3GPP TSG-T (Terminals) Meeting #15
Jeju, Korea, 6 – 8 March 2002

Tdoc TP-020075

Source: T3

Title: Draft TS 31.115 V1.0.0: Secured Packet Structure for (U)SIM Toolkit Applications

Document for: Information

3GPP T3 Meeting #22
Marbella, Spain, 22 - 25 Jan 2002

Tdoc T3-020122
Revised T3-020049

Technical Specification

3rd Generation Partnership Project; Technical Specification Group Terminals; Secured packet structure for (U)SIM Toolkit applications (Release 5)

Keywords
SIM, USIM, SMS, Smart 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.

Introduction

This specification is the result of a split of TS 23.048 REL-5 between the generic part and the bearers specific application. The generic part has been transferred to SCP. This specification is the bearers specific part.

1 Scope

The present document specifies the structure of the Secured Packets in implementations using Short Message Service Point to Point (SMS-PP) and Short Message Service Cell Broadcast (SMS-CB), based on TS 102 225 [9].

It is applicable to the exchange of secured packets between an entity in a 3G or GSM PLMN and an entity in the (U)SIM.

Secured Packets contain application messages to which certain mechanisms according to TS 102 224 [2] 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 (U)SIM. 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] ETSI TS 102 224: "Security mechanisms for UICC based Applications".

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

[6] 3GPP TS 23.041: "Technical realization of Cell Broadcast Service (CBS)".

[7] 3GPP TS 24.012: "Short Message Service Cell Broadcast (SMSCB) support on the mobile radio interface".

[8] 3GPP TS 23.038: "Alphabets and language-specific information".

[9] ETSI TS 102 225: “Secured Packet Structure for UICC Applications”

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions of TS 102 225 [9] and the following definitions apply:

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

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

3.2 Abbreviations

For the purpose of the present document, the abbreviations of TS 102 225 [9] and the following abbreviations apply:

CBC	Cipher Block Chaining
CBS	Cell Broadcast Service
DCS	Data Coding Scheme
IEI	Information Element Identifier
IEIDL	Information Element Identifier Data Length
IED	Information Element Data
MID	Message IDentifier
MO-SMS	Mobile Originated Short Message
MT-SMS	Mobile Terminated Short Message
PLMN	Public Land Mobile Network
PP	Page Parameter
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
USIM	Universal Subscriber Identity Module

4 Implementation for SMS-PP

4.1 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.

