3GPP TSG-T (Terminals) Meeting #13
Beijing, China, 19 - 21 September, 2001

Tdoc TP-010201

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
T3-010595	03.48	A019	R99	F	Clarifications on padding and Anti Replay Counter
T3-010551	03.48	A020	R99	F	Correction to example in Annex A
T3-010544	23.048	001	Rel-4	F	Correction to APDU access mechanism in annex A
T3-010545	23.048	002	Rel-5	A	Correction to APDU access mechanism in annex A
T3-010598	23.048	003	Rel-4	F	USIM input and output commands for Remote File management
T3-010599	23.048	004	Rel-5	A	USIM input and output commands for Remote File management
T3-010596	23.048	005	Rel-4	F	Clarifications on padding and Anti Replay Counter
T3-010597	23.048	006	Rel-5	A	Clarifications on padding and Anti Replay Counter

3GPP T3 (USIM) Meeting #20
Marseille, France, 3 - 5 September, 2001

Tdoc T3-010595

CR-Form-v3

CHANGE REQUEST

⌘ **03.48** **CR** **A019** ⌘ rev **-** ⌘ Current version: **8.6.0** ⌘

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

Proposed change affects: ⌘ (U)SIM [X] ME/UE [ ] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Clarifications on padding and Anti Replay Counter
Source:	⌘	T3
Work item code:	⌘	***Date:*** ⌘ 05/09/01
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 use of the padding octets when it is necessary is not clear: the padding octets are used for ciphering. The padding octets for the calculation of RC/CC/DS are not included in the secured data.
- In the case “No counter available” in the coding of the first byte of the SPI, the counter has to be present in the message even if it is unused.
- The description of the management of the Anti Replay counter in section 5.1.4 applies when the replay and sequence checking is done (b5 of the first octet of the SPI equals to 1) and not in the other cases.
- The”next counter value” is the one received in the incoming message in the case the security checks are passed successfully.

Summary of change: ⌘

- Clarify the use of padding octets.
- Clarify the case “No counter available” in the coding of the first octet of the SPI.
- Clarify when the counter management section applies.
- Clarify the behaviour of the counter when the security checks have been passed successfully in the case b5 of the first byte of SPI is equal to 1.

Consequences if not approved: ⌘

Clauses affected: ⌘ §5.1, §5.1.1, §5.1.3, §5.1.4, §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.

5.1 Command Packet structure

The Command Header precedes the Secured Data in the Command Packet, and is of variable length.

The Command Packet shall be structured according to table 1.

Table 1: Structure of the Command Packet

Element	Length	Comment
Command Packet Identifier (CPI)	1 octet	Identifies that this data block is the secured Command Packet.
Command Packet Length (CPL)	Variable	This shall indicate the number of octets from and including the Command Header Identifier to the end of the Secured Data, including any padding octets required for ciphering.
Command Header Identifier (CHI)	1 octet	Identifies the Command Header.
Command Header Length (CHL)	Variable	This shall indicate the number of octets from and including the SPI to the end of the RC/CC/DS.
Security Parameter Indicator (SPI)	2 octets	see detailed coding in section 5.1.1.
Ciphering Key Identifier (KIc)	1 octet	Key and algorithm Identifier for ciphering.
Key Identifier (KID)	1 octet	Key and algorithm Identifier for RC/CC/DS.
Toolkit Application Reference (TAR)	3 octets	Coding is application dependent.
Counter (CNTR)	5 octets	Replay detection and Sequence Integrity counter.
Padding counter (PCNTR)	1 octet	This indicates the number of padding octets used for ciphering at the end of the secured data.
Redundancy Check (RC), Cryptographic Checksum (CC) or Digital Signature (DS)	Variable	Length depends on the algorithm. A typical value is 8 octets if used, and for a DS could be 48 or more octets; the minimum should be 4 octets.
Secured Data	Variable	Contains the Secured Application Message and possibly padding octets used for ciphering.

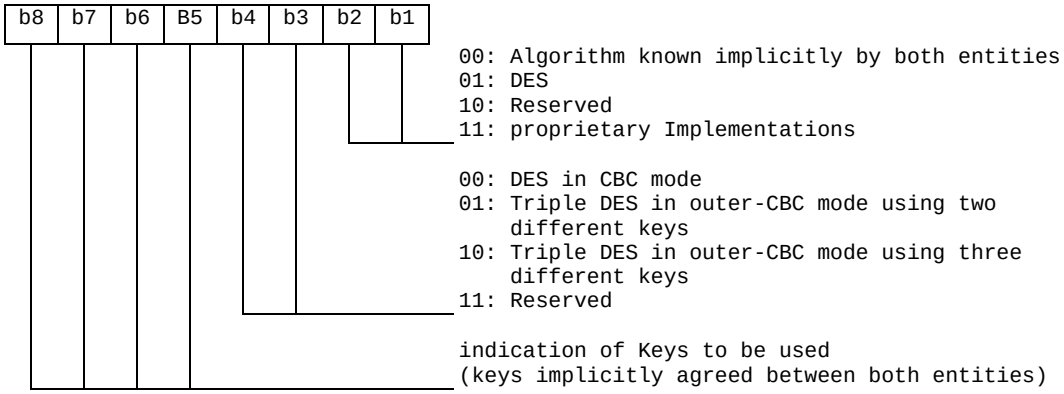
5.2 Response Packet structure

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 used for ciphering.

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 [20].

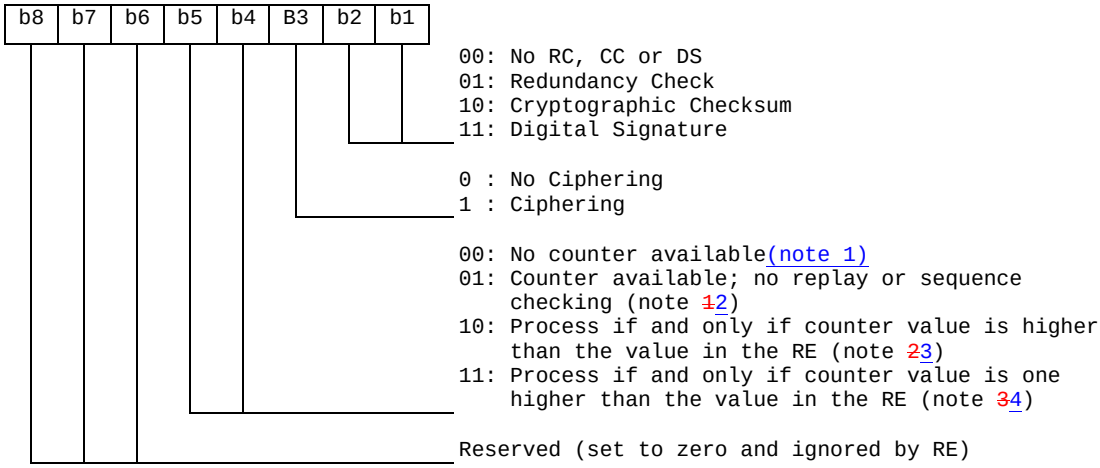
The initial chaining value for CBC modes shall be zero. For the CBC modes the counter (CNTR) shall be used. If padding is required, the padding octets shall be coded hexadecimal '00'.~~,~~ These octets shall not be included in the secured data.

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]).

5.1.1 Coding of the SPI

The SPI is coded as below.

First Octet:



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

NOTE ~~1~~2:In this case the counter value is used for information purposes only, (e.g. date or time stamp). If the Command Packet was successfully unpacked, the counter value can be forwarded from the Receiving Entity to the Receiving Application. This depends on proprietary implementations and happens in an application dependent way.

NOTE ~~2~~3:The counter value is compared with the counter value of the last received Command Packet. This is tolerant to failures on the transport level (i.e. losses of Command Packets). A possible scenario is a global update.

NOTE ~~3~~4:This provides strict control in addition to security indicated in Note 3~~2~~.

5.1.4 Counter Management

If in the first SPI byte b4b5=00 (No counter available) the counter field shall be ignored by the RE and the RE shall not update the counter.

If b5 of the first SPI byte is equal to 1 then ~~T~~the following rules shall apply to counter management, with the goal of preventing replay and synchronisation attacks:

- The SE sets the counter value. It shall only be incremented.
- The RE shall update~~increment~~ the counter to its next value upon receipt of a Command Packet after the corresponding security checks (i.e. RC/CC/DS and CNTR verification) have been passed successfully.

  The next counter value is the one received in the incoming message.
- When the counter value reaches its maximum value the counter is blocked.

If there is more than one SE, care has to be taken to ensure that the counter values remain synchronised between the SE's to what the RE is expecting, irrespective of the transport mechanism employed.

The level of security is indicated via the proprietary interface between the Sending/Receiving Application and Sending/Receiving Entity. Application designers should be aware that if the Sending Application requests "No RC/CC/DS" or "Redundancy Check" and "No Counter Available" from the SE, no security is applied to the Application Message and therefore there is an increased threat of malicious attack.

3GPP T3 Meeting #20
Marseille, France, 3 - 5 September 2001

Tdoc T3-010551

CR-Form-v4

CHANGE REQUEST

⌘ **03.48** **CR** **A020** ⌘ ev **-** ⌘ Current version: **8.6.0** ⌘

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

Proposed change affects: ⌘ (U)SIM [X] ME/UE [ ] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Correction to APDU access mechanism
Source:	⌘	T3
Work item code:	⌘	***Date:*** ⌘ 9/4/2001
Category:	⌘	**F** ***Release:*** ⌘ R99

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 example given as possible combination of access conditions is wrong
Summary of change:	⌘	ADM0 access condition is mapped on bit 5 of the LSB byte of Access Domain Data value. In the example, the Access Domain Data value shall then be 0x0010 and not 0x0008.The same change applies for ADM1.
Consequences if not approved:	⌘	Example is not aligned with what is specified

Clauses affected:	⌘	A.1.4.2.3.2
Other specs affected:	⌘	[ ] Other core specifications ⌘ [ ] Test specifications [ ] O&M Specifications
Other comments:	⌘	

How to create CRs using this form:

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

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

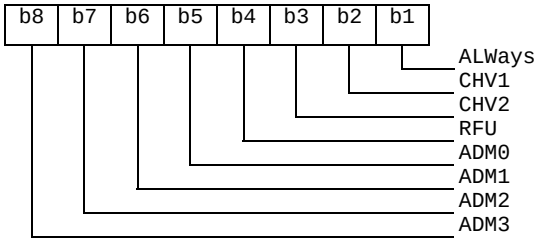
A.1.4.2.3.2 APDU access mechanism

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.

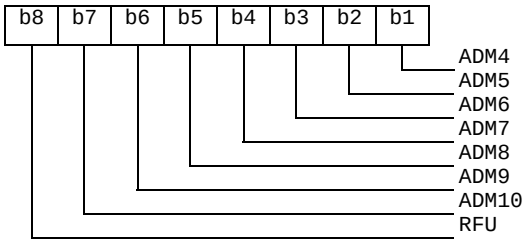
The APDU Access Domain Data is a bit map combination of the file access condition levels described in TS 11.11. When the bit is set the associated Access Condition is granted.

The APDU Access Domain Data is coded as follows:

Byte 1: (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
:	:
0x00~~08~~10	ADM 0
:	:
0x00~~1~~20	ADM 1
:	:
0x00~~1~~22	ADM 1 and CHV1
:	:

3GPP T3 Meeting #20
Marseille, France, 3 - 5 September 2001

Tdoc T3-010544

CR-Form-v4

CHANGE REQUEST

⌘ **23.048** **CR** **001** ⌘ ev **-** ⌘ Current version: **4.0.0** ⌘

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

Proposed change affects: ⌘ (U)SIM [X] ME/UE [ ] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Correction to APDU access mechanism in annex A
Source:	⌘	T3
Work item code:	⌘	***Date:*** ⌘ 5/9/2001
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:	⌘	During the conversion of T3-010434 (after the T3 #19 meeting) from a draft specification into a CR suitable for presentation to TSG-T #12, a section of annex A was incorrectly omitted.
Summary of change:	⌘	The relevant piece from Annex A is re-added.
Consequences if not approved:	⌘	The APDU access mechanism would not be implementable.

Clauses affected:	⌘	A.1.4.2.3.2		
Other specs affected:	⌘	[X] Other core specifications [ ] Test specifications [ ] O&M Specifications	⌘	An corresponding CR is also required for the release-5 version of TS 23.048
Other comments:	⌘			

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

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

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

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

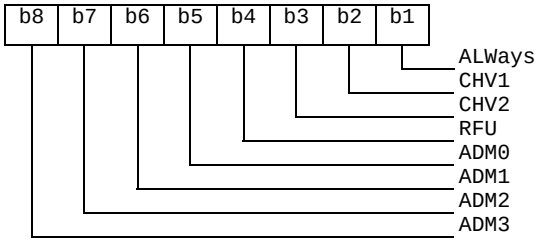
A.1.4.2.3.2 APDU access mechanism

This mechanism shall be used, if supported, by the framework if the Access Domain Parameter value is '01'. It shall use the Access Domain Data passed at applet instantiation to define the access conditions fulfilled while the toolkit applet is running.

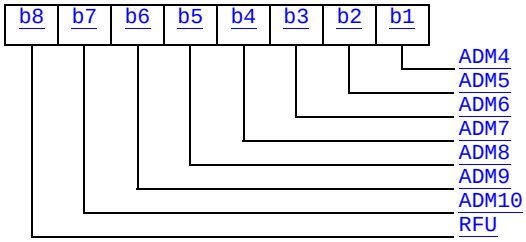
The APDU Access Domain Data is a bit map combination of the file access condition levels described in 3GPP TS 51.011. When the bit is set the associated Access Condition is granted.

The APDU Access Domain Data is coded as follows:

Byte 1: (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
:	:
0x00~~08~~10	ADM 0
:	:
0x00~~1~~20	ADM 1
:	:
0x00~~1~~22	ADM 1 and CHV1
:	:

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

3GPP T3 Meeting #20
Marseille, France, 3 - 5 September 2001

Tdoc T3-010545

CR-Form-v4

CHANGE REQUEST

⌘ **23.048** **CR** **002** ⌘ ev **-** ⌘ Current version: **5.0.0** ⌘

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

Proposed change affects: ⌘ (U)SIM [X] ME/UE [ ] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Correction to APDU access mechanism in annex A
Source:	⌘	T3
Work item code:	⌘	***Date:*** ⌘ 5/9/2001
Category:	⌘	**A** ***Release:*** ⌘ REL-5

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

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
REL-4 (Release 4)
REL-5 (Release 5)

Reason for change:	⌘	During the conversion of T3-010434 (after the T3 #19 meeting) from a draft specification into a CR suitable for presentation to TSG-T #12, a section of annex A was incorrectly omitted.
Summary of change:	⌘	The relevant piece from Annex A is re-added.
Consequences if not approved:	⌘	The APDU access mechanism would not be implementable.

Clauses affected:	⌘	A.1.4.2.3.2
Other specs affected:	⌘	[ ] Other core specifications ⌘ [ ] Test specifications [ ] O&M Specifications
Other comments:	⌘	

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

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

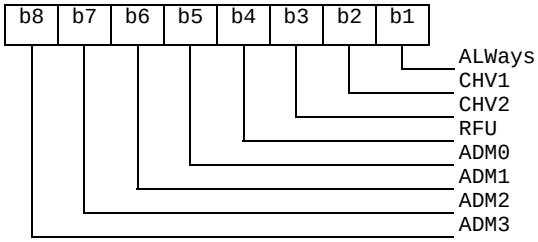
A.1.4.2.3.2 APDU access mechanism

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.

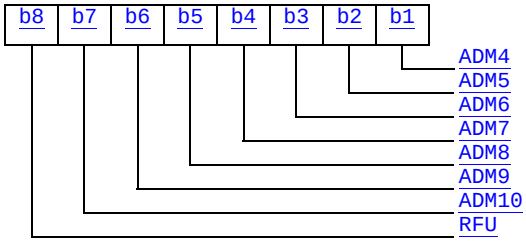
The APDU Access Domain Data is a bit map combination of the file access condition levels described in 3GPP TS 51.011. When the bit is set the associated Access Condition is granted.

The APDU Access Domain Data is coded as follows:

Byte 1: (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
:	:
0x00~~08~~10	ADM 0
:	:
0x00~~1~~20	ADM 1
:	:
0x00~~1~~22	ADM 1 and CHV1
:	:

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

3GPP T3 (USIM) Meeting #20
Marseille, France, 3 - 5 September, 2001

Tdoc T3-010598

CR-Form-v3

CHANGE REQUEST

⌘ **23.048** **CR** **003** ⌘ rev **-** ⌘ Current version: **4.0.0** ⌘

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

Proposed change affects: ⌘ (U)SIM [X] ME/UE [ ] Radio Access Network [ ] Core Network [ ]

Title:	⌘	USIM input and output commands for Remote File management
Source:	⌘	T3
Work item code:	⌘	***Date:*** ⌘ 05/09/01
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:	⌘	To apply to 3G
Summary of change:	⌘	Add the USIM input and output commands for Remote File management, which are different from the SIM input and output commands and refer to 3GPP TS 31.101 for the description of these commands.
Consequences if not approved:	⌘	Impossible to do remote management on the USIM File System. Proprietary solutions.

Clauses affected:	⌘	§2.1, §8.2.3, §8.2.4		
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.

2.1 Normative references

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.048: "Security Mechanisms for the (U)SIM Application Toolkit - Stage 1".

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

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

[5] 3GPP TS 51.011: "Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[6] 3GPP TS 31.111: "3rd Generation Partnership Project; Technical Specification Group Terminals; USIM Application Toolkit (USAT)".

[7] ISO/IEC 7816-4 (1995): "Identification cards -- Integrated circuit(s) cards with contacts -- Part 4: Interindustry commands for interchange".

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

[9] ISO 8731-1:1987 "Banking -- Approved algorithms for message authentication -- Part 1: DEA".

[10] ISO/IEC 10116:1997 "Information technology -- Security techniques -- Modes of operation for an n-bit block cipher".

[11] 3GPP TS 23.041: "Technical realisation of Short Message Service Cell Broadcast (SMSCB)".

[12] 3GPP TS 24.012: "Short Message Service Cell Broadcast (SMSCB) support on the mobile radio interface".

[13] 3GPP TS 23.038: "Alphabets and language-specific information".

[14] Open Platform Card Specification version 2.0.1 (see http://www.globalplatform.org/)

[15] 3GPP TS 43.019: "Subscriber Identity Module Application Programming Interface (SIM API); SIM API for Java Card™; Stage 2".

[16] 3GPP TS 31.101: "UICC-Terminal Interface, Physical and Logical Characteristics".

8.2.1 SIM Input Commands

The standardised commands are listed in table 10. The commands are as defined in 3GPP TS 51.011 [5], except that the SELECT command is extended from the one in 3GPP TS 51.011 [5] to include "SELECT by path" as defined in ISO/IEC 7816-4 [7].

Table 10: Input Commands

Operational command
SELECT
UPDATE BINARY
UPDATE RECORD
SEEK
INCREASE
VERIFY CHV
CHANGE CHV
DISABLE CHV
ENABLE CHV
UNBLOCK CHV
INVALIDATE
REHABILITATE

8.2.2 SIM Output Commands

The commands listed in table 11 are defined in 3GPP TS 51.011 [5]. These commands shall only occur once in a command string and, if present, shall be the last command in the string. The Response Data shall be placed in the Additional Response Data element of the Response Packet. If SMS is being used, these should result in the generation of a single SM by the UICC .

Table 11: Output commands

Operational command
READ BINARY
READ RECORD
GET RESPONSE

8.2.3 USIM Input Commands

~~To be defined~~

The standardised commands are listed in table 12. The commands are as defined in 3GPP TS 31.101[16].

Table 12: USIM Input Commands

Operational command
SELECT
UPDATE BINARY
UPDATE RECORD
SEARCH RECORD
INCREASE
VERIFY PIN
CHANGE PIN
DISABLE PIN
ENABLE PIN
UNBLOCK PIN
DEACTIVATE FILE
ACTIVATE FILE

The SELECT command shall not include the selection by DF name corresponding to P1='04' in the Command Parameters of SELECT (see 3GPP TS 31.101[16])

8.2.4 USIM output ~~Input~~ Commands

~~To be defined~~

The standardised commands are listed in table 13. The commands are as defined in 3GPP TS 31.101[16].

These commands shall only occur once in a command string and, if present, shall be the last command in the string. The Response Data shall be placed in the Additional Response Data element of the Response Packet.

Table 13: USIM Output Commands

Operational command
READ BINARY
READ RECORD
GET RESPONSE

3GPP T3 (USIM) Meeting #20
Marseille, France, 3 - 5 September, 2001

Tdoc T3-010599

CR-Form-v3

CHANGE REQUEST

⌘ **23.048** **CR** **004** ⌘ rev **-** ⌘ Current version: **4.0.0** ⌘

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

Proposed change affects: ⌘ (U)SIM [X] ME/UE [ ] Radio Access Network [ ] Core Network [ ]

Title:	⌘	USIM input and output commands for Remote File management
Source:	⌘	T3
Work item code:	⌘	***Date:*** ⌘ 05/09/01
Category:	⌘	**A** ***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:	⌘	To apply to 3G
Summary of change:	⌘	Add the USIM input and output commands for Remote File management, which are different from the SIM input and output commands and refer to 3GPP TS 31.101 for the description of these commands.
Consequences if not approved:	⌘	Impossible to do remote management on the USIM File System. Proprietary solutions.

Clauses affected:	⌘	§2.1, §8.2.3, §8.2.4		
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.

2.1 Normative references

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.048: "Security Mechanisms for the (U)SIM Application Toolkit - Stage 1".

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

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

[5] 3GPP TS 51.011: "Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[6] 3GPP TS 31.111: "3rd Generation Partnership Project; Technical Specification Group Terminals; USIM Application Toolkit (USAT)".

[7] ISO/IEC 7816-4 (1995): "Identification cards -- Integrated circuit(s) cards with contacts -- Part 4: Interindustry commands for interchange".

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

[9] ISO 8731-1:1987 "Banking -- Approved algorithms for message authentication -- Part 1: DEA".

[10] ISO/IEC 10116:1997 "Information technology -- Security techniques -- Modes of operation for an n-bit block cipher".

[11] 3GPP TS 23.041: "Technical realisation of Short Message Service Cell Broadcast (SMSCB)".

[12] 3GPP TS 24.012: "Short Message Service Cell Broadcast (SMSCB) support on the mobile radio interface".

[13] 3GPP TS 23.038: "Alphabets and language-specific information".

[14] Open Platform Card Specification version 2.0.1 (see http://www.globalplatform.org/)

[15] 3GPP TS 43.019: "Subscriber Identity Module Application Programming Interface (SIM API); SIM API for Java Card™; Stage 2".

[16] 3GPP TS 31.101: "UICC-Terminal Interface, Physical and Logical Characteristics".

8.2.1 SIM Input Commands

The standardised commands are listed in table 10. The commands are as defined in 3GPP TS 51.011 [5], except that the SELECT command is extended from the one in 3GPP TS 51.011 [5] to include "SELECT by path" as defined in ISO/IEC 7816-4 [7].

Table 10: Input Commands

Operational command
SELECT
UPDATE BINARY
UPDATE RECORD
SEEK
INCREASE
VERIFY CHV
CHANGE CHV
DISABLE CHV
ENABLE CHV
UNBLOCK CHV
INVALIDATE
REHABILITATE

8.2.2 SIM Output Commands

The commands listed in table 11 are defined in 3GPP TS 51.011 [5]. These commands shall only occur once in a command string and, if present, shall be the last command in the string. The Response Data shall be placed in the Additional Response Data element of the Response Packet. If SMS is being used, these should result in the generation of a single SM by the UICC .

Table 11: Output commands

Operational command
READ BINARY
READ RECORD
GET RESPONSE

8.2.3 USIM Input Commands

~~To be defined~~

The standardised commands are listed in table 12. The commands are as defined in 3GPP TS 31.101[16].

Table 12: USIM Input Commands

Operational command
SELECT
UPDATE BINARY
UPDATE RECORD
SEARCH RECORD
INCREASE
VERIFY PIN
CHANGE PIN
DISABLE PIN
ENABLE PIN
UNBLOCK PIN
DEACTIVATE FILE
ACTIVATE FILE

The SELECT command shall not include the selection by DF name corresponding to P1='04' in the Command Parameters of SELECT (see 3GPP TS 31.101[16])

8.2.4 USIM output ~~Input~~ Commands

~~To be defined~~

The standardised commands are listed in table 13. The commands are as defined in 3GPP TS 31.101[16].

These commands shall only occur once in a command string and, if present, shall be the last command in the string. The Response Data shall be placed in the Additional Response Data element of the Response Packet.

Table 13: USIM Output Commands

Operational command
READ BINARY
READ RECORD
GET RESPONSE

3GPP T3 (USIM) Meeting #20
Marseille, France, 3 - 5 September, 2001

Tdoc T3-010596

CR-Form-v3

CHANGE REQUEST

⌘ **23.048** **CR** **005** ⌘ rev **-** ⌘ Current version: **4.0.0** ⌘

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

Proposed change affects: ⌘ (U)SIM [X] ME/UE [ ] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Clarifications on padding and Anti Replay Counter Alignment with 03.48 V8.6.0 R99
Source:	⌘	T3
Work item code:	⌘	***Date:*** ⌘ 05/09/01
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 use of the padding octets when it is necessary is not clear: the padding octets are used for ciphering. The padding octets for the calculation of RC/CC/DS are not included in the secured data.
- In the case “No counter available” in the coding of the first byte of the SPI, the counter has to be present in the message even if it is unused.
- The description of the management of the Anti Replay counter in section 5.1.4 has to be clarified depending on the value of the first octet if the SPI.
- The”next counter value” is the one received in the incoming message in the case the security checks are passed successfully.
- A CR on 03.48 R99 has not been included in 23.048 REL-4 during the conversion.

