Nexo Revista Científica
Vol. 35, No. 04, pp. 1021-1047/Diciembre 2022

ISSN-E 1995-9516
Universidad Nacional de Ingeniería

http://revistas.uni.edu.ni/index.php/Nexo
https://doi.org/10.5377/nexo.v35i04.15543

A review of short message service protocol

Una revisión del protocolo de servicio de mensajes cortos

Sayed Javad Mousavi, Kamal Chaharsooghi*, Gholam Ali Montazer

Department of Information technology, Industrial engineering Faculty, Tarbiat Modares University, Tehran, Iran.
*Corresponding author E-mail: skch@modares.ac.ir

(recibido/received: 12-agosto-2022; aceptado/accepted: 21-octubre-2022)

ABSTRACT

There are many ways to send and receive an electronic message, but SMS is more popular and nowadays used for one time password (OTP) as a part of authentication in many web applications, internet of things (IoT) access, password reset, mobile banking (M-banking), etc. Therefore, we must know how the protocol works and about its security. This protocol is designed to manage federatively (i.e., the mobile network is managing partially by many independent operators and it doesn't need to have a central operator for the whole network. Also, many independent centrally managed networks can connect together to make a bigger network). We reviewed SMS protocol and its network structure, message structure, network entities, entities' connection, and some security-related issues. Finally, this protocol is evaluated if it can provide Identification, Authentication, Integrity, Nonrepudiation, Confidentiality, and Availability.

Keywords: SMS, short messaging system, Security, Network entity, transfer layer, Application layer, Relay layer, Transfer protocol data unit, Transfer protocol user data, Short message types.

RESUMEN

Hay muchas formas de enviar y recibir un mensaje electrónico, pero el SMS es más popular y hoy en día se usa para la contraseña de un solo uso (OTP) como parte de la autenticación en muchas aplicaciones web, acceso a Internet de las cosas (IoT), restablecimiento de contraseña, banca móvil (M-banking), etc. Por lo tanto, debemos saber cómo funciona el protocolo y sobre su seguridad. Este protocolo está diseñado para gestionar de forma federativa (es decir, la red móvil está gestionada parcialmente por muchos operadores independientes y no necesita tener un operador central para toda la red. Además, muchas redes independientes gestionadas de forma centralizada pueden conectarse entre sí para hacer un mayor la red). Revisamos el protocolo SMS y su estructura de red, estructura de mensajes, entidades de red, conexión de entidades y algunos problemas relacionados con la seguridad. Finalmente, se evalúa si este protocolo puede proporcionar Identificación, Autenticación, Integridad, No repudio, Confidencialidad y Disponibilidad.

Palabras clave: SMS, sistema de mensajería corta, seguridad, entidad de red, capa de transferencia, capa de aplicación, capa de retransmisión, unidad de datos del protocolo de transferencia, datos de usuario del protocolo de transferencia, tipos de mensajes cortos.

1 NTRODUCTION

There are lots of messaging protocols, nevertheless, we focused on the Short Messaging System protocol as a popular messaging protocol. This protocol has no central authority, therefore, it's more scalable. Also, it gives the user ability to change its service provider without losing his/her contacts. Each identity is unique over the entire network, but, if a user changes its service provider, its identity will change, and if he/she has his/her contacts so he/she can communicate with them again. So, it's obvious that a user can communicate with any user over the network without the need to change its service provider.
We tried to detail the protocol as can as possible to enable us to evaluate it. SMS has long practical experiences, so it has a very large functional system. Besides, due to its too many GSM Technical Specifications, it has many changes. Also, it has its physical infrastructure. Therefore, it needs more details. SMS is more mature than other protocols. We should pay attention that every single change in a protocol should be backward compatible. The backward compatibility helps systems still work with old nodes. Therefore, SMS has lots of specifications.
We know, SMS is used as part of many authentications in web-based services like all Google services, Yahoo Mail, and many other less popular web-based services. It's because SMS is more available and easy to use for end-users. What if the SMS has a security issue. In this paper, we tried to clearly address SMS security by evaluating the Identification, Authentication, Integrity, Nonrepudiation, Confidentiality, and Availability.
In section 2 we briefly introduce the short messaging service. In section 3 network entities and their connection are described. Section 4 describes the network layers in brief. More details are in the following sections. Section 5 describes the physical layer that consists of two or three layers, and also, is the more complicated part of the network. Section 6 describes the relay layer and its data packet structure that passes between the layer entities. Section 7 describes the transfer layer and its packet structure which is called the Data Unit. Section 8 is mostly focused on the layer packet called User Data. In section 9, we evaluate the system from the security point of view including Identification, Authentication, Integrity, Nonrepudiation, Confidentiality, and Availability.

2 SMS network

The first SMS was sent on third December 1992, and its text was "Happy new year". It was sent by an engineer to his coworker (BBC, 2002). SMS is part of GSM[1] surplus services. GSM was developed by ETSI[2] for the second-generation (2G) digital cellular network. This mobile cellular network officially began to work in Finland in 1991(Huurdeman, 2003). In the next section, we'll review network architecture, making of SMS, and SMS transmission according to GSM specifications.

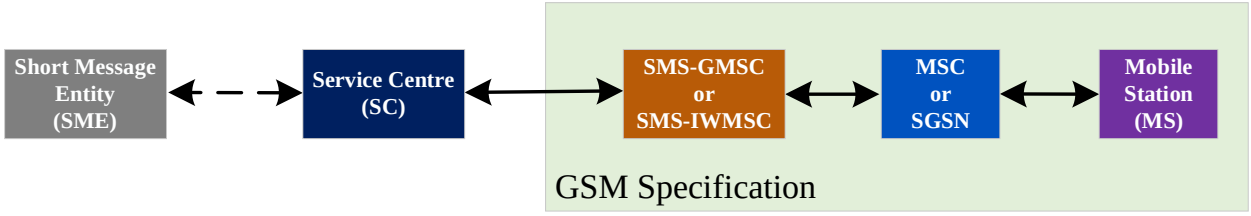

Figure 1: entities directly contribute to SMS service

[1] Global System for Mobile communication
[2] European Telecommunications Standards Institute

3 Network entities

Figure 1 shows the transmission of an SMS from an originator (that can be a mobile device) to an SMS Entity (That can be a mobile device or another device capable of sending an SMS) through other network entities.

In the GPRS network, SMS goes through SGSN[3] instead of MSC. An operator can merge SMS-GMSC[4] or SMS-IWMSC[5] with SC. GSM has no condition on the connection between SC and SMS-GMSC or SMS-IWMSC below the transfer layer but there is a condition on the SC itself as part of the SMS network that is described in the 3GPP TS 23.040 (ETSI, 2020b). This specification has some suggestions for an appropriate lower layer but it can define in the agreement between SC and PLMN. Therefore, the connection to SC and the connection of SC to other SMEs is out of the GSM specification. SMS network is part of PLMN[6] that can connect to a PSTN[7], so an SME can be an entity inside the connected PSTN. But we only address SMS in a PLMN or between PLMNs. An SC can connect to multiple PLMNs at the same time, so it can connect to multiple SMS-GMSC or SMS-IWMSC.

