3GPP TSG-T (Terminals) Meeting #14 Kyoto, Japan, 12 - 14 December 2001

Source:T3Title:Change Requests on secure messaging (TS 03.48 / 23.048)Document for:Approval

This document contains change requests to TS 03.48 and TS 23.048 as agreed by T3.

T3 Doc	Spec	CR	Rel	Cat	Subject
T3-010780	03.48	A021	R99	F	Clarification of the APDU Access Domain
T3-010787	03.48	A022	R99	F	Correction of Response Header Length (RHL) definition
T3-010776	23.048	007	Rel-5	В	Definition of a Minimum Security Level
T3-010777	23.048	800	Rel-5	С	Maximum number of timer allowed for applet instance
T3-010781	23.048	011	Rel-4	F	Clarification of the APDU Access Domain
T3-010782	23.048	012	Rel-5	А	Clarification of the APDU Access Domain
T3-010783	23.048	013	Rel-4	F	Clarification on computation of DES in CBC mode
T3-010784	23.048	014	Rel-5	А	Clarification on computation of DES in CBC mode
T3-010788	23.048	015	Rel-4	F	Correction of Response Header Length (RHL) definition
T3-010789	23.048	016	Rel-5	A	Correction of Response Header Length (RHL) definition

Revised T3-010729

				CHA	NGE	ERE	EQ	UES	Т				CR-Form-v3
ж	0	<mark>3.48</mark>	CR	A021		ж r	ev	Ħ	Cu	rrent vers	sion:	8.7.0	ж
For <u>HELP</u> on t	using	this fo	rm, se	e botton	n of thi	s page	e or l	look at t	he po	p-up text	over i	the ¥ sy	mbols.
Proposed change	affec	ts: X	(U)	SIMX	ME	/UE		Radio	Acces	s Networ	k	Core N	letwork
Title: ೫	Cla	rificati	on of tl	ne APDI	J Acce	ess Do	omaii	า.					
Source: ೫	T3												
Work item code: ೫										<i>Date:</i> ສ	07/	<mark>11/2001</mark>	
Category: ж	F								Re	elease: ೫	R9	9	
	Use one of the following categories:Use one of the following releases:F (essential correction)2A (corresponds to a correction in an earlier release)R96B (Addition of feature),R97C (Functional modification of feature)R98D (Editorial modification)R99D (Editorial modifications of the above categories canREL-4be found in 3GPP TR 21.900.REL-5C (Release 5)							9leases: 2) 3) 7) 3) 9)					
Reason for change	e: ¥	The on MSB	descrip notatio	tion of t ons is co	he byte onfusin	es of t g : by	he a te 1	<mark>ccess d</mark> may be	omair repla	paramet ced with b	ers w byte 2	ith the L and vice	SB and e-versa.
Summary of chang	уе: Ж	Remo numb	oval of bers, al	MSB ar ligneme	nd LSB nt of th	notat e exe	tions mple	, reorde e.	ering c	f the byte	s acc	ording to	the bytes
Consequences if not approved:	Ħ	Risk card.	of inter	operabi	lity iss	ues or	n acc	cess doi	main p	paramete	rs unc	lerstand	ing by the
Clauses affected:	ж	A.1.4.	2.3.2										
Other specs Affected:	¥	X 0 X Te 0	ther co est spe &M Sp	re speci cification ecification	ificatio ns ons	ns	ж	23.048 11.13	3 (Rel·	-4 and Re	el-5)		
Other comments:	ж												

How to create CRs using this form:

- 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 <u>ftp://www.3gpp.org/specs/</u> 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.

A.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 TS 11.11. When the bit is set the associated Access Condition is granted.

The APDU Access Domain Data is coded as follows:



EXAMPLE:

<u>xamples of pPossible combinations of fulfilled</u> Access <u>conditions</u> <u>Conditions are shown below</u>:

ADD value	Applet access condition fulfilled
0x0000<u>'00 00'</u>	No access
0x0001<u>'00 01'</u>	ALWays
0x0002<u>'00 02'</u>	CHV1
0x0003<u>'00 03'</u>	ALWays and CHV1
0x0004<u>'00 04'</u>	CHV2
0x0005<u>'00 05'</u>	ALWays and CHV2
0x0006<u>'00 06'</u>	CHV1 and CHV2
<u>:</u>	
0x0010<u>'00 10'</u>	ADM-0
<u>:</u>	
0x0020<u>'00 20'</u>	ADM-1
<u> </u>	
0x0022 '00 22'	ADM-1 and CHV1
<u>:</u>	
<u>'01 00'</u>	ADM4
<u>:</u>	
<u>'40 00'</u>	<u>ADM10</u>
<u>:</u>	<u>.</u>
<u>'41 37'</u>	ADM10 and ADM4 and ADM1 and
	ADM0 and CHV2 and CHV1 and
	ALWays
<u>1</u>	1