Summary of change: ⌘

- Clarify the use of padding octets.
- Clarify the case “No counter available” in the coding of the first octet of the SPI.
- Clarify the behaviour of the counter when the security checks have been passed successfully in the case b5 of the first byte of SPI is equal to 1.
- Clarify the behaviour of the counter in the case b4b5 of the first byte of SPI is equal to 00 (no counter available)
- Clarification of the Anti Replay Counter management

Consequences if not approved: ⌘

Clauses affected:	⌘	§5.1, §5.1.1, §5.1.3, §5.1.4, §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.

5.1 Command Packet structure

The Command Header precedes the Secured Data in the Command Packet, and is of variable length.

The Command Packet shall be structured according to table 1.

Table 1: Structure of the Command Packet

Element	Length	Comment
Command Packet Identifier (CPI)	1 octet	Identifies that this data block is the secured Command Packet.
Command Packet Length (CPL)	Variable	This shall indicate the number of octets from and including the Command Header Identifier to the end of the Secured Data, including any padding octets required for ciphering.
Command Header Identifier (CHI)	1 octet	Identifies the Command Header.
Command Header Length (CHL)	Variable	This shall indicate the number of octets from and including the SPI to the end of the RC/CC/DS.
Security Parameter Indicator (SPI)	2 octets	see detailed coding in section 5.1.1.
Ciphering Key Identifier (KIc)	1 octet	Key and algorithm Identifier for ciphering.
Key Identifier (KID)	1 octet	Key and algorithm Identifier for RC/CC/DS.
Toolkit Application Reference (TAR)	3 octets	Coding is application dependent.
Counter (CNTR)	5 octets	Replay detection and Sequence Integrity counter.
Padding counter (PCNTR)	1 octet	This indicates the number of padding octets used for ciphering at the end of the secured data.
Redundancy Check (RC), Cryptographic Checksum (CC) or Digital Signature (DS)	Variable	Length depends on the algorithm. A typical value is 8 octets if used, and for a DS could be 48 or more octets; the minimum should be 4 octets.
Secured Data	Variable	Contains the Secured Application Message and possibly padding octets used for ciphering.

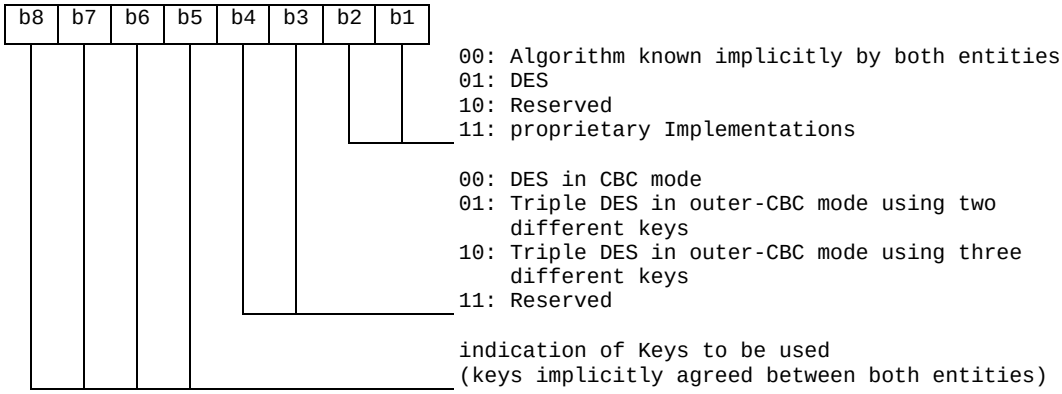
5.2 Response Packet structure

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.

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 [20].

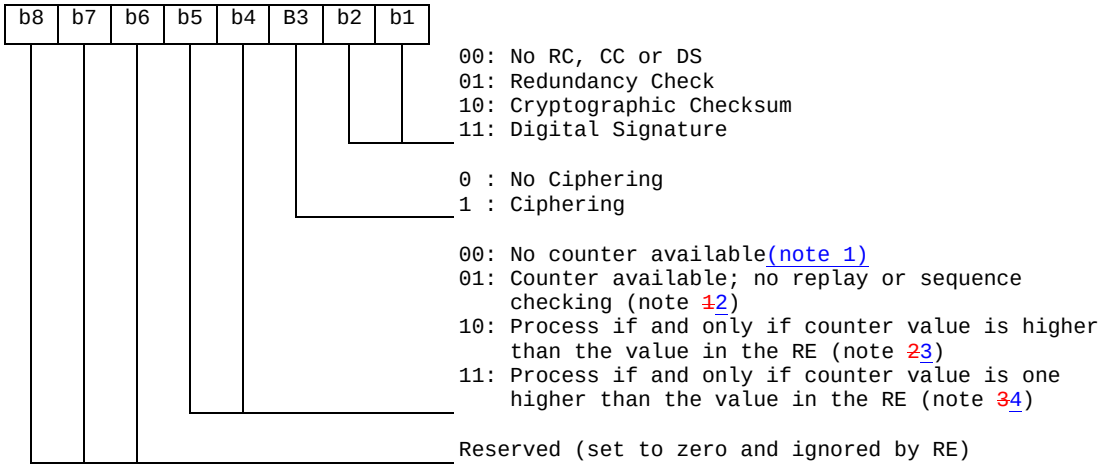
The initial chaining value for CBC modes shall be zero. For the CBC modes the counter (CNTR) shall be used. If padding is required, the padding octets shall be coded hexadecimal '00'. These octets shall not be included in the secured data.