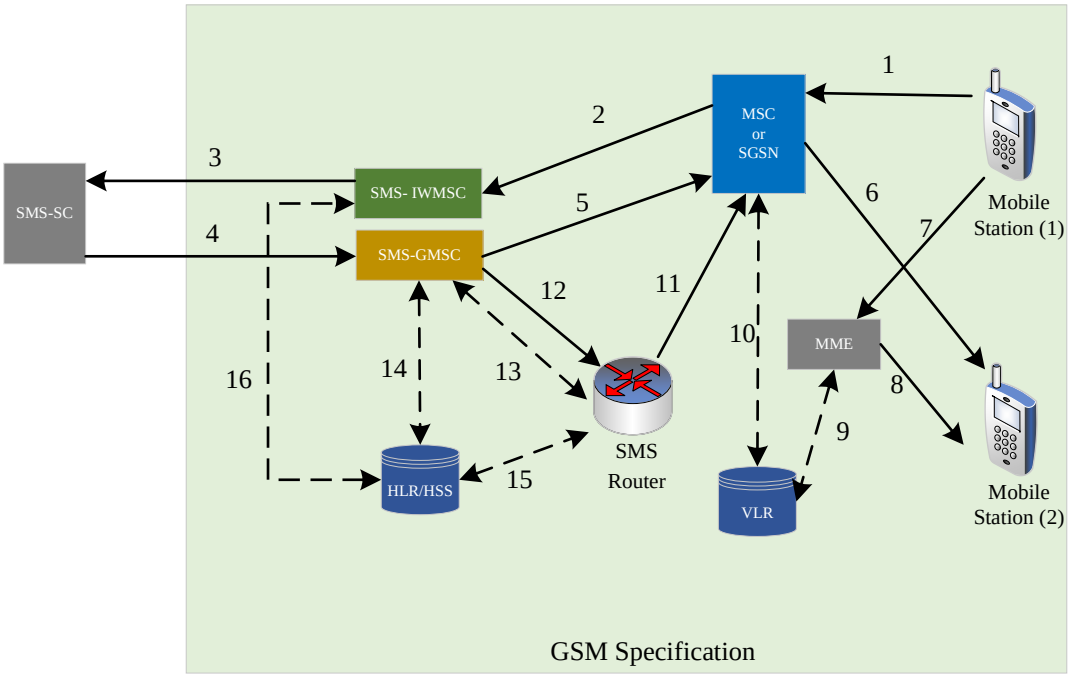

Figure 2: Short message entities inside the GSM network in transfer layer (ETSI, 2020b; Peersman et al., 2000). SMS data moves on the black lines and necessary routing data moves on the dashed lines.

3.1 Structure of SMS entities and their connection inside the PLMN

Short message entities of a GSM network are shown in Figure 2. This figure contains entities of a specific PLMN. In more a general case many PLMNs can connect to each other to help an SMS originate in one PLMN and receipt in the other. Also, delivery or error reports can originate in one PLMN and receipt on the other. Figure 2 illustrates originated short message or report from one mobile device and then goes to the SC. Then, it shows originated short message or report from SC and then goes to the other mobile

[3] Serving GPRS Support Node
[4] Gateway MSC for Short Message Service
[5] Interworking MSC For Short Message Service
[6] Public Lands Mobile Network
[7] Public Switched Telephone Network

device. Therefore, these two paths are different, MS[8] to SC and SC to MS. According to 3GPP TS 23.040 (ETSI, 2020b), one SC can connect to many PLMN so it can connect to many MSC. Each PLMN defines a specific number for connected SC. In Figure 2, if the type of network is EPS[9], the SMS should go through line 7 to MME[10] and then SMS goes from MME to MS on line 8. MME only works as a relay on the EPS network. This kind of network is described in 3GPP TS 23.272 (ETSI, 2020c). Also, the 5G network has similar entities but the network architecture and functionalities of entities are more advanced and included functions and entities addressed in this paper according to 3GPP TS 23.501 (ETSI, 2021a).

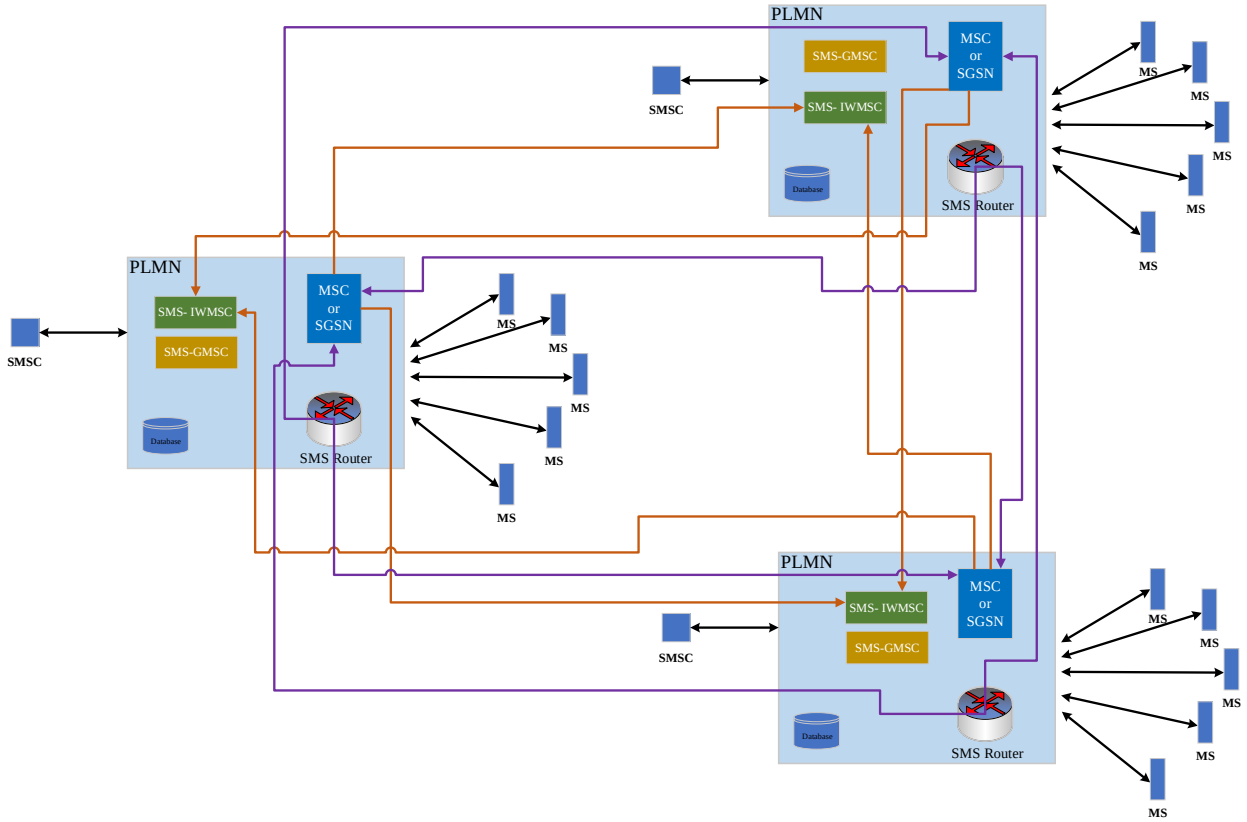

Figure 3: An example of how two or more PLMNs are connected to send and receive SMS. Orange line depicts a connection to MSC or SGSN while it has visitor MS. Each violet line depicts a connection from MSC o SGSN to SMS-IWMSC while it is in another PLMN and has the recipient MS.

3.2 SMS originated in MS

According to Figure 2, originated short message goes through line 1 from MS to MSC or SGSN. This Short message has SC's address. This address is defined according to PLMN rules. If originating MS was in its PLMN, the short message would go through line 2 from MSC or SGSN to SMS-IWMSC. If MS was in the visiting PLMN (i.e. not its original PLMN), the short message would deliver to its SMS-IWMSC by visiting PLMN. There may be some network between visiting PLMN and MS original PLMN. Then, depending on operator configuration, SMS-IWMSC searches the HLR[11] database through line 16. The result of this search is the IMSI[12] of the recipient MS. Also if the recipient was from another network, it

[8] Mobile Station
[9] Evolved Packet System
[10] Mobility Management Entity
[11] Home Location Register
[12] International Mobile Subscriber Identity

would identify the agreement between the current PLMN and the recipient's PLMN if it exists. If MS is from the current PLMN, the short message would go through line 3 to deliver to SC.

3.3 MS terminating short message

According to Figure 2 short message goes through line 4 from SC to SMS-GMSC. This entity searches HLR through line 14. The result of the search is a path to the recipient's MSC or SGSN. If the recipient's MSC or SGSN was at the current PLMN, the short message would go through line 5 otherwise it goes through line 12 from SMS-GMSC to SMS Router. If the short message went to the SMS Router, it would send the short message through line 11 to the recipient's MSC or SGSN in the recipient's PLMN. In both cases either recipient in the current PLMN or another PLMN, the short message will be delivered to the recipient's MS through line 6 (ETSI, 2020b). Before delivery of the short message, MSC or SGSN needs the Current Location Area Identification and Connection Status of the MS, that MSC or SGSN should query the VLR[13]/HSS[14] through line 10 for them (ETSI, 2021b). If SMS Router exists in the network (SMS Router is optional), the routing information to the recipient's MSC or SGSN would send to HLR through line 14 and the result would go through line 15 to SMS Router. It stores the originator's SMS-GMSC information and sends back the information to HLR through line 15. Then HLR sends a confirmation of the received information and a command to inform the SC to SMS Router through line 15. Then, the SMS Router should send all necessary parameters to SMS-GMSC through line 13.

3.4 Multi-PLMN SMS

SMS transfer from visitor MS to its recipient and SMS transfer from MS to a recipient in another PLMN described in the section 3.2 and 3.3. Accordingly, the connections between two or more PLMN can be illustrated as depicted in Figure 3. This is a simplified example. In reality, an SMS may pass through many PLMNs to submit to its recipient.

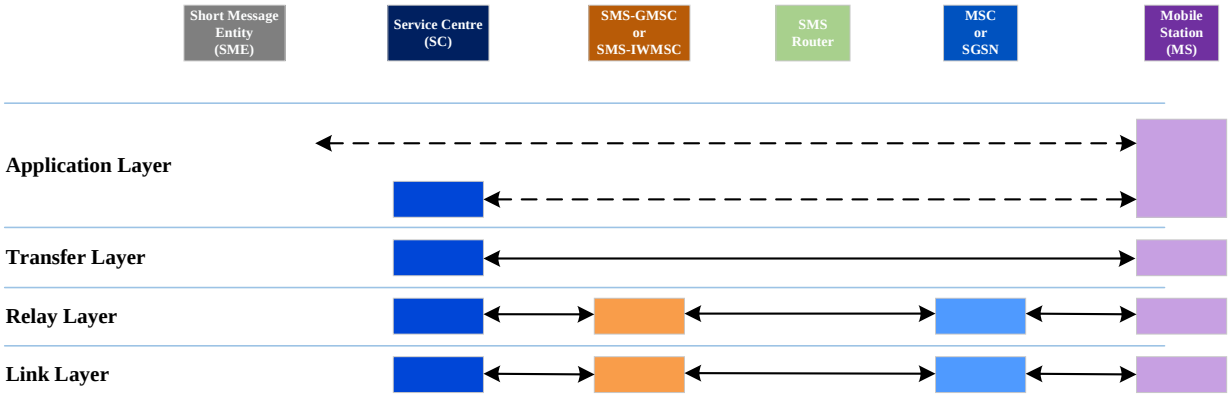

Figure 4: SMS entities and network layers (ETSI, 2020b)

4 Network layers

According to (ETSI, 2001) SMS entities in the 3G, 4G, LTE[15], and 5G[16] can be illustrated as in Figure 4. SMS Router doesn't exist in the primary GSM network and GPRS network. SMS Router is an optional functional entity, that is only needed for MS terminating SMS (SMS from SC to MS). In this figure, an SMS Router is only needed when an SMS goes from left to right. Each entity illustrated in Figure 4 is described as follows.

[13] Visitor Location Register
[14] Home Subscriber Server
[15] Long Term Evolution
[16] Fifth generation technology standard for broadband cellular networks

MS[17]: a mobile device or a device that can connect to a BTS[18] and send or receive an SMS. Also, you should put SIM[19] in it (Peersman et al., 2000).
MSC[20]: one of the network's main components that is similar to a switching node in the PSTN[21] and ISDN[22]. Also, it can do subscriber-related functions like registration, authentication, location update, Handover, and routing to roaming subscribers. MSC is agate to PSTN or ISDN and a medium for SC (Peersman et al., 2000).
SGSN[23]: service support for GPRS. This node is an exchange for the packet switching function. The geographical area of connected MS to this network is called SGSN (ETSI, 2001).
SMS-GMSC[24]: SMS gateway is one of the MSC functions to receive SMS from SC. After receiving SMS according to its headers, searches HLR for routing and send it to MS's SGSN or VMSC[25] (ETSI, 2001).
SMS-IWMSC[26]: SMS exchange is one of the MSC functions that receive SMS from inside the PLMN and sends it to SC (ETSI, 2001).
SC[27]: Service center is a function in the mobile network to relay, store, and forward SMS between SME and MS. SC isn't part of GSM PLMN but can be integrated with MSC (ETSI, 2001).
SME[28]: can be any device with the ability to send and receive SMS, like an SMS device in PSTN or ISDN, MS in another PLMN, or another SC.
Each MS-originated SMS must deliver to the SC. Then, SC regenerates another SMS according to the received SMS and sends it to its destination recipient address.
Each layer in Figure 4 has its specific packet data. This packet generates by its layer entity according to the layer protocol. The Data packet name of each layer is listed in Table 1. In the transfer layer, SC and MS are communicating independently. It does even not depend on other PLMN devices when it goes through other PLMN. SMS body and headers do not change. In the relay layer, SMS headers may change from MS to SC, but SMS headers don't change between every two peers in Figure 5 and Figure 6. These peer connect directly in the SM-RL layer. Each entity in the SM-RL layer is a function in the SMS network and is independent of network physical devices. In lower layers, physical devices are connected to each other, and packet structure varies from one peer to another peer (ETSI, 2001).
Each data packet in Table 1 is described in the following sections. Packet headers in the SM-RL may change from entity to entity for the exact same message. Some of the header fields remain after went through some entities but their value may change. SM-LL layer protocols define the physical connection between network devices and their services. In the circuit-switched service networks, the connection between MSC and MS consists of three sub-layers (ETSI, 2020a).

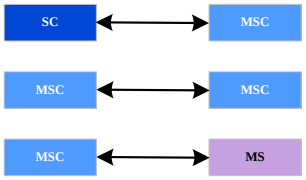

Figure 5: Independent connected entities in the SM-RL layer

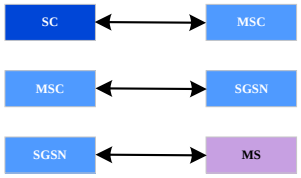

Figure 6: Independent connected entities in the SM-RL layer of the GPRS network

[17] Mobile Station (or simply a mobile device)
[18] Base Transceiver Station
[19] Subscriber Identity Module
[20] Mobile Switching Centre
[21] Public Switched Telephone Network
[22] Integrated Services Digital Network
[23] Serving GPRS Support Node
[24] Gateway MSC for Short Message Service
[25] Visited MSC
[26] Interworking MSC For Short Message Service
[27] Service Center
[28] Short Message Entity

Table 1: Data packet and protocols of each layer in the SMS network

Layer	Data Packet
Application layer (SM-AL[29])	TP-UD[30]
Transfer Layer (SM-TL[31])	TPDU[32]
Relay layer (SM-RL[33])	Data packet structure and its protocol depend on connected entities
Lower layers (SM-LL[34])	Data packet structure and its protocol depend on connected entities

The three sub-layer of SM-RL between MSC and MS are as follows (ETSI, 2020a).

- CM-sublayer[35]
- MM-sublayer[36]
- RR-sublayer[37]

Also, the connection between SGSN and MS in the GPRS-based network in A/Gb mode (i.e connection between MS and network core is established through BSC and BTS (ETSI, 2020g)) consists of the following three sub-layers (ETSI, 2020a).

- CM-sublayer[38]
- LLC-sublayer[39]
- GRR-sublayer[40]

Also, the connection between SGSN and MS in the packet-switched service networks in the S1 mode (i.e tunneling between MS and MSC through Packet Switched connection) consists of the following two layers (ETSI, 2020a). Packet Switched connection is a peer-to-peer UMTS[41] (or 3G) connection between MS and a node in the domain of the core network. Some circuit switching functions can be done by MMS in the EPS system.

- CM-sublayer
- In the MSC side SGs[42] sub-layer and in the MS side EMM[43] sublayer

The connection between MS and MME in the packet-switched service network in the S1 mode (i.e transfer message between Ms and MME through MME layer) consists of the following two sub-layer (ETSI, 2020a).

- CM-sublayer
- EMM-sublayer

The connection between MS and SMSF[44] in the N1 mode (i.e send and receive a message to and from 5G core network entities) consists of the following three sublayers (ETSI, 2020a).

[29] Short Message Application Layer
[30] Transfer Protocol User Data
[31] Short Message Transfer Layer
[32] Transfer Protocol Data Unit
[33] Short Message Relay Layer
[34] Short Message Lower Layers
[35] Connection Management Sublayer
[36] Mobility Management sublayer
[37] Radio Resource Management sublayer
[38] Connection Management Sublayer
[39] Logical Link Control Sublayer
[40] GPRS Radio Resource Sublayer
[41] Universal Mobile Telecommunications System
[42] Signaling Gateways
[43] Evolved Packet System (EPS) Mobility Management sublayer

- CM-sublayer
- In the SMSF side N2 sub-Layer and in the MS side 5GMM sub-layer

On the other hand, according to (ETSI, 2001)., the connection between SMS-GMSC/SMS-IWMSC and MSC/SGSN in the SM-RL and SM-LL has two different types.

1. SMS-GMSC/SMS-IWMSC and MSC/SGSN in the same PLMN
2. SMS-GMSC/SMS-IWMSC and MSC/SGSN in the different PLMN

In the first one, the PLMN operator selects one of the following protocols.

- PSPDN
- SS7

In the second one, SS7 is the default protocol otherwise it defines by the operator's agreement (ETSI, 2004).

There is no defined protocol in the SM-RL and SM-LL between SMS-GMSC/SMS-IWMSC and SC. SC and PLMN operators define it in the agreement with following criteria (ETSI, 2001).

1. Provide all necessary services for SM-RL
2. Should be based on an accepted protocol in the general domain
3. Should allow internal open communication

An SC can connect to multiple PLMN and multiple different MSC (i.e different SMS-GMSC/SMS-IWMSC) inside a PLMN.

5 Network function in the SM-LL layer

As mentioned previously, the connection between SMS-GMSC/SMS-IWMSC and SC is not defined as well as the connection between SMS-GMSC/SMS-IWMSC and MSC/SGSN, these are up to the operators of PLMN and SC. Therefore, we can only address the connection between MSC/SGSN and MS. SM-LL in this connection has two to three sub-layers that describe in the following sections.

5.1 CM sub-layer

This layer produces necessary services to the Relay layer. Entities in this sub-layer and lower sub-layers are called SMC[45]. SMCs inside MS and inside SGSN/MSC connect each other using SM-CP[46] protocol.

Regardless of GPRS or GSM connection, MS must have at least two SMEs (i.e two for GPRS and two for GSM). These two SMEs can provide simultaneous send and receive of SMS. It must not use the two SMEs in one direction (e.g only send or only receive).

Similar to MS, MSC/SGSN must have two SMEs per connection to be able to handle concurrent send and receive. More details are in (ETSI, 2020a).

5.2 MM sub-layer

Mobility management sub-layer supports user terminal. For example, it informs the network of the current MS location. Also, it can provide privacy for user identification. MM sub-layer should provide connection management services for CM sub-layer. All MM procedures could be done if the RR connection between MS and the network was established, otherwise, MM will establish the RR connection (ETSI, 2003).

5.3 RR sub-layer

This sub-layer manages shared radio resources (e.g physical channel and data link communication over control channel). The main purpose of this layer is to establish, maintain, and release RR connections that allow point-to-point conversation of MS and the network. This conversation includes cell selection and reselection and handover (ETSI, 2020a).

---

[44] SMS Function (5G)

[45] Short Message Control

[46] Short Message Service Control Protocol

5.4 LCC sub-layer

It provides a reliable logical link between MS and SGSN. LCC sub-layer is completely independent of lower sub-layers, therefore it can be used over any type of GPRS radio link. The purpose of the LCC protocol is to deliver information to the layer's entities and it supports the following (ETSI, 2020d).

- Support multiple MS in one interface
- Support multiple layer's entities in one MS

Sub-layer functions are as follows.

- Provide multiple logical links separated by DLCI[47]
- Preservation of frames sequences on the logical link (sequence control)
- Detection of transfer error, format error, and operation error on a logical link
- Recovery of transfer error, format error, and operation error
- Notification for irrecoverable error
- Flow control
- Using a hash algorithm to ensure data accuracy

5.5 GRR sub-layer

The purposes of this layer, in brief, are as follow (ETSI, 2020f).

- Assign and release resources of GPRS channels
- Supervising GPRS channels to detect low utilized and congestion channel
- Initiation of the congestion control procedure
- Distribution of GPRS channel configuration information to MSs.

5.6 GMM sub-layer

Mobility management is the layer's protocol task, that includes attaching GPRS, detaching GPRS, security, routing area update, location update, activation context for PDP[48], and deactivation of PDP (ETSI, 2020f).

5.7 SGs sub-layer

This layer is responsible for mobility management and paging between EPS[49] and CS[50]. Also, specifically, this layer can be used for MS originating and MS terminating SMS (ETSI, 2020c). SGs interface can be used for connection between VLR and MME. Also, this interface can be used in some processes related to circuit-switched through MME. Specific messages relay related to GSM circuit-switched services and location management coordination can be done using messages on the SGs interface that are used between an MME in EPS and VLR. Stream control transmission protocol is also used in this layer (ETSI, 2020e).

5.8 EMM sub-layer

The main purpose of this layer is to support the mobility of user's devices, which includes informing the network about the device's current location and privacy of user identity. Also, it provides services to the session management layer and SMS entity in the CM[51] layer. It must initiate the establishment of NAS[52] signaling connection, and only after the establishment of this connection, EMM operations can be done. This layer also should do the authentication, secure mode control, and identification (ETSI, 2021c).

---

[47] Data Link Connection Identifier
[48] Packet Data Protocol
[49] Evolved Packet System
[50] Circuit Switched
[51] Connection Management
[52] Non-Access Stratum

5.9 N20 sub-layer

In this layer, the N20 messages transfer between AMF[53] and SMSF. AMF forwards MS messages to SMSF. AMF adds IMEISV information, MS's current location, and local time zone to the message. According to this information, SMSF can record an accurate charge (ETSI, 2021d).

5.10 5GMM sub-layer

The main functions of this sublayer are as follows.

- Providing transfer service from core network entity message to MS.
- Alow the network function to subscribe or unsubscribe in a specific message notification from MS to the core network.
- Alow the network function to subscribe or unsubscribe in a specific information notification of AN[54].
- Providing service to initiate messages toward AN.
- Security context management
- Transfer and management of MS information

This sub-layer is connected to the AMF, including handover capability, sending SMS on NAS, location-based services, continuity of single radio call, optimization of radio capability signaling, authentication, authorization to the one part of the network, CIoT[55] support, and WUS[56] transfer (ETSI, 2021a).

Table 2: the naming of connections in SM-RL

Connected entities	Connection name
SC $\rightleftarrows$ MSC	C_1
MSC $\rightleftarrows$ MSC	C_2
MSC $\rightleftarrows$ MS	C_3
MSC $\rightleftarrows$ SGSN	C_2'
SGSN $\rightleftarrows$ MS	C_3'

6 All data units in the relay layer (SM-RL[57])

There are different packet types between different entities according to GSM technical specifications. There 6 types of messages with specific headers. These 6 types of messages are as follows (ETSI, 2001, 2020b).