			(CHAN	IGE	RE	Q	UE	ST				CR-Form-v3
ж	03	<mark>3.48</mark>	CR	A022		¥ r	ev		ж	Current ver	sion:	8.7.0) ^ж
For <u>HELP</u> on u	sing ti	his for	m, see	bottom	of this	s page	e or l	look a	at the	pop-up tex	t ovei	rthe	ymbols.
Proposed change a	affect	s: #	(U)	SIM X	ME	/UE		Radio	o Aco	cess Netwo	rk	Core I	Network
Title: ¥	Corre	ection	of Res	sponse H	leade	r Leng	<mark>gth (</mark> l	RHL)	defir	nition			
Source: ೫	T3												
Work item code: Ж										Date: ៖	6 <mark>07</mark>	/11/01	
Category: ж	F									Release: a	8 <mark>R</mark> 9	9	
	Use <u>c</u> l L Detai be for	one of a F (ess A (con B (Ada C (Fur D (Edi led exp und in	the follo respond dition of actional torial m blanatio 3GPP	owing cate orrection, ds to a cc f feature), modifica odificatio ons of the FR 21.900	egories) prrection tion of on) above 0.	s: n in an feature catege	o eari e) ories	lier rel s can	lease,	Use <u>one</u> o 2 () R96 R97 R98 R99 REL-4 REL-5	f the fe (GSI (Rel (Rel (Rel (Rel (Rel (Rel	ollowing r M Phase 2 ease 1990 ease 1990 ease 1990 ease 4) ease 5)	eleases: 2) 5) 7) 8) 9)
Reason for change	e: #	The	existin	<mark>a definiti</mark>	on of I	RHL is	s no	t corre	ect.				
Summary of chang	уе: Ж	Corre the C	ect the comma	faulty de and Pack	efinitio ket stru	n. The ucture	e co in c	orrection chapte	on is er 5.1	in line with I.	the ir	nplemen	tation of
Consequences if not approved:	ж	Ther defin	e is a i ition.	risk of di	fferent	imple	eme	ntatio	ns dı	ue to differe	nt inte	erpretatio	ons of RHL
Clauses affected:	ж	§ 5.2											
Other specs affected:	ж	01 Te	her co est spe &M Sp	re speci cification ecificatio	fication ns ons	ns	ж						
Other comments:	ж	This	correc	<mark>tion is n</mark> e	eeded	in all	late	<mark>r vers</mark>	ions	<mark>of 03.48 ar</mark>	d 23.	<mark>048 as w</mark>	vell.
How to create CRs	usino	ı this '	form										

- 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 <u>ftp://www.3gpp.org/specs/</u> 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.

CI

5.2 Response Packet structure

Table 3: Structure of the Response Packet

Element	l enath	Comment
Response Packet Identifier (RPI)	1 octet	Identifies a Response Packet.
Response Packet Length (RPL)	variable	Indicates the number of octets from and including RHI to the of Additional Response data, including any padding octets.
Response Header Identifier (RHI)	1 octet	Identifies the Response Header.
Response Header Length (RHL)	variable	Indicates the number of octets from and including <u>TAR</u> <u>RC/CC/DS</u> to the end of the <u>RC/CC/DS</u> Response Status Corrected.
Toolkit Application Reference (TAR)	3 octets	This shall be a copy of the contents of the TAR in the Comm Packet.
Counter (CNTR)	5 octets	This shall be a copy of the contents of the CNTR in the Com Packet.
Padding counter (PCNTR)	1 octet	This indicates the number of padding octets at the end of the Additional Response Data.
Response Status Code Octet	1 octet	Codings defined in Table 5.
Redundancy Check (RC), Cryptographic Checksum (CC) or Digital Signature (DS)	variable	Length depending on the algorithm indicated in the Commar Header in the incoming message. A typical value is 4 to 8 oc or zero if no RC/CC/DS is requested.
Additional Response Data	variable	Optional Application Specific Response Data, including poss padding octets.

Unless indicated otherwise, the RPL and RHL shall be coded according to ISO/IEC 7816-6 [8].

Table 4: Linear Representation of Response Packet

RPI	RPL	RHI	RHL	TAR	CNTR	PCNTR	Status Code	RC/CC/DS	Additi Respo Data padd
					Note 1	Note 1	Note 1	Note 1	Note 1
	Note 3		Note 3	Note 2	Note 2	Note 2	Note 2		Note 2
NOTE 1 NOTE 2 NOTE 3	NOTE 1: If ciphering is indicated in the Command Packet SPI then these fields shall be ciphered. NOTE 2: These fields shall be included in the calculation of the RC/CC/DS. NOTE 3: Part or all of these fields may also be included in the calculation of the RC/CC/DS, depending on implementation (e.g. SMS).								

If ciphering is indicated, first the RC/CC/DS shall be calculated as indicated in Note 2, and then ciphering shall be applied, as indicated in note 1.

If the SPI indicates that a specific field is unused, than its contents shall be set to zero, and ignored by the recipient of the Response Packet.

If the SPI in the Command Packet indicates that no RC, CC or DS is present in the Command Header, this field shall be of zero length.

If the Padding Counter content is zero, this shall indicate no padding octets are present, or no padding is necessary.

