3GPP TS 23.048 V5.9.0 (2005-06)

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Security mechanisms for the (U)SIM application toolkit; Stage 2 (Release 5)

Keywords
GSM, UMTS, SIM, USIM, SMS, card, security

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document specifies the structure of the Secured Packets in a general format and in implementations using Short Message Service Point to Point (SMS-PP) and Short Message Service Cell Broadcast (SMS-CB).

Furthermore, the coding is specified for a set of common application commands within the secured packets. This set is a subset of commands specified in 3GPP TS 51.011 [5] and allows remote management of files on the UICC in conjunction with SMS and the Data Download to UICC feature of 3GPP TS 31.111.

For UICCs based on 3GPP TS 43.019 [15], the set of commands used in the remote applet management is defined in the present document. This is based on the Open Platform card management specification [14]. For UICCs based on other technologies, other loading mechanisms may be used.

The present document is applicable to the exchange of secured packets between an entity in a 3G or GSM PLMN and an entity in the UICC.

Secured Packets contain application messages to which certain mechanisms according to 3GPP TS 22.048 have been applied. Application messages are commands or data exchanged between an application resident in or behind the 3G or GSM PLMN and on the UICC. The Sending/Receiving Entity in the 3G or GSM PLMN and the UICC are responsible for applying the security mechanisms to the application messages and thus turning them into Secured Packets.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

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

[2] 3GPP TS 22.048: "Security mechanisms for the (Universal) Subscriber Interface Module (U)SIM Application Toolkit; Stage 1".

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

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

[5] 3GPP TS 51.011 Release 4: "Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[6] 3GPP TS 31.111: "USIM Application Toolkit (USAT)".

[7] ISO/IEC 7816-4: "Information technology - Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange".

[8] Void

[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 realization of Cell Broadcast Service (CBS)".

[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".

[17] Schneier, Bruce: "Applied Cryptography Second Edition: Protocols, Algorithms and Source code in C", John Wiley & Sons, 1996, ISBN 0-471-12845-7.

[18] ETSI TS 101 220 "Smart Cards; ETSI numbering system for telecommunication application providers".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Application Layer: layer above the Transport Layer on which the Application Messages are exchanged between the Sending and Receiving Applications

Application Message: package of commands or data sent from the Sending Application to the Receiving Application, or vice versa, independently of the transport mechanism

NOTE 1: An Application Message is transformed with respect to a chosen Transport Layer and chosen level of security into one or more secured packets.

Card Manager: An application in charge of application management as defined in the Open Platform Card Specification [14].

Command Header: Security Header of a Command Packet. It includes all fields except the Secured Data

Command Packet: Secured Packet transmitted by the Sending Entity to the Receiving Entity, containing a secured Application Message

Counter: mechanism or data field used for keeping track of a message sequence

NOTE 2: This could be realised as a sequence oriented or time stamp derived value, maintaining a level of synchronisation between the Sending Entity and the Receiving Entity.

Cryptographic Checksum: string of bits derived from some secret information, (e.g. a secret key), part or all of the Application Message, and possible further information (e.g. part of the Security Header)

NOTE 3: The secret key is known to the Sending Entity and to the Receiving Entity. The Cryptographic Checksum is often referred to as Message Authentication Code.

DES: standard cryptographic algorithm specified as DEA in ISO 8731-1 [9]

Digital Signature: string of bits derived from some secret information, (e.g. a secret key), the complete Application Message, and possible further information (e.g. part of the Security Header)

NOTE 4: The secret information is known only to the Sending Entity. Although the authenticity of the Digital Signature can be proved by the Receiving Entity, the Receiving Entity is not able to reproduce the Digital Signature without knowledge of the secret information owned by the Sending Entity.

Message Identifier: two-octet field used to identify the source and type of the message

Page Parameter: single octet field used to represent the CBS page number in the sequence and the total number of pages in the SMS-CB message

Receiving Application: the entity to which the Application Message is destined

Receiving Entity: the entity where the Secured Packet is received (e.g. SMS-SC, UICC, USSD entry point, or dedicated (U)SIM Toolkit Server) and where the security mechanisms are utilised

NOTE 5: The Receiving Entity processes the Secured Packets.

Redundancy Check: string of bits derived from the Application Message and possible further information for the purpose of detecting accidental changes to the message, without the use of any secret information

Response Header: security Header of a Response Packet

Response Packet: secured Packet transmitted by the Receiving Entity to the Sending Entity, containing a secured response and possibly application data

Secured Data: field contains the Secured Application Message and possibly padding octets

Security Domain: An application in charge of security management as defined in the Open Platform Card Specification [14]

Secured Packet: information flow on top of which the level of required security has been applied

NOTE 6: An Application Message is transformed with respect to a chosen Transport Layer and chosen level of security into one or more Secured Packets.

Security Header: that part of the Secured Packet which consists of all security information (e.g. counter, key identification, indication of security level, checksum or Digital Signature)

Sender Identification: this is the simple verification of the identity of the Sending Entity by the Receiving Entity comparing the sender identity with an apriori stored identity of the sender at the Receiving Entity.

Sending Application: entity generating an Application Message to be sent

Sending Entity: this is the entity from which the Secured Packet originates (e.g. SMS-SC, UICC, USSD entry point, or dedicated (U)SIM Toolkit Server) and where the security mechanisms are invoked

NOTE 7: The Sending Entity generates the Secured Packets to be sent.

Serial Number: two octet field which identifies a particular message.

NOTE 8: It is linked to the Message Identifier and is altered every time the message is changed.

Short Message: information that may be conveyed by means of the SMS Service as defined in 3G TS 23.040 [3].

Status Code: this is an indication that a message has been received (correctly or incorrectly, indicating reason for failure).

Transport Layer: this is the layer responsible for transporting Secured Packets through the 3G and GSM network.

NOTE 9: The transport layer implements one or more transport mechanisms, (e.g. SMS or USSD).

Unsecured Acknowledgement: this is a Status Code included in a response message

3.2 Abbreviations

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

ADD	Access Domain Data
ADP	Access Domain Parameter

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

4 Overview of Security System

An overview of the secure communication related to the (U)SIM Application Toolkit together with the required security mechanisms is given in 3GPP TS 22.048, (see figure 1).