RP-MO-DATA[58]: carrying TPDU packet data of upper layer from MS to SC (TPDU will explain later).
RP-MT-DATA[59]: carrying TPDU packet data of upper layer from SC to MS.
RP-ACK[60]: conformation of RP-MO-DATA, RP-MT-DATA, or RP-SM-MEMORY-AVAILABLE.
RP-ERROR[61]: informs the originator entity of unsuccess transfer of RP-MO-DATA or RP-MT-DATA.
RP-ALERT-SC[62]: to inform SC that MS is in the recovery operation. Information goes from HLR to SC.
RP-SM-MEMORY-AVAILABLE[63]: to inform the network that MS has memory to receive one or more SMS. Information goes from MS to HLR.

[53] Access and Mobility Management Function
[54] Access Network
[55] Cellular IoT
[56] Wake Up Signal
[57] Short Message Relay Layer
[58] Relay Protocol Mobile Originated Data
[59] Relay Protocol Mobile Terminated Data
[60] Relay Protocol Acknowledging
[61] Relay Protocol Error
[62] Relay Protocol Alert Service Center
[63] Relay Protocol Short Message Memory Available

Data elements of each message (packet) will explain in the following sections. This message transfer between peers in Figure 5 and Figure 6. Every two connected peers are named as in Table 2.

Table 3: Data element of RP-MO-DATA in SM-RL layer

Data element	Connection name					Description
	C_1	C_2	C_3	C_2'	C_3'	
RP-OA[64]	*	*	∅	*	∅	Originating MS address
RP-DA[65]	∅	*	*	*	*	SC recipient address
RP-UD[66]	*	*	*	*	*	** Parameter includes TPDU
* Mandatory at the connection ∅ The field doesn't exist in the connection ** Transfer Protocol Data Unit for the above layer						

Table 4: Data elements of RP-MT-DATA in SM-RL layer

Data element	Connection name					Description
	C_1	C_2	C_3	C_2'	C_3'	
RP-PRI[67]	*	∅	∅	∅	∅	If originator SC has some messages to deliver, this parameter defines whether the message transfer or not.
RP-MMS[68]	O	O	∅	O	∅	This parameter defines whether more messages are in the SC or not to deliver.
RP-OA	*	*	*	*	*	Originator SC address
RP-DA	*	*	∅	*	∅	Recipient MS address
RP-UD	*	*	*	*	*	** Parameter includes TPDU
RP-MTI[69]	O	∅	∅	∅	∅	This parameter defines whether the TPDU is a message or a delivery report
RP-SMEA[70]	O	∅	∅	∅	∅	Originator SME address
* Mandatory parameter for the connection ∅ Doesn't exists in the connection O Optional for the connection ** Transfer Protocol Data Unit for the above layer						

6.1 RP-MO-DATA

All data elements of this packet are listed in the Table 3. Also, this table informs if an element is mandatory or not in the specifically mentioned connection. The number of bytes and other criteria of each element varies according to its connection and is defined in the GSM 04.11 (ETSI, 2000) and 3GPP TS 24.011 (ETSI, 2020a).

6.2 RP-MT-DATA

The data elements of this packet are listed in Table 4. Also, it defines whether an element is mandatory, optional, or doesn't exist in the connection. More details about data elements are described in the GSM 04.11 (ETSI, 2000).

[64] Relay Protocol Originating Address
[65] Relay Protocol Destination Address
[66] Relay Protocol User Data
[67] Relay Protocol Priority Request
[68] Relay Protocol More Messages to Send
[69] Relay Protocol Message Type Indicator
[70] Relay Protocol originating SME-Address

6.3 RP-ACK

This packet only contains the RP-User-Data parameter, that this parameter includes TPDU. In this SM-RL packet, the TPDU can only contain SMS-SUBMIT-REPORT or SMS-DELIVER-REPORT for the above layer.

Table 5: Data element of RP- ERROR in the SM-RL layer

Data element	Connection name					Description
	C_1	C_2	C_3	C_2'	C_3'	
RP-MSI[71]	*	∅	∅	∅	∅	This element only exists in the packet from SMS-GMSC to SC. It informs about the WMI*** update.
RP-CS[72]	*	*	*	*	*	This parameter informs the error type in unsuccess message transfer.
RP-MSIsdn[73]	*	∅	∅	∅	∅	This parameter only exists when RP-MT-DATA transfer is unsuccessful due to unreachable MS or MS memory full. Therefore this parameter defines if the MS is unreachable or reachable but its memory is full.
RP-UD	O	O	O	O	O	** Parameter includes TPDU
* Mandatory parameter for the connection ∅ Doesn't exists in the connection ** Transfer Protocol Data Unit for the above layer *** MS-related data in the HLR or VLR and defines how many messages waiting in the one or more SCs due to unsuccessful delivery to MS.						

6.4 RP-ERROR

Data elements or parameters of this packet are listed in Table 5 with a brief description of each element. A more detailed description of each element is in GSM 04.11 (ETSI, 2000).

Table 6: Data elements of RP-ALERT-SC packet in the SM-RL layer

Data element	Connection name					Description
	C_1	C_2	C_3	C_2'	C_3'	
RP-MSIsdn RP-IMSI[74]	O	O	O	O	O	ISDN[75] identity of the MS
O Optional for the connection						

6.5 RP-ALERT-SC

As listed in Table 6, this packet only contains RP-MSIsdn or RP-IMSI parameters, that using each of them is optional but only one of them is mandatory. These parameters against the RP-ERROR parameter define MS is again reachable. Therefore, SC can try to deliver the message again. This message goes from HLR to SC.

6.6 RP-SM-MEMORY-AVAILABLE

As mentioned in Table 7, this packet only contains one parameter. This parameter only uses to inform SC that MS memory is empty and it's ready to receive the message.

Table 7: Data element of RP-SM-MEMORY-AVAILABLE in the SM-RL layer

Data element	Connection name	Description

[71] Relay Protocol MW Set Indication
[72] Relay Protocol Cause
[73] Relay Protocol international MS ISDN number
[74] Relay Protocol International-Mobile-Subscriber-Identity
[75] Integrated Services Digital Network

	C_1	C_2	C_3	C_2'	C_3'	
RP-IMSI[76]	*	*	∅	*	∅	International MS identity
* Mandatory parameter for the connection ∅ Doesn't exists in the connection						

7 Data units in the SM-TL[77] layer

TPDU[78] is responsible to transfer data in this layer. According to Table 8 and ilustration in Figure 7, bit number 0 and bit number 1 called TP-MTI in the first byte of TPDU defines message type. These two-byte can define 6 types and one reserve type of message. Type of message defines the application of other 6 bits of the first byte. Also, it defines other headers bytes (octets). In brief, this layer adds the TPDU header to TP-UD as the body. Also, there are some headers in the TP-UD packet that add by the application layer.

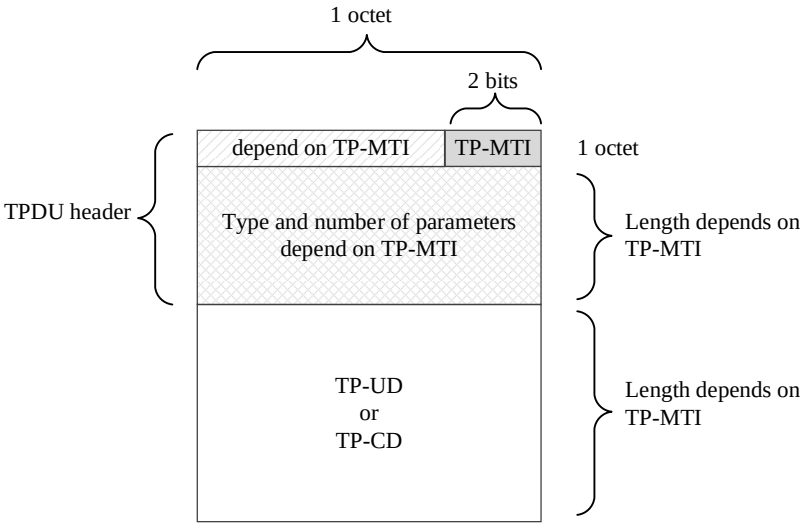

Figure 7: TPDU header and body in the SM-TL layer

Table 8: All message type the TP-MTI can define

Bit No. 1	Bit No. 2	Message type	Originator	Recipient
0	0	SMS-DELIVER	SC	MS
0	0	SMS-DELIVER REPORT	MS	SC
0	1	SMS-STATUS-REPORT	SC	MS
0	1	SMS-COMMAND	MS	SC
1	0	SMS-SUBMIT	MS	SC
1	0	SMS-SUBMIT-REPORT	SC	MS
1	1	Reserved	-	-

All message types are listed in Table 1. Each message type will explain separately in the following sections. Each parameter of these messages that are illustrated in the following sections will be briefly explained in section 7.7.

