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

Tdoc TP-010242

Source: T3

Title: 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	B	Definition of a Minimum Security Level
T3-010777	23.048	008	Rel-5	C	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	A	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	A	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

3GPP T3 (USIM) Meeting #21
Kyoto, Japan, 5 - 7 November 2001

Tdoc T3-010780
Revised T3-010729

CR-Form-v3

CHANGE REQUEST

⌘ **03.48 CR A021** ⌘ rev ⌘ Current version: **8.7.0** ⌘

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

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

Title:	⌘	Clarification of the APDU Access Domain.		
Source:	⌘	T3		
Work item code:	⌘		***Date:*** ⌘	07/11/2001
Category:	⌘	**F**	***Release:*** ⌘	R99

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:	⌘	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 change:	⌘	Removal of MSB and LSB notations, reordering of the bytes according to the bytes numbers, alignement of the exemple.
Consequences if not approved:	⌘	Risk of interoperability issues on access domain parameters understanding by the card.

Clauses affected:	⌘	A.1.4.2.3.2	
Other specs Affected:	⌘	☒ Other core specifications ☒ Test specifications □ O&M Specifications	⌘ 23.048 (Rel-4 and Rel-5) 11.13
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.

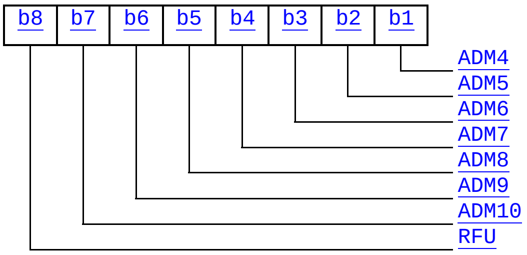
A.1.4.2.3.2 APDU access mechanism

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.

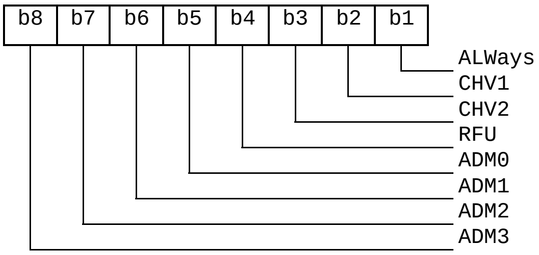
The APDU Access Domain Data is a bit map combination of the file access condition levels described in TS 11.11. When the bit is set the associated Access Condition is granted.

The APDU Access Domain Data is coded as follows:

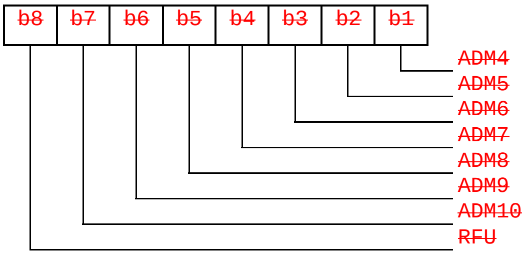
Byte 1:



Byte ~~1~~2: ~~(LSB)~~



~~Byte 2: (MSB)~~



EXAMPLE:

~~xamples of p~~Possible combinations of fulfilled Access ~~conditions~~Conditions are shown below:

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

3GPP T3 (USIM) Meeting #21
Kyoto,Japan, 5 - 7 November, 2001

Tdoc T3-010787

CR-Form-v3

CHANGE REQUEST

⌘	**03.48**	**CR**	**A022**	⌘	rev		⌘	Current version:	**8.7.0** ⌘

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

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

Title:	⌘	Correction of Response Header Length (RHL) definition		
Source:	⌘	T3		
Work item code:	⌘		***Date:*** ⌘	07/11/01
Category:	⌘	**F**	***Release:*** ⌘	R99
		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:	⌘	The existing definition of RHL is not correct.
Summary of change:	⌘	Correct the faulty definition. The correction is in line with the implementation of the Command Packet structure in chapter 5.1.
Consequences if not approved:	⌘	There is a risk of different implementations due to different interpretations of RHL definition.

Clauses affected:	⌘	§ 5.2		
Other specs affected:	⌘	□ Other core specifications □ Test specifications □ O&M Specifications	⌘	
Other comments:	⌘	This correction is needed in all later versions of 03.48 and 23.048 as well.		

How to create CRs using this form:

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

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

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

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

5.2 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 e 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 TAR ~~RC/CC/DS~~to the end of the RC/CC/DS~~Response Status Code 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 Comm 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 Command 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	Additio Respo Data w paddi
					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 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.

3GPP T3 (USIM) Meeting #21
Kyoto, Japan, 5-7 November, 2001

Tdoc T3-010776
Revised T3-010649

CR-Form-v4

CHANGE REQUEST

⌘ **23.048** **CR** **007** ⌘ ev **-** ⌘ Current version: **5.1.0** ⌘

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

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

Title:	⌘	Minimum Security Level for applet triggering on 03.48 formatted messages		
Source:	⌘	T3		
Work item code:	⌘		***Date:*** ⌘	07/11/01
Category:	⌘	**B**	***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:	⌘	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 change:	⌘	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 □ 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.

5.2 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 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 (TAR)	3 octets	This shall be a copy of the contents of the TAR in the Command 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), Cryptographic Checksum (CC) or Digital Signature (DS)	variable	Length depending on the algorithm indicated in the Command Header in the incoming message. A typical value is 4 to 8 octets, 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].

Table 4: Linear Representation of Response Packet

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 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.

Table 5: Response Status Codes

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
'0A'	Insufficient security level
~~'0A'~~ '0B' - 'FF'	Reserved for future use.

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)	\
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)	

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	Name
1	MSL Parameter (see A.1.4.2.5.1)
n-1	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	Support	MSL Data length
'00'	RFU	RFU	N/A
'01'	Minimum SPI1 (see A.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.1.4.2.5.2 Minimum SPI1

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

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

If SPI1.b2b1 is equal to or greater than MSLD.b2b1 and

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

if SPI1.b5b4 is equal to or greater than MSLD.b5b4

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

3GPP T3 (USIM) Meeting #21
Kyoto, Japan, 5-7 November, 2001

Tdoc T3-010777
Revised T3-010680

CR-Form-v3

CHANGE REQUEST

⌘ **23.048 CR 008** ⌘ rev **-** ⌘ Current version: **5.1.0** ⌘

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

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

Title:	⌘ Maximum number of timers allowed for applet instance		
Source:	⌘ T3		
Work item code:	⌘	***Date:*** ⌘	07/11/01
Category:	⌘ **C**	***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: ⌘	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: ⌘	No standard way to process an invalid maximum number of timers

Clauses affected: ⌘	5.2	
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://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)	\
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)	/

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.

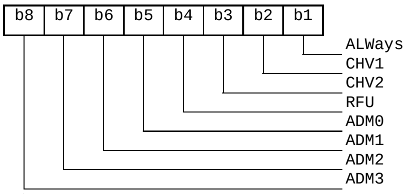
A.1.4.2.3.2 APDU access mechanism

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.

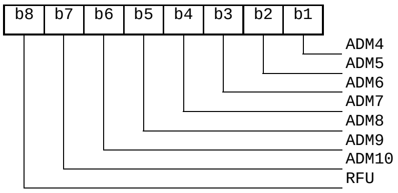
The APDU Access Domain Data is a bit map combination of the file access condition levels described in GSM 11.11. When the bit is set the associated Access Condition is granted.

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

3GPP T3 (USIM) Meeting #21
Kyoto, Japan, 5 - 7 November 2001

Tdoc T3-010781
Revised T3-010729

CR-Form-v3

CHANGE REQUEST

⌘	**23.048**	**CR**	**011**	⌘	rev		⌘	Current version: **4.1.0** ⌘

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

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

Title:	⌘	Clarification of the APDU Access Domain.		
Source:	⌘	T3		
Work item code:	⌘		***Date:*** ⌘	07/11/2001
Category:	⌘	**F**	***Release:*** ⌘	REL-4

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:	⌘	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 change:	⌘	Removal of MSB and LSB notations, reordering of the bytes according to the bytes numbers, alignement of the exemple.
Consequences if not approved:	⌘	Risk of interoperability issues on access domain parameters understanding by the card.

Clauses affected:	⌘	A.1.4.2.3.2		
Other specs Affected:	⌘	☒ Other core specifications	⌘	03.98 R99 and 23.048 REL-5
		☒ Test specifications		11.13
		□ O&M Specifications		
Other comments:	⌘			

How to create CRs using this form:

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

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

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

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

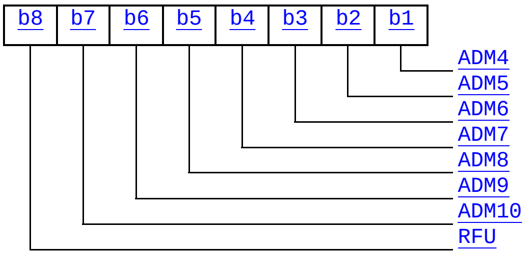
A.1.4.2.3.2 APDU access mechanism

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.

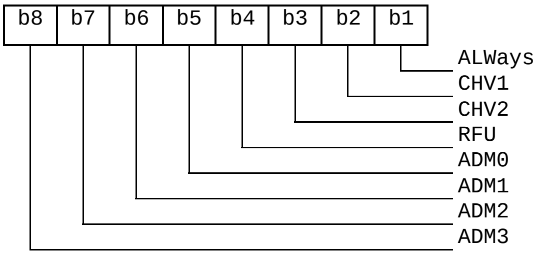
The APDU Access Domain Data is a bit map combination of the file access condition levels described in TS 11.11. When the bit is set the associated Access Condition is granted.

The APDU Access Domain Data is coded as follows:

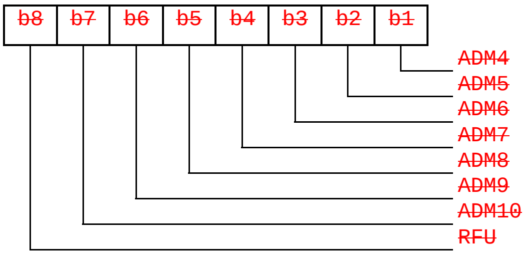
Byte 1:



Byte ~~1~~2: ~~(LSB)~~



~~Byte 2: (MSB)~~



EXAMPLE:

~~xamples of p~~Possible combinations of fulfilled Access ~~conditions~~Conditions are shown below:

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

3GPP T3 (USIM) Meeting #21
Kyoto, Japan, 5 - 7 November 2001

Tdoc T3-010782
Revised T3-010729

CR-Form-v3

CHANGE REQUEST

⌘ **23.048 CR 012** ⌘ rev ⌘ Current version: **5.1.0** ⌘

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

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

Title:	⌘	Clarification of the APDU Access Domain.		
Source:	⌘	T3		
Work item code:	⌘		***Date:*** ⌘	07/11/2001
Category:	⌘	**A**	***Release:*** ⌘	REL-5

Use <u>one</u> 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 <u>one</u> 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 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 change:	⌘	Removal of MSB and LSB notations, reordering of the bytes according to the bytes numbers, alignement of the exemple.
Consequences if not approved:	⌘	Risk of interoperability issues on access domain parameters understanding by the card.

Clauses affected:	⌘	A.1.4.2.3.2		
Other specs Affected:	⌘	☒ Other core specifications ☒ Test specifications □ O&M Specifications	⌘	03.98 R99 and 23.048 REL-4 11.13
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.

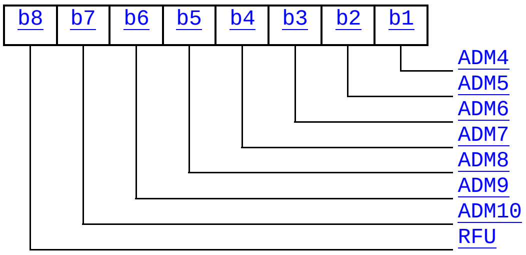
A.1.4.2.3.2 APDU access mechanism

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.

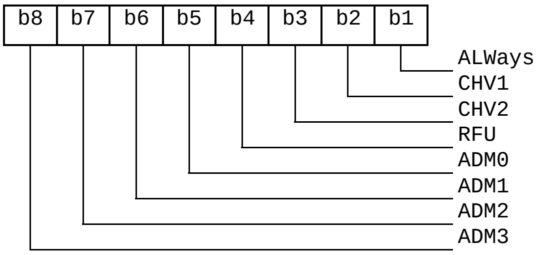
The APDU Access Domain Data is a bit map combination of the file access condition levels described in TS 11.11. When the bit is set the associated Access Condition is granted.

