

3GPP2 C.S0078-0
Version 1.0
Version Date: October 2006



3RD GENERATION
PARTNERSHIP
PROJECT 2
"3GPP2"

Secured Packet Structure for CDMA Card Application Toolkit (CCAT) Applications

Revision 1.0

COPYRIGHT

3GPP2 and its Organizational Partners claim copyright in this document and individual Organizational Partners may copyright and issue documents or standards publications in individual Organizational Partner's name based on this document. Requests for reproduction of this document should be directed to the 3GPP2 Secretariat at secretariat@3gpp2.org. Requests to reproduce individual Organizational Partner's documents should be directed to that Organizational Partner. See www.3gpp2.org for more information.

1	Contents	
2	1 INTRODUCTION	3
3	2 SCOPE	3
4	3 REFERENCES	4
5	4 DEFINITIONS, SYMBOLS, ABBREVIATIONS AND CODING CONVENTIONS	6
6	4.1 DEFINITIONS	6
7	4.2 ABBREVIATIONS	6
8	5 IMPLEMENTATION OF SMS-PP	7
9	5.1 STRUCTURE OF THE UDH IN A SECURED SHORT MESSAGE POINT-TO-POINT	7
10	5.2 STRUCTURE OF THE COMMAND PACKET CONTAINED IN A SINGLE SHORT MESSAGE POINT-TO-	
11	POINT 7	
12	5.3 A COMMAND PACKET CONTAINED IN CONCATENATED SHORT MESSAGES POINT-TO-POINT	9
13	5.4 STRUCTURE OF THE RESPONSE PACKET.....	10
14	5.5 A RESPONSE PACKET CONTAINED IN CONCATENATED SHORT MESSAGES POINT-TO-POINT	12
15	6 IMPLEMENTATION OF SMS BROADCAST	13
16		

1 No text.

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19

1 INTRODUCTION

The present document specifies the bearer specific part of secured packets structure. The generic part is specified in ETSI TS 102 225 [13].

2 SCOPE

The present document specifies the structure of the Secured Packets based on ETSI TS 102 225 [13].

The structure of the Secured Packets shall comply with the one defined in ETSI TS 102 225 [13]. The present document only contains additional requirements or explicit limitations for CCAT applications.

It is applicable to the exchange of secured packets between an entity in a CDMA network and an entity in the R-UIM/CSIM.

Secured Packets contain application messages to which certain mechanisms according to [11] have been applied. Application messages are commands or data exchanged between an application resident in or behind the CDMA network and on the R-UIM/CSIM. The Sending/Receiving Entity in the CDMA network and the R-UIM/CSIM are responsible for applying the security mechanisms to the application messages and thus turning them into Secured Packets.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31

3 REFERENCES

The following standards contain provisions that, through reference in this text, constitute provisions of this Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based upon this Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. ANSI and TIA maintain registers of currently valid national standards published by them.

- [1] ETSI TS 102 221 "Smart Cards; UICC-Terminal interface; Physical and logical characteristics (Release 7) ".
- [2] 3GPP TS 31.101 "UICC-Terminal interface; Physical and logical characteristics ".
- [3] 3GPP TS 31.900 "SIM/USIM internal and external Interworking aspects"
- [4] C.S0074-0, UICC-Terminal interface Physical and Logical characteristics for cdma2000 Spread Spectrum Systems.
- [5] C.S0023-C, Removable User Identity Module for Spread Spectrum Systems,
- [6] C.S0035-A, CDMA Card Application Toolkit (CCAT).
- [7] C.S0015-B, Short Message Service (SMS) for Wideband Spread Spectrum Systems.
- [8] ETSI TS 101 220: "Smart cards; ETSI numbering system for telecommunication application providers".
- [9] 3GPP TS 11.11, Release 99: "Specification of the Subscriber Identity Module - Mobile Equipment Interface"
- [10] 3GPP TS 51.011, Release 4: "Specification of the Subscriber Identity Module - Mobile Equipment Interface"
- [11] ETSI TS 102 224: "Smart Cards; Security mechanisms for UICC based Applications - Functional requirements".
- [12] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS)".
- [13] ETSI TS 102 225: "Smart Cards; Secured packet structure for UICC based applications".

- 1 [14] ETSI TS 102 127: "Smart cards; Transport protocol for CAT applications;
- 2 Stage 2".
- 3 [15] C.S0065-0, cdma2000 Application on UICC for Spread Spectrum Systems,.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22

4 DEFINITIONS, SYMBOLS, ABBREVIATIONS AND CODING CONVENTIONS

For the purposes of the present document, the definitions, symbols, and abbreviations specified in ETSI TS 102 225 [13], C.S0015-B [7], C.S0023-C [5], C.S0065-0[15] and the following apply.

4.1 DEFINITIONS

R-UIM: Removable User Identity Module residing on a non-UICC based platform as defined in [5].

CSIM: cdma2000 Subscriber Identify Module specified in C.S0065-0 [15]. A cdma2000^{®1} Application residing on the UICC, an IC card specified in C.S0074-0 [4].

Short Message: Information that may be conveyed by means of the SMS Service as defined in C.S0015-B [7].

4.2 ABBREVIATIONS

IEI	Information Element Identifier
IEIDL	Information Element Identifier Data Length
IED	Information Element Data
SM	Short Message
SMS	Short Message Service
SMS-PP	Short Message Service – Point-to-Point

¹ cdma2000[®] is the trademark for the technical nomenclature for certain specifications and standards of the Organizational Partners (OPs) of 3GPP2. Geographically (and as of the date of publication), cdma2000[®] is a registered trademark of the Telecommunications Industry Association (TIA-USA) in the United States.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37

5 IMPLEMENTATION OF SMS-PP

5.1 Structure of the UDH in a Secured Short Message Point-to-Point

The coding of the SMS Deliver , SMS Submit Message and SMS User Acknowledgement User Data subparameter 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 HEADER_IND bit shall be set as defined in C.S0015-B [7].

However, in the case of a Response Packet originating from the R-UIM/UICC, due to the inability of the R-UIM/UICC to indicate to an ME that the HEADER_IND bit should be set, the Response Packet SMS will not have the HEADER_IND bit set, and the Sending Entity shall treat the Response Packet as if the HEADER_IND bit was set.

The generalized 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 [12]. 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 [12] 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 [12].

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

- One single Response Packet shall be sent back to the Sending Entity using SMS User Acknowledgement . 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" (see Table 3), and
 - 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.

5.2 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

1 the remainder of the Command Header: the Secured Data follows on immediately as the
2 remainder of the SM element.

3 The relationship between the Command Packet and its inclusion in the UDH structure of a
4 single Short Message defined in TS 23.040 [12] is as following:

- 5
- 6 • CPI is mapped to IEIa defined in TS 23.040 [12] and shall be set to '70'.
 - 7 • IEDa defined in TS 23.040 [12] shall be a null field and its length IEIDLa shall be set to
8 '00'.

9 The following Table 1 indicates the Command Packet contained in a single SMS-PP. It is a
10 particular implementation for single SMS-PP of the generic Command Packet structure
11 described in TS 102 225 [13].

12
13

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 as the length of BER-TLV data objects described in TS 101 220 [8].
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 as the length of BER-TLV data objects described in TS 101 220 [8].
SPI to RC/CC/DS in the Command Header	Variable	The remainder of the Command Header as described in TS 102 225 [13].
Secured Data	Variable	Applicative Message, including possible padding octets as described in TS 102 225 [13].

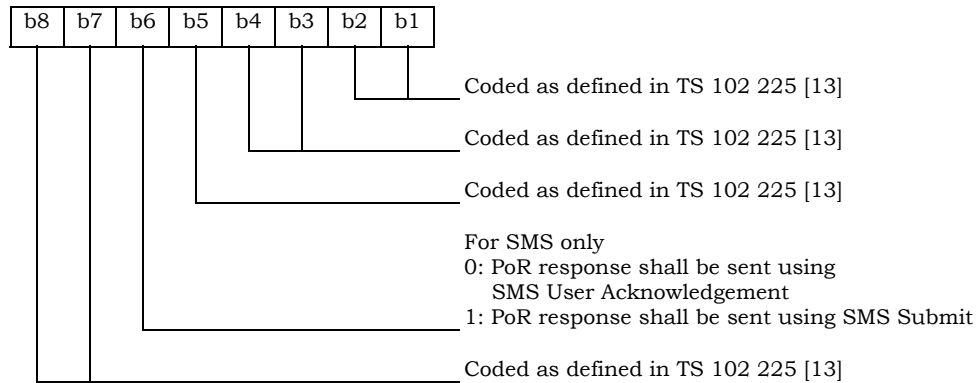
14
15 NOTE: Whilst not absolutely necessary in this particular instance, this field is necessary
16 for the case where concatenated Short Message is employed (see section 5.3).

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

21 The SPI shall be coded as specified in TS 102 225 [13]. The bit 6 of the second octet is used for
22 SMS only and shall be coded as followed:

23

1 Second Octet:



2

3

4 **5.3 A Command Packet Contained in Concatenated Short Messages Point-to-Point**

5 If a Command Packet is longer than 140 octets (including the Command Header), it shall be
6 concatenated according to TS 23.040[12].

7 The relationship between the Command Packet and its inclusion in the structure of a
8 concatenated Short Message defined in TS 23.040[12] is as following:

9

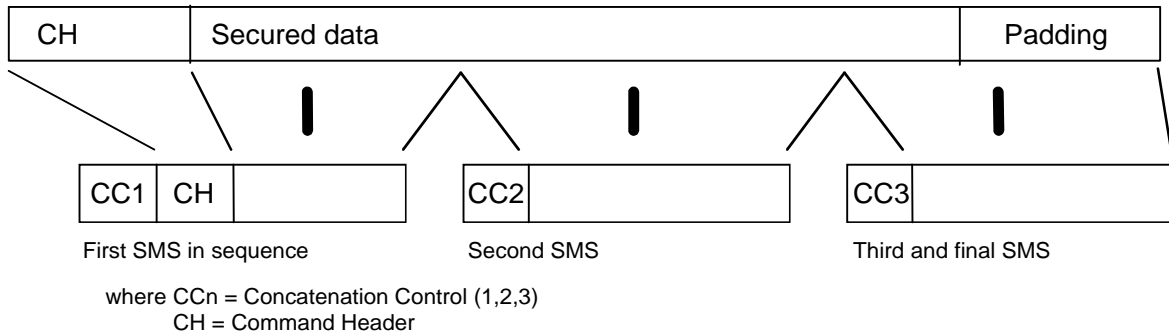
- 10 • The entire Command Packet including the Command Header shall be separated into its
11 component concatenated parts. The structure of the Command Packet contained in a
12 concatenated SMS-PP is as described in Table 1 of this specification.
- 13 • The first Short Message shall contain the Concatenation Control Header as defined in TS
14 23.040[12] identified by IEIx and the Command Packet Identifier (CPI) in the User Data
15 Header. The relationship between the Command Packet and its inclusion in the structure
16 of the first concatenated Short Message is as described in section 5.2 for a single Short
17 Message.

18 NOTE: The ordering of the various elements of the UDH defined in TS 23.040[12] is not
19 important.

- 20 • In each subsequent Short Message in the concatenated series, the Concatenation Control
21 Header shall be present. The Concatenation Control Header shall be set as defined in TS
22 23.040[12]. The CPI, CPL and Command Header shall not be present.

23 Example of concatenation, 8-bit reference number: if in the first Short Message the
24 Concatenation Control Header is identified by IEIa, the CPI is mapped to IEIb and no other IEI
25 is present, then the UDHL field contains the length of the total User Data Header i.e the
26 Concatenation Control Header, the CPI and IEIDLb (UDHL shall be set to '07' with IEIa set to
27 '00'). In subsequent Short Message's in the concatenated series, the UDHL contains the length
28 of the Concatenation Control Header only, as there is no subsequent Command Packet
29 Information Element CPI and IEIDLb).

- 1 If the data is ciphered, then it is ciphered as described above, before being broken down into
 2 individual concatenated elements. The Concatenation Control Header of the UDH in each SM
 3 shall not be ciphered.
- 4 In order to achieve a modulo 8 length of the data before the RC/CC/DS field in the Command
 5 Header, the Command Packet Length[CPL] and the Command Header Length [CHL] shall be
 6 included in the calculation of RC/CC/DS if used. These fields shall not be ciphered.
- 7 The SPI shall be coded as specified in TS 102 225 [13]. The bit 6 of the second octet is used
 8 only for SMS and shall be coded as described for a single short message.
- 9 An example illustrating the relationship between a Command Packet split over a sequence of
 10 three Short Messages is shown in Figure 1.



- 11
- 12 The Command Header includes here CPL, CHL, SPI to RC/CC/DS

13 **Figure 1: Example of Command Split Using Concatenated Point-to-Point SMS**

14 **5.4 Structure of the Response Packet**

15 The Response Packet is as follows. This message is generated by the Receiving Entity and
 16 possibly includes some data supplied by the Receiving Application, and returned to the
 17 Sending Entity/Sending Application. In the case where the Receiving Entity is the R-
 18 UIM/UICC, the process for generating the Response Packet is dependent on bit 6 of the
 19 second octet of the SPI.

- 20 • In the case when bit 6 of the second octet of the SPI is '0', the Response Packet is
 21 generated on the R-UIM/UICC and retrieved by the ME from the R-UIM/UICC, and
 22 included in the User-Data part of the SMS User Acknowledgement returned to the
 23 network.
- 24 • In the case when bit 6 of the second octet of the SPI is '1', the Response Packet is
 25 generated on the R-UIM/UICC and fetched by the ME from the R-UIM/UICC which
 26 returns it as Send Short Message proactive command.

27 The structure of an SMS User Acknowledge/SMS Submit User Data object is defined in
 28 C.S0015-B [7].

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

33 The relationship between the Response Packet and its inclusion in the UDH structure of a
 34 single Short Message defined in TS 23.040 [12] is as following:

- 1 • RPI is mapped to IEIa defined in TS 23.040 [12] and shall be set to '71'.
 2 • IEDa defined in TS 23.040[12] shall be a null field and its length IEIDL a shall be set to
 3 '00'.

4 The following Table 2 indicates the Response Packet contained in a single SMS-PP. It is a
 5 particular implementation for single SMS-PP of the generic Response Packet structure
 6 described in TS 102 225[13].

7
 8

Table 2: Structure of the Response Packet Contained in the SM (8 bit data)

Generalised Response Packet Elements	Length	Description
Response Packet Length	2 octets	Length of the Response Packet (RPL), coded over 2 octets, and shall not be coded as the length of BER-TLV data objects described in TS 101 220[8]. (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 as the length of BER-TLV data objects described in TS 101 220[8].
TAR to RC/CC/DS elements in the Response Header	Variable	The remainder of the Response Header as described in TS 102 225[13].
Secured Data	Variable	Additional Response Data (optional), including padding octets as described in TS 102 225[13].

9

10 NOTE: This field is not absolutely necessary but is placed here to maintain compatibility
 11 with the structure of the Command Packet when included in a SMS Submit or SMS
 12 Deliver.

13 In order to achieve a modulo 8 length of the data before the RC/CC/DS field in the Response
 14 Header, Response Packet Length [RPL], Response Header Length [RHL] and the three preceding
 15 octets (UDHL, IEIa and IEIDL a defined in TS 23.040[12]) shall be included in the calculation of
 16 RC/CC/DS if used. These fields shall not be ciphered.

17

18

Table 3: Response Status Codes

Status Code (hexadecimal)	Meaning
'00' to '0A'	See TS 102 225[13].
'0B'	Actual response data to be sent using SMS Submit.
'0C' - 'FF'	See TS 102 225[13].

19

1 **5.5 A Response Packet Contained in Concatenated Short Messages Point-to-Point**

- 2 • The relationship between the Response Packet and its inclusion in the structure of a
3 concatenated Short Message defined in TS 23.040[12] is as following: The entire
4 Response Packet including the Response Header shall be separated into its component
5 concatenated parts. The structure of the Response Packet contained in a concatenated
6 SMS-PP is as described in Table 2 of this specification.
- 7 • The first Short Message shall contain the Concatenation Control Header as defined in
8 TS 23.040[12] identified by IEIx and the Response Packet Identifier (RPI) in the User
9 Data Header. The relationship between the Response Packet and its inclusion in the
10 structure of the first concatenated Short Message is as described in section 5.4 for a
11 single Short Message.

12 NOTE: the ordering of the various elements of the UDH defined in TS 23.040[12] is not
13 important.

- 14 • In each subsequent Short Message in the concatenated series, the Concatenation
15 Control Header shall be present. The concatenation Control Header shall be set as
16 defined in TS 23.040[12]. The RPI, RPL and Response Header shall not be present.

17 Example of concatenation, 8-bit reference number:

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

24

25 If the data is ciphered, then it is ciphered as specified in TS 102 225[13], before being broken
26 down into individual concatenated elements. The concatenation Control Header of the UDH in
27 each SM shall not be ciphered.

28 In order to achieve a modulo 8 length of the data before the RC/CC/DS field in the Response
29 Header, the RPL, the RHL and three octets set to '02' '71' '00', which precede the RPL, shall be
30 included in the calculation of RC/CC/DS if used. These fields shall not be ciphered.

1 **6 IMPLEMENTATION OF SMS BROADCAST**

2 The structure of SMS Broadcast is as defined in C.S0015-B [7]. The secured packet structure
3 for SMS Broadcast shall follow the implementation of SMS-PP as described in Section 5 above.
4 However, as there is no response mechanism defined for SMS Broadcast, these following
5 conditions shall be followed:

- 6 ▪ SMS User Acknowledgement and SMS Submit are not applicable for SMS Broadcast
7 implementation.
- 8 ▪ The defined structure and implementation of Response Packet described in Section 5 is not
9 applicable to SMS Broadcast implementation.
- 10 ▪ If a (Secured) Response Packet is sent via another bearer, the structure shall be defined by
11 the Receiving Application.

12

13