ETSI TS 131 115 V15.1.0 (2020-07)

TECHNICAL SPECIFICATION

**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 15.1.0 Release 15)**

Reference

RTS/TSGC-0631115vf10

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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

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.

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].

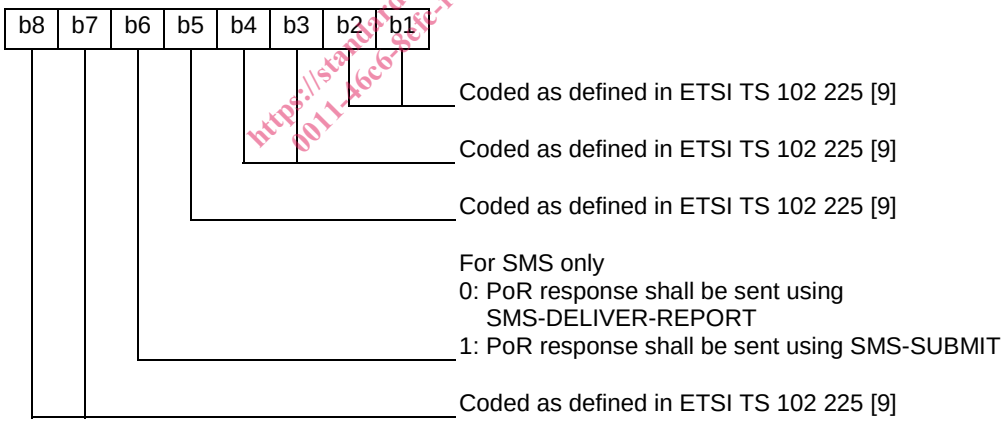
NOTE: Whilst not absolutely necessary in this particular instance, this field is necessary for the case where concatenated Short Message is employed (see clause 4.3).

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: