ETSI TS 131 115 V17.0.0 (2022-04)

**Digital cellular telecommunications system (Phase 2+) (GSM);
Universal Mobile Telecommunications System (UMTS);
LTE;
Secured packet structure for (Universal)
Subscriber Identity Module (U)SIM Toolkit applications
(3GPP TS 31.115 version 17.0.0 Release 17)**

Reference
RTS/TSGC-0631115vh00

Keywords
GSM,LTE,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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Legal Notice

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. These shall be interpreted as being references to the corresponding ETSI deliverables.

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

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

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.

In the present document, modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

can indicates that something is possible

cannot indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

will indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

will not indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

might indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

might not indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

is (or any other verb in the indicative mood) indicates a statement of fact

is not (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

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), Short Message Service Cell Broadcast (SMS-CB), Unstructured Supplementary Service Data (USSD) and and Hyper Text Transfer Protocol (HTTP) based on ETSI TS 102 225 [9].

The structure of the Secured Packets shall comply with the one defined in ETSI 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 PLMN and an entity in the (U)SIM.

Secured Packets contain application messages to which certain mechanisms according to ETSI TS 102 224 [2] have been applied. Application messages are commands or data exchanged between an application resident in or behind the PLMN and on the (U)SIM. The Sending/Receiving Entity in the 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 V8.0.0: "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] ETSI TS 101 220 "Smart Cards; ETSI numbering system for telecommunication application providers".

[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 V12.1.0: "Smart Cards; Secured packet structure for UICC based applications".

[10] 3GPP TS 24.090: "Unstructured Supplementary Service Data (USSD) – Stage 3".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI 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 TS 23.040 [3].

USSD message: information that may be conveyed in the USSD-String field of a Facility message as defined in TS 24.090 [10].

3.2 Abbreviations

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

CBC	Cipher Block Chaining
CBS	Cell Broadcast Service
CCF	Concatenation Control Field
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
PFI	Packet Format Information
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
UM	USSD message
USIM	Universal Subscriber Identity Module
USSD	Unstructured Supplementary Service Data

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 follow the coding and rules as defined in ETSI TS 102 225 [9].
- 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 ETSI 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 as the length of BER-TLV data objects described in ETSI TS 101 220 [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 as the length of BER-TLV data objects described in ETSI TS 101 220 [5].
SPI to RC/CC/DS in the Command Header	Variable	The remainder of the Command Header as described in ETSI TS 102 225 [9].
Secured Data	Variable	Application Message, including possible padding octets as described in ETSI TS 102 225 [9].

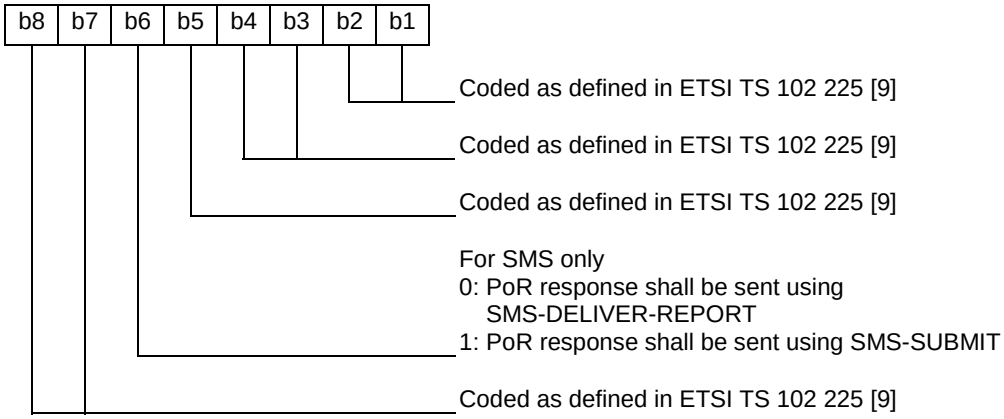
NOTE: Whilst not absolutely necessary in this particular instance, this field is necessary for the case where concatenated Short Message is employed (see clause 4.3).

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.

When receiving a secured Command Packet requesting a Proof of Receipt (PoR), the Receiving Entity shall follow the coding and rules as defined in ETSI TS 102 225 [9]. The Receiving Entity shall verify the authenticity of the Sending Entity. If the Receiving Entity cannot authenticate the Sending Entity, the Receiving Entity shall not send any Response Packet and discard the Command Packet with no further action being taken, as described in ETSI TS 102 225 [9], clause 4.1.