The APDU Access Domain Data is coded as follows:

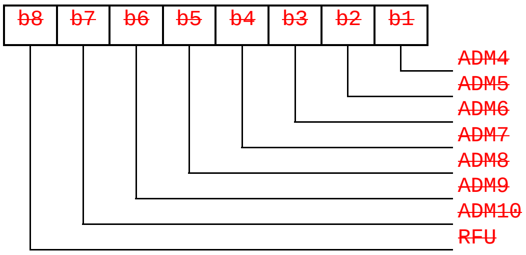
Byte 1:



Byte ~~1~~2: ~~(LSB)~~



~~Byte 2: (MSB)~~



EXAMPLE:

~~xamples of p~~Possible combinations of fulfilled Access ~~conditions~~Conditions are shown below:

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

3GPP T3 (USIM) Meeting #21
Kyoto, Japan, 5 - 7 November 2001

Tdoc T3-010783
Revised T3-010728

CR-Form-v4

CHANGE REQUEST

⌘	**23.048**	**CR**	**013**	⌘	ev	**-**	⌘	Current version:	**4.1.0**	⌘

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

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

Title:	⌘	Clarification on computation of DES in CBC mode		
Source:	⌘	T3		
Work item code:	⌘		***Date:*** ⌘	07/11/01
Category:	⌘	**F**	***Release:*** ⌘	REL-4

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 requirement introduced by this sentence is not clear and a clarification could lead to backward compatibility issues.
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, § 5.1.3		
Other specs affected:	⌘	☒ Other core specifications	⌘	23.048 REL-5
		□ 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:

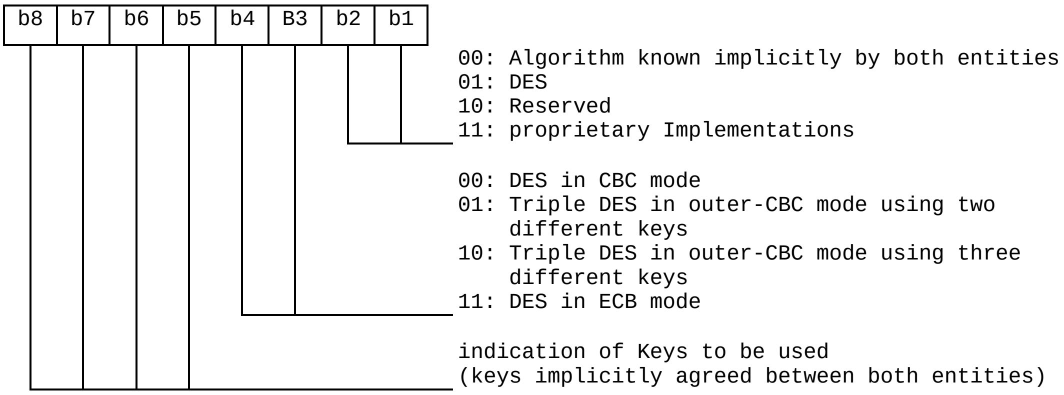
1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

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.



```
00: Algorithm known implicitly by both entities
01: DES
10: Reserved
11: proprietary Implementations

00: DES in CBC mode
01: Triple DES in outer-CBC mode using two
    different keys
10: Triple DES in outer-CBC mode using three
    different keys
11: DES in ECB mode

indication of Keys to be used
(keys implicitly agreed between both entities)
```

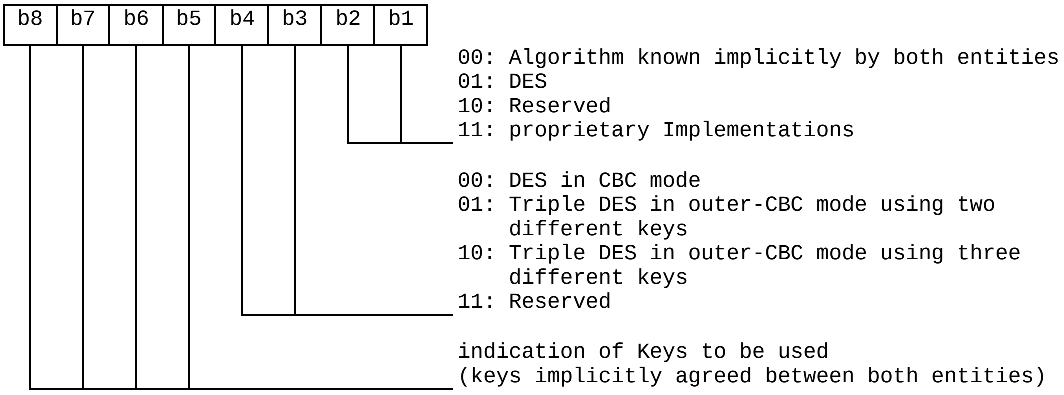
DES is the algorithm specified as DEA in ISO 8731-1 [9]. DES in CBC mode is described in ISO/IEC 10116 [10]. Triple DES in outer-CBC mode is described in section 15.2 of [17]. DES in ECB mode is described in ISO/IEC 10116 [10].