Tdoc T3-010776

Revised T3-010649

	CHANGE REQUEST
ж	23.048 CR 007
For <u>HELP</u> on u	sing 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: ೫	Minimum Security Level for applet triggering on 03.48 formatted messages
Source: ೫	Т3
Work item code: #	Date: 業 07/11/01
Category: Ж	BRelease: %REL-5Use one of the following categories:Use one of the following releases:F (correction)2A (corresponds to a correction in an earlier release)R96B (addition of feature),R97C (functional modification of feature)R98D (editorial modification)R99D (editorial modification)R99D tetailed explanations of the above categories canREL-4be found in 3GPP TR 21.900.REL-5
Reason for change	2: ¥ Provide a standard means for the receiving entity to check if the security level of an incoming 03.48 formatted message is sufficient before forwarding the message to the receiving application.
Summary of chang	ge: # The minimum security level to be checked by the receiving entity is defined in the receiving application installation parameters : addition of the field indicating the minimum security level in the GSM Applet specific parameters of the INSTALL command.
Consequences if not approved:	* The security level of incoming 03.48 formatted messages cannot be checked by the receiving entity, thus allowing a receiving application to receive unsecured messages without control by the receiving entity.
Clauses affected:	¥ § 5.2, § A.1.4.2.1, § A.1.4.2.5
Other specs affected:	% Other core specifications % Test specifications 0&M Specifications
Other comments:	X
How to create CRs	using this form:

- 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 <u>ftp://ftp.3gpp.org/specs/</u> 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.

5.2 Response Packet structure

Table 3:	Structure	of the Res	ponse Packet
----------	-----------	------------	--------------

Element	Length	Comment
Response Packet Identifier (RPI)	1 octet	Identifies a Response Packet.
Response Packet Length (RPL)	variable	Indicates the number of octets from and including RHI to the end
		of Additional Response data, including any padding octets
		required for ciphering.
Response Header Identifier (RHI)	1 octet	Identifies the Response Header.
Response Header Length (RHL)	variable	Indicates the number of octets from and including RC/CC/DSto
		the end of the Response Status Code octet.
Toolkit Application Reference	3 octets	This shall be a copy of the contents of the TAR in the Command
(TAR)		Packet.
Counter (CNTR)	5 octets	This shall be a copy of the contents of the CNTR in the Command
		Packet.
Padding counter (PCNTR)	1 octet	This indicates the number of padding octets used for ciphering at
		the end of the Additional Response Data.
Response Status Code Octet	1 octet	Codings defined in table 5.
Redundancy Check (RC),	variable	Length depending on the algorithm indicated in the Command
Cryptographic Checksum (CC) or		Header in the incoming message. A typical value is 4 to 8 octets,
Digital Signature (DS)		or zero if no RC/CC/DS is requested.
Additional Response Data	variable	Optional Application Specific Response Data, including possible
		padding octets.

Unless indicated otherwise, the RPL and RHL shall be coded according to ISO/IEC 7816-6 [8].

RPI	RPL	RHI	RHL	TAR	CNTR	PCNTR	Status Code	RC/CC/DS	Additional Response Data with padding
					note 1	note 1	note 1	note 1	note 1
	note 3		note 3	note 2	note 2	note 2	note 2		note 2
NOTE 1:If ciphering is indicated in the Command Packet SPI then these fields shall be ciphered.NOTE 2:These fields shall be included in the calculation of the RC/CC/DS.NOTE 3:Part or all of these fields may also be included in the calculation of the RC/CC/DS, depending on									
	impleme	ntation (e	.g. SMS).						

If ciphering is indicated, first the RC/CC/DS shall be calculated as indicated in note 2, and then ciphering shall be applied, as indicated in note 1.

If the SPI indicates that a specific field is unused, than its contents shall be set to zero, and ignored by the recipient of the Response Packet.

If the SPI in the Command Packet indicates that no RC, CC or DS is present in the Command Header, this field shall be of zero length.

If the Padding Counter content is zero, this shall indicate no padding octets are present, or no padding is necessary.

Status Code (hexadecimal)	Meaning
'00'	PoR OK.
'01'	RC/CC/DS failed.
'02'	CNTR low.
'03'	CNTR high.
'04'	CNTR Blocked
'05'	Ciphering error.
'06'	Unidentified security error. This code is for the case where the Receiving Entity cannot correctly interpret the Command Header and the Response Packet is sent unciphered with no RC/CC/DS.
'07'	Insufficient memory to process incoming message.
'08'	This status code "more time" should be used if the Receiving Entity/Application needs more time to process the Command Packet due to timing constraints. In this case a later Response Packet should be returned to the Sending Entity once processing has been completed.
'09'	TAR Unknown
<u>'0A'</u>	Insufficient security level
<u>'0A' '0B'</u> - 'FF'	Reserved for future use.

