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 [X] ME/UE [ ] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Clarification on Put Key command
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	20/08/02
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)*

Reason for change:	⌘	The description of the Put Key command may lead to different interpretations
Summary of change:	⌘	- Clarify the use of the KIK key - Clarify the description of the Put Key command
Consequences if not approved:	⌘	Possible misunderstandings

Clauses affected:	⌘	§ A 1.7		
Other specs affected:	⌘	[X] Other core specifications [ ] Test specifications [ ] O&M Specifications	⌘	TS 102 226
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://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.

A.1.7 PUT KEY

The Put Key command shall be coded according to the Open Platform specification [14]. The references to DAP (Data Authentication Pattern) fields are not applicable for Over The Air Application Management.
The keys which may be updated by the PUT KEY command refer to the transport security keys, i.e. KID and KIc in a Secured Packet. In addition, a third key type is defined: KIK. This key is used to ~~protect~~ encrypt the key data value of the PUT KEY command ~~itself~~.
One or several keys within an existing key set version may be replaced using the Put Key command.

Keys within a key set are structured in the following way:

	Key Set Version 0	**Key Set Version 1**	**….**	**Key Set Version n (maximum 'F')**
Key Index 1	Reserved	KIc 1		KIc n
Key Index 2	Reserved	KID 1		KID n
Key Index 3	Reserved	KIK 1		KIK n

A card may have up to 15 key set versions each containing 3 key indexes. These versions numbers represent the indication of keys to be used in bits 8 to 5 in the coding of KIc and KID (see clauses 5.1.2 and 5.1.3). Each key index represents:

- Key Index 1: KIc;
- Key Index 2: KID;
- Key Index 3: KIK.

Key Sets can only be changed with the PUT KEY command once the card has been issued. New Key Sets cannot be created using PUT KEY command at post issuance. Key used for securing the PUT KEY command is the key index 3 of the same key set version as the changed key. Key Set version 0 defined in OP for the creation of keys is not relevant for the present document.
A key set version number shall never be updated using the PUT KEY command.
This command shall be executed by the Card Manager or a Security Domain depending on the TAR in the case of Over The Air Application Management.

3GPP TSG-T3 #24
Seattle, United States, 19 –22 August 2002

Tdoc T3-020676
Tdoc T3-020541

CR-Form-v3

CHANGE REQUEST

⌘ **23.048** **CR** **023** ⌘ rev **-** ⌘ Current version: **5.3.0** ⌘

*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 [X] ME/UE [ ] Radio Access Network [ ] Core Network [ ]

Title:	⌘	USIM specific behaviour for Response Packets (Using SMS-PP)
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	21/08/02
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:	⌘	Need for definition of USIM specific items and suppression of copy/paste from other specifications.
Summary of change:	⌘	Definition of USIM specific behaviour for response packets. Inconsistency with other specification may exist in the future.
Consequences if not approved:	⌘	Standard is incomplete.

Clauses affected:	⌘	8.3, 8.4, 9.3.1, 9.3.2		
Other specs Affected:	⌘	[X] Other core specifications [ ] Test specifications [ ] O&M Specifications	⌘	TS 31.116
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.

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

~~Table 14 summarises the behaviour of the SIM's RE/RA with regard to PoR~~

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.

~~Table 14: 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 File Management Application shall be formatted according to table ~~15~~14:

Table ~~15~~14: Format of additional response data

Length	Name
1	Number of commands executed within the command script (see note)
2	Last executed command status word
X	Last executed command response data if available (i.e., if the last command was an outgoing command)
NOTE:	This field shall be set to '01' if one command was executed within the command script, '02' if two commands were executed, etc…

~~8.4 USIM specific behaviour for Response Packets (Using SMS-PP)~~

~~To be defined.~~

9.3 Response Packets

9.3.1 (U)SIM Response Packets

The behaviour of the (U)SIM's RE/RA with regard to PoR is the same as the one defined for Remote File Management (see clause 8.3).

~~9.3.2 USIM Response Packets~~

~~To be defined~~

3GPP TSG-T3 #24
Seattle, United States, 19 –22 August 2002

Tdoc T3-020675
(revised from T3-020540)

CR-Form-v4

CHANGE REQUEST

⌘ **23.048** **CR** **024** ⌘ ev **-** ⌘ Current version: **5.3.0** ⌘

*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 [X] ME/UE [ ] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Toolkit Access with modified secret code status
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	21/08/02
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)

Reason for change:	⌘	The access rights granted to an application when the status of a secret code is modified (e.g. disabled or blocked) need to be clarified.
Summary of change:	⌘	Addition of a note clarifying that the access rights granted to an application are independent from the secret code status.
Consequences if not approved:	⌘	The access rights of an application could change in a way not predictable for the application.