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.



```
00: Algorithm known implicitly by both entities
01: DES
10: Reserved
11: proprietary Implementations

00: DES in CBC mode
01: Triple DES in outer-CBC mode using two
    different keys
10: Triple DES in outer-CBC mode using three
    different keys
11: Reserved

indication of Keys to be used
(keys implicitly agreed between both entities)
```

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]).

3GPP T3 (USIM) Meeting #21
Kyoto, Japan, 5 - 7 November 2001

Tdoc T3-010784
Revised T3-010728

CR-Form-v4

CHANGE REQUEST

⌘	**23.048**	**CR**	**014**	⌘	ev	**-**	⌘	Current version: **5.1.0** ⌘

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

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

Title:	⌘	Clarification on computation of DES in CBC mode		
Source:	⌘	T3		
Work item code:	⌘		***Date:*** ⌘	07/11/01
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 requirement introduced by this sentence is not clear and a clarification could lead to backward compatibility issues.
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, § 5.1.3		
Other specs affected:	⌘	☒ Other core specifications ☐ Test specifications ☐ O&M Specifications	⌘	23.048 REL-4
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:

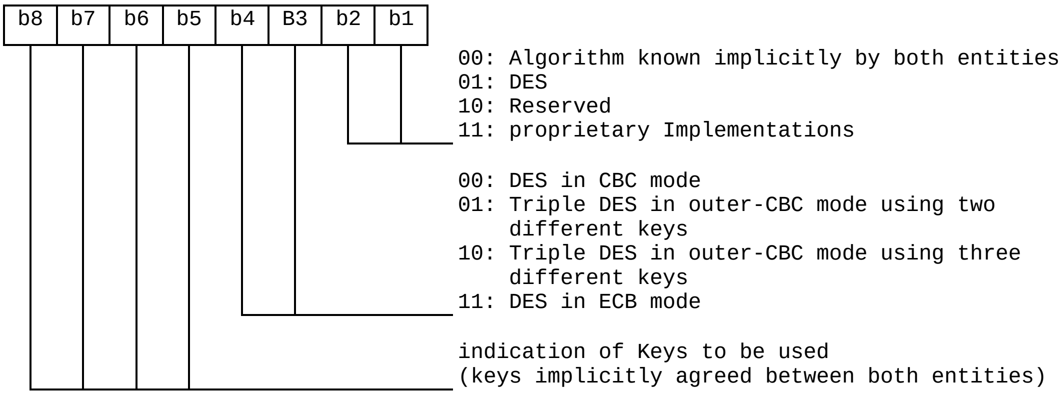
1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

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.


b8
b7
b6
b5
b4
B3
b2
b1
00: Algorithm known implicitly by both entities
01: DES
10: Reserved
11: proprietary Implementations
00: DES in CBC mode
01: Triple DES in outer-CBC mode using two different keys
10: Triple DES in outer-CBC mode using three different keys
11: DES in ECB mode
indication of Keys to be used
(keys implicitly agreed between both entities)

