TS 101 181 V6.1.0 (1998-07)

Technical Specification

Digital cellular telecommunications system (Phase 2+); Security Mechanisms for the SIM application toolkit; Stage 2 (GSM 03.48 version 6.1.0 Release 97)

GLOBAL SYSTEM FOR
MOBILE COMMUNICATIONS

Reference

RTS/SMG-090348Q6R1 (axo030c3.PDF)

Keywords

Digital cellular telecommunications system,
Global System for Mobile communications (GSM)

ETSI

Postal address

F-06921 Sophia Antipolis Cedex - FRANCE

Office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16
Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Internet

secretariat@etsi.fr
http://www.etsi.fr
http://www.etsi.org

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available **free of charge** from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.fr/ipr or http://www.etsi.org/ipr).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This ETSI Technical Specification (TS) has been produced by the Special Mobile Group (SMG) of the European Telecommunications Standards Institute (ETSI).

This TS defines the stage 1 description for the standardised security mechanisms in conjunction with the SIM Application Toolkit for the interface between a GSM PLMN Entity and a SIM within the digital cellular telecommunications system.

The contents of this TS are subject to continuing work within SMG and may change following formal SMG approval. Should SMG modify the contents of this TS it will then be republished by ETSI with an identifying change of release date and an increase in version number as follows:

Version 6.x.y

where:

6 indicates GSM Release 1997 of Phase 2+;

x the second digit is incremented for all other types of changes, i.e. technical enhancements, corrections, updates, etc.

y the third digit is incremented when editorial only changes have been incorporated in the specification.

1 Scope

This document specifies the structure of the Secured Packets in a general format and in an implementation using the Short Message Service (SMS).

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 GSM 11.11 [5] and allows remote management of files on the Subscriber Identity Module (SIM) in conjunction with SMS and the SIM Data Download feature of GSM 11.14 [6].

This specification is applicable to the exchange of secured packets between an entity in a GSM PLMN and an entity in the SIM.

Secured Packets contain application messages to which certain mechanisms according to GSM 02.48 [2] have been applied. Application messages are commands or data exchanged between an application resident in or behind the GSM PLMN and on the SIM. The Sending/Receiving Entity in the GSM PLMN and the SIM are responsible for applying the security mechanisms to the application messages and thus turning them into Secured Packets.

2 References

References may be made to:

a) specific versions of publications (identified by date of publication, edition number, version number, etc.), in which case, subsequent revisions to the referenced document do not apply; or

b) all versions up to and including the identified version (identified by "up to and including" before the version identity); or

c) all versions subsequent to and including the identified version (identified by "onwards" following the version identity); or

d) publications without mention of a specific version, in which case the latest version applies.

A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

2.1 Normative references

[1] GSM 01.04: "Digital cellular telecommunications system (Phase 2+); Abbreviations and acronyms".

[2] GSM 02.48: "Digital cellular telecommunications system (Phase 2+); Security Mechanisms for the SIM Application Toolkit - Stage 1".

[3] GSM 03.40: "Digital cellular telecommunications system (Phase 2+); Technical realization of the Short Message Service (SMS) Point-to-Point (PP)".

[4] GSM 04.11: "Digital cellular telecommunications system (Phase 2+); Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface".

[5] GSM 11.11: "Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[6] GSM 11.14: "Digital cellular telecommunications system (Phase 2+); Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[7] ISO/IEC 7816-4: "1995 Information technology -- 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".

2.2 Informative references

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

3 Definitions and abbreviations

3.1 Definitions

For the purposes of this specification, the following definitions apply:

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

Application Message: The package of commands or data sent from the Sending Application to the Receiving Application, or vice versa, independently of the transport mechanism. An Application Message is transformed with respect to a chosen Transport Layer and chosen level of security into one or more secured packets.

Command Header: The Security Header of a Command Packet.

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

Counter: A mechanism or data field used for keeping track of a message sequence. 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: A 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). 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: a standard cryptographic algorithm specified as DEA in ISO 8731-1 [9].

Digital Signature: A 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). 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.

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

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

Redundancy Check: A 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: The Security Header of a Response Packet.

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

Secured Packet: The information flow on top of which the level of required security has been applied. 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: The entity generating an Application Message to be sent.

Sending Entity: This is the entity from which the Secured Packet originates (e.g. SMS-SC, SIM, USSD entry point, or dedicated SIM Toolkit Server) and where the security mechanisms are invoked. The Sending Entity generates the Secured Packets to be sent.

Short Message: Information that may be conveyed by means of the SMS Service as defined in GSM 03.40 [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 GSM network. 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

In addition to those below, abbreviations used in this specification are listed in GSM 01.04.

CBC	Cipher Block Chaining
CC	Cryptographic Checksum
CNTR	Counter
CHI	Command Header Identifier
CHL	Command Header Length
CPI	Command Packet Identifier
CPL	Command Packet Length
DES	Data Encryption Standard
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
MO-SMS	Mobile Originated Short Message
MT-SMS	Mobile Terminated Short Message
PCNTR	Padding Counter
PLMN	Public Land Mobile Network
PoR	Proof of Receipt
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	Subscribers Identity Module
SM	Short Message
SMS	Short Message Service
SMS-SC	Short Message Service - Service Centre
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
USSD	Unstructured Supplementary Services Data

4 Overview of Security System

An overview of the secure communication related to the SIM Application Toolkit together with the required security mechanisms is given in GSM 02.48 [2], (see figure 1).

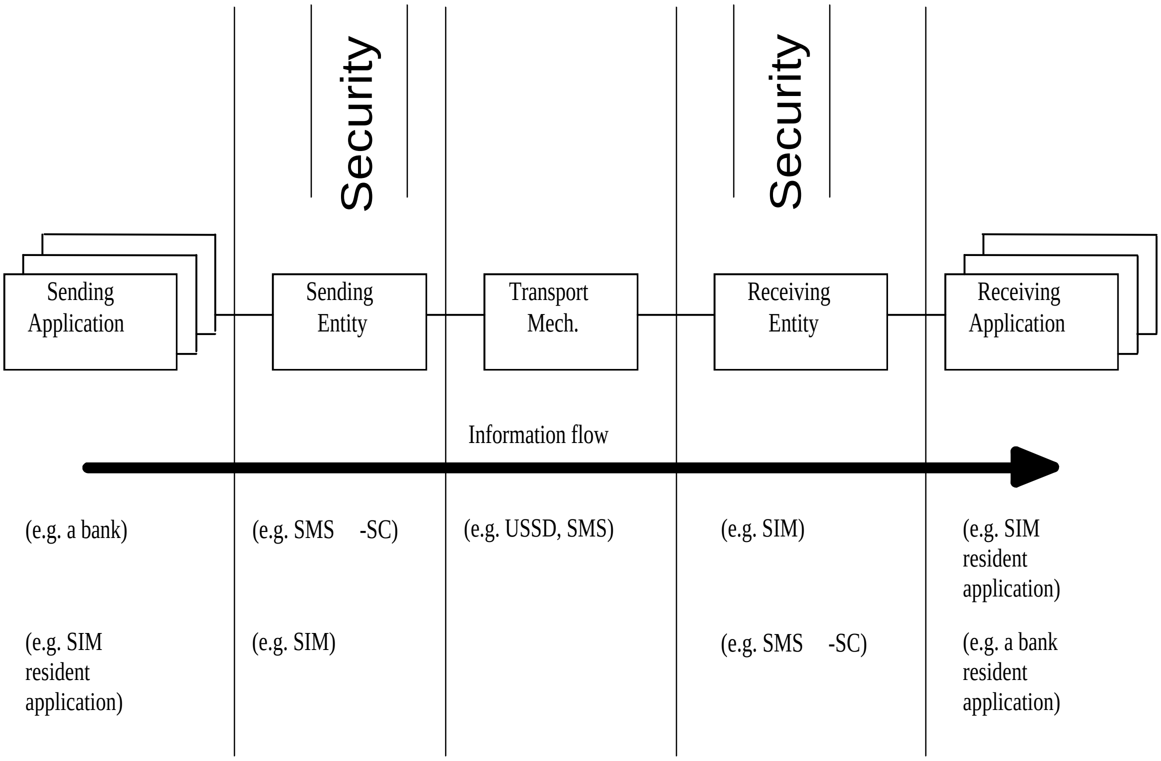


Figure 1: System Overview

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 this specification.

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).

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.
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 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.

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

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.

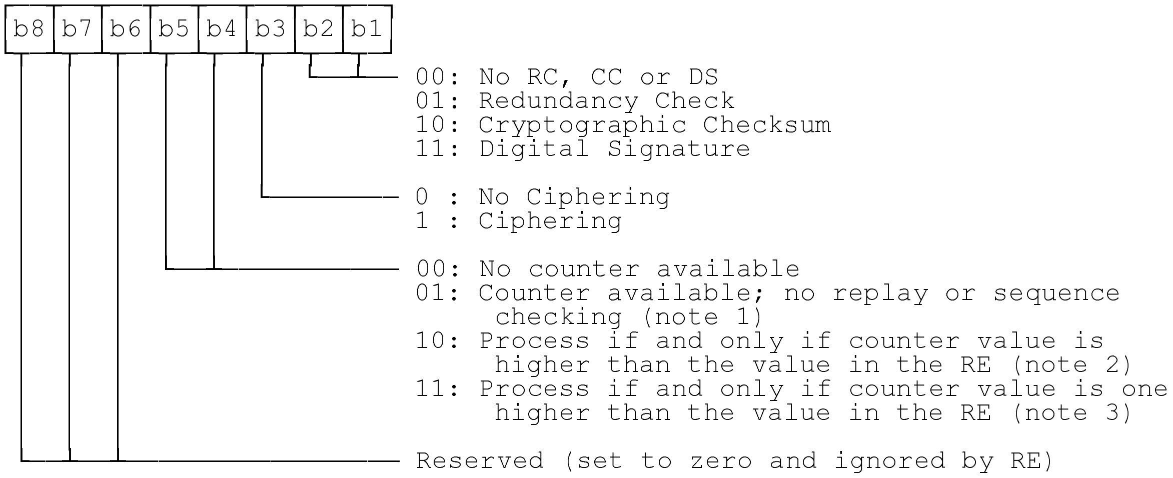
If the SPI indicates that no RC, CC or DS is present in the Command Header, the RC/CC/DS field shall be of zero length.

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:



b8 b7 b6 b5 b4 b3 b2 b1

00: No RC, CC or DS
01: Redundancy Check
10: Cryptographic Checksum
11: Digital Signature

0 : No Ciphering
1 : Ciphering

00: No counter available
01: Counter available; no replay or sequence checking (note 1)
10: Process if and only if counter value is higher than the value in the RE (note 2)
11: Process if and only if counter value is one higher than the value in the RE (note 3)

Reserved (set to zero and ignored by RE)

NOTE 1: 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 2: 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: This provides strict control in addition to security indicated in Note 2.

```
Second octet:
┌──┬──┬──┬──┬──┬──┬──┬──┐
│b8│b7│b6│b5│b4│b3│b2│b1│
└┬─┴┬─┴┬─┴┬─┴┬─┴┬─┴┬─┴┬─┘
 │  │  │  │  │  │  └┬─┴── 00: No PoR reply to the Sending Entity (SE)
 │  │  │  │  │  │       01: PoR required to be sent to the SE
 │  │  │  │  │  │       10: Reserved
 │  │  │  │  │  │       11: Reserved
 │  │  │  │  │  │
 │  │  │  │  └┬─┴─────── 00: No security applied to PoR response to SE
 │  │  │  │             01: PoR response with simple RC applied to it
 │  │  │  │             10: PoR response with CC applied to it
 │  │  │  │             11: PoR response with DS applied to it
 │  │  │  │
 │  │  │  └───────────── 0 : PoR response shall not be ciphered
 │  │  │                1 : PoR response shall be ciphered
 │  │  │
 └──┴──┴─────────────── Reserved (set to zero and ignored by RE)
```

5.1.2 Coding of the KIc

The KIc is coded as below.

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

DES is the algorithm specified as DEA in ISO 8731-1 [9]. DES in CBC mode is described in ISO/IEC 10116 [10]. Triple DES in outer-CBC mode is described in section 15.2 of [20]. DES in ECB mode is described in ISO/IEC 10116 [10].

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

5.1.3 Coding of the KID

The KID is coded as below.

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

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

5.1.4 Counter Management

The following rules shall apply to counter management:

- 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 the RE shall increment the counter to its next value upon receipt of a Command Packet irrespective of whether or not the Command Packet could be successfully unpacked.

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.

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.
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 at the end of the Additional Response Data.
Response Status Code Octet	1 octet	Codings defined in Table 5.
Redundancy Check (RC), Cryptographic Checksum (CC) or Digital Signature (DS)	variable	Length depending on the algorithm indicated in the Command Header in the incoming message. A typical value is 4 to 8 octets, or zero if no RC/CC/DS is requested.
Additional Response Data	variable	Optional Application Specific Response Data, including possible padding octets.

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

Table 4: Linear Representation of Response Packet

RPI	RPL	RHI	RHL	TAR	CNTR	PCNTR	Status Code	RC/CC/DS	Additional Response Data with padding
					Note 1	Note 1	Note 1	Note 1	Note 1
				Note 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.

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’ - ‘FF’	Reserved for future use.

6 Implementation for SMS

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

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 GSM 03.40 [3]. However, in the case of a Response Packet originating from the SIM, due to the inability of the SIM 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.

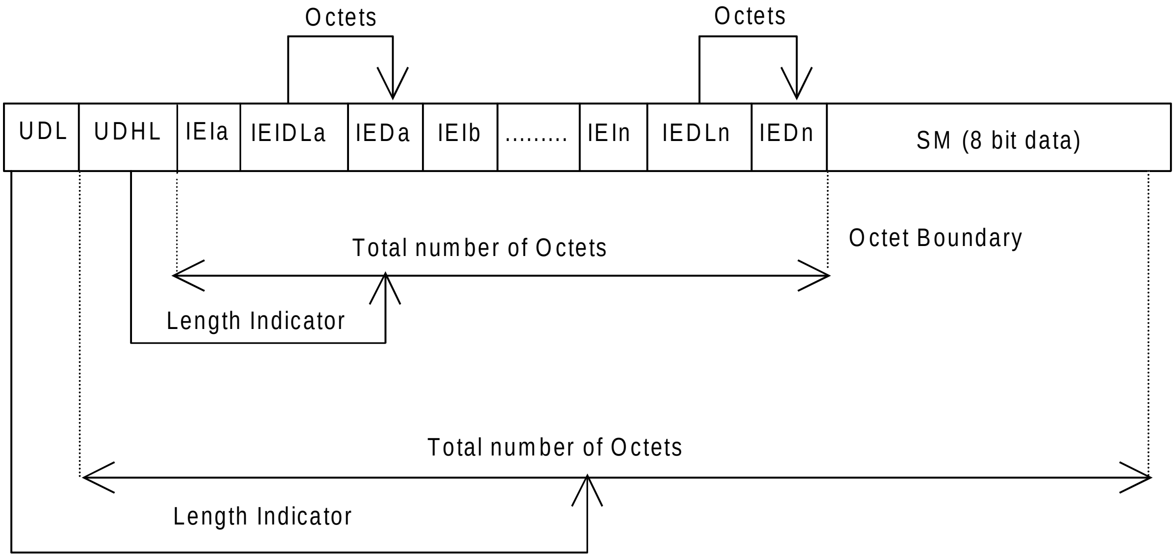


Figure 2: Structure of User Data Header in the Short Message

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 this specification. Values '70' and '71' are used in this specification, 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

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

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 GSM 03.40 [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, coded over 2 octets, and shall not be coded according to ISO/IEC 7816-6 [8].
	Length of the Command Header	Length of the Command Header, coded over one octet, and shall not be coded according to ISO/IEC 7816-6 [8].
	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 subclause 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

If a Command Packet is longer than 140 octets (including the Command Header), it shall be concatenated according to GSM 03.40 [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

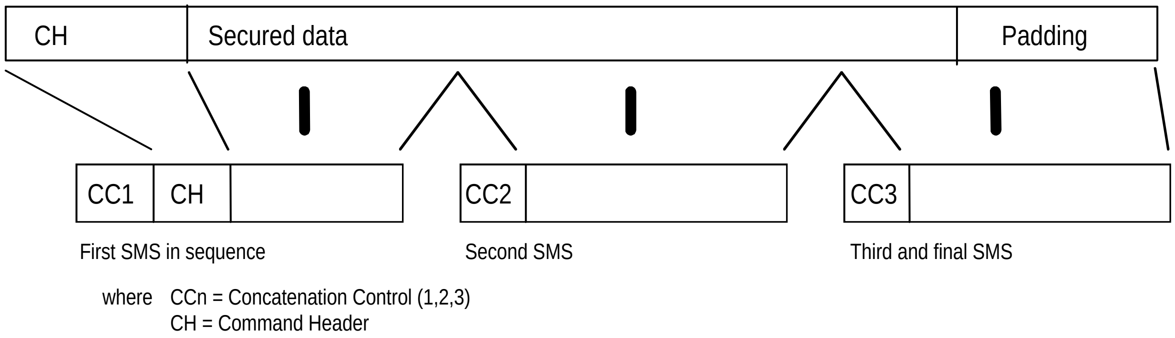
SMS specific elements	Generalised Command Packet Elements (Refer to Table 1)	Comments
UDL		Indicates the length of the entire SM
UDHL	='07'	The first octet of the content or User Data part of the Short Message itself. Length of the total User Data Header, in this case, includes the length of IEIa + IEIDLa + 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 GSM 03.40 [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 GSM 03.40 [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, coded over 2 octets, and shall not be coded according to ISO/IEC 7816-6 [8].
	Length of the Command Header	Length of the Command Header, coded over one octet, and shall not be coded according to ISO/IEC 7816-6 [8].
	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.



6.4 Structure of the Response Packet in SMS-REPORT type

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 SIM, this Response Packet is generated on the SIM, retrieved by the ME from the SIM, and included in the User-Data part of the SMS-DELIVER-REPORT returned to the network. The structure of the PoR response is given in Table 8.

Table 8: Relationship of Response Packet in UDH for SMS-DELIVER/SUBMIT-REPORT

SMS-REPORT specific elements	Generalised Response Packet Elements (Refer to Table 3)	Comments
UDL		Indicates the length of the entire SMS-REPORT
UDHL	='02'	The first octet of the content of the SMS-REPORT 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 GSM 03.40 [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, coded over 2 octets, and shall not be coded according to ISO/IEC 7816-6 [8]. (see note)
	Length of the Response Header	Length of the Response Header, coded over one octet, and shall not be coded according to ISO/IEC 7816-6 [8].
	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 GSM 03.40 [3].

7 Standardised SIM toolkit commands for Remote File Management

There are two elements to Remote File Management on the SIM; the first is the behaviour of the SIM resident Toolkit Application which performs the Remote File Management, and the second is the command structure in the SIM Data Download message, see GSM 11.14 [6]. Access conditions for the GSM files as seen by the SIM 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 SIM. These access conditions may be dependent on the level of security applied to the SIM Data Download message (e.g. SMS).

7.1 Behaviour of the Remote File Management Application

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

2. The application shall take parameters from the SIM Data Download message and shall act upon the 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 SIM Data Download Message 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 SIM 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 SIM may issue a REFRESH command according to GSM 11.14 [6]. However, this is application dependent and therefore out of scope of this specification.

7.2 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 GSM 11.11 [5].

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

7.2.1 Class 1 Commands

The standardised commands are listed in table 9. The commands are as defined in GSM 11.11 [5], except that the SELECT command is extended from the one in GSM 11.11 [5] to include "SELECT by path" as defined in ISO/IEC 7816-4 [7]. The following list of commands require a Class 1 implementation of the SIM Application Toolkit, see GSM 11.14 [6].

Table 9: Class 1 Commands

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

The GET RESPONSE command 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.

Administrative commands are not defined, and remain proprietary to SIM manufacturers.

7.2.2 Class 2 Commands

The list of commands contained in table 10 require a Class 2 implementation of the SIM Application Toolkit. If SMS is being used, these should result in the generation of a single SM by the SIM application containing the relevant data as a result of executing these commands.

Table 10: Class 2 commands

Operational command
READ BINARY READ RECORD

7.3 SIM specific behaviour for Response Packets (Using SMS)

Table 11 summarises the behaviour of the SIM's RE/RA with regard to PoR.

Table 11: SIM specific behaviour

PoR	successful case	Unsuccessful cases (see table 5)
No	'90 00' or '91 XX', null RP-ACK	'90 00' or '91 XX', null RP-ACK OR '9E 00', null RP-ERROR
Yes	'9F XX' (PoR OK, status code '00').	'9E XX' (security error of some kind).

NOTE : in the case where no proof of Receipt is required by the sending entity, it is however permissible for the SIM to send back data using '9F XX' in the successful case or '9E XX' in the unsuccessful case.

If the SIM responds with the '90 00' or '91 XX' code, then there is no User Data to be included in an SMS-DELIVER-REPORT; the ME sends a "null" RP-ACK, with no User Data attached.

In the case of a '9F XX' or '9E XX' response from the SIM, 'XX' indicates the length of the response data to be obtained from the SIM using a later GET RESPONSE command, or states that no additional information is given ('XX' = '00'). The response obtained from the SIM is the complete Response Packet to be included in the User Data part of the SMS-DELIVER-REPORT which will be returned to the Sending Entity as the TP part of the RP-ACK in the '9F XX' case, or as the TP part of the RP-ERROR in the '9E XX' case. In the case of a '9E XX' response from the SIM, the value of the TP-FCS element of the RP-ERROR shall be 'SIM data download error'. Because the SIM is unable to indicate to the ME that the TP-UDHI bit is to be set, the Sending Entity receiving the Response Packet shall expect the UDH structure in any event. See GSM 04.11 [4] for more detail of the structure of the RP-ACK and RP-ERROR protocol element, and GSM 03.40 [3] for more detail of the SMS-DELIVER-REPORT structure.

Annex A (informative): Change History

This annex lists all changes made to this document since its initial approval by ETSI committee, SMG.

SMG#	SMG tdoc	SMG9 tdoc	VERS	CR	REV	PHASE	CAT	SUBJECT	Resulting Version
s24	0888/97		2.0.1					GSM 03.48 approved by SMG plenary 24 (December 1997)	5.0.0
Note: Version changed to 6.0.0 in line with decision at SMG #25 stating that release 97 documents shall be version 6.x.y									
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

History

Document history		
V6.0.0	April 1998	Publication
V6.1.0	July 1998	Publication

ISBN 2-7437-2390-4
Dépôt légal : Juillet 1998