[76] Relay Protocol International-Mobile-Subscriber-Identity
[77] Short Message-Transfer Layer
[78] Transfer Protocol Data Unit

7.1 SMS-DELIVER

This type of message goes from SC to MS in the transfer layer. This layer adds some header to the TP-UD (or user data) packet. After adding headers, the structure of the message is as Figure 8. Each parameter in this figure is briefly explained in section 7.7.

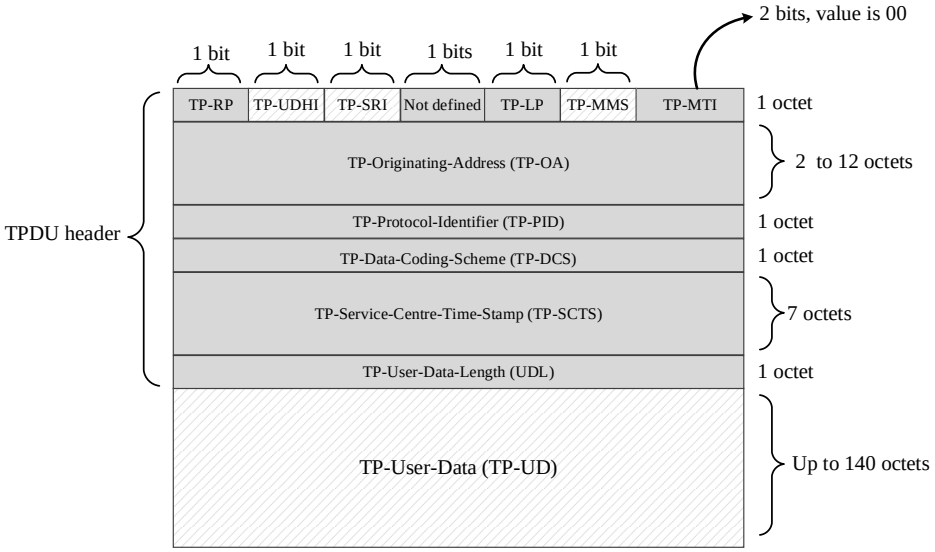

Figure 8: structure of TPDU message of type SMS-DELIVER. Crosshatched are optional.

7.2 SMS-DELIVER-REPORT

This message is a positive or negative confirmation of SMS-DELIVER or SMS-STATUS REPORT messages, that send as a response. Therefore it has two different structures, one for error and the other for confirmation. Each of them is explained in the following sections.

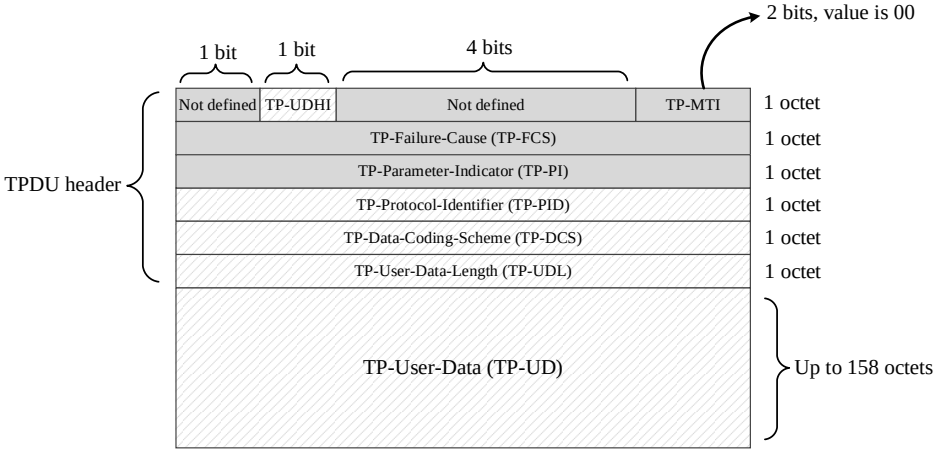

Figure 9: Header and structure of TPDU of type SMS-DELIVER-REPORT for error. Crosshatched are optional.

7.2.1 SMS-DELIVER-REPORT for error

Header elements of this message are illustrated in Figure 9. In this type of message, the TP-UD will only exist if the recipient is MS.

7.2.2 SMS-DELIVER-REPORT for conformation

Headers of this message type are illustrated in Figure 10. Also, it shows each header position and length in bit and byte. TP-UD will only exist if the recipient is MS.

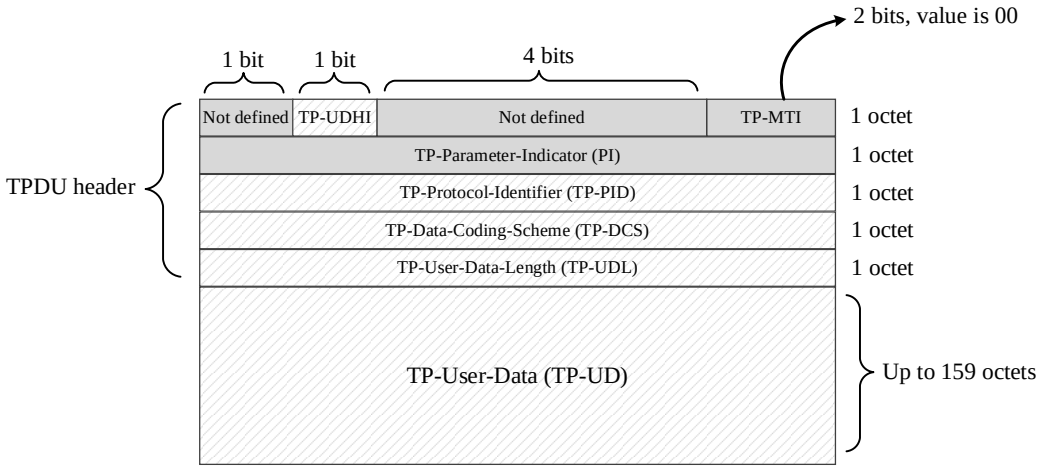

Figure 10: Header and structure of TPDU of type SMS-DELIVER-REPORT for conformation. Crosshatched are optional.

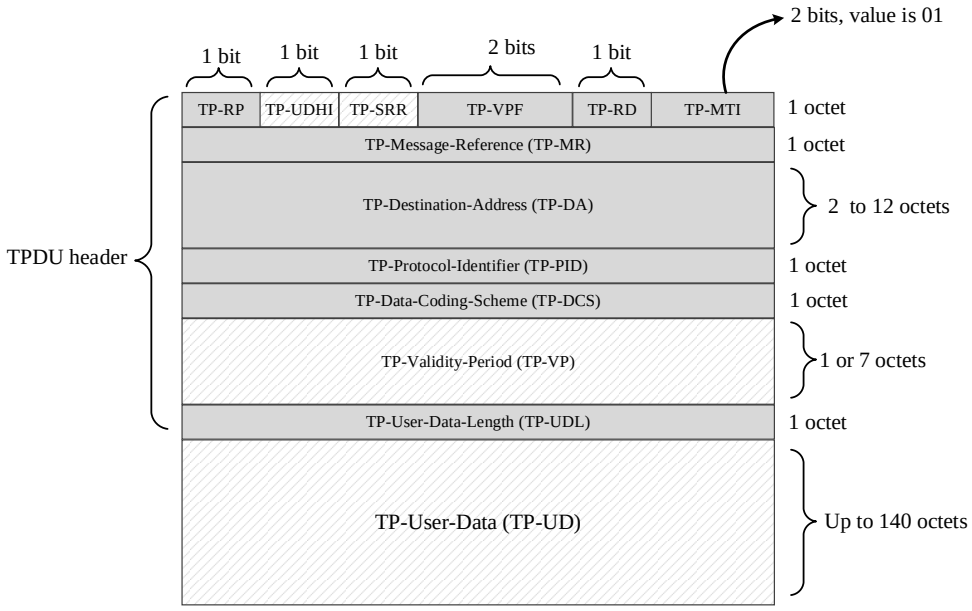

Figure 11: SMS-SUBMIT message type and its header. Crosshatched are optional.