Table 5: Response Status Codes

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, and 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)	١
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	
<u>1</u>	Length of Minimum Security Level field	
<u>0-n</u>	Minimum Security Level (MSL) (see A.1.4.2.5)	

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.1.4.2.5 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	<u>Name</u>
<u>1</u>	MSL Parameter (see A.1.4.2.5.1)
<u>n-1</u>	MSL Data

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

A.1.4.2.5.1 MSL Parameter

The possible values for the MSL Parameter are:

Value	Name	<u>Support</u>	MSL Data length
<u>'00'</u>	RFU	<u>RFU</u>	N/A
<u>'01'</u>	Minimum SPI1 (see A.1.4.2.5.2)	Optional	<u>1</u>
<u>'02' to '7F'</u>	RFU	<u>RFU</u>	<u>N/A</u>
'80' to 'FE'	Reserved for Proprietary Mechanisms	Optional	<u>N/A</u>
'FF'	RFU	RFU	N/A

A.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.



Revised T3-010680

	CR-Form-v3						
ж	23.048 CR 008 [#] rev _ [#] Current version: 5.1.0 [#]						
For <u>HELP</u> on u	sing this form, see bottom of this page or look at the pop-up text over the $#$ symbols.						
Proposed change a	affects: # (U)SIM X ME/UE Radio Access Network Core Network						
Title: ೫	Maximum number of timers allowed for applet instance						
Source: ೫	Т3						
Work item code: Ж	Date:						
Category: ж	C Release: # REL-5						
	Use one of the following categories:Use one of the following releases:F (essential correction)2(GSM Phase 2)A (corresponds to a correction in an earlier release)R96(Release 1996)B (Addition of feature),R97(Release 1997)C (Functional modification of feature)R98(Release 1998)D (Editorial modification)R99(Release 1999)Detailed explanations of the above categories canREL-4(Release 4)be found in 3GPP TR 21.900.REL-5(Release 5)						
Reason for change: # The behaviour when applet required more than the maximum number of timer allowed by the card is not clear. Summary of change: # If the maximum number of timers required is greater than '08' (maximum number of timers 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:	X No standard way to process an invalid maximum number of timers						
Clauses affected:	¥ 5.2						
Other specs Affected:	% Other core specifications % Test specifications 0&M Specifications						
Other comments:	¥						

How to create CRs using this form:

- 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.

A.1.4.2.1 GSM Applet Specific Parameters

The applet parameters field is used to specify the resources the applet instance can use. These resources include the timers, and menu items for the Set Up Menu. 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)	١
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

If the maximum number of timers required is greater than '08' (maximum numbers of timers specified in 3GPP 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 SIM 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.1.4.2.2 Memory space

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

A.1.4.2.3 Access domain

The access domain is used to specify the SIM 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)
n-1	Access Domain Data (ADD)

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

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 GSM 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 GSM File System	Mandatory	0

If an applet with Access Domain Parameter 'FF' (i.e. No Access to the GSM File System) tries to access a GSM file (e.g. invoke the updateBinary(...) method) the framework shall throw the SIMViewException (AC_NOT_FULFILLED).

NOTE: The file access conditions specified in GSM 11.11 [5] are relevant for the SIM/ME interface only. The file access conditions specified in the access domain parameter are used internally by the card operating system.

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.1.4.2.3.2 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 GSM 11.11. When the bit is set the associated Access Condition is granted.

The APDU Access Domain Data is coded as follows:

Byte 1: (LSB)



Byte 2: (MSB)



Possible combinations of Access conditions:

ADD value	Applet access condition fulfilled
0x0000	No access
0x0001	ALWays
0x0002	CHV1
0x0003	ALWays and CHV1
0x0004	CHV2
0x0005	ALWays and CHV2
0x0006	CHV1 and CHV2
:	
0x0008	ADM 0
:	•
0x0010	ADM 1
:	
0x0012	ADM 1 and CHV1
:	

A.1.4.2.3.3 3GPP access mechanism

[To be defined]

A.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

				CHAI	NGE	ERE	EQ	UES	т				CR-Form-v3
æ	23.	048	CR	011		ж re	ev		ж (Current vers	sion:	4.1.0	ж
For <u>HELP</u> on u	using	this fo	rm, se	e bottom	of thi	s page	e or	look at	the	pop-up text	over	the ¥ syl	mbols.
Proposed change	affect	ts: #	(U)	SIM X	ME	/UE		Radic	o Acc	ess Networ	k	Core N	etwork
Title: %	Cla	rificatio	on of t	ne APDL	J Acce	<mark>ss Do</mark>	mai	n.					
Source: ೫	T3												
Work item code: #										Date: ೫	07/	11/2001	
Category: ж	F									Release: ೫	RE	L-4	
	Use of the formation of	one of t F (esse A (corr B (Ado C (Fun D (Edin led exp und in :	the follo ential c respon- lition of octional torial m lanatic 3GPP	owing cate orrection) ds to a co f feature), modification ns of the FR 21.90(egories prrection tion of i n) above).	r in an feature catego	e <i>erl</i> e) pries	ier relea can	ase)	Use <u>one</u> of 2 R96 R97 R98 R99 REL-4 REL-5	the fo (GSN (Rele (Rele (Rele (Rele (Rele	Mowing re A Phase 2 ease 1996 ease 1997, ease 1998 ease 1999 ease 4) ease 5)	leases:))))
Reason for change	e: #	The d MSB	lescrip notatio	<mark>tion of th</mark> ons is co	<mark>ne byte</mark> nfusin	es of t g : by	he a te 1	ccess may be	doma e rep	ain paramet laced with b	ers w byte 2	ith the LS and vice	SB and -versa.
Summary of chang	уе: Ж	Remo numb	oval of ers, a	MSB an lignemer	d LSB nt of th	notat e exe	tions mple	, reord e.	lering	g of the byte	s acc	ording to	the bytes
Consequences if not approved:	Ħ	Risk o card.	of inter	operabil	ity iss	ues or	n aco	cess do	omai	n paramete	rs und	derstandi	ng by the
Clauses affected:	ж	A.1.4.	2.3.2										
Other specs Affected:	ж	X Ot X Te Ot	her co st spe &M Sp	re specification ecification ecification	fication ns ons	าร	ж	03.98 11.13	3 R99	9 and 23.04	8 RE	L-5	
Other comments:	ж												

How to create CRs using this form:

- 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 <u>ftp://www.3gpp.org/specs/</u> 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.

A.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 TS 11.11. When the bit is set the associated Access Condition is granted.

The APDU Access Domain Data is coded as follows:



EXAMPLE:

<u>xamples of pPossible combinations of fulfilled</u> Access <u>conditions</u> <u>Conditions are shown below</u>:

ADD value	Applet access condition fulfilled
0x0000<u>'00 00'</u>	No access
0x0001<u>'00 01'</u>	ALWays
0x0002<u>'00 02'</u>	CHV1
0x0003<u>'00 03'</u>	ALWays and CHV1
0x0004<u>'00 04'</u>	CHV2
0x0005<u>'00 05'</u>	ALWays and CHV2
0x0006<u>'00 06'</u>	CHV1 and CHV2
<u>:</u>	
0x0010<u>'00 10'</u>	ADM-0
<u>:</u>	
0x0020<u>'00 20'</u>	ADM-1
<u> </u>	
0x0022 '00 22'	ADM-1 and CHV1
<u>:</u>	
<u>'01 00'</u>	ADM4
<u>:</u>	
<u>'40 00'</u>	<u>ADM10</u>
<u>:</u>	<u>.</u>
<u>'41 37'</u>	ADM10 and ADM4 and ADM1 and
	ADM0 and CHV2 and CHV1 and
	ALWays
<u>1</u>	1

			CHAN	IGE RI	EQ	UEST				CR-Form-v3
æ	23.0	<mark>48</mark> CR	012	۲ ¥ r	ev	ж	Current vers	sion:	5.1.0	ж
For <u>HELP</u> on L	using th	is form, se	e bottom	of this pag	e or l	ook at the	e pop-up text	over the	e Ж syn	nbols.
Proposed change	affects	:₩ (U)	SIM X	ME/UE		Radio Ac	ccess Networ	k	Core Ne	twork
Title: %	Clarif	ication of t	he APDU	Access Do	omair	າ.				
Source: अ	T3									
Work item code: %							<i>Date:</i> ສ	07/11	1/2001	
Category: ж	Α						Release: Ж	REL-	5	
	F A B C D Detaile be foun	contribution (essential of (correspon (Addition o (Functiona (Editorial n d explanatio d in 3GPP	correction) ds to a cor f feature), I modification ondification ons of the a TR 21.900	rection in ar ion of feature) above categ	n earli e) ories	er release) can	2 () R96 R97 R98 R99 REL-4 REL-5	(GSM F (Releas (Releas (Releas (Releas (Releas (Releas	Phase 2) Se 1996) Se 1997) Se 1998) Se 1999) Se 4) Se 5)	<i>70353.</i>
Reason for change	Reason for change: # The description of the bytes of the access domain parameters with the LSB and MSB notations is confusing : byte 1 may be replaced with byte 2 and vice-versa.									
Summary of chang	ge: ፝ F n	Removal of umbers, a	MSB and lignement	LSB nota t of the exe	tions mple	, reorderir	ng of the byte	s accor	ding to	the bytes
Consequences if not approved:	ж F c	Risk of inte ard.	roperabilit	ty issues o	n acc	ess doma	ain paramete	rs unde	rstandin	g by the
Clauses affected:	ж <mark>А</mark>	.1.4.2.3.2								
Other specs Affected:	ж <mark>х</mark>	Other co Test spe O&M Sp	ore specifi ecifications pecification	cations s ns	ж	03.98 R9 11.13	99 and 23.04	8 REL-	4	
Other comments:	ж									

How to create CRs using this form:

- 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 <u>ftp://www.3gpp.org/specs/</u> 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.

A.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 TS 11.11. When the bit is set the associated Access Condition is granted.

The APDU Access Domain Data is coded as follows:



EXAMPLE:

<u>xamples of pPossible combinations of fulfilled</u> Access <u>conditions</u> <u>Conditions are shown below</u>:

ADD value	Applet access condition fulfilled
0x0000<u>'00 00'</u>	No access
0x0001<u>'00 01'</u>	ALWays
0x0002<u>'00 02'</u>	CHV1
0x0003<u>'00 03'</u>	ALWays and CHV1
0x0004<u>'00 04'</u>	CHV2
0x0005<u>'00 05'</u>	ALWays and CHV2
0x0006<u>'00 06'</u>	CHV1 and CHV2
<u>:</u>	
0x0010<u>'00 10'</u>	ADM-0
<u>:</u>	
0x0020<u>'00 20'</u>	ADM-1
<u> </u>	
0x0022 '00 22'	ADM-1 and CHV1
<u>:</u>	
<u>'01 00'</u>	ADM4
<u>:</u>	
<u>'40 00'</u>	<u>ADM10</u>
<u>:</u>	<u>.</u>
<u>'41 37'</u>	ADM10 and ADM4 and ADM1 and
	ADM0 and CHV2 and CHV1 and
	ALWays
<u>1</u>	1

		CHANG								
^ж 2:	<mark>3.048</mark> (CR <mark>013</mark>	¥ .ev	- #	Current version	^{on:} 4.1.0	ж			
For <u>HELP</u> on using	g this form	, see bottom of th	nis page or l	ook at the	pop-up text o	over the X syn	nbols.			
Proposed change affe	ects: #	(U)SIM X M	E/UE	Radio Acc	cess Network	Core Ne	twork			
Title: ೫ C	larification	on computation	of DES in C	BC mode						
Source: ೫ T	3									
Work item code: #					<i>Date:</i>	07/11/01				
Category: # F Release: # REL-4 Use one of the following categories: Use one of the following releases: 2 (GSM Phase 2) A (corresponds to a correction in an earlier release) R96 (Release 1996) B (addition of feature), R97 (Release 1997) C (functional modification of feature) R98 (Release 1998) D (editorial modification) R99 (Release 1999) Detailed explanations of the above categories can REL-4 (Release 4) be found in 3GPP TR 21.900. REL-5 (Release 5)										
reason for onange.	lead to I	backward compat	ibility issue	S.						
Summary of change: ३	B Deletic for the	n of the sentence computation of D	e "For the C ES in CBC	BC modes mode.	the counter	(CNTR) shall I	be used"			
Consequences if and approved:	Risk of	different interpre	tations lead	ling to inte	roperability p	problems				
Clauses affected:	€ <mark>§ 5.1.2</mark>	, § 5.1.3								
Other specs ३ affected:	K Othe Test	er core specificati specifications A Specifications	ons ¥	23.048 F	REL-5					

Other comments: #

How to create CRs using this form:

- 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 <u>ftp://ftp.3gpp.org/specs/</u> 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.

If the indication of the key to be used refers to an Open Platform key set version number, the algorithm to be used with the key shall be the algorithm associated with the key (as described in the Open Platform specification [14]).

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. For the CBC modes the counter (CNTR) shall be used. If padding is required, the padding octets shall be coded hexadecimal '00'. These octets shall not be included in the secured data.

If the indication of the key to be used refers to an Open Platform key set version number, the algorithm to be used with the key shall be the algorithm associated with the key (as described in the Open Platform specification [14]).

					.01					
ж	23.048	8 CR 014	ж	.ev -	ж C	Current vers	ion: 5.	1.0	ж	
For <u>HELP</u> on u	sing this fo	orm, see bottom	of this pag	e or look	at the p	pop-up text	over the	Ж syn	nbols.	
Proposed change a	offects:	(U)SIM X	ME/UE	Rad	lio Acce	ess Network	Co	ore Net	twork	
Title: Ж	Clarifica	tion on computa	ation of DES	in CBC	mode					
Source: ೫	T3									
Work item code: Ж						<i>Date:</i>	07/11/0)1		
Category: #	F Use <u>one</u> o F (cc A (cc B (ac C (fu D (ec Detailed e: be found in : X The lead	f the following cat rrection) presponds to a co dition of feature), nctional modification (planations of the or 3GPP <u>TR 21.90</u> requirement intr to backward co	tegories: prection in a tion of feature n) e above categ <u>0</u> . roduced by mpatibility i	n earlier ro e) gories can this sente ssues.	F elease) ence is	Release: # Use <u>one</u> of 2 R96 R97 R98 R99 REL-4 REL-5	REL-5 the followi (GSM Pha (Release (Release (Release (Release (Release	ing rele: ase 2) 1996) 1997) 1998) 1999) 4) 5) fication	ases:	
Summary of chang	e: ೫ Del for	etion of the sen the computatior	tence "For t of DES in	he CBC CBC mod	modes de.	the counter	(CNTR)	shall b	e used"	
Consequences if not approved:	ж <mark>Ris</mark>	k of different int	erpretations	leading	to inter	operability p	oroblems			
Clauses affected:	<mark>፝ </mark>	1.2, § 5.1.3								
Other specs affected:) X %	Other core spec est specificatio D&M Specificati	ifications ns ons	ж <mark>23</mark>	.048 RI	EL-4				

Other comments:

How to create CRs using this form:

- 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 <u>ftp://ftp.3gpp.org/specs/</u> 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.