The SPI shall be coded as specified in ETSI 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:

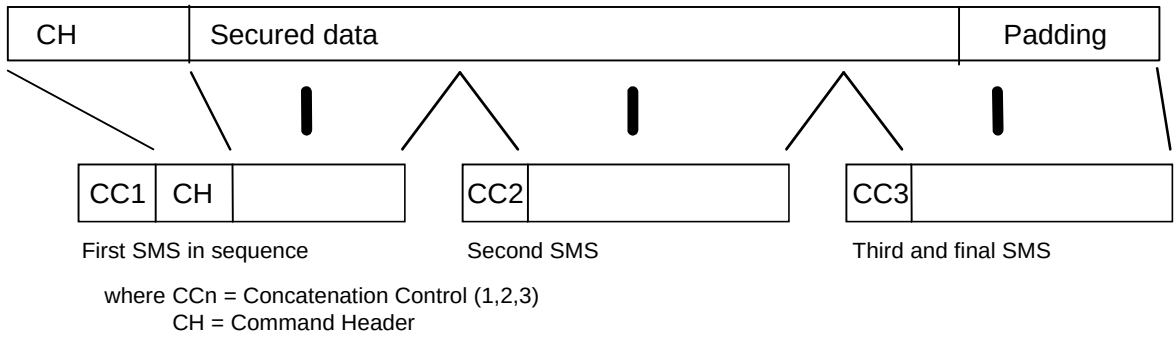
if in the first Short Message the Concatenation Control Header isidentified by IEIa, the CPI is mapped to IEIb and no other IEI is present, then the UDHL fieldcontains the length of the total User Data Header i.e the Concatenation Control Header, the CPI and IEIDLb (UDHL shall be set to '07' with IEIa 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 and shall follow the rules 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 ETSI 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 as the length of BER-TLV data objects described in ETSI TS 101 220 [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 as the length of BER-TLV data objects described in ETSI TS 101 220 [5].
TAR to RC/CC/DS elements in the Response Header	Variable	The remainder of the Response Header as described in ETSI TS 102 225 [9]. Response Status Codes are defined in clause 7.
Secured Data	Variable	Additional Response Data (optional), including padding octets as described in ETSI 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.

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 as the length of BER-TLV data objects described in ETSI TS 101 220 [5].
RHI		(RHI) Null field.
RHL	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 ETSI TS 101 220 [5].
TAR to RC/CC/DS elements in the Response Header	Variable	The remainder of the Response Header as described in ETSI TS 102 225 [9].
Secured Data	Variable	Additional Response Data (optional), including padding octets as described in ETSI TS 102 225 [9].

If the data is ciphered, then it is ciphered as specified in ETSI 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 clause.

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 ETSI 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.

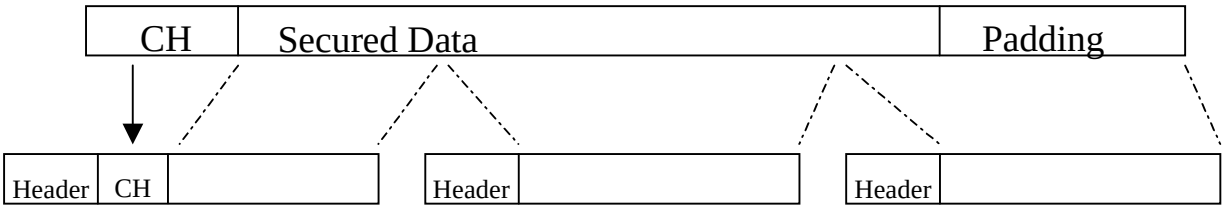
- SN, DCS, PP shall be coded as defined in TS 23.041 [6] for Cell Broadcast.

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 3GPP specifications by the Sending Entity. The Secured CBS message is formatted in accordance with the 3GPP 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.

6 Implementation for USSD

The USSD application mode enables the transparent transport of data between an application residing in the network and a UICC based application. In such a case, to secure the payload of USSD operations, security mechanisms defined in TS 102 225 [9] shall be applied to the USSD messages. Generic secured Command Packet and secured Response Packet as defined in TS 102 225 [9] are contained, as defined hereafter, in the UM part of the USSD String. The USSD String shall be formatted according to annex X, where the PFI byte indicates that Application Data are formatted according to the present document.

