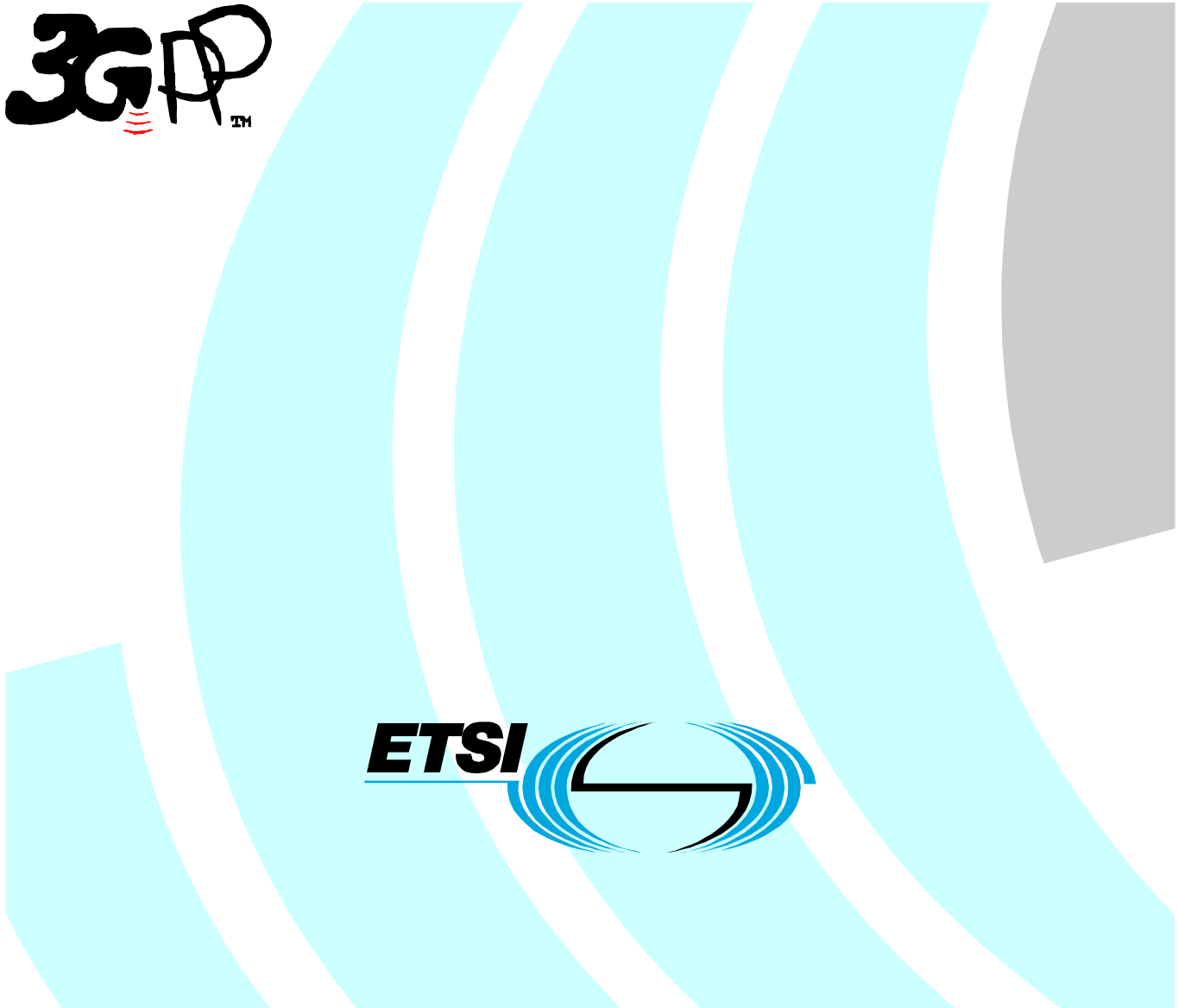
ETSI TS 131 115 V6.4.0 (2004-12)

Technical Specification

**Universal Mobile Telecommunications System (UMTS);
Secured packet structure for (Universal)
Subscriber Identity Module (U)SIM Toolkit applications
(3GPP TS 31.115 version 6.4.0 Release 6)**



Reference
DTS/TSGT-0331115v640

Keywords
UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - 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

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 ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

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 ETSI 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 Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp .

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

The present document is the result of a split of TS 23.048 Release 5 between the generic part and the bearers specific application. The generic part has been transferred to SCP. The present document 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].

The structure of the Secured Packets shall comply with the one defined in TS 102 225 [9]. The present document only contains additional requirements or explicit limitations for SIM/USIM applications.

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 and/or edition number or version number) 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 Release 6: "Smart Cards; Security mechanisms for UICC based Applications - Functional requirements".

[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): "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 Release 6: "Smart Cards; Secured packet structure for UICC based applications".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TS 102 225 [9] and the following 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 3GPP TS 23.040 [3].

3.2 Abbreviations

For the purpose of the present document, the abbreviations given in TS 102 225 [9] and the following 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 Service
MT-SMS	Mobile Terminated Short Message Service
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 in a secured Short Message Point to Point

The coding of the SMS-DELIVER, SMS-SUBMIT, SMS-DELIVER-REPORT header shall indicate that the data is binary (8 bit data), 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 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.

The generalised structure of the UDH in the Short Message element is contained in the User Data part of the Short Message element and is described in TS 23.040 [3]. The Command Packet and the Response Packet are partially mapped into this UDH structure.

Information Element Identifiers (IEI's) values range '70 - 7F' are reserved in TS 23.040 [3] for use in the present document and allocated as follows:

- '70' and '71' are specified in the present document
- values '72 - 7D' are reserved for future use
- '7E' and '7F' are for proprietary implementations.

If a Response Packet (Response Header + Data) is too large to be contained in a single Short Message (including the Response Header), it shall be concatenated according to TS 23.040 [3].

If it is indicated in the SPI2 of a Command Packet to send back a PoR using SMS-DELIVER-REPORT and if the Response Packet is too large to be contained in a single SMS-DELIVER-REPORT - TP element, then:

- One single Response Packet shall be sent back to the SE using SMS-DELIVER-REPORT. This Response Packet:
  - Shall not contain any additional response data
  - Shall contain the Response Status Code set to "Actual response data to be sent using SMS-SUBMIT"
  - The security applied to this Response Packet shall be the one indicated in the SPI2 of the Command Packet.
- This shall be followed by a complete Response Packet, contained in one SMS-SUBMIT element or in a concatenated Short Message composed of several SMS-SUBMIT elements.

4.2 Structure of the Command Packet contained in a Single Short Message Point to Point

CPI identifies the Command Packet and indicates that the first portion of the SM (8 bit data) contains the Command Packet Length (CPL), the Command Header Length (CHL) followed by the remainder of the Command Header: the Secured Data follows on immediately as the remainder of the SM element.

The relationship between the Command Packet and its inclusion in the UDH structure of a single Short Message defined in TS 23.040 [3] is as following:

- CPI is mapped to IEIa defined in TS 23.040 [3] and shall be set to '70'.
- IEDa defined in TS 23.040 [3] shall be a null field and its length IEIDLa shall be set to '00'.

The following Table 1 indicates the Command Packet contained in a single SMS-PP. It is a particular implementation for single SMS-PP of the generic Command Packet structure described in TS 102 225 [9].

Table 1: Structure of the Command Packet contained in the SM (8 bit data)

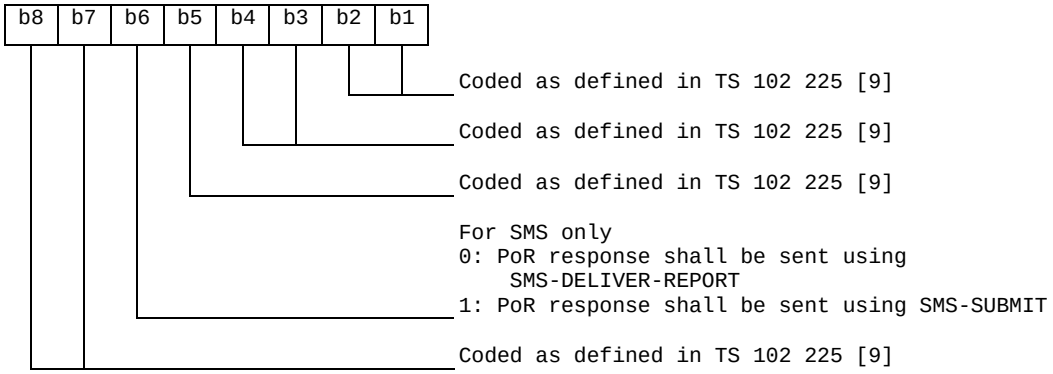
Command Packet Elements	Length	Description
Command Packet Length	2 octets (see NOTE)	Length of the Command Packet (CPL), coded over 2 octets, and shall not be coded according to ISO/IEC 7816-6 [5].
Command Header Identifier	Null field	(CHI) Null field.
Command Header Length	1 octet	Length of the Command 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	Variable	The remainder of the Command Header as described in TS 102 225 [9].
Secured Data	Variable	Application Message, including possible padding octets as described in TS 102 225 [9].

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

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 TS 23.040 [3].

The relationship between the Command Packet and its inclusion in the structure of a concatenated Short Message defined in TS 23.040 [3] is as following:

- The entire Command Packet including the Command Header shall be separated into its component concatenated parts. The structure of the Command Packet contained in a concatenated SMS-PP is as described in Table 1 of this specification.
- The first Short Message shall contain the Concatenation Control Header as defined in TS 23.040 [3] identified by IEIx and the Command Packet Identifier (CPI) in the User Data Header. The relationship between the Command Packet and its inclusion in the structure of the first concatenated Short Message is as described in clause 4.2 for a single Short Message.

NOTE: The ordering of the various elements of the UDH defined in TS 23.040 [3] is not important.

- In each subsequent Short Message in the concatenated series, the Concatenation Control Header shall be present. The Concatenation Control Header shall be set as defined in TS 23.040[3]. The CPI, CPL and Command Header shall not be present.

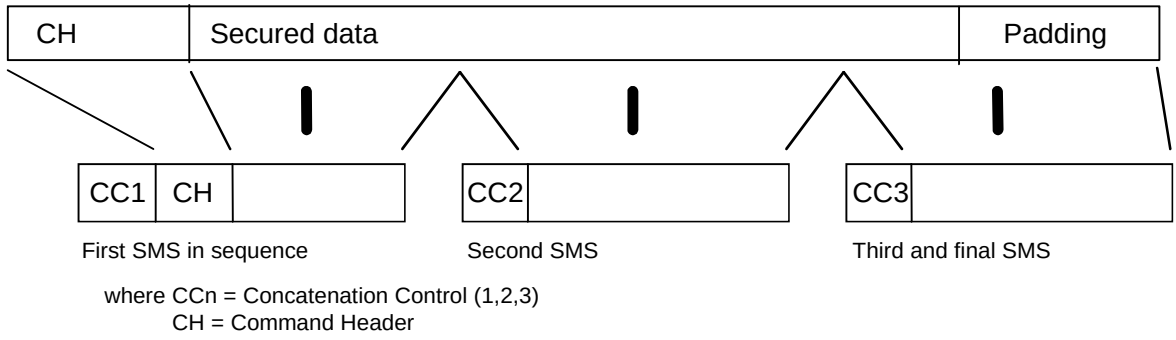
Example of concatenation, 8-bit reference number: if in the first Short Message the Concatenation Control Header isidentified by IEIa, the CPI is mapped to IEIb and no other IEI is present, then the UDHL fieldcontains the length of the total User Data Header i.e the Concatenation Control Header, the CPI and IEIDLb (UDHL shall be set to '07' with IEIa set to '00'). In subsequent Short Message's in the concatenated series, the UDHL contains the length of the Concatenation Control Header only, as there is no subsequent Command Packet Information Element CPI and IEIDLb).