Clauses affected:	⌘	Annex A.1.4.2.3.1
Other specs affected:	⌘	[X] Other core specifications ⌘ TS 31.116 [ ] 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://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.

A.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.1.4.2.3.2)	Optional	2
'02'	3GPP access mechanism (see A.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 doesn't 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.

3GPP TSG-T3 #24
Seattle, United States, 19 –22 August 2002

Tdoc T3-020638

CR-Form-v7

CHANGE REQUEST

⌘ **23.048** **CR** **025** ⌘ **rev** **-** ⌘ Current version: **5.3.0** ⌘

*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:	⌘	Clarification on letter “n” describing the length of parameters of the Install(Install) command
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	21/08/2002
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 letter "n" is mentioned several times in the tables describing the length of the different parameters of the Install(Install) command. There is no direct relation between the length of the different parameters in the same table of length "n". The letter "n" is seen as a generic integer there.
Summary of change:	⌘	Replace letter “n” in the install(Install) command description by letter “p” to describe the length of the Access Domain and letter “q” to describe the length of the Minimum Security Level.
Consequences if not approved:	⌘	This could lead to a misinterpretation of the specification.

Clauses affected:	⌘	§ A.1.4.2, § A.1.4.2.1, § A.1.4.2.5,

Other specs affected:	Y	N			
⌘	X		Other core specifications	⌘	TS 102 226
			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/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.

A.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
	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)
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.1.4.2.1)

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.1.4.2.1 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 defines the menu position and the menu identifier of the menus activating the applet. The following format is used to code the applet parameters:

Length	Name	Value
1	Length of Access Domain field	
1-p~~n~~	Access Domain (see A.1.4.2.3)	
1	Priority level of the Toolkit applet instance (see A.1.4.2.4)	
1	Maximum number of timers allowed for this applet instance	
1	Maximum text length for a menu entry	
1	Maximum number of menu entries allowed for this applet instance	= m
1	Position of the first menu entry ('00' means last position)	\
1	Identifier of the first menu entry ('00' means don't care)	|
	….	| = 2*m bytes
1	Position of the last menu entry ('00' means last position)	|
1	Identifier of the last menu entry ('00' means don't care)	/
1	Maximum number of channels for this applet instance	
1	Length of Minimum Security Level field	
0-g~~n~~	Minimum Security Level (MSL) (see A.1.4.2.5)	

A.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.1.4.2.3.1)
p~~n~~-1	Access Domain Data (ADD)

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

A.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.1.4.2.5.1)
g~~n~~-1	MSL Data

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

3GPP TSG-T3 #24
Seattle, United States, 19 –22 August 2002

Tdoc T3-020674

CR-Form-v4

CHANGE REQUEST

⌘ **23.048** **CR** **026** ⌘ ev **-** ⌘ Current version: **5.3.0** ⌘

*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 [X] ME/UE [ ] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Minimum Security Level for the Remote Management Applications and Access conditions for Remote File Management Application.
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	22/08/02
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)*

Reason for change:	⌘	For 43.019 compliant cards, use the Minimum Security Level mechanism for the Remote Management Applications. The files that may be accessed by the Remote File Management Application and the operation allowed on these files are not standardised.
Summary of change:	⌘	For 43.019 compliant cards, the minimum security level to be checked by the Remote Management Applications is defined by a Minimum Security Level (as defined in A.1.4.2.5). For 43.019 compliant cards, the access conditions for the Remote File Management Application is defined with an Access Domain as defined in A.1.4.2.3.
Consequences if not approved:	⌘	Inconsistency between Remote Management Applications and other applications.

Clauses affected:	⌘	Annex A		
Other specs affected:	⌘	[X] Other core specifications [ ] Test specifications [ ] O&M Specifications	⌘	ETSI TS 102 226, TS 31.116
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://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.

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

A.~~2~~21 Applet Management Commands for TS 43.019 compliant cards

This ~~annex~~ chapter describes the commands for Applet Management.

A complying card shall support at least the DES CBC algorithm for cryptographic computations.

Command status words placed in the Additional Response Data element of the Response Packet shall be coded according to the Open Platform specification [14].

~~A.1~~A.~~2~~21.1 Commands Description

The minimum security applied to a Secured Packet containing Applet Management Commands shall be integrity using CC or DS, and in all cases, this security shall replace Data Authentication Patterns used in Open Platform commands for secure messaging.

~~A.1.1~~A.~~2~~21.1.1 DELETE

The Delete command shall be coded according to the Open Platform specification [14]. The references to DAP (Data Authentication Pattern) fields are not applicable for Over The Air Application Management.

NOTE: This command may be extended in the future to allow for other type of deletion since the command data uses TLV structure.

[…]

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)
n-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.1.4.2.3.2)	Optional	2
'02'	3GPP access mechanism (see A.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.

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.

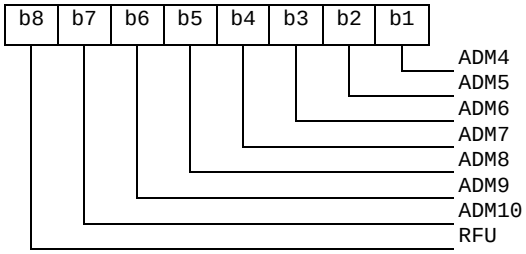
A. 1.1.4.2.3.2 APDU access mechanism

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.

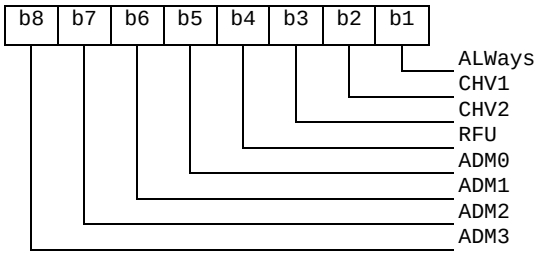
The APDU Access Domain Data is a bit map combination of the file access condition levels described in 3GPP TS 51.011. When the bit is set the associated Access Condition is granted.

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.1.1.4.2.5 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)
n-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.

[…]

A.2 Security of messages sent to the Remote Management Applications

A.2.1 Minimum Security Level

In order to control the access to the Remote Management Applications (Remote File Management and Remote Applet Management applications), a Minimum Security Level as defined in Annex A.1.1.4.2.5 shall be assigned to each one of these applications. This Minimum Security Level shall be checked for all Secured Packet sent to one of these applications.

The Receiving Entity shall manage this Minimum Security Level as described in Annex A.1.1.4.2.5.

A.2.2 Remote File Management Access Conditions

In order to control the access conditions of the Remote File Management Applications, an Access Domain as defined in A.1.1.4.2.3 shall be assigned to each Remote File Management Application.

CR-Form-v7

CHANGE REQUEST

⌘ TS 31.115 CR 001 ⌘ 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: UICC apps⌘ [X] ME [ ] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Editorial corrections to remove some duplicate specification work
Source:	⌘	T3
Work item code:	⌘	***Date:*** ⌘ 21/08/2002
Category:	⌘	D

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:	⌘	Removing the extensive extracts of TS 23.040 included in the specification to only make references
Summary of change:	⌘	• Add the word data (for 8 bit data) to clearly reference the correct figure in TS 23.040 • Remove the figure (fig 1) that was already part of TS 23.040 to replace it by a reference to the specification • Format Information Element Identifiers related to this document as a list to underline that this specifies the ones reserved in TS 23.040 for this document
Consequences if not approved:	⌘	Difficulty to maintain specification as some information is duplicated in several specifications

Clauses affected:	⌘				
Other specs affected:	⌘	Y	N		⌘
		[ ]	[ ]	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/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.

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 and/or edition number or version number) 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 TR 21.905: "Vocabulary for 3GPP Specifications".

[2] ETSI TS 102 224: "Smart Cards; Security mechanisms for UICC based Applications - Functional requirements".

[3] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS)".

[4] 3GPP TS 24.011: "Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface".

[5] ISO/IEC 7816-6 (1996): "Identification cards - Integrated circuit(s) cards with contacts - Part 6: Interindustry data elements".

[6] 3GPP TS 23.041: "Technical realization of Cell Broadcast Service (CBS)".

[7] 3GPP TS 24.012: "Short Message Service Cell Broadcast (SMSCB) support on the mobile radio interface".

[8] 3GPP TS 23.038: "Alphabets and language-specific information".

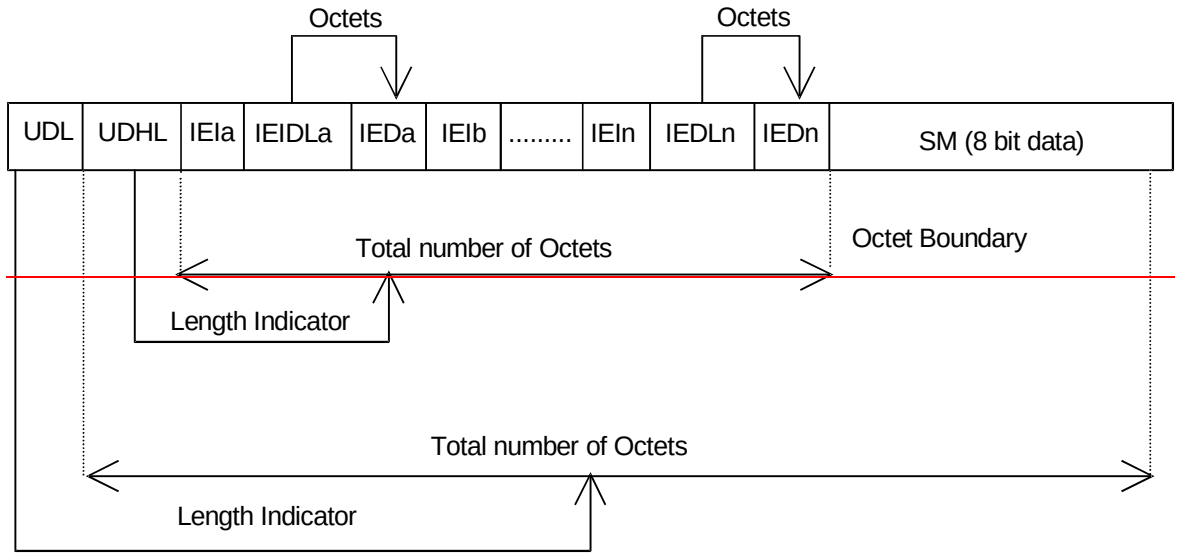
[9] ETSI TS 102 225: "Smart Cards; Secured packet structure for UICC based applications".

4 Implementation for SMS-PP

4.1 Structure of the UDH of the Security Header in a Short Message Point to Point

The coding of the SMS-DELIVER, SMS-SUBMIT, SMS-DELIVER-REPORT or SMS-SUBMIT-REPORT header shall indicate that the data is binary (8 bit data), and not 7 bit or 16 bit. In order to invoke the UDH functionality of relevant SMS element, the UDHI bit shall be set as defined in 3GPP TS 23.040 [3].].

However, in the case of a Response Packet originating from the UICC, due to the inability of the UICC to indicate to a ME that the UDHI bit should be set, the Response Packet SMS will not have the UDHI bit set, and the Sending Entity shall treat the Response Packet as if the UDHI bit was set.



~~Figure 1: Structure of User Data Header in the Short Message Point to Point~~

The generalised structure of the UDH in the Short Message element ~~is shown in figure 2, which~~ is contained in the User Data part of the Short Message element and is described in 3GPP TS 23.040 [3]. The Command Packet and the Response Packet are partially mapped into this UDH structure.

Information Element Identifiers (IEI's) values range '70 - 7F' are reserved in 3GPP TS 23.040 [3] for use in the present document~~.~~ and allocated as follows:

~~Values '70' and '71' are used in the present document,~~

- '70' and '71' are specified in this document,
- values '72 - 7D' are reserved for future use, ~~and~~
- '7E' and '7F' are for proprietary implementations.

Where a Response Packet is too large to be contained in a single SMS-DELIVER-REPORT or SMS-SUBMIT-REPORT TP element, a Response Packet containing the Status Code "more time" should be returned to the SE using the SMS-REPORT element, followed by a complete Response Packet, contained in a SMS-DELIVER or SMS-SUBMIT element, which may be concatenated.

3GPP TSG-T3 #24
Seattle, United States, 19 –22 August 2002

Tdoc T3-020678

CR-Form-v3

CHANGE REQUEST

⌘ **31.116** **CR** **001** ⌘ 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 [X] ME/UE [ ] Radio Access Network [ ] Core Network [ ]

Title:	⌘	USIM specific behaviour for Response Packets (Using SMS-PP)
Source:	⌘	T3
Work item code:	⌘	TEI
Date:	⌘	21/08/02
Category:	⌘	**F**
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:	⌘	Need for definition of USIM specific items and suppression of copy/paste from other specifications.
Summary of change:	⌘	Definition of USIM specific behaviour for response packets. Inconsistency with other specification may exist in the future.
Consequences if not approved:	⌘	Standard is incomplete.

Clauses affected:	⌘	§ 4.2.1, § 4.2.2		
Other specs Affected:	⌘	[X] Other core specifications [ ] Test specifications [ ] O&M Specifications	⌘	TS 23.048
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.

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

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

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.

~~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 TS 102 226 [5].

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

~~[TBD]~~