The Data Coding Scheme of the USSD String (as defined in TS 23.038 [8]) shall be set to 0x96 (DCS = '10010110') to indicate that data is binary (8 bit data), and formatted according to annex X. In USSD Application mode, which uses an 8-bit character set, the maximum length of the USSD String field is 160 bytes.

Command and Response packets exceeding 159 bytes shall be segmented as described in clauses 6.2 and 6.4.

6.1 Structure of the Command Packet contained in a Single USSD Message

The UM field of an USSD String contains the Command Packet.

The Command Packet shall be coded as the generic Command Packet described in TS 102 225 [9].

In the Command Packet, the Command Packet Identifier (CPI) value is '03' and the Command Header Identifier (CHI) is a Null field.

CPI, CPL and CHL shall be included in the calculation of the RC/CC/DS.

The SPI shall be coded as specified in TS 102 225 [9].

6.2 Structure of the Command Packet contained in concatenated USSD Messages

If the Command Packet, which is structured as described in clause 6.1, is longer than 159 bytes (including the Command Header) then it shall be handled as follows.

- The entire Command Packet including the Command Header shall be separated into its component concatenated parts.
- The Command Packet is handled as a Concatenated USSD Message as described in annex X of the present document.
- The Command Packet Header will only be present in the first segment of a concatenated message.

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

CPI, CPL and CHL shall be included in the calculation of the RC/CC/DS.

The SPI shall be coded as specified in TS 102 225 [9].

An example illustrating a Command Packet split over a sequence of three messages is shown below.

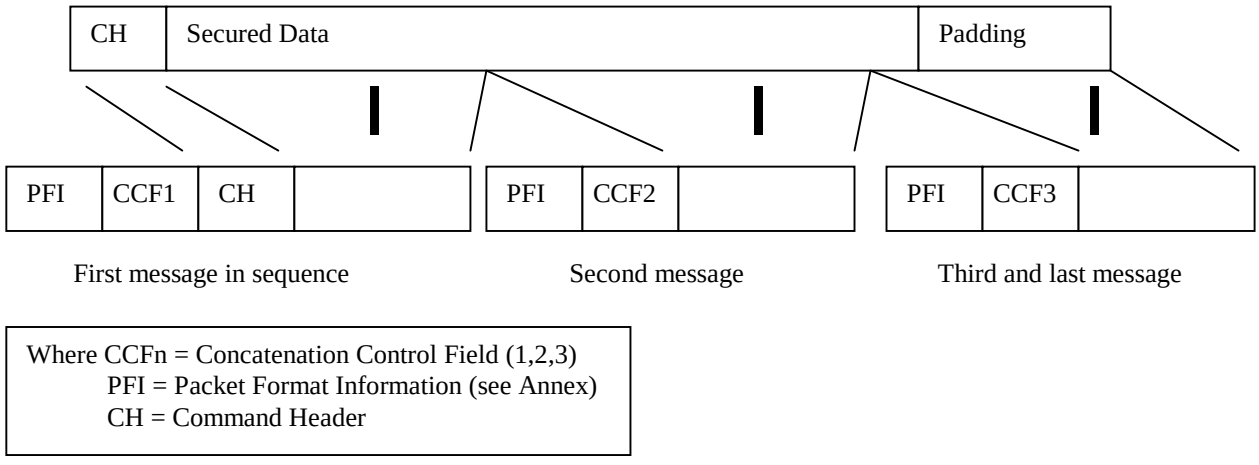


Figure 4: Example of command split using concatenated USSD messages

6.3 Structure of the Response Packet

The Response Packet 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, this Response Packet is generated on the UICC, retrieved by the ME from the UICC, and included in the Return Result Component of a Facility message (see TS 24.090 [10]) returned to the network.

The USSD operations are defined in TS 24.090 [10].

The UM field of an USSD String contains the Response Packet.

The Response Packet shall be coded as the generic Response Packet described in TS 102 225 [9].

In the Response Packet, the Response Packet Identifier (RPI) value is '04' and the Response Header Identifier (RHI) is a Null field.

RPI, RPL and RHL shall be included in the calculation of the RC/CC/DS.

Coding of Response Status Codes is defined in clause 7.

6.4 Structure of the Response Packet contained in concatenated USSD Messages

If the Response Packet, which is structured as described in clause 6.3, is longer than 159 bytes (including the Response Header) then it shall be handled as follows.