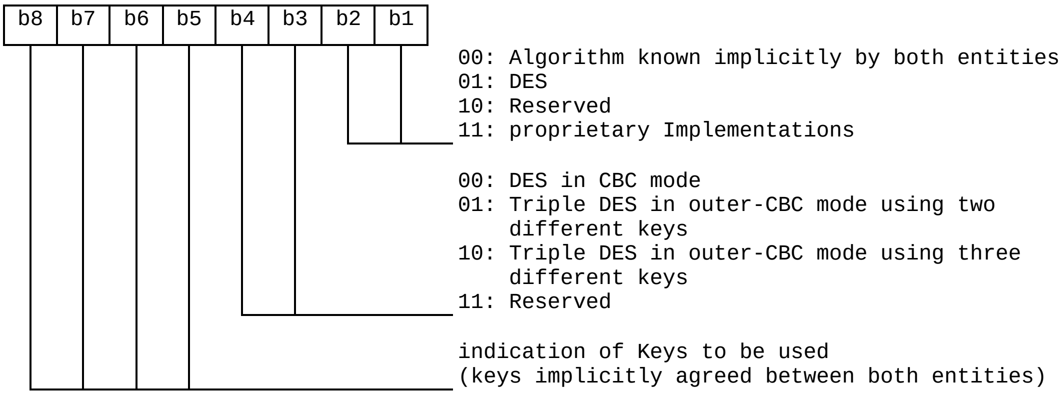
DES is the algorithm specified as DEA in ISO 8731-1 [9]. DES in CBC mode is described in ISO/IEC 10116 [10]. Triple DES in outer-CBC mode is described in section 15.2 of [17]. DES in ECB mode is described in ISO/IEC 10116 [10].

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.


b8
b7
b6
b5
b4
b3
b2
b1
00: Algorithm known implicitly by both entities
01: DES
10: Reserved
11: proprietary Implementations
00: DES in CBC mode
01: Triple DES in outer-CBC mode using two different keys
10: Triple DES in outer-CBC mode using three different keys
11: Reserved
indication of Keys to be used
(keys implicitly agreed between both entities)

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]).

3GPP T3 (USIM) Meeting #21
Kyoto,Japan, 5 - 7 November, 2001

Tdoc T3-010788

CR-Form-v3

CHANGE REQUEST

⌘	**23.048**	**CR**	**015**	⌘	rev		⌘	Current version:	**4.1.0** ⌘

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

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

Title: ⌘	Correction of Response Header Length (RHL) definition		
Source: ⌘	T3		
Work item code: ⌘		***Date:*** ⌘	07/11/01
Category: ⌘	**F**	***Release:*** ⌘	REL-4
	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: ⌘	The existing definition of RHL is not correct.
Summary of change: ⌘	Correct the faulty definition. The correction is in line with the implementation of the Command Packet structure in chapter 5.1.
Consequences if not approved: ⌘	There is a risk of different implementations due to different interpretations of RHL definition.

Clauses affected: ⌘	§ 5.2	
Other specs affected: ⌘	□ Other core specifications ⌘ □ Test specifications □ O&M Specifications	
Other comments: ⌘	This correction is needed in all later versions of 03.48 and 23.048 as well.	

How to create CRs using this form:

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

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

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

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

5.2 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 e 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 TAR ~~RC/CC/DS~~to the end of RC/CC/DS~~the Response Status Cod 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 Comm Packet.
Padding counter (PCNTR)	1 octet	This indicates the number of padding octets used for cipherin 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 Command 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 w paddi
					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 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.

3GPP T3 (USIM) Meeting #21
Kyoto,Japan, 5 - 7 November, 2001

Tdoc T3-010789

CR-Form-v3

CHANGE REQUEST

⌘	**23.048**	**CR**	**016**	⌘	rev		⌘	Current version:	**5.1.0**	⌘

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

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

Title:	⌘ Correction of Response Header Length (RHL) definition			
Source:	⌘ T3			
Work item code:	⌘		***Date:*** ⌘	07/11/01
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:	⌘	The existing definition of RHL is not correct.
Summary of change:	⌘	Correct the faulty definition. The correction is in line with the implementation of the Command Packet structure in chapter 5.1.
Consequences if not approved:	⌘	There is a risk of different implementations due to different interpretations of RHL definition.

Clauses affected:	⌘	§ 5.2	
Other specs affected:	⌘	☐ Other core specifications ☐ Test specifications ☐ O&M Specifications	⌘
Other comments:	⌘	This correction is needed in all later versions of 03.48 and 23.048 as well.	

How to create CRs using this form:

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

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

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

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

5.2 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 e 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 TAR ~~RC/CC/DS~~to the end of RC/CC/DS~~the Response Status Cod 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 Comm Packet.
Padding counter (PCNTR)	1 octet	This indicates the number of padding octets used for cipherin 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 Command 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 w paddi
					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 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.