If the indication of the key to be used refers to an Open Platform key set version number, the algorithm to be used with the key shall be the algorithm associated with the key (as described in the Open Platform specification [14]).

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. For the CBC modes the counter (CNTR) shall be used. If padding is required, the padding octets shall be coded hexadecimal '00'. These octets shall not be included in the secured data.

If the indication of the key to be used refers to an Open Platform key set version number, the algorithm to be used with the key shall be the algorithm associated with the key (as described in the Open Platform specification [14]).

						CR-Form-v3				
CHANGE REQUESI										
[#] 2	<mark>3.048</mark>	CR <mark>015</mark>	¥ rev	ж	Current vers	^{ion:} 4.1.0 [#]				
For <u>HELP</u> on using	For HELP on using this form, see bottom of this page or look at the pop-up text over the # symbols.									
Proposed change affe	cts: ೫	(U)SIM X	ME/UE	Radio Ac	cess Network	Core Network				
Title: ೫ Co	rrection	<mark>of Response H</mark>	eader Length ((RHL) defi	nition					
Source: ೫ T:	3									
Work item code: 🕱					Date: ೫	07/11/01				
Category: ೫ F					Release: #	REL-4				
Use Det be	e <u>one</u> of t F (esse A (corr B (Add C (Fun D (Edin cailed exp found in :	the following cate ential correction) responds to a col lition of feature), nctional modification torial modification lanations of the a 3GPP TR 21.900	egories: rrection in an ear ion of feature) n) above categorie:	rlier release s can	Use <u>one</u> of 2 9) R96 R97 R98 R99 REL-4 REL-5	the following releases: (GSM Phase 2) (Release 1996) (Release 1997) (Release 1998) (Release 1999) (Release 4) (Release 5)				
Reason for change: \$	the e	existina definitio	on of RHL is no	ot correct.						
Summary of change: a	Corre the C	ect the faulty de Command Pack	finition. The co et structure in c	orrection is chapter 5.	s in line with t 1.	he implementation of				
Consequences if not approved:	C There defin	e is a risk of difi ition.	ferent impleme	entations d	ue to differen	t interpretations of RHL				
Clauses affected: 3	§ <u>§ 5.2</u>									
Other specs	Contraction of the second seco	her core specif est specification &M Specificatio	ications							
Other comments: 3	this Chis	correction is ne	eded in all late	er versions	of 03.48 and	23.048 as well.				

How to create CRs using this form:

- 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 <u>ftp://www.3gpp.org/specs/</u> 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.

5.2 Response Packet structure

Table 3: Structure of the Response Packet

Element	Length	Comment
Response Packet Identifier (RPI)	1 octet	Identifies a Response Packet.
Response Packet Length (RPL)	variable	Indicates the number of octets from and including RHI to the of Additional Response data, including any padding octets required for ciphering.
Response Header Identifier (RHI)	1 octet	Identifies the Response Header.
Response Header Length (RHL)	variable	Indicates the number of octets from and including <u>TAR</u> <u>RC/CC/DS</u> to the end of <u>RC/CC/DS</u> the <u>Response Status Cod</u> octet.
Toolkit Application Reference (TAR)	3 octets	This shall be a copy of the contents of the TAR in the Comma Packet.
Counter (CNTR)	5 octets	This shall be a copy of the contents of the CNTR in the Comr Packet.
Padding counter (PCNTR)	1 octet	This indicates the number of padding octets used for cipherir the end of the Additional Response Data.
Response Status Code Octet	1 octet	Codings defined in Table 5.
Redundancy Check (RC), Cryptographic Checksum (CC) or Digital Signature (DS)	variable	Length depending on the algorithm indicated in the Comman- Header in the incoming message. A typical value is 4 to 8 oct or zero if no RC/CC/DS is requested.
Additional Response Data	variable	Optional Application Specific Response Data, including possi padding octets.

Unless indicated otherwise, the RPL and RHL shall be coded according to ISO/IEC 7816-6 [8].

Table 4: Linear Representation of Response Packet

RPI	RPL	RHI	RHL	TAR	CNTR	PCNTR	Status Code	RC/CC/DS	Additi Respo Data padd	
					note 1	note 1	note 1	note 1	note 1	
	note 3		note 3	note 2	note 2	note 2	note 2		note 2	
NOTE 1: NOTE 2: NOTE 3:	NOTE 1: If ciphering is indicated in the Command Packet SPI then these fields shall be ciphered. NOTE 2: These fields shall be included in the calculation of the RC/CC/DS. NOTE 3: Part or all of these fields may also be included in the calculation of the RC/CC/DS, depending on implementation (e.g. SMS).									

If ciphering is indicated, first the RC/CC/DS shall be calculated as indicated in Note 2, and then ciphering shall be applied, as indicated in note 1.