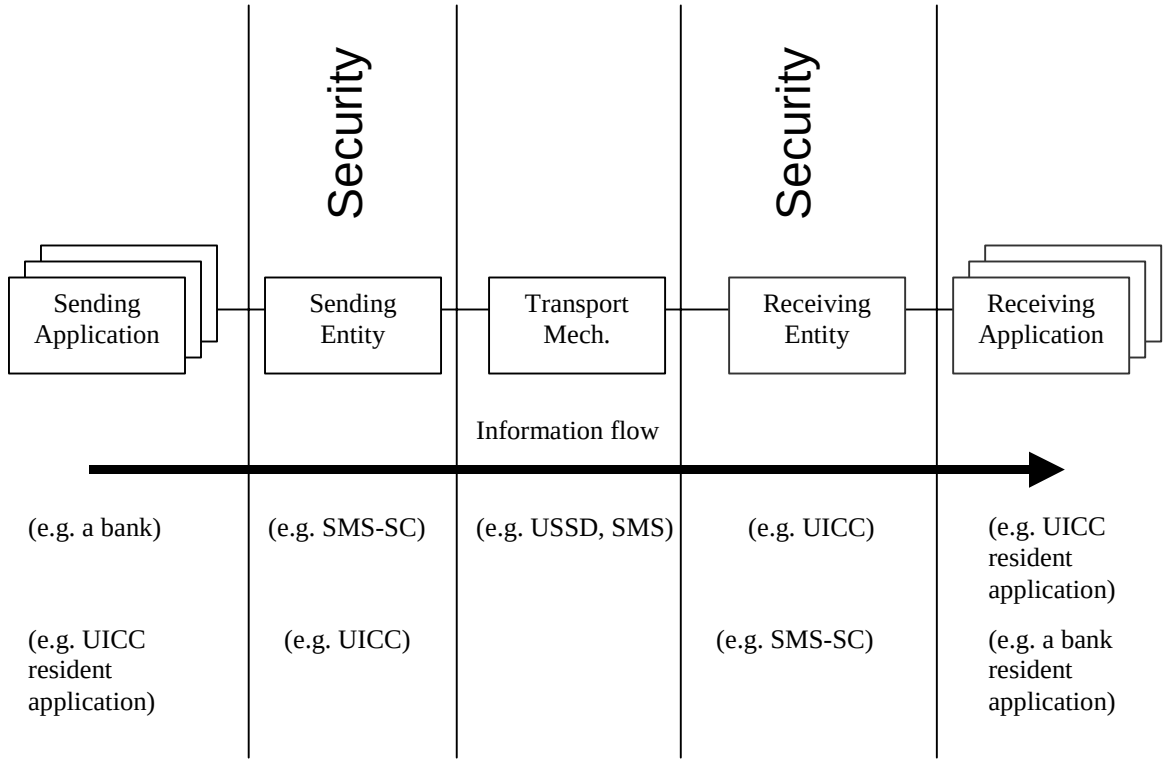


Figure 1: System Overview

The Sending Application prepares an Application Message and forwards it to the Sending Entity, with an indication of the security to be applied to the message.

The Sending Entity prepends a Security Header (the Command Header) to the Application Message. It then applies the requested security to part of the Command Header and all of the Application Message, including any padding octets. The resulting structure is here referred to as the (Secured) Command Packet.

Under normal circumstances the Receiving Entity receives the Command Packet and unpacks it according to the security parameters indicated in the Command Header. The Receiving Entity subsequently forwards the Application Message to the Receiving Application indicating to the Receiving Application the security that was applied. The interface between the Sending Application and Sending Entity and the interface between the Receiving Entity and Receiving Application are proprietary and therefore outside the scope of the present document.

If so indicated in the Command Header, the Receiving Entity shall create a (Secured) Response Packet. The Response Packet consists of a Security Header (the Response Header) and optionally, application specific data supplied by the Receiving Application. Both the Response Header and the application specific data are secured using the security mechanisms indicated in the received Command Packet. The Response Packet will be returned to the Sending Entity, subject to constraints in the transport layer, (e.g. timing).

Although there is no direct acknowledgement to an SMS-CB message in 3GPP TS 24.012 [12], the Sending Application may have requested a response. In this case a (Secured) Response Packet could be sent using a different bearer by the Receiving Application.

In some circumstances a security related error may be detected at the Receiving Entity. In such circumstances the Receiving Entity shall react according to the following rules:

1) nothing shall be forwarded to the Receiving Application. i.e. no part of the Application Message, and no indication of the error.

2) if the Sending Entity does not request a response (in the Command Header) the Receiving Entity discards the Command Packet and no further action is taken.

3) if the Sending Entity does request a response and the Receiving Entity can unambiguously determine what has caused the error, the Receiving Entity shall create a Response Packet indicating the error cause. This Response Packet shall be secured according to the security indicated in the received Command Packet.

4) if the Sending Entity does request a response and the Receiving Entity cannot determine what has caused the error, the Receiving Entity shall send a Response Packet indicating that an unidentified error has been detected. This Response Packet is sent without any security being applied.

5) If the Receiving Entity receives an unrecognisable Command Header (e.g. an inconsistency in the Command Header), the Command Packet shall be discarded and no further action taken.

5 Generalised Secured Packet structure

Command and Response Packets have the same overall structure consisting of a variable length security header within a variable length shell. To model this, use is made of a double TLV -tag, length, value- structure.

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 clause 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.

Unless indicated otherwise, the CPL and the CHL shall be coded as the lengthof BER-TLV data objects described in TS 101 220 [18].

Table 2: Linear Representation of Command Packet

CPI	CPL	CHI	CHL	SPI	KIc	KID	TAR	CNTR	PCNTR	RC/CC/DS	Secured Data with Padding
								Note 1	Note 1	Note 1	Note 1
	Note 3		Note 3	Note 2	Note 2	Note 2	Note 2	Note 2	Note 2		Note 2

NOTE 1: These fields are included in the data to be ciphered if ciphering is indicated in the Security Header.
NOTE 2: These fields are 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, the Sending Entity shall set the contents of this field to zero, and the Receiving Entity shall ignore the contents.

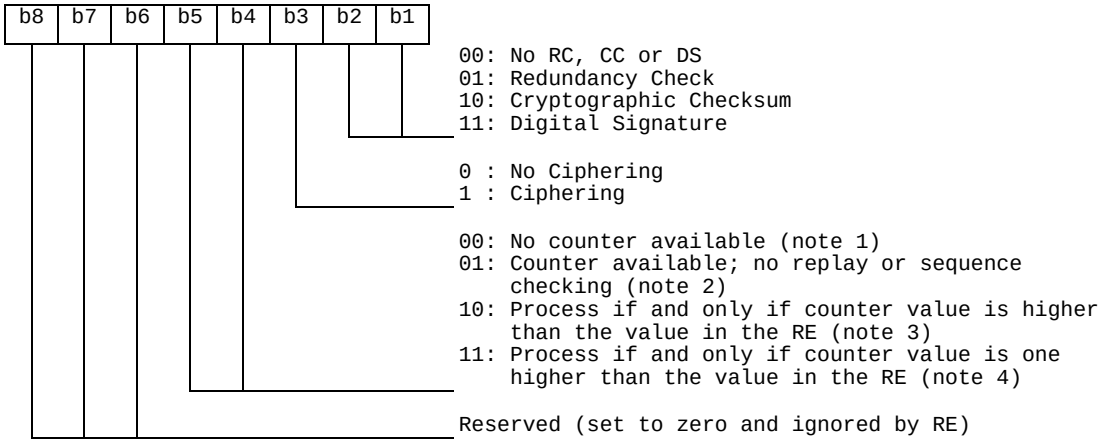
If the SPI indicates that no RC, CC or DS is present in the Command Header, the RC/CC/DS field shall be of zero length.

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

5.1.1 Coding of the SPI

The SPI is coded as below.