If the data is ciphered, then it is ciphered as described above, before being broken down into individual concatenated elements. The Concatenation Control Header 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.



The Command Header includes here CPL, CHL, SPI to RC/CC/DS

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
- fetched by the ME from the UICC after the Send Short Message proactive command.

The structure of an SMS-DELIVER/SUBMIT User Data object is defined in TS 23.040 [3].

RPI identifies the Response Packet and indicates that the first portion of the SM (8 bit data) contains the Response Packet Length (RPL), the Response Header Length (RHL) followed by the remainder of the Response Header: the Secured Data follows on immediately as the remainder of the SM element.

The relationship between the Response Packet and its inclusion in the UDH structure of a single Short Message defined in TS 23.040 [3] is as following:

- RPI is mapped to IEIa defined in TS 23.040 [3] and shall be set to '71'.
- IEDa defined in TS 23.040 [3] shall be a null field and its length IEIDLa shall be set to '00'.

The following Table 3 indicates the Response Packet contained in a single SMS-PP. It is a particular implementation for single SMS-PP of the generic Response Packet structure described in TS 102 225 [9].

Table 3: Structure of the Response Packet contained in the SM (8 bit data)

Generalised Response Packet Elements (Refer to table 3)	Length	Description
Response Packet Length	2 octets	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.
Response Header Length	1 octet	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	Variable	The remainder of the Response Header as described in TS 102 225 [9].
Secured Data	Variable	Additional Response Data (optional), including padding octets as described in TS 102 225 [9].

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 defined in TS 23.040 [3]) shall be included in the calculation of RC/CC/DS if used. These fields shall not be ciphered.

Table 4: Response Status Codes

Status Code (hexadecimal)	Meaning
'00' to "0A"	See TS 102 225 [9]
'0B'	Actual response data to be sent using SMS-SUBMIT.
'0C' - 'FF'	See TS 102 225 [9]

4.5 A Response Packet contained in Concatenated Short Messages Point to Point

- The relationship between the Response Packet and its inclusion in the structure of a concatenated Short Message defined in TS 23.040 [3] is as following:The entire Response Packet including the Response Header shall be separated into its component concatenated parts. The structure of the Response Packet contained in a concatenated SMS-PP is as described in Table 5 of this specification.

- The first Short Message shall contain the Concatenation Control Header as defined in TS 23.040 [3] identified by IEIxand the Response Packet Identifier (RPI) in the User Data Header. The relationship between the Response Packet and its inclusion in the structure of the first concatenated Short Message is as described in clause 4.4 for a single Short Message.

NOTE: the ordering of the various elements of the UDH defined in TS 23.040 [3] is not important.

- In each subsequent Short Message in the concatenated series, the Concatenation Control Header shall be present. The concatenation Control Header shall be set as defined in TS 23.040 [3]. The RPI, RPL and Response Header shall not be present.

Example of concatenation, 8-bit reference number:

if in the first Short Message the Concatenation Control Header is identified by IEIa, the RPI is mapped to IEIb and no other IEI is present, then the UDHL field contains the length of the total User Data Header i.e the Concatenation Control Header, the RPI and IEIDLb (UDHL shall be set to '07' with IEIa set to '00'). In subsequent Short Message's in the concatenated series, the UDHL contains the length of the Concatenation Control Header only, as there is no subsequent Response Packet Information Element (RPI and IEIDLb).

Table 5: Structure of the Response Packet contained in the SM (8 bits data)

SMS-REPORT specific Elements (Refer to table 3)	Length	Comments
RPL	2 octets	Length of the Response Packet (RPL), coded over 2 octets, and shall not be coded according to ISO/IEC 7816-6 [5].
RHI		(RHI) Null field.
RHL	1 octet	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	Variable	The remainder of the Response Header as described in TS 102 225 [9].
Secured Data	Variable	Additional Response Data (optional), including padding octets as described in TS 102 225 [9].

If the data is ciphered, then it is ciphered as specified in TS 102 225 [9], before being broken down into individual concatenated elements. The concatenation Control Header 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 Response Header, the RPL, the RHL and three octets set to '02' '71' '00', which precede the RPL, shall be included in the calculation of RC/CC/DS if used. These fields shall not be ciphered.

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 TS 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 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 subclause.

A range of values has been reserved in 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.

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 defined in TS 23.041 [6] is the following:

- CPI coded on 2 octets is mapped to MID defined in TS 23.041 [6] and the range is from (hexadecimal) '1080' to '109F'. This range is reserved in TS 23.041 [6].

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 TS 23.041 [6] to identify the Command Packet are MID values which are coded on 2 octets.

- SN, DCS, PP shall be coded as defined in TS 23.041[6] for GSM Cell Broadcast.

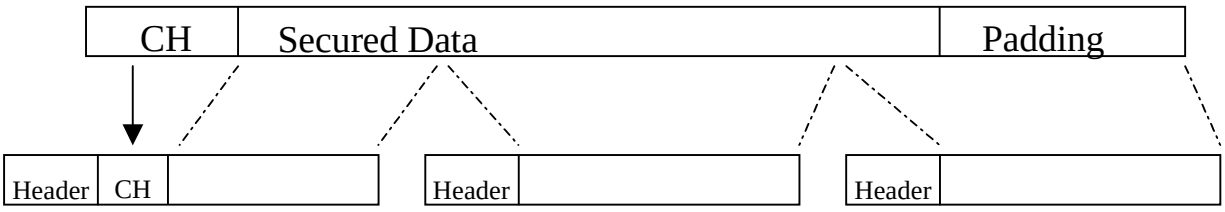
The structure of the Command Packet contained in the Content of Message of the first CBS page is as described in Table 1 of this specification.

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 TS 23.041 [6] (i.e. SN, MID, DCS and PP) and CH = Command Header includes here the CPL, CHL, SPI to RC/CC/DS.

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.

Annex A (informative): Change History

This annex lists all changes made to the present document.

History Table									
Date	**Meeting**	**Tdoc**	**CR**	**Rev**	**Rel**	**Cat**	**Changes**	**Old**	**New**
2001-10	T3 API #9	T3a010197					Initial version is based on 3GPP TS 23.048 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					Submitted to 3GPP T3#22. Editorial changes.	0.0.1	0.0.2
2002-03	TP-15	TP-020075					Document submitted to TSG-T#15 for information.	0.0.2	1.0.0
2002-05	T3#23	T3-020397					Document submitted to 3GPP T3#23 for approval.	1.0.0	1.0.1
2002-06	TP-16	TP-020126					Document for approval	1.0.1	2.0.0
							Comment: T #16 approved the specification for Release 6.		6.0.0
2002-09	TP-17	TP-020209	001		Rel-6	D	Editorial corrections to remove some duplicate specification work	6.0.0	6.1.0
2002-12	TP-18	TP-020284	002		Rel-6	A	Clarification on the RC/CC/DS coding in SPI2	6.1.0	6.2.0
2003-12	TP-22	TP-030255	003	-	Rel-6	F	Remove TS 23.040 duplicated information	6.2.0	6.3.0
			004	-	Rel-6	B	Response Packet in Concatenated Short Messages Point to Point		
2004-12	TP-26	TP-040260	005		Rel-6	F	Correction of non-specific references to SCP documents	6.3.0	6.4.0

History

Document history		
V6.4.0	December 2004	Publication