If the SPI indicates that a specific field is unused, than its contents shall be set to zero, and ignored by the recipient of the Response Packet.

If the SPI in the Command Packet indicates that no RC, CC or DS is present in the Command Header, this field shall be of zero length.

If the Padding Counter content is zero, this shall indicate no padding octets are present, or no padding is necessary.

						CR-Form-v3				
	CHANGE REQUEST									
ж <mark>2</mark>	23.048	CR <mark>016</mark>	ж rev	X	Current vers	^{ion:} 5.1.0 [#]				
For <u>HELP</u> on using this form, see bottom of this page or look at the pop-up text over the # symbols.										
Proposed change aff	ects: Ж	(U)SIM X	ME/UE	Radio Aco	cess Network	Core Network				
Title: ೫ <mark>С</mark>	orrection	of Response H	eader Length (RHL) defir	nition					
Source: ೫ <mark>-</mark>	Г3									
Work item code: ℜ					<i>Date:</i>	07/11/01				
Category: ж I	-				Release: ೫	REL-5				
U D be	se <u>one</u> of f F (ess A (cor B (Add C (Fur D (Edi etailed exp e found in	the following cate ential correction) responds to a cor dition of feature), nctional modification torial modification blanations of the a 3GPP TR 21.900	gories: rection in an ear ion of feature) n) above categories	rlier release, s can	Use <u>one</u> of 2 R96 R97 R98 R99 REL-4 REL-5	the following releases: (GSM Phase 2) (Release 1996) (Release 1997) (Release 1998) (Release 1999) (Release 4) (Release 5)				
Posson for change:	99 Tho	ovicting definition	on of PHL is no	t correct						
Summary of change:	ترجم المراجعة المراجعة مراجعة المراجعة المرا	ect the faulty de Command Pack	finition. The co	prrection is chapter 5.1	in line with th 1.	he implementation of				
Consequences if not approved:	ដ <mark>ី Ther</mark> defin	e is a risk of diff ition.	erent impleme	ntations du	ue to differen	t interpretations of RHL				
Clauses affected:	¥ <mark>§5.</mark> 2									
Other specs affected:	# 01 Te	her core specifiest specification M Specification	ications ೫ s ns							
Other comments:	¥ This	correction is ne	eded in all late	r versions	of 03.48 and	23.048 as well.				

How to create CRs using this form:

- 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 <u>ftp://www.3gpp.org/specs/</u> 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.

5.2 Response Packet structure

Table 3: Structure of the Response Packet

Element	Length	Comment
Response Packet Identifier (RPI)	1 octet	Identifies a Response Packet.
Response Packet Length (RPL)	variable	Indicates the number of octets from and including RHI to the of Additional Response data, including any padding octets required for ciphering.
Response Header Identifier (RHI)	1 octet	Identifies the Response Header.
Response Header Length (RHL)	variable	Indicates the number of octets from and including <u>TAR</u> <u>RC/CC/DS</u> to the end of <u>RC/CC/DS</u> the <u>Response Status Cod</u> <u>octet</u> .
Toolkit Application Reference (TAR)	3 octets	This shall be a copy of the contents of the TAR in the Comma Packet.
Counter (CNTR)	5 octets	This shall be a copy of the contents of the CNTR in the Comr Packet.
Padding counter (PCNTR)	1 octet	This indicates the number of padding octets used for cipherir the end of the Additional Response Data.
Response Status Code Octet	1 octet	Codings defined in table 5.
Redundancy Check (RC), Cryptographic Checksum (CC) or Digital Signature (DS)	variable	Length depending on the algorithm indicated in the Comman- Header in the incoming message. A typical value is 4 to 8 oct or zero if no RC/CC/DS is requested.
Additional Response Data	variable	Optional Application Specific Response Data, including possi padding octets.

Unless indicated otherwise, the RPL and RHL shall be coded according to ISO/IEC 7816-6 [8].

Table 4: Linear Representation of Response Packet

RPI	RPL	RHI	RHL	TAR	CNTR	PCNTR	Status Code	RC/CC/DS	Additi Respo Data padd	
					note 1	note 1	note 1	note 1	note 1	
	note 3		note 3	note 2	note 2	note 2	note 2		note 2	
NOTE 1: NOTE 2: NOTE 3:	NOTE 1: If ciphering is indicated in the Command Packet SPI then these fields shall be ciphered. NOTE 2: These fields shall be included in the calculation of the RC/CC/DS. NOTE 3: Part or all of these fields may also be included in the calculation of the RC/CC/DS, depending on implementation (e.g. SMS).									

If ciphering is indicated, first the RC/CC/DS shall be calculated as indicated in note 2, and then ciphering shall be applied, as indicated in note 1.

If the SPI indicates that a specific field is unused, than its contents shall be set to zero, and ignored by the recipient of the Response Packet.

If the SPI in the Command Packet indicates that no RC, CC or DS is present in the Command Header, this field shall be of zero length.

If the Padding Counter content is zero, this shall indicate no padding octets are present, or no padding is necessary.