7.3 SMS-SUBMIT

This message type goes from MS to SC. Body of this message type composed bay user. Therefore the end-user can write and read SMS-SUBMIT and SMS-DELIVER respectively. The body of this message includes the TP-UD packet from the above layer. This layer adds its headers to TP-UD to make the transport layer packet. The structure of this message is as Figure 11. Each parameter in this figure is briefly explained in section 7.7.

7.4 SMS-SUBMIT-REPORT

This message type is a response to SMS-SUBMIT or SMS-COMMAND and has two different types one for error and the other for confirmation. Each of them is described in the following section.

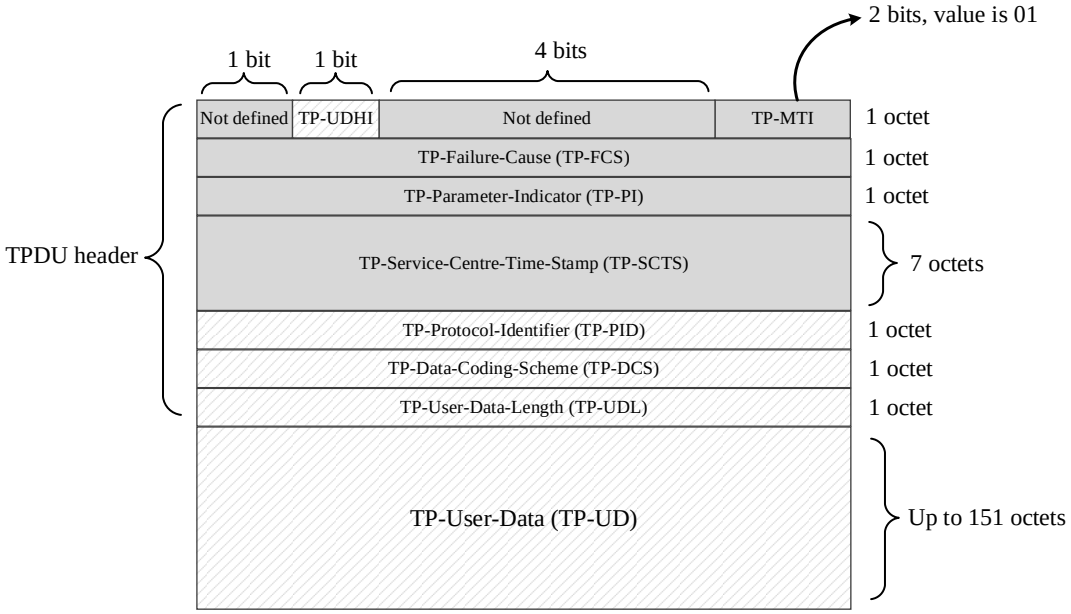

Figure 12: SMS-SUBMIT-REPORT message for the error. Crosshatched are optional.

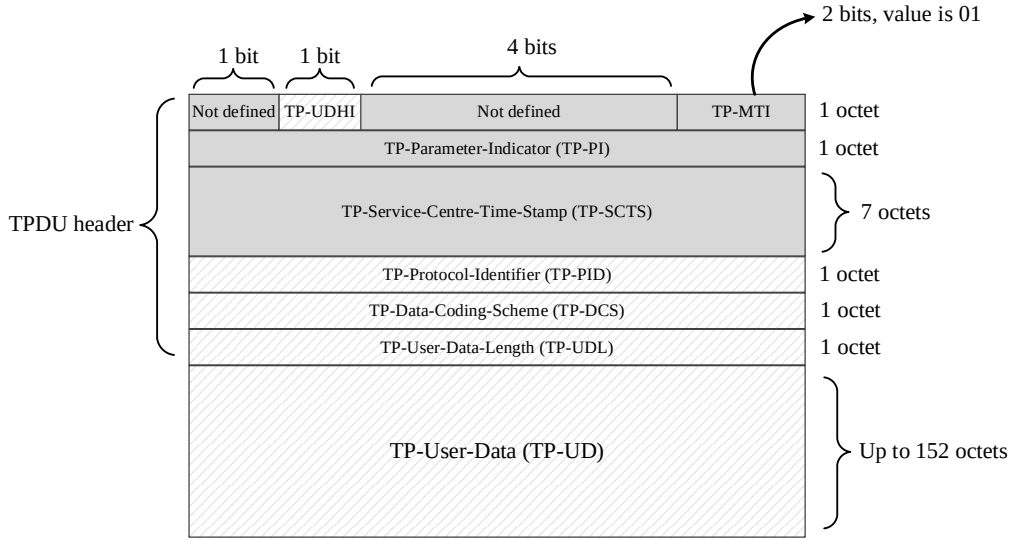

Figure 13: SMS-SUBMIT-REPORT message for the confirmation. Crosshatched are optional.

7.4.1 SMS-SUBMIT-REPORT for error

The structure of this message is illustrated in Figure 12. It includes mandatory and optional headers and their length in bit or byte.

7.4.2 SMS-SUBMIT-REPORT for conformation

The structure of this message is depicted in Figure 13. We tried to illustrate all necessary information like headers name, headers position, header length, and headers necessity in the packet's figure in all sections as well as in this section.

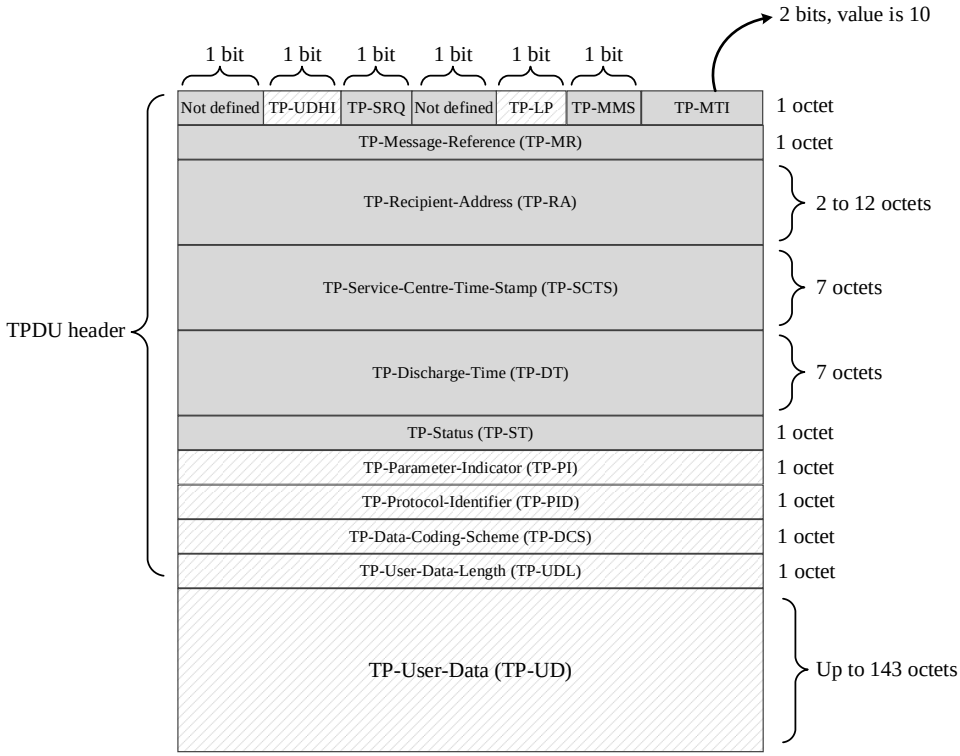

Figure 14: structure of SMS-STATUS-REPORT packet. Crosshatched are optional.