- The entire Response Packet including the Response Header shall be separated into its component concatenated parts.
- The Response Packet is handled as a Concatenated USSD Message as described in annex X of the present document.
- The Response Packet Header will only be present in the first segment of a concatenated message.

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

RPI, RPL and RHL shall be included in the calculation of the RC/CC/DS.

An example illustrating a Response Packet split over a sequence of three messages is shown below.

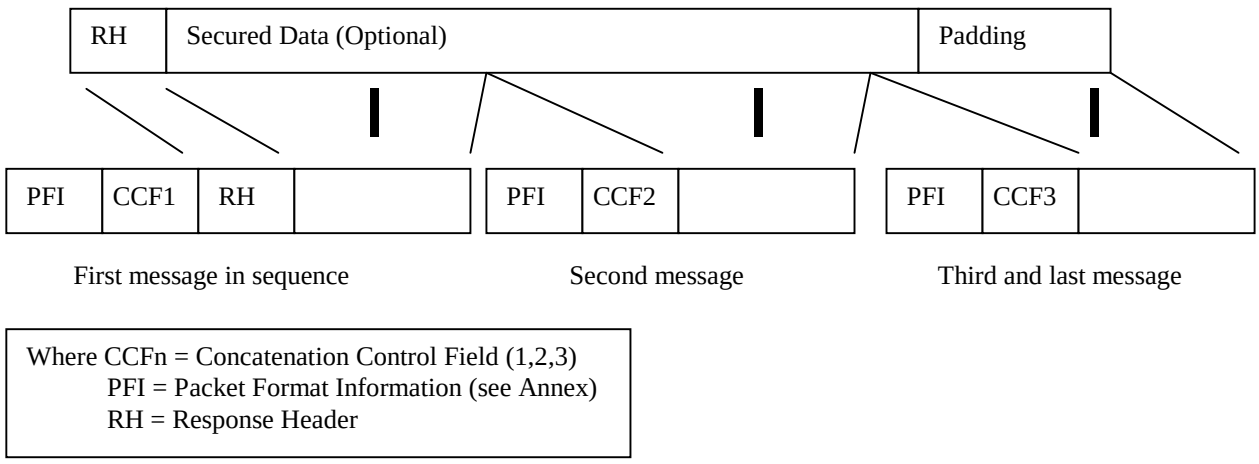


Figure 5: Example of Response split using concatenated USSD messages

If it is indicated in the SPI2 of a Command Packet to send back a PoR and if the Response Packet is too large to be contained in a single USSD String, then:

- One single Response Packet shall be sent back to the SE using the Return Result Component contained in the subsequent Facility message. This Response Packet:
  - Shall not contain any additional response data

- Shall contain the Response Status Code set to '0C' ('Actual response data to be sent using a ProcessUnstructuredSS-Request invoke component (i.e. using SEND USSD proactive command) ').
- 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 a concatenated USSD Message as defined above

7 Specific 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. See clause 4.4.
'0C'	Actual response data to be sent using a ProcessUnstructuredSS-Request invoke component (i.e. using Send USSD proactive command). See clause 6.3
'0D' – 'FF'	See TS 102 225 [9]

Specific Response Status Codes

8 Implementation for HTTP

The security for data exchange over TCP is provided by TLS. The HTTP protocol is used on top of TLS to provide encapsulation of the data and information about the receiving entity.

See ETSI TS 102 225 [9]

Annex A (normative): USSD String format

For the purpose of UICC-based application, the USSD String shall be coded as follows:

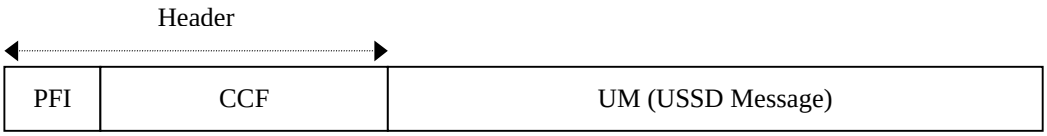
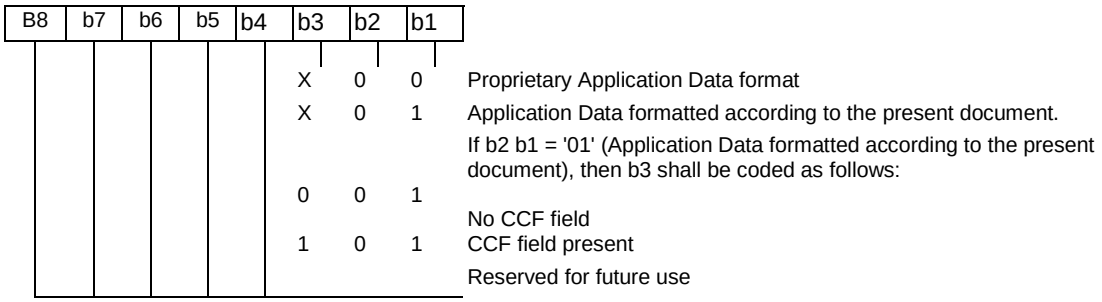