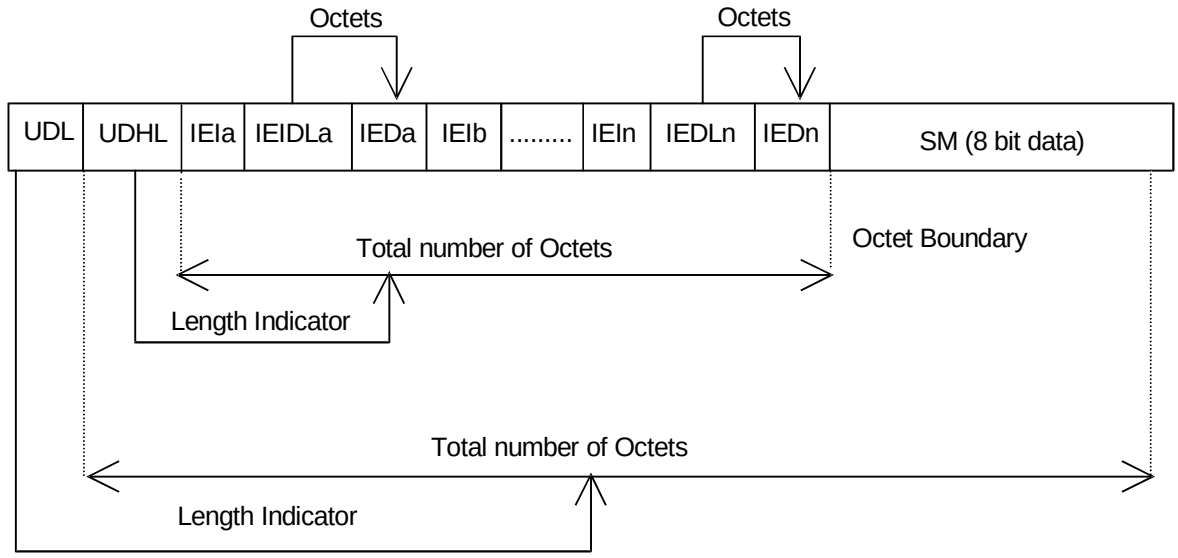


Figure 1: Structure of User Data Header in the Short Message Point to Point

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.

4.2 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 1.

Table 1: 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 1), 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 according to ISO/IEC 7816-6 [5].
	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 according to ISO/IEC 7816-6 [5].
	SPI to RC/CC/DS in the Command Header	The remainder of the Command Header.
	Secured Data	Application Message, including possible padding octets.

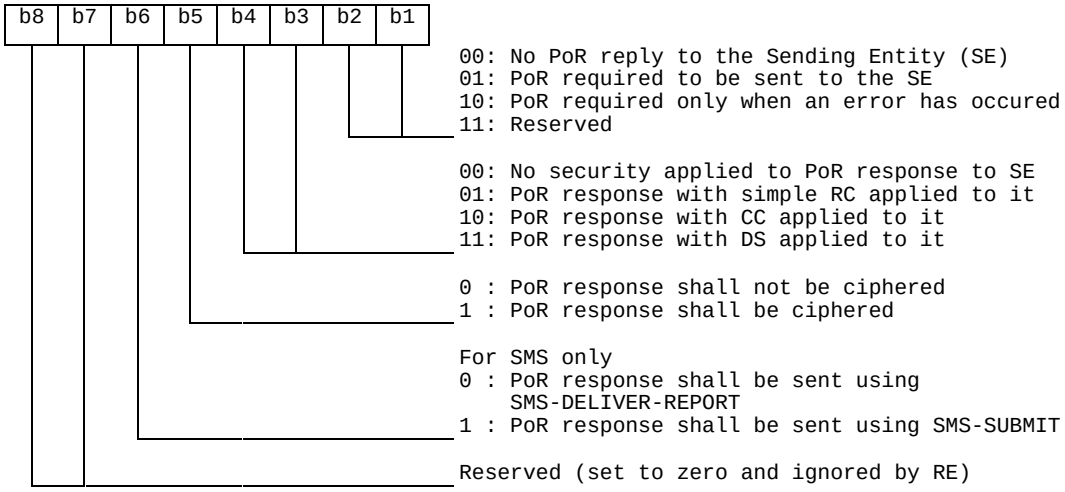
NOTE: Whilst not absolutely necessary in this particular instance, this field is necessary for the case where concatenated Short Message is employed (see clause 4.3).

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.

The SPI shall be coded as specified in TS 102 225 [9]. The b6 of the second octet is used for SMS only and shall be coded as followed:

Second Octet:



4.3 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 2; the ordering of the various elements of the UDH is not important.

Table 2: 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 1), 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 according to ISO/IEC 7816-6 [5].
	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 according to ISO/IEC 7816-6 [5].
	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 2, 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 2. 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.

The SPI shall be coded as specified in TS 102.225 [9]. The b6 of the second octet is used only for SMS and shall be coded as described for a single short message.

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

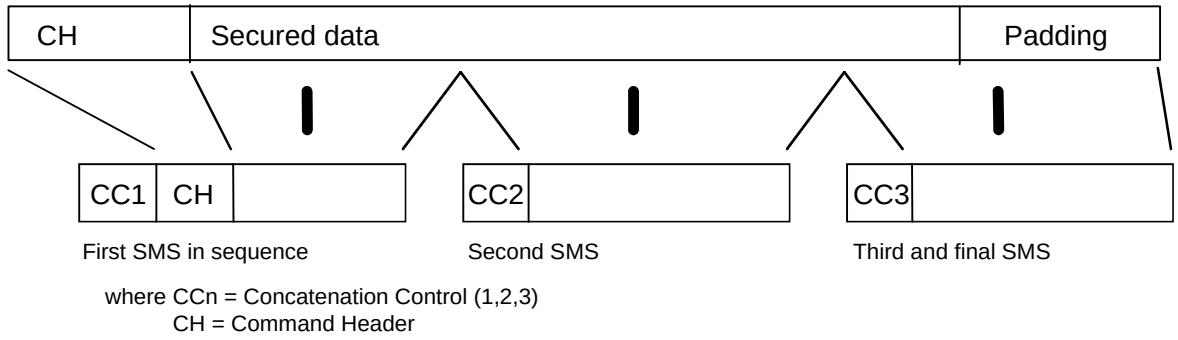


Figure 2: Example of command split using concatenated point to point SMS

4.4 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 3: 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 according to ISO/IEC 7816-6 [5]. (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 according to ISO/IEC 7816-6 [5].
	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].

5 Implementation for SMS-CB

5.1 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 [7]. 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 [6]. 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[6] 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.

5.2 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 4.

Table 4: 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[6]. 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[6]. (see note)
DCS		Refer to 3GPP TS 23.041[6]. Coded on 1 octet containing the alphabet coding and language as defined in GSM 23.038[8].
PP		Refer to 3GPP TS 23.041[6]. 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 according to ISO/IEC 7816-6 [5].
	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.

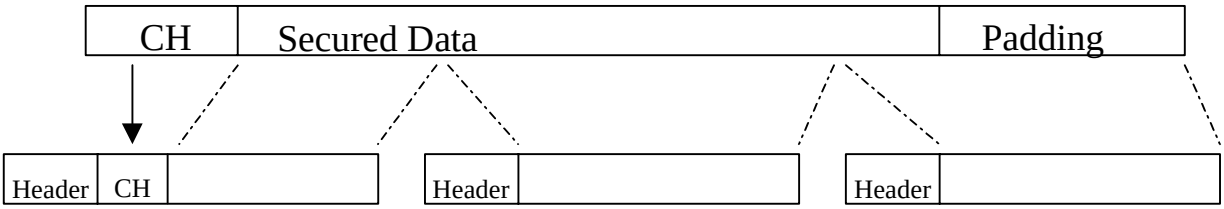
NOTE: Generally, the CPI is coded on 1 octet, as specified in table 1 of TS 102 225 [9]. However, the CPI for the SMS-CB message is coded on 2 octets as the values reserved in 3GPP TS 23.041 [6] to identify the Command Packet are MID values which are coded on 2 octets.

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 3G and GSM specifications by the Sending Entity. The Secured CBS message is formatted in accordance with the 3G and 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 3: Example of command split using concatenated CB SMS

5.3 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.

Change History

This annex lists all changes made to the present document.

History Table					
Date	**Meeting**	**Tdoc**	**Changes**	**Old**	**New**
2001-10	T3 API #9	T3a010197	Initial version is based on 3GPP TS 23.0048 v5.1.0	-	0.0.0
2001-11	T3#21	T3-010671	Submitted to 3GPP T3#21. Editorial changes.	0.0.0	0.0.1
2002-01	T3#22	T3-020122~~049~~	Submitted to 3GPP T3#22. Editorial changes.	0.0.1	0.0.2
2002-03	T#15	TP-020075	Document submitted to TSG-T#15 for information.	0.0.2	1.0.0

Rapporteurs: Sophie Viallet (sophie.viallet@gemplus.com) and Florence Martin (flmartin@montrouge.sema.slb.com)