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]).

5.1.1 Coding of the SPI

The SPI is coded as below.

First Octet:



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

NOTE 12: In this case the counter value is used for information purposes only, (e.g. date or time stamp). If the Command Packet was successfully unpacked, the counter value can be forwarded from the Receiving Entity to the Receiving Application. This depends on proprietary implementations and happens in a application dependent way.

NOTE 23: The counter value is compared with the counter value of the last received Command Packet. This is tolerant to failures on the transport level (i.e. losses of Command Packets). A possible scenario is a global update.

NOTE 34: This provides strict control in addition to security indicated in Note 32.

5.1.4 Counter Management

If in the first SPI byte b4b5=00 (No counter available) the counter field shall be ignored by the RE and the RE shall not update the counter.

If b5 of the first SPI byte is equal to 1 then ~~T~~the following rules shall apply to counter management, with the goal of preventing replay and synchronisation attacks:

- The SE sets the counter value. It shall only be incremented.

~~- When the counter value reaches its maximum value the counter is blocked .~~

- ~~In order to prevent replay attacks t~~The RE shall update ~~increment~~ the counter to its next value upon receipt of a Command Packet after the corresponding security checks (i.e. RC/CC/DS and CNTR verification) have been passed successfully. ~~irrespective of whether or not the Command Packet could be successfully unpacked.~~

  The next counter value is the one received in the incoming message.

- When the counter value reaches its maximum value the counter is blocked.

If there is more than one SE, care has to be taken to ensure that the counter values remain synchronised between the SE's to what the RE is expecting, irrespective of the transport mechanism employed.

The level of security is indicated via the proprietary interface between the Sending/Receiving Application and Sending/Receiving Entity. Application designers should be aware that if the Sending Application requests "No RC/CC/DS" or "Redundancy Check" and "No Counter Available" from the SE, no security is applied to the Application Message and therefore there is an increased threat of malicious attack.

3GPP T3 (USIM) Meeting #20
Marseille, France, 3 - 5 September, 2001

Tdoc T3-010597

CR-Form-v3

CHANGE REQUEST

⌘ **23.048** **CR** **006** ⌘ rev **-** ⌘ Current version: **4.0.0** ⌘

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

Proposed change affects: ⌘ (U)SIM [X] ME/UE [ ] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Clarifications on padding and Anti Replay Counter Alignment with 03.48 V8.6.0 R99
Source:	⌘	T3
Work item code:	⌘	***Date:*** ⌘ 05/09/01
Category:	⌘	**A** ***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 use of the padding octets when it is necessary is not clear: the padding octets are used for ciphering. The padding octets for the calculation of RC/CC/DS are not included in the secured data.
- In the case “No counter available” in the coding of the first byte of the SPI, the counter has to be present in the message even if it is unused.
- The description of the management of the Anti Replay counter in section 5.1.4 has to be clarified depending on the value of the first octet if the SPI.
- The”next counter value” is the one received in the incoming message in the case the security checks are passed successfully.
- A CR on 03.48 R99 has not been included in 23.048 REL-4 during the conversion.

Summary of change: ⌘

- Clarify the use of padding octets.
- Clarify the case “No counter available” in the coding of the first octet of the SPI.
- Clarify the behaviour of the counter when the security checks have been passed successfully in the case b5 of the first byte of SPI is equal to 1.
- Clarify the behaviour of the counter in the case b4b5 of the first byte of SPI is equal to 00 (no counter available)
- Clarification of the Anti Replay Counter management

Consequences if not approved: ⌘

Clauses affected:	⌘	§5.1, §5.1.1, §5.1.3, §5.1.4, §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.

5.1 Command Packet structure

The Command Header precedes the Secured Data in the Command Packet, and is of variable length.

The Command Packet shall be structured according to table 1.

Table 1: Structure of the Command Packet

Element	Length	Comment
Command Packet Identifier (CPI)	1 octet	Identifies that this data block is the secured Command Packet.
Command Packet Length (CPL)	Variable	This shall indicate the number of octets from and including the Command Header Identifier to the end of the Secured Data, including any padding octets required for ciphering.
Command Header Identifier (CHI)	1 octet	Identifies the Command Header.
Command Header Length (CHL)	Variable	This shall indicate the number of octets from and including the SPI to the end of the RC/CC/DS.
Security Parameter Indicator (SPI)	2 octets	see detailed coding in section 5.1.1.
Ciphering Key Identifier (KIc)	1 octet	Key and algorithm Identifier for ciphering.
Key Identifier (KID)	1 octet	Key and algorithm Identifier for RC/CC/DS.
Toolkit Application Reference (TAR)	3 octets	Coding is application dependent.
Counter (CNTR)	5 octets	Replay detection and Sequence Integrity counter.
Padding counter (PCNTR)	1 octet	This indicates the number of padding octets used for ciphering at the end of the secured data.
Redundancy Check (RC), Cryptographic Checksum (CC) or Digital Signature (DS)	Variable	Length depends on the algorithm. A typical value is 8 octets if used, and for a DS could be 48 or more octets; the minimum should be 4 octets.
Secured Data	Variable	Contains the Secured Application Message and possibly padding octets used for ciphering.

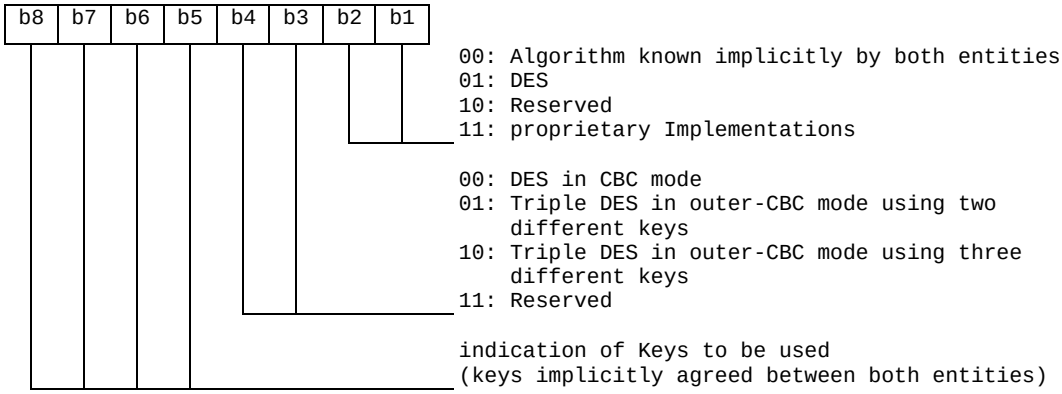
5.2 Response Packet structure

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.

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 [20].

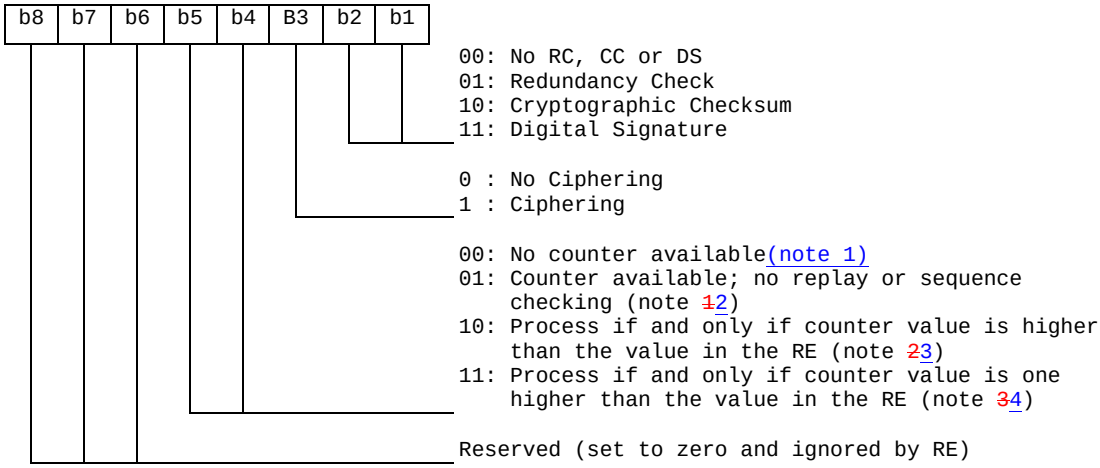
The initial chaining value for CBC modes shall be zero. For the CBC modes the counter (CNTR) shall be used. If padding is required, the padding octets shall be coded hexadecimal '00'. These octets shall not be included in the secured data.

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]).

5.1.1 Coding of the SPI

The SPI is coded as below.

First Octet:



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

NOTE 12: In this case the counter value is used for information purposes only, (e.g. date or time stamp). If the Command Packet was successfully unpacked, the counter value can be forwarded from the Receiving Entity to the Receiving Application. This depends on proprietary implementations and happens in a application dependent way.

NOTE 23: The counter value is compared with the counter value of the last received Command Packet. This is tolerant to failures on the transport level (i.e. losses of Command Packets). A possible scenario is a global update.

NOTE 34: This provides strict control in addition to security indicated in Note 32.

5.1.4 Counter Management

If in the first SPI byte b4b5=00 (No counter available) the counter field shall be ignored by the RE and the RE shall not update the counter.

If b5 of the first SPI byte is equal to 1 then ~~T~~the following rules shall apply to counter management, with the goal of preventing replay and synchronisation attacks:

- The SE sets the counter value. It shall only be incremented.

~~- When the counter value reaches its maximum value the counter is blocked .~~

- ~~In order to prevent replay attacks t~~The RE shall update ~~increment~~ the counter to its next value upon receipt of a Command Packet after the corresponding security checks (i.e. RC/CC/DS and CNTR verification) have been passed successfully. ~~irrespective of whether or not the Command Packet could be successfully unpacked.~~

  The next counter value is the one received in the incoming message.

- When the counter value reaches its maximum value the counter is blocked.

If there is more than one SE, care has to be taken to ensure that the counter values remain synchronised between the SE's to what the RE is expecting, irrespective of the transport mechanism employed.

The level of security is indicated via the proprietary interface between the Sending/Receiving Application and Sending/Receiving Entity. Application designers should be aware that if the Sending Application requests "No RC/CC/DS" or "Redundancy Check" and "No Counter Available" from the SE, no security is applied to the Application Message and therefore there is an increased threat of malicious attack.