Figure 6: USSD String format

The header of an USSD Message may contain two fields:

- A mandatory PFI field, which is coded on 1 byte. The PFI contains information on the format of the USSD String.
- An optional CCF field, which is coded on 3 bytes. The CCF field presence is indicated by the PFI.

The PFI is coded as follows.



The usage of CCF field allows USSD Messages to be concatenated to form a longer message. The CCF field contains information set by the application so that the receiving entity is able to re-assemble the received Ums in the correct order. Additionally, the CCF contains a reference number, which allows the receiving entity to discriminate between messages. The CCF octets shall be coded as follows.

Octet 1: Concatenated USSD Message reference number.

This octet shall contain a modulo-256 counter indicating the reference number for a particular USSD Message, Concatenated or not. This reference number shall remain constant for every USSD Message that makes up a particular Concatenated USSD Message.

Octet 2: Total number of USSD Messages in the Concatenated USSD Message.

This octet shall contain a value in the range 1 to 255 indicating the total number of USSD Messages constituting the Concatenated USSD Message. The value shall start at 1 and remain constant for every USSD Message that makes up the Concatenated USSD message. If the value is zero then the receiving entity shall ignore the whole USSD Message.

Octet 3: Sequence number of the current USSD Message.

This octet shall contain a value in the range 1 to 255 indicating the sequence number of a particular USSD Message within the Concatenated USSD Message. The value shall start at 1 and increment by one for every USSD Message sent within the Concatenated USSD Message. If the value is zero or the value is greater than the value in octet 2 then the receiving entity shall ignore the whole USSD Message.

The UM field contains the actual application data (e.g. secure Command/Response Packets coded according to the present document).

In each USSD String in a concatenated series, the PFI and CCF fields shall be present.

Annex B (informative): Change History

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2005-06	CP-28	CP-050141	0005	-	B	Introduction of secured data download for USSD	7.0.0
2007-06	CP-36	CP-070301	0007	1	F	Correction of the reference to ETSI TS 102 225	7.1.0
2008-12	CP-42	CP-080907	0008	1	B	Introduction of AES and deprecation of DES	8.0.0
2009-03	-	-	-	-	-	Figure 2 fixed	8.0.1
2009-12	CT-46	CP-091011	0010	1	F	References update	8.1.0
2009-12	CT-46	CP-090995	0011	1	B	Secured message structure for HTTP	9.0.0
2011-03	SP-51					Automatic upgrade to Rel-10	10.0.0
2012-03	CT-55	CP-120148	0014	1	A	Correction to ETSI TS 102 225 reference	10.1.0
2012-09	CT-57	CP-120623	0016	3	C	Enhancements to the security of the SMS OTA download mechanisms	11.0.0
2013-03	CT-59	CP-120148	0023	2	B	Update of references to ETSI TS 102 225 and 3GPP TS 24.090 specifications	12.0.0
2014-12	CT-66	CP-140961	0025	-	F	Correction of handling of Proof of Receipt	12.1.0
2015-06	CT-68	CP-150388	0026	-	F	Correction of handling of Proof of Receipt	12.2.0
2015-12	SP-70			-		Automatic upgrade to Rel-13	13.0.0
2017-03	SA-75	-	-	-	-	Automatic upgrade to Rel-14	14.0.0
2019-01	CT-81			-		Automatic upgrade to Rel-15	15.0.0
2020-03	CT#87e	CP-200088	0034	-		Secured packet usability in networks beyond GSM and 3G	16.0.0
2022-04	CT#95e	-	-	-	-	Update to Rel-17 version (MCC)	17.0.0

History

Document history		
V17.0.0	April 2022	Publication