First Octet:



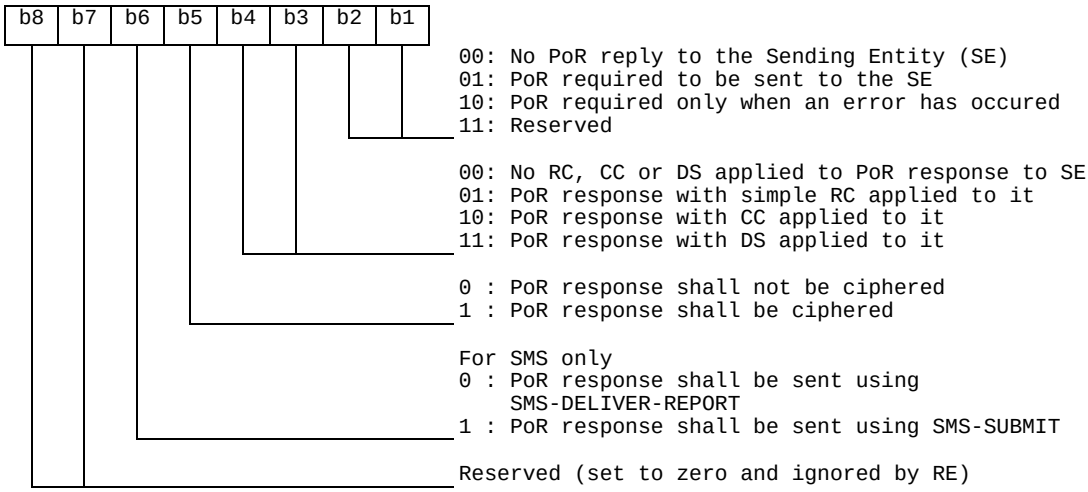
NOTE 1: In this case the counter field is present in the message.

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

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

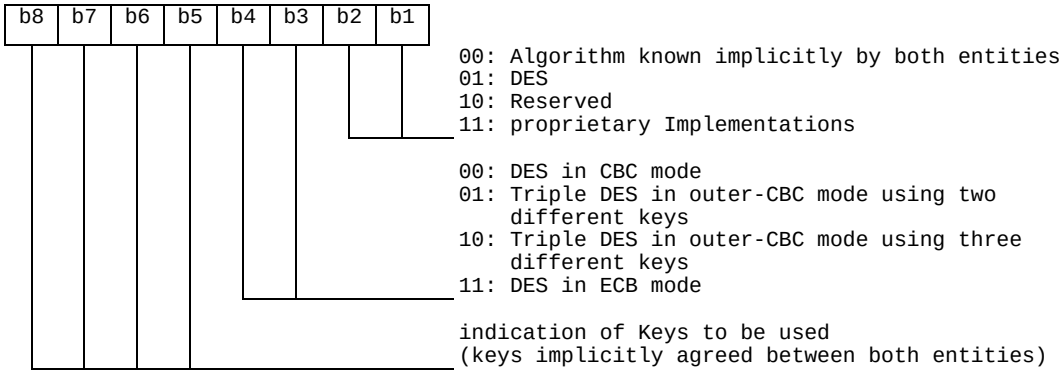
NOTE 4: This provides strict control in addition to security indicated in note 3.

Second Octet:



5.1.2 Coding of the KIc

The KIc is coded as below.



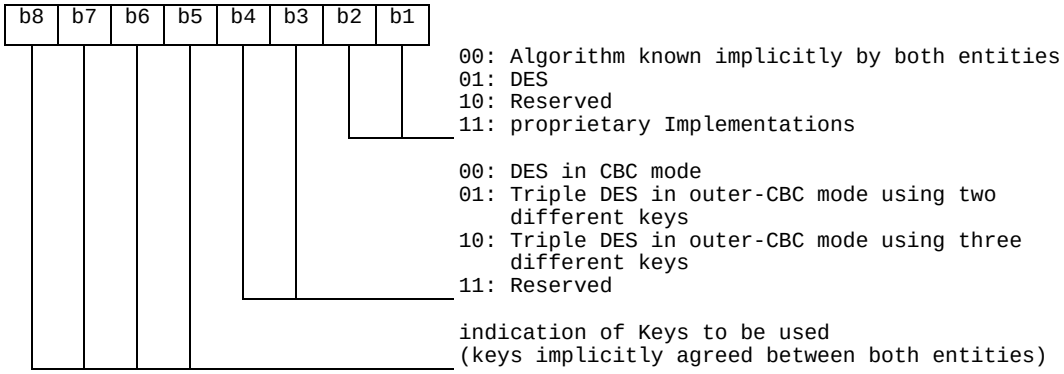
DES is the algorithm specified as DEA in ISO 8731-1 [9]. DES in CBC mode is described in ISO/IEC 10116 [10]. Triple DES in outer-CBC mode is described in section 15.2 of [17]. DES in ECB mode is described in ISO/IEC 10116 [10].

The initial chaining value for CBC modes shall be zero.

For Open Platform security architecture compliant cards see Annex B.

5.1.3 Coding of the KID

The KID is coded as below.



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

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

For Open Platform security architecture compliant cards see Annex B.

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 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 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.

For Open Platform security architecture compliant cards see Annex B.

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 TAR to the end of RC/CC/DS.
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 as the lengthof BER-TLV data objects described in TS 101 220 [18].

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
'0B' - 'FF'	Reserved for future use.

6 Implementation for SMS-PP

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

The coding of the SMS-DELIVER, SMS-SUBMIT, SMS-DELIVER-REPORT or SMS-SUBMIT-REPORT header shall indicate that the data is binary (8 bit), and not 7 bit or 16 bit. In order to invoke the UDH functionality of relevant SMS element, the UDHI bit shall be set as defined in 3GPP TS 23.040 [3]. However, in the case of a Response Packet originating from the UICC, due to the inability of the UICC to indicate to a ME that the UDHI bit should be set, the Response Packet SMS will not have the UDHI bit set, and the Sending Entity shall treat the Response Packet as if the UDHI bit was set.

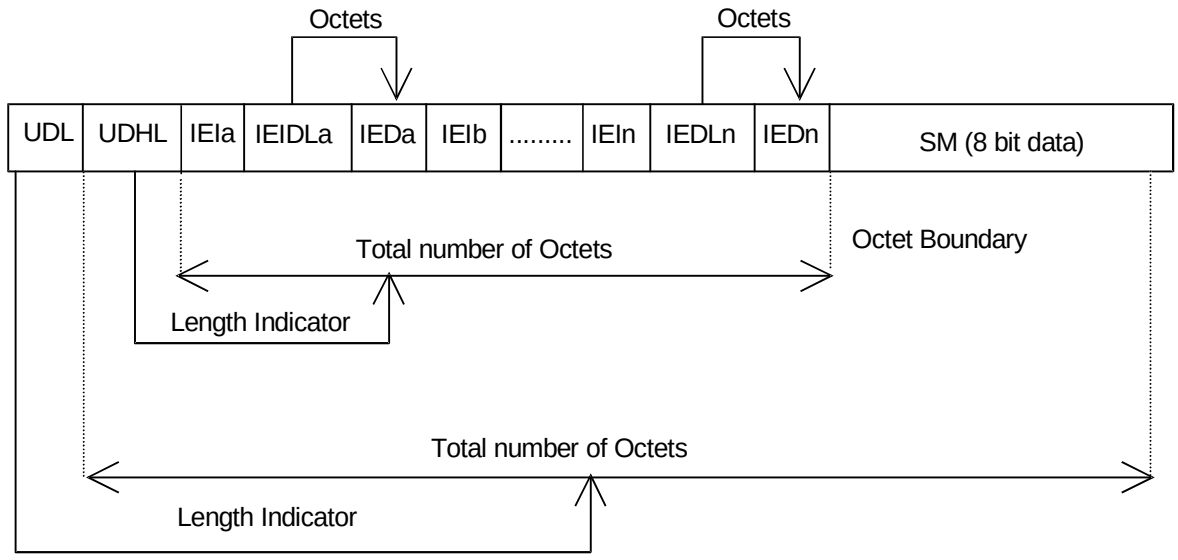


Figure 2: Structure of User Data Header in the Short Message Point to Point

The generalised structure of the UDH in the Short Message element is shown in figure 2, which is contained in the User Data part of the Short Message element. The Command Packet and the Response Packet are partially mapped into this UDH structure.