7.5 SMS-STATUS-REPORT

This message type is used to send the status report of SMS-COMMAND and SMS-SUBMIT from SC to MS. The structure of this message is depicted in Figure 14.

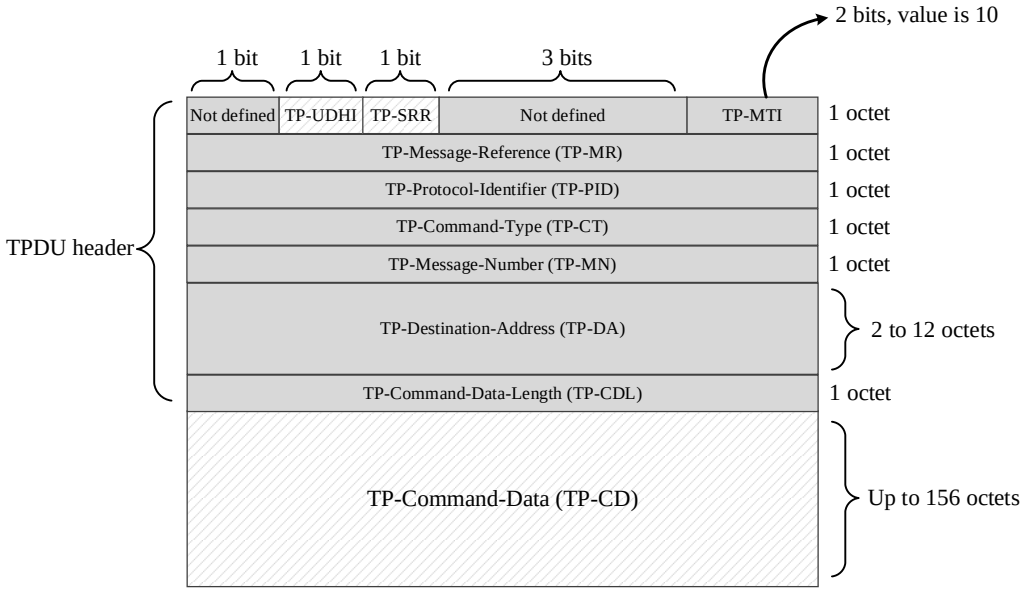

Figure 15: structure of SMS-COMMAND packet. Crosshatched are optional.

7.6 SMS-COMMAND

This message type is a command for MS to SC. The command can be a request to delete a message, cancel of TP-Status-Report-Request, ask for the status of an SMS, etc. The structure of this message is

illustrated in Figure 15. As similar to other packets, the figure contains header name, header length in bit or byte, header necessity, and header position. The header is sometimes called field, header field, parameter, or packet parameter. In the rest of the document we mostly use the word parameter as in the GSM technical specification.

7.7 Header fields (parameters) in the TPDU packet of all message type

There are many parameters in all TPDU message types. Some of them are common and some are specific to one type. Common parameters in the different message types are interpreted differently. All parameters are described in the following.

TP-Message-Type-Indicator (TP-MTI): This parameter defines message type. It was described in early section 7.

TP-More-Messages-to-Send (TP-MMS): it is a 1-bit parameter. If the value is 0, it means the length of the message is more than one. This parameter appears in the SMS-DELIVER and SMS-STATUS-REPORT. If its value is 0 in the SMS-STATUS-REPORT message it means some messages or reports are waiting to deliver to the MS.

TP-Loop-Prevention (TP-LP): This 1-bit parameter appears in the SMS-Deliver and SMS-Status-Report message. It defines to prevent from making a loop. If its value is 1, it means that it's a forwarded or spawned message.

TP-Status-Report-Qualifier (TP-SRQ): This 1-bit parameter appears in the SMS-STATUS-REPORT message. If its value was 0, this message would send to response to the SMS-SUBMIT message, otherwise, it's a result of the SMS-COMMAND message.

TP-Reject-Duplicates (TP-RD): It's a 1-bit parameter in the SMS-SUBMIT message. If its value was 1, it would say to SC that it sent a message with similar TP-DA and TP-MR from the same originating address. If it is redundant, SC deletes it and informs the MS. Sending the redundant message will be continued until MS is informed from SC. The number of sending repetitions is 1 to 3 times. After that, the user will inform about the message sending failure.

TP-Validity-Period-Format (TP-VPF): It's a 2-bit parameter in the SMS-SUBMIT message. This parameter defines the type of Time in the field TP-VP. That can have 4 types including Relative, Improved, Absolute, and Unavailable.

TP-Status-Report-Request (TP-SRR): It's a 1-bit parameter in the SMS-SUBMIT and SMS-COMMAND messages. If its value was 1, it would be a request from SC to inform about the current message status.

TP-Reply-Path (TP-RP): It's a 1-bit parameter in the SMS-DELIVER and SMS-SUBMIT messages. If its value was 1, the message would have the reply path parameter in its headers that is a specific SC address. In the SMS-SUBMIT message, MS informs SC to set the necessary parameters for the reply path in the message. In the SMS-DELIVER message, SC informs the MS that the reply path is in the TP-Originating-Address parameter and RP-Originating-Address parameter in the above layer.

TP-User-Data-Header-Indicator (TP-UDHI): It's a 1-bit parameter in all message types. If its value was 1, the TP-UD would have the header.

TP-Status-Report-Indication (TP-SRI): It's a 1-bit parameter in the SMS-DELIVER message. If its value is 1, the originating SME asks for the message status report from the recipient entity. The recipient entity can be MS or any other entity in the network.

TP-Originating-Address (TP-OA): it's a 2 to 12 byte (octet) in the SMS-DELIVER message. It contains the originator address according to addressing rules.

TP-Protocol-Identifier (TP-PID): It's a 1-byte (octet) in the all messages type. It defines the protocol of the above layer or shows the communication to the specific type of device.

TP-Command-Type (TP-CT): It's a 1-byte (octet) parameter in the SMS-COMMAND message. It defines the type of operation SMS-COMMAND asks from SC.

TP-Message-Number (TP-MN): It's a 1-byte (octet) parameter in the SMS-COMMAND message. It defines the SMS number before the current command. It's the value of TP-MR from the previous SMS.

TP-Data-Coding-Scheme (TP-DCS): It's a 1-byte (octet) in all message types except SMS-COMMAND message. It defines the Coding scheme (e.g 7-bit, 8-bit, UCS2, or … alphabet) in the TP-UD. Although, it defines the message category (3GPP, 1999).
TP-Service-Centre-Time-Stamp (TP-SCTS): It's a 7-byte parameter in the SMS-DELIVER, SMS-SUBMIT-REPORT, and SMS-STATUS-REPORT messages. It defines SC local time in the year, month, day, hour, minute, and second. Also, shows time zone difference from GMT[79].
TP-Discharge-Time (TP-DT): This parameter contains the time for the last try to deliver the message to its recipient. If an error occurred, it contains the time of the last try or time for a decision by SC. SC decision will be in the TP-ST parameter in the SMS-STATUS-REPORT message.
TP-Status (TP-ST): It's a 1-byte (octet) parameter in the SMS-STATUS-REPOR message. It contains the status of the last message sent to SC. SMS-STATUS-REPOR message is a response to SMS-SUBMIT and SMS-COMMAND messages.
TP-User-Data-Length (TP-UDL): This parameter is in all message types except SMS-COMMAND. It defines the length of the TP-UD including the header and body. But it depends on Coding Scheme. If it's 7-bit coding, the parameter contains the number of 7-bit bytes of TP-UD. If it's 8-bit or 16-bit coding, the parameter contains the number of 8-bit bytes of TP-UD. The 16-bