Source: T3

Title: CRs to TS 31.115: Secured packet structure for (U)SIM Toolkit applications

Document for: Approval

This document contains the following change requests:

Spec	CR	Rev	Phase	Subject	Cat	new ver.	Doc-2nd-Level
31.115	003	-	Rel-6	Remove TS 23.040 duplicated information	F	6.3.0	T3-031013
31.115	004	-	Rel-6	Response Packet in Concatenated Short Messages Point to Point	B	6.3.0	T3-031014

3GPP TSG-T3 #29
Dallas, US, 18 – 21 November 2003

Tdoc T3-031013
Revised T3-030916

3GPP TSG-T3 SWG API #19
Munich, Germany, 7-10 October 2003

Tdoc ⌘ *T3a-030417*

CR-Form-v7

CHANGE REQUEST

| ⌘ | **31.115** CR **003** | ⌘**rev** | **-** | ⌘ | Current version: | **6.2.0** | ⌘ |

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

Proposed change affects: UICC apps⌘ **X**   ME ☐   Radio Access Network ☐   Core Network ☐

Title:	⌘	Remove TS 23.040 duplicated information	
Source:	⌘	T3	
Work item code: ⌘		TEI	***Date:*** ⌘ 20/11/2003
Category:	⌘	**F**	***Release:*** ⌘ Rel-6

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

Use one of the following releases:
2 *(GSM Phase 2)*
R96 *(Release 1996)*
R97 *(Release 1997)*
R98 *(Release 1998)*
R99 *(Release 1999)*
Rel-4 *(Release 4)*
Rel-5 *(Release 5)*
Rel-6 *(Release 6)*

Reason for change:	⌘	Avoid duplication between specifications
Summary of change: ⌘		Remove all TS 23.040 duplicated informations and refer directly to TS 23.040
Consequences if not approved:	⌘	

Clauses affected:	⌘	§ 4, § 5

	Y	N		
Other specs affected: ⌘			Other core specifications	⌘
			Test specifications	
			O&M Specifications	

Other comments:	⌘	

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

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

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

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

4   Implementation for SMS-PP

4.1 4.1 Structure of the UDH ~~of the Security Header~~ in a secured 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 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 ~~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.

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 ~~3GPP~~ 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 ~~3GPP~~ 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.

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   Structure of the~~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.~~

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: ~~Relationship of Command Packet in UDH for single Short Message Point to Point~~ Structure of the Command Packet contained in the SM (8 bit data)

| ~~SMS specific elements~~	~~Generalised~~ Command Packet Elements	Length	~~Comments~~ Description
~~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~~ Command Packet Length ~~(2 octets)(note)~~	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.
	~~Length of the~~ 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).

~~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:
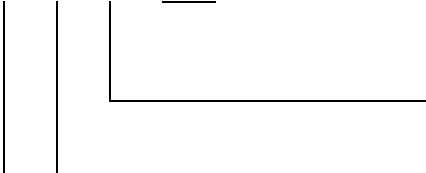
Second Octet:

B8	b7	b6	b5	b4	b3	b2	B1
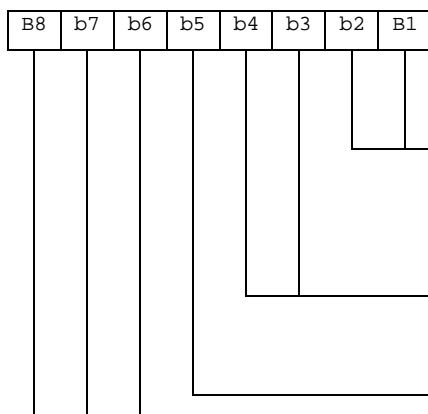
~~00: No PoR reply to the Sending Entity (SE)~~
~~01: PoR required to be sent to the SE~~
~~10: PoR required only when an error has occured~~
~~11: Reserved~~ Coded as defined in TS 102 225 [9]

~~00: No RC, CC or DS 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~~ Coded as defined in TS 102 225 [9]

~~0: PoR response shall not be ciphered~~
~~1: PoR response shall be ciphered~~ Coded as defined in TS 102 225

```
                                    For SMS only
                                    0: PoR response shall be sent using
                                       SMS-DELIVER-REPORT
                                    1: PoR response shall be sent using SMS-SUBMIT

                                    Reserved (set to zero and ignored by RE)Coded as
                                    defined in TS 102 225
```

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].

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:

- In this case, tThe entire Command Packet including the Command Header shall be assembled, and then 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 eConcatenation User DataControl Header as defined in TS 23.040 [3] identified by IEIx and the Command Packet Identifier (CPI) in the User Data Header. in no particular order. 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. CPI is mapped to IEIy defined in TS 23.040 [3] and shall be set to '70'. IEDy defined in TS 23.040 [3] shall be a null field and its length IEIDLy shall be present in the UDH and set to '00'.

 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 is identified by IEIa, the CPI 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 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).

 Subsequent Short Messages shall contain only the eConcatenation ControlUser Data Header. The eConcatenation Control 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 concatenation Control Header shall be set as defined in TS 23.040.

Example of a first concatenated Short Message: IEIa identifies the Concatenation Control Header. CPI is mapped to IEIb and identifies the Command Packet. CPI shall be set to '70', IEDb defined in TS 23.040 [3] shall be a null field and its length IEIDLb shall be set to '00'. In the first Short Message, the UDHL field contains the length of the Concatenation Control Header and the CPI (UDHL shall be set to '07'), whereas 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 Header.

The structure of the Command Packet contained in a concatenated SMS-PP is as described in Table 1 of this specification.

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

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 eConcatenation eControl Header 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.

where CCn = Concatenation Control (1,2,3)
CH = Command Header
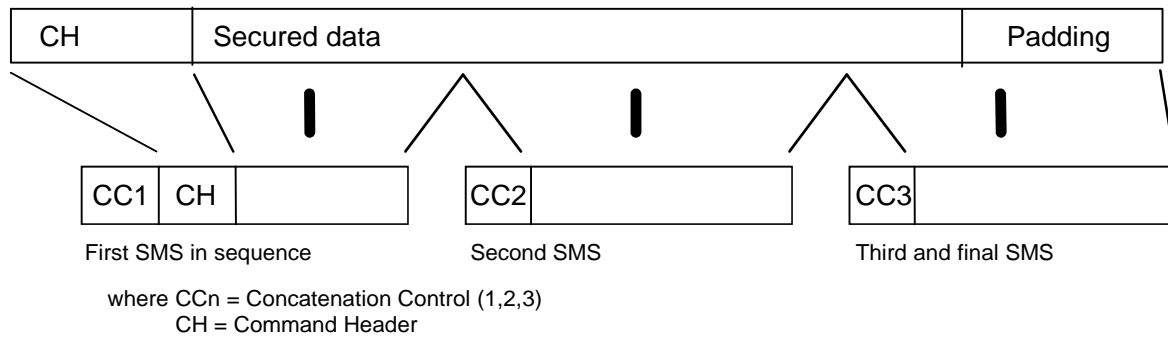
The Command Header includes here CPL, CHL, SPI to RC/CC/DS

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

- retrieved fetched by the ME from the UICC usingafter 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)

~~Relationship of Response Packet in UDH~~

~~SMS-REPORT specific elements~~	~~Generalised~~SMS-REPORT ~~Response Packet~~specific Elements (Refer to table 3)	Length	~~Comments~~Description
~~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~~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~~note~~)
	~~Response Header Identifier~~Response Header Identifier		(RHI) Null field.
	~~Length of the Response Header~~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] ~~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 ~~3GPP~~ 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 subclause.

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 defined in TS 23.041 [6] is the following:~~indicated in table 4.~~

- 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.

~~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
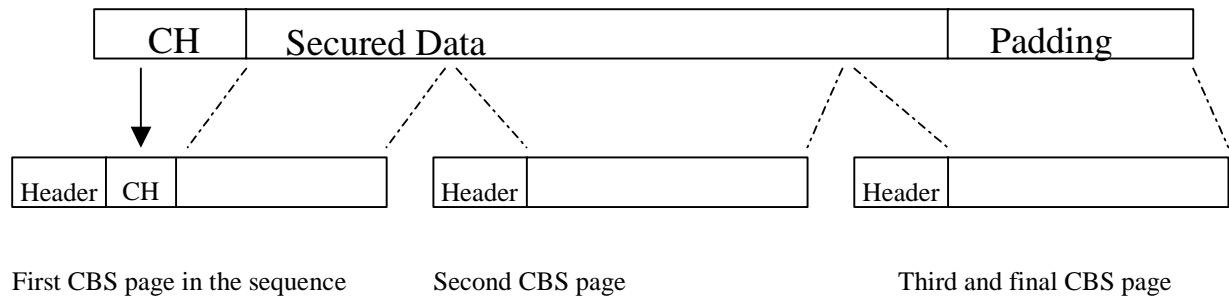
In the above figure, Header = 6 Octet header as defined in TS~~GSM 0~~23.041 [6] (i.e. SN, MID, DCS and PP) and CH = Command Header includes here the CPL, CHL, SPI to RC/CC/DS.

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.

3GPP TSG-T3 #29
Dallas, US, 18 – 21 November 2003

Tdoc T3-031014
Revised T3-030924

3GPP TSG-T3 SWG API #1
Munich, Germany, 7 - 10 October 2003

Tdoc ⌘T3a-030415

CR-Form-v7

CHANGE REQUEST

| ⌘ | **31.115** CR **004** | ⌘**rev** | **-** | ⌘ | Current version: | **6.2.0** | ⌘ |

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

Proposed change affects: UICC apps⌘ **X**   ME ☐ Radio Access Network ☐ Core Network ☐

Title:	⌘ Response Packet in Concatenated Short Messages Point to Point

Source:	⌘ T3

Work item code:⌘	TEI		**Date:** ⌘	21/11/2003

Category:	⌘ **B**		**Release:** ⌘	Rel-6

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

Use *one* of the following releases:
2   (GSM Phase 2)
R96   (Release 1996)
R97   (Release 1997)
R98   (Release 1998)
R99   (Release 1999)
Rel-4   (Release 4)
Rel-5   (Release 5)
Rel-6   (Release 6)

Reason for change: ⌘	Only the Response Packet for single SMS-PP is defined

Summary of change:⌘	Specify the structure of Response Packet for Concatenated Short Messages Point to Point Addition of a new response status code "Actual response data to be sent using SMS-SUBMIT"

Consequences if not approved:	⌘	

Clauses affected:	⌘	§4.1, §4.4, § 4.5

		Y	**N**		
Other specs affected:	⌘			Other core specifications	⌘
				Test specifications	
				O&M Specifications	

Other comments:	⌘	The value '0B' for the new Response Status Code shall be reserved by SCP in TS 102 225

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

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

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

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

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 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 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.

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 3GPP 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 3GPP 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.

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.

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 Whereif thea Response Packet is too large to be contained in a single SMS-DELIVER-REPORT- or SMS-SUBMIT-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.

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.

- 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.

4.4   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].

Table 5: 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 4 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 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 Messages 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 4: 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.