Information Element Identifiers (IEI's) values '70 - 7F' are reserved for use in the present document. Values '70' and '71' are used in the present document, values '72 - 7D' are reserved, and '7E' and '7F' are for proprietary implementations.

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

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

The relationship between the Command Packet and its inclusion in the UDH structure of a single Short Message with no other UDH elements is indicated in table 6.

Table 6: Relationship of Command Packet in UDH for single Short Message Point to Point

SMS specific elements	Generalised Command Packet Elements (Refer to table 1)	Comments
UDL		Indicates the length of the entire SM.
UDHL	='02'	The first octet of the content or User Data part of the Short Message itself. Length of the total User Data Header, in this case, includes the length of IEIa + IEIDLa + IEDa (see figure 2), and is '02' in this case.
IEIa	CPI= '70'	Identifies this element of the UDH as the Command Packet Identifier. This value is reserved in 3GPP TS 23.040 [3].
IEIDLa	='00'	Length of this object, in this case the length of IEDa, which is zero, indicating that IEDa is a null field..
IEDa		Null field.
SM (8 bit data)	Length of Command Packet (2 octets)(note)	Length of the Command Packet (CPL), coded over 2 octets, and shall not be coded as the lengthof BER-TLV data objects described in TS 101 220 [18].
	Command Header Identifier	(CHI) Null field.
	Length of the Command Header	Length of the Command Header (CHL), coded over one octet, and shall not be coded as the lengthof BER-TLV data objects described in TS 101 220 [18].
	SPI to RC/CC/DS in the Command Header	The remainder of the Command Header.
	Secured Data	Application Message, including possible padding octets.

NOTE: Whilst not absolutely necessary in this particular instance, this field is necessary for the case where concatenated Short Message is employed (see clause 6.3).

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

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

6.3 A Command Packet contained in Concatenated Short Messages Point to Point

If a Command Packet is longer than 140 octets (including the Command Header), it shall be concatenated according to 3GPP TS 23.040 [3]. In this case, the entire Command Packet including the Command Header shall be assembled, and then separated into its component concatenated parts. The first Short Message shall contain the concatenation User Data Header and the Command Packet Identifier in the UDH in no particular order. Subsequent Short Messages shall contain only the concatenation User Data Header. The concatenation Header contains a Reference number that will allow the Receiving Entity to link individual Short Messages together to re-assemble the original Command Packet before unpacking the Command Packet.

The relationship between the Command Packet and its inclusion in the structure of the first concatenated Short Message is indicated in table 7; the ordering of the various elements of the UDH is not important.

Table 7: Relationship of Command Packet in UDH for concatenated Short Message Point to Point

SMS specific elements	Generalised Command Packet Elements (Refer to table 1)	Comments
UDL		Indicates the length of the entire SM
UDHL	='07'	The first octet of the content or User Data part of the Short Message itself. Length of the total User Data Header, in this case, includes the length of IEIa + IEIDLa + IEDa + IEIb + IEIDLb + IEDb (see figure 2), which is '07' in this case.
IEIa	'00', indicating concatenated short message	identifies this Header as a concatenation control header defined in 3GPP TS 23.040 [3].
IEIDLa	Length of Concatenation header	length of the concatenation control header (= 3).
IEDa	3 octets containing data concerned with concatenation	These octets contain the reference number, sequence number and total number of messages in the sequence, as defined in 3GPP TS 23.040 [3].
IEIb	CPI= '70'	Identifies this element of the UDH as the Command Packet Identifier.
IEIDLb	='00'	Length of this object, in this case the length of IEDb alone, which is zero, indicating that IEDb is a null field.
IEDb		Null field.
SM (8 bit data)	Length of Command Packet (2 octets)	Length of the Command Packet (CPL), coded over 2 octets, and shall not be coded as the lengthof BER-TLV data objects described in TS 101 220 [18].
	Command Header Identifier	(CHI) Null field.
	Length of the Command Header	Length of the Command Header (CHL), coded over one octet, and shall not be coded as the lengthof BER-TLV data objects described in TS 101 220 [18].
	SPI to RC/CC/DS in the Command Header	The remainder of the Command Header.
	Secured Data (part)	Contains the first portion of the Secured Data. The remaining Secured Data will be contained in subsequent concatenated short messages.

In the case where the Command Packet requires to be concatenated, then in table 7, IEIa identifies the concatenation control element of the Short Message, and is repeated in each subsequent Short Message in the concatenated series. In the first Short Message alone, in this example, IEIb identifies the Command Packet, which indicates that the first portion of the content of the Short Message contains the Command Header, which is followed immediately by the secured data as the SM part in table 7. In the first Short Message, the UDHL field contains the length of the concatenation control and the Command Packet Identifier, whereas in subsequent Short Message's in the concatenated series, the UDHL contains the length of the concatenation control only, as there is no subsequent Command Header.

If the data is ciphered, then it is ciphered as described above, before being broken down into individual concatenated elements. The concatenation control portion of the UDH in each SM shall not be ciphered.

In order to achieve a modulo 8 length of the data before the RC/CC/DS field in the Command Header, the Length of the Command Packet and the Length of the Command Header shall be included in the calculation of RC/CC/DS if used. These fields shall not be ciphered.

An example illustrating the relationship between a Command Packet split over a sequence of three Short Messages is shown below.

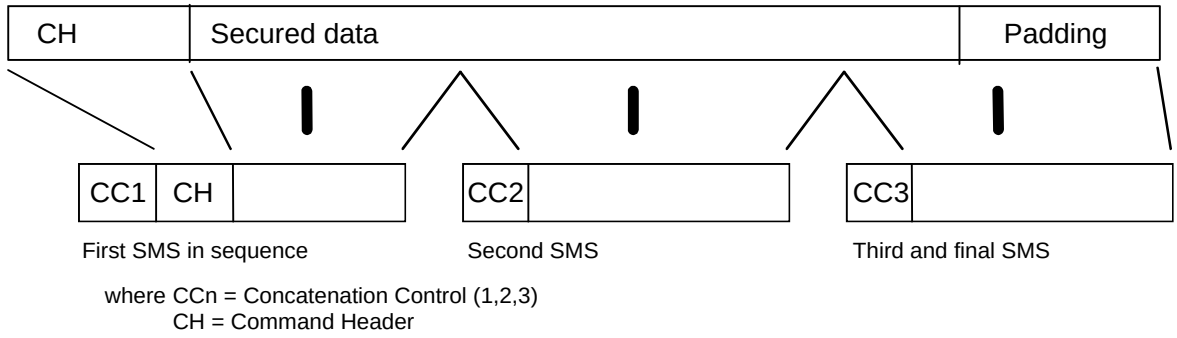


Figure 3: Example of command split using concatenated point to point SMS

6.4 Structure of the Response Packet

The Response Packet is as follows. This message is generated by the Receiving Entity and possibly includes some data supplied by the Receiving Application, and returned to the Sending Entity/Sending Application. In the case where the Receiving Entity is the UICC, depending on bit 6 of the second octet of the SPI, this Response Packet is generated on the UICC, either:

- retrieved by the ME from the UICC, and included in the User-Data part of the SMS-DELIVER-REPORT returned to the network;

or

- retrieved by the ME from the UICC using the Send Short Message proactive command.

Table 8: Relationship of Response Packet in UDH

SMS-REPORT specific elements	Generalised Response Packet Elements (Refer to table 3)	Comments
UDL		Indicates the length of the entire SMS
UDHL	='02'	The first octet of the content of the SMS itself. Length of the total User Data Header, in this case, includes the length of IEIa + IEIDLa + IEDa.
IEIa	RPI= '71'	Identifies this element of the UDH as the Response Packet Identifier. This value is reserved in 3GPP TS 23.040 [3].
IEIDLa	='00'	Length of this object, in this case the length of IEDa alone, which is zero, indicating that IEDa is a null field.
IEDa		Null field.
SM (8 bit data)	Length of Response Packet	Length of the Response Packet (RPL), coded over 2 octets, and shall not be coded as the lengthof BER-TLV data objects described in TS 101 220 [18]. (see note)
	Response Header Identifier	(RHI) Null field.
	Length of the Response Header	Length of the Response Header (RHL), coded over one octet, and shall not be coded as the lengthof BER-TLV data objects described in TS 101 220 [18].
	TAR to RC/CC/DS elements in the Response Header	The remainder of the Response Header.
	Secured Data	Additional Response Data (optional), including padding octets.

NOTE: This field is not absolutely necessary but is placed here to maintain compatibility with the structure of the Command Packet when included in a SMS-SUBMIT or SMS-DELIVER.

In order to achieve a modulo 8 length of the data before the RC/CC/DS field in the Response Header, the Length of the Response Packet, the Length of the Response Header and the three preceding octets (UDHL, IEIa and IEIDLa in the above table) shall be included in the calculation of RC/CC/DS if used. These fields shall not be ciphered.

The structure of an SMS-DELIVER/SUBMIT-REPORT User Data object is very similar to that of the SMS-SUBMIT or SMS-DELIVER, see 3GPP TS 23.040 [3].

7 Implementation for SMS-CB

7.1 Structure of the CBS page in the SMS-CB Message

The CBS page sent to the MS by the BTS is a fixed block of 88 octets as coded in GSM 24.012 [12]. The 88 octets of CBS information consist of a 6-octet header and 82 user octets.

The 6-octet header is used to indicate the message content as defined in 3GPP TS 23.041 [11]. This information is required to be transmitted unsecured in order for the ME to handle the message in the correct manner (e.g. interpretation of the DCS).

The content of the message shall be secured as defined in this clause.

A range of values has been reserved in 3GPP TS 23.041[11] to indicate SMS-CB Data Download messages that are secured and unsecured. A subset of these values is used to indicate the Command Packet for CBS messages. This range is from (hexadecimal) '1080' to '109F' and is included in the structure of the Command Packet as illustrated in table 9.

7.2 A Command Packet contained in a SMS-CB message

The relationship between the Command Packet and its inclusion in the SMS-CB message structure is indicated in table 9.

Table 9: Relationship of Command Packet in the first CBS page of an SMS-CB message

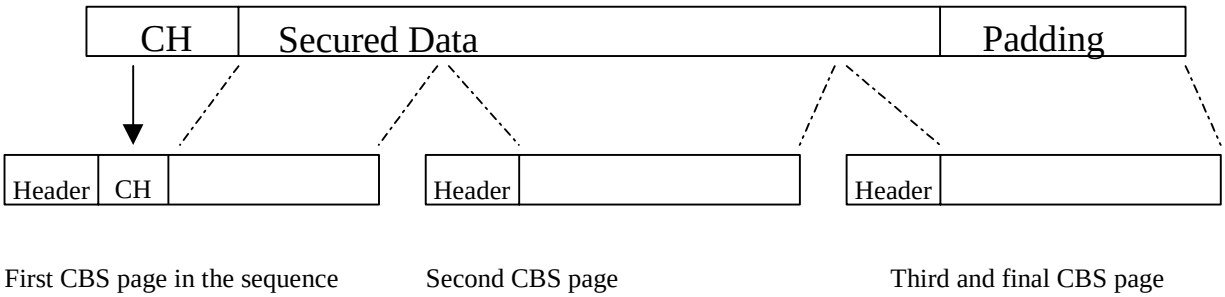
SMS-CB specific elements	Generalised Command Packet Elements (Refer to table 1)	Comments
SN		Refer to 3GPP TS 23.041[11]. Coded on 2 octets containing the ID of a particular message.
MID	CPI='1080' to '109F'	Coded on 2 octets containing the source and type of the message. The Command Packet Identifier range is reserved in 3GPP TS 23.041[11]. (see note)
DCS		Refer to 3GPP TS 23.041[11]. Coded on 1 octet containing the alphabet coding and language as defined in GSM 23.038[13].
PP		Refer to 3GPP TS 23.041[11]. Coded on 1 octet to indicate the page number and total number of pages.
Content of Message	CPL	Length of the Command Packet, coded over 2 octets, and shall not be coded as the lengthof BER-TLV data objects described in TS 101 220 [18].
	CHI	The Command Header Identifier. Null field.
	CHL	This shall indicate the number of octets from and including the SPI to the end of the RC/CC/DS field. Binary coded over 1 octet.
	SPI to RC/CC/DS in the Command Header	The remainder of the Command Header.
	Secured Data	Application Message, including possible padding octets.

NOTE: Generally, the CPI is coded on 1 octet, as specified in table 1. However, the CPI for the SMS-CB message is coded on 2 octets as the values reserved in 3GPP TS 23.041 [11] to identify the Command Packet are MID values which are coded on 2 octets.

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

Securing of the complete CBS message is achieved outside the GSM specifications by the Sending Entity. The Secured CBS message is formatted in accordance with the GSM specifications and transmitted to the MS as CBS pages. The CBS pages are received by the ME and sent directly to the UICC, by analysing the MID value. The UICC shall then reassemble, decrypt and process the message.

An example illustrating the relationship between a Command Packet split over a sequence of three SMS-CB pages is shown below.



First CBS page in the sequence Second CBS page Third and final CBS page

In the above figure, Header = 6 Octet header as defined in GSM 03.41 (i.e. SN, MID, DCS and PP) and CH = Command Header

Figure 4: Example of command split using concatenated CB SMS

7.3 Structure of the Response Packet for a SMS-CB Message

As there is no response mechanism defined for SMS-CB, there is no defined structure for the (Secured) Response Packet. However, if a (Secured) Response Packet is sent via another bearer the structure shall be defined by the Receiving Application.

8 Standardised (U)SIM toolkit commands for Remote File Management

There are two elements to Remote File Management on the UICC; the first is the behaviour of the UICC resident Toolkit Application which performs the Remote File Management, and the second is the command structure in the SIM Data Download message, see 3GPP TS 31.111 [6]. Access conditions for the 3G and GSM files as seen by the UICC resident application, are not standardised. These are under the control of the application designer, in co-operation with the Network Operator or Service Provider owning the UICC. These access conditions may be dependent on the level of security applied to the Data Download to UICC message (e.g. SMS-PP).

8.1 Behaviour of the Remote File Management Application

1. The parameter(s) in the Data Download Message to UICC is either a single command, or a list of commands, which shall be processed sequentially.

2. The application shall take parameters from the Data Download Message to UICC and shall act upon the 3G and/or GSM files according to these parameters.

3. A Command "session" is defined as starting upon receipt of the parameter/command list, and ends when the parameter list in the Data Download Message to UICC is completed, or when an error is detected which shall halt further processing of the command list.

4. At the beginning and end of a Command "session" the logical state, (e.g. file pointers) of the UICC as seen from the ME shall not be changed to an extent sufficient to disrupt the behaviour of the ME. If changes in the logical state have occurred that the ME needs to be aware of, the application on the UICC may issue a REFRESH command according to 3GPP TS 31.111 [6]. However, this is application dependent and therefore out of scope of the present document.

5. The following directory shall be implicitely selected and be the current directory at the beginning of a Command "session" :

   - the MF for a Command "session" sent to a UICC Shared File System (as defined in TS 101 220 [18]) or SIM File System (as defined in TS 101 220 [18]) Remote File Management Application,

   - the ADF for a Command "session" sent to a USIM File System (as defined in TS 101 220 [18]) Remote File Management Application.

8.2 Coding of the commands

A command string may contain a single command or a sequence of commands. Each command is coded according to the generalised structure defined below; each element other than the Data field is a single octet; see 3GPP TS 51.011 [5].

Class byte (CLA)	Instruction code (INS)	P1	P2	P3	Data

If a command has P3='00', then the UICC shall send back all available response parameters/data.

Administrative commands have not yet been defined, and thus, remain proprietary to UICC manufacturers for the present.

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

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 commands

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

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

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

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

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

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

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

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

If a proof of Receipt is required by the sending entity, the Additional Response Data sent by the Remote File Management Application shall be formatted according to table 14:

Table 14: Format of additional response data

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

8.4 void

9 Open Platform commands for Remote Applet Management

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

9.1 Remote Applet Management Application behaviour

9.1.1 Package Loading

The Package Loading process allows the Network Operator or Service Provider to load new packages onto the UICC. The Network Operator or Service Provider manages the loading of a package through a loading session with the card.

A loading session consists of the sequence of commands as described in Figure 5.

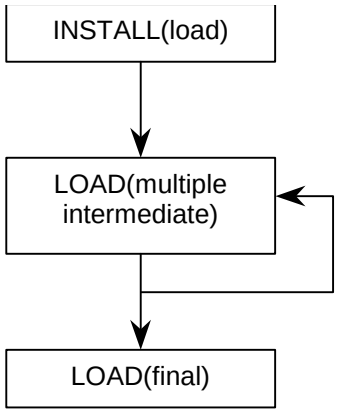


Figure 5: Loading session sequence of commands

Depending on the applet size, several SMS might be use for the package loading.

The commands are defined in Annex A.

9.1.2 Applet Installation

The Applet Installation process allows the Network Operator or Service Provider to install a new application onto the UICC . The installation may only be performed if the corresponding package has already been loaded onto the card. The Applet Installation is performed using the INSTALL(install) command, as defined in annex A.

9.1.3 Package Removal

The Package Removal process is performed using the DELETE command, as defined in annex A. The Package removal procedure shall be performed by the UICC as defined below:

1. If non removed applications installed from this package remain, the card shall reject the removal with the corresponding status error code.

2. If the package is referred by other package(s), the card shall reject the removal with the corresponding status error code.

9.1.4 Applet Removal

The Applet Removal process shall be performed using the DELETE command, as defined in Annex A. The UICC shall remove the components that make up the applet.

9.1.5 Applet Locking / Unlocking

The Applet locking (and unlocking) procedure allows the Network Operator or Service Provider to disable (and enable) an applet using the SET STATUS command as defined in Annex A. When an applet is locked, it shall not be possible to be triggered or selected, and all of its menu entries will be disabled (i.e. removed from the SET UP MENU command).

9.1.6 Applet Parameters Retrieval

The Applet Parameters Retrieval procedure allows the Network Operator or Service Provider to remotely request the parameters of an applet. This procedure is performed using the GET DATA command as defined in annex A.

9.2 Commands coding

Commands are coded as for the Remote File Management procedure, each command is coded as an APDU.

The messages for the Card Manager shall have a TAR value set to '000000' in hexadecimal.

9.2.1 Input Commands

The following table extends table 10 defined in clause 8.2.1.

Table 15: Applet Management input commands

Operational command
DELETE
SET STATUS
INSTALL
LOAD
PUT KEY

9.2.2 Output Commands

The following table extends table 11 defined in 8.2.2.

Table 16: Applet Management output commands

Operational command
GET STATUS
GET DATA

9.3 Response Packets

9.3.1 (U)SIM Response Packets

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

9.3.2 void

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

A.1 Applet Management Commands for TS 43.019 compliant cards

This chapter describes the commands for Applet Management.

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

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

A.1.1 Commands Description

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

A.1.1.1 DELETE

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

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

A.1.1.2 GET DATA

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

The command Get Data is extended to retrieve specific card information with tag values in P1 and P2. The following values have been defined:

- 'FF 1F': Menu Parameters Tag, this retrieves the menu parameters of an applet;
- 'FF 20': Card Resources Tag, this retrieves information on the card resources used and available;
- 'FF 21' to 'FF 7F': reserved for allocation in the present document.

A.1.1.2.1 Menu Parameters

The following format is used to code the command data :

Bytes	Description	Length
1	Application AID tag = '4F'	1
2	Application AID length	1
3 - (X+2)	Application AID	X = 5 - 16

After the successful execution of the command, the following data is returned by a GET RESPONSE command:

Bytes	Description	Length
1	First item position	1
2	First item identifier	1
…	…	…
X - 1	Last item position	1
X	Last item identifier	1

A.1.1.2.2 Card Resources Information

After the successful execution of the command, the following data is returned:

Bytes	Description	Length
1-2	Free E²PROM	2
3	Number of installed applets	1

A.1.1.3 GET STATUS

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

A.1.1.4 INSTALL

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

A.1.1.4.1 Install (Load)

The Load File DAP field is a Cryptographic Checksum, a Digital Signature or a Redundancy Check calculated over the CAP file as transmitted in the subsequent Load commands. The exact generation of this field is outside the scope of the present document. If a DES algorithm in CBC mode is used the initial chaining value shall be zero. If padding is required, the padding octets shall be coded hexadecimal '00'.

NOTE: The Load File DAP CC, DS or RC is verified by the Card Manager.

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

Presence	Length	Name
Mandatory	1	Tag of System Parameters constructed field 'EF'
	1	Length of System Parameters constructed field
	4-n	System Parameters constructed value field.

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

Presence	Length	Name
Mandatory	1	Tag of non volatile memory space required for package loading field: 'C6'
	1	Length of non volatile memory space required for package loading field
	2	Non Volatile memory space (in bytes) required for package loading (see note)
Optional	1	Tag of non volatile memory requirements for installation field: 'C8'
	1	Length of non volatile memory requirements for installation
	2	Non volatile memory required for installation in byte
Optional	1	Tag of volatile memory requirements for installation field: 'C7'
	1	Length of memory requirements for installation
	2	Volatile memory required for installation in byte
NOTE: The memory space required indicates the minimum size that shall be available onto the card to download the application. The UICC must reject the applet downloading if the required size is not available on the card.		

A.1.1.4.2 Install (Install)

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

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

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

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

Presence	Length	Name
Mandatory	1	Tag of non volatile memory requirements for installation field: 'C8'
	1	Length of non volatile memory requirement for installation (see A.1.1.4.2.2)
	2	Non volatile memory required for installation in byte (see A.1.1.4.2.2)
Mandatory	1	Tag of volatile memory requirements for installation field: 'C7'
	1	Length of volatile memory requirement for installation (see A.1.1.4.2.2)
	2	Volatile memory required for installation in byte (see A.1.1.4.2.2)
Conditional (see Note)	1	Tag of toolkit applet specific parameters field: 'CA'
	1	Length of toolkit applet specific parameters field
	6-n	Toolkit Applet specific Parameters (see A.1.1.4.2.1)
Note: This TLV object is mandatory for Applets implementing the *ToolkitInterface* as defined in TS 43.019 [15].		

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

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

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

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

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

A.1.1.4.2.1 Toolkit Applet Specific Parameters

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

Presence	Length	Name	Value
Mandatory	1	Length of Access Domain field	
Mandatory	1-p	Access Domain (see A.1.1.4.2.3)	
Mandatory	1	Priority level of the Toolkit applet instance (see A.1.1.4.2.4)	
Mandatory	1	Maximum number of timers allowed for this applet instance	
Mandatory	1	Maximum text length for a menu entry	
Mandatory	1	Maximum number of menu entries allowed for this applet instance	= m
Conditional See Note 1	/	Position of the first menu entry ('00' means last position)	
Conditional See Note 1	|	Identifier of the first menu entry ('00' means don't care)	
Conditional See Note 1	2*m bytes |	….	
Conditional See Note 1	|	Position of the last menu entry ('00' means last position)	
Conditional See Note 1	\	Identifier of the last menu entry ('00' means don't care)	
Optional	1	Maximum number of channels for this applet instance	
Optional	1	Length of Minimum Security Level field	
Conditional See Note 2	0-q	Minimum Security Level (MSL) (see A.1.1.4.2.5)	

The Presence column specifies whether it is mandatory or optional or conditional to include the corresponding parameter in the command data. If an optional parameter is included, then all the previous parameters in the above table shall be included also.
Note 1: The Position and the Identifier of a menu entry are mandatory if m is greater than 0.
Note 2: The MSL shall be included in the Toolkit Applet Specific Parameters if the length of MSL field is greater than 0.

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

The following default values shall be assigned to the application for the following parameters if not present in the command data:

Name	Value
Maximum number of channels for this applet instance	See Note
Length of Minimum Security Level field	'00'
Note: This value shall be configurable by the card issuer.	

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

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

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

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

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

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

A.1.1.4.2.2 Memory space

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

A.1.1.4.2.3 Access domain

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

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

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

A.1.1.4.2.3.1 Access Domain Parameter

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

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

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

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

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

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

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

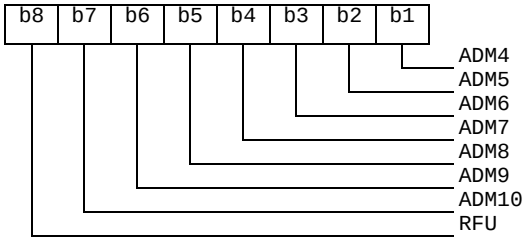
A.1.1.4.2.3.2 APDU access mechanism

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

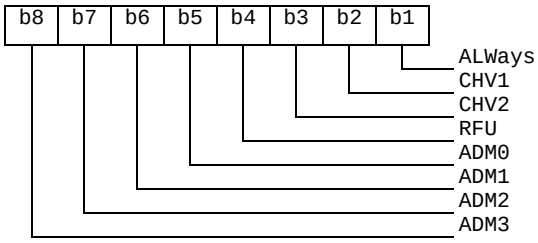
The APDU Access Domain Data is a bit map combination of the file access condition levels described in 3GPP TS 51.011. When the bit is set the associated Access Condition is granted.

The APDU Access Domain Data is coded as follows:

Byte 1:



Byte 2:



EXAMPLE: Possible combinations of fulfilled Access Conditions are shown below:

ADD value	Applet access condition fulfilled
'00 00'	No access
'00 01'	ALWays
'00 02'	CHV1
'00 03'	ALWays and CHV1
'00 04'	CHV2
'00 05'	ALWays and CHV2
'00 06'	CHV1 and CHV2
:	:
'00 10'	ADM0
:	:
'00 20'	ADM1
:	:
'00 22'	ADM1 and CHV1
:	:
'01 00'	ADM4
:	:
'40 00'	ADM10
:	:
'41 37'	ADM10 and ADM4 and ADM1 and ADM0 and CHV2 and CHV1 and ALWays
:	:

A.1.1.4.2.3 3GPP Access Mechanism

TBD

A.1.1.4.2.4 Priority level of the Toolkit applet

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

- '00' : RFU
- '01' : Highest priority level

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

A.1.1.4.2.5 Coding of the Minimum Security Level

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

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

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

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

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

A.1.1.4.2.5.1 MSL Parameter

The possible values for the MSL Parameter are:

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

A.1.1.4.2.5.2 Minimum SPI1

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

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

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

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

A.1.1.5 LOAD

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

The load block data is created by taking successive blocks of the data from the Java Card CAP file components in the order described in the Java Card specification.

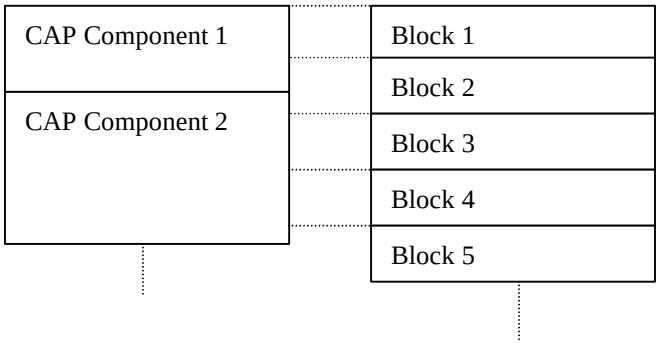


Figure 6: Relationship between CAP File components and Load File Blocks

A.1.1.6 SET STATUS

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

A.1.1.7 PUT KEY

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

The keys which may be updated by the PUT KEY command refer to the transport security keys, i.e. KID and KIc in a Secured Packet. In addition, a third key type is defined: KIK. This key is used to encrypt the key data value of the PUT KEY command.

One or several keys within an existing key set version may be replaced using the Put Key command.

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

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

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

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

Key Sets can only be changed with the PUT KEY command once the card has been issued. New Key Sets cannot be created using PUT KEY command at post issuance. Key used for securing the PUT KEY command is the key index 3 of the same key set version as the changed key. Key Set version 0 defined in OP for the creation of keys is not relevant for the present document.

A key set version number shall never be updated using the PUT KEY command.

This command shall be executed by the Card Manager or a Security Domain depending on the TAR in the case of Over The Air Application Management.

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

A.2.1 Minimum Security Level

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

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

A.2.2 Remote File Management Access Conditions

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

A.3 Security Management for Applet Management using APDUs

A.3.1 Selection of Card Manager and Security Domain

This topic is for further study.

A.3.2 Mutual authentication

This topic is for further study.

A.3.3 APDU's DAP Computation

This topic is for further study.

Annex B (normative): Relation between security layer and Open Platform security architecture

This annex only applies to cards implementing the security architecture defined in the Open Platform Card Specification [14].

The security of Application Messages (i.e. RC/CC/DS, ciphering/deciphering, counter management) shall be managed by the Security Domain of the Application.

B.1 Key set version - counter association within a Security Domain

A separate and different counter shall be associated to each key set version as described in the following table:

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

B.2 Security keys KIc, KID

The indication of the key to be used in the KIc and KID fields shall refer 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 Card specification [14]).

The key set version number indicated in the KIc and KID fields shall be identical when different from 0. If the key set version numbers are different (and both different from 0) then the message shall be rejected with the “Unidentified security error” Response Status Code.

Annex C (informative): Change History

This annex lists all changes made to the present document since its initial approval.

Meeting	Plenary Tdoc	WG tdoc	VERS	CR	REV	REL	CAT	SUBJECT	Resulting Version
s24	0888/97		2.0.1					GSM 03.48 approved by SMG plenary #24 (December 1997)	5.0.0
s25	98-0159	98p069	5.0.0	A001		R97	F	User data header indication for secure messaging.	6.0.0
s26	98-0401	98p250	6.0.0	A002		R97	F	RP-ACK RP-ERROR for SIM data download error	6.1.0
s28	P-99-183	98p430	6.1.0	A003		R97	F	Clarification about the CHI field in the command packet and RHI field in the response packet	7.0.0
	P-99-183	99p069		A004	1	R98	C	Modification for networks not supporting RP-ACK	
s29	P-99-411	9-99-202	7.0.0	A006		R99	B	Enhancement to incorporate Cell Broadcast Messages	8.0.0
s30	P-99-669	9-99-312	8.0.0	A007	2	R99	B	SIM Toolkit Applications loading and management	8.1.0
s31	P-00-136	9-00-131	8.1.0	A008		R99	F	Alignment of 03.48 with updated OP specification	8.2.0
	P-00-136	9-00-135		A009		R99	F	Enhancement to allow data sharing	
	P-00-136	9-00-136		A010		R99	F	Clarification of proof of receipt	
Note: SMG #31 agreed to transfer this specification to the 3GPP. Thus, CRs listed below were approved at 3GPP TSG-T									
TP-08	TP-000098	T3-000288	8.2.0	A011		R99	F	Clarification of the TAR for the Card Manager	8.3.0
TP-09	TP-000147	T3-000458	8.3.0	A012		R99	F	Modification of the fields to be included in the 03.48 response packet checksum computation.	8.4.0
	TP-000147	T3-000462		A013		R99	F	Clarification of the KID and KIC fields for Open Platform keys.	
	TP-000147	T3-000451		A014		R99	F	Clarification on Access Domain parameters in Install(Install) command	
TP-11	TP-010037	T3-010107	8.4.0	A015		R99	F	Clarification of the Anti Replay Counter management	8.5.0
TP-12	TP-010104	T3-010410	8.5.0	A017		R99	F	Correction to the Open Platform specification reference	5.0.0
	TP-010104	T3-010434		A018		Rel-4	F	Alignment with 3G release-4 specifications *NOTE: This CR (A018) converts the terminology in the specification to apply to both GSM and 3G. With this change, the specification number changes from TS 03.48 to TS 23.048.*	
	TP-010104	T3-010371		A016		Rel-5	B	Support of the bearer independent protocol feature	
TP-13	TP-010201	T3-010545	5.0.0	002		Rel-5	A	Correction to APDU access mechanism in annex A	5.1.0
	TP-010201	T3-010599		004		Rel-5	A	USIM input and output commands for Remote File management	
	TP-010201	T3-010597		006		Rel-5	A	Clarifications on padding and Anti Replay Counter	
TP-14	TP-010242	T3-010776	5.1.0	007		Rel-5	B	Definition of a Minimum Security Level	5.2.0
	TP-010242	T3-010777		008		Rel-5	C	Maximum number of timer allowed for applet instance	
	TP-010242	T3-010782		012		Rel-5	A	Clarification of the APDU Access Domain	
	TP-010242	T3-010784		014		Rel-5	A	Clarification on computation of DES in CBC mode	
	TP-010242	T3-010789		016		Rel-5	A	Correction of Response Header Length (RHL) definition	
TP-15	TP-020063	T3-020111	5.2.0	017		Rel-5	B	Define link between Open Platform Security Domain and 23.048 secure messaging	5.3.0
	TP-020063	T3-020113		019		Rel-5	F	Clarifications on Access Domain Parameter	
TP-17	TP-020209	T3-020661	5.3.0	020		Rel-5	F	Maximum number of channels allowed for this applet instance	5.4.0
		T3-020672		021		Rel-5	A	Clarification on computation of DES in CBC mode	
		T3-020673		022		Rel-5	F	Clarification on Put Key command	
		T3-020676		023		Rel-5	F	USIM specific behaviour for Response Packets (Using SMS-PP)	
		T3-020675		024		Rel-5	F	Toolkit Access with modified secret code status	
		T3-020638		025		Rel-5	F	Clarification on letter “n” describing the length of parameters of the Install(Install) command	
		T3-020674		026		Rel-5	F	Minimum Security Level for the Remote Management Applications and Access conditions for Remote File Management Application.	
TP-18	TP-020284	T3-020887	5.4.0	027		Rel-5	F	Clarification of the Install(Install) command in case of installing a non Toolkit Applet	5.5.0
		T3-020894		028		Rel-5	F	Clarification on the RC/CC/DS coding in SPI2	
		T3-020929		029		Rel-5	F	Mandatory/Optional/Conditional data in the Toolkit Applet Specific Parameters field	
TP-19	TP-030025	T3-030142	5.5.0	030		Rel-5	F	Starting directory for the RFM Applications	5.6.0
		T3-030164		031		Rel-5	F	Correction on behaviour for Response Packet	
		T3-030200		033		Rel-5	F	Implementation for SMS-CB in 3G	
		T3-030193		034		Rel-5	F	Default values assigned to the application for optional parameters if not present in the install(install) command data.	
TP-20	TP-030119	T3-030440	5.6.0	035		Rel-5	F	Correction of the ’System Parameters constructed value field’	5.7.0
TP-22	TP-030257	T3-031003	5.7.0	036		Rel-5	F	Cell Broadcast Data Download secure messages in UMTS	5.8.0
CP-28	CP-050136	C6-050476	5.8.0	038		Rel-5	F	ISO/IEC 7816-Series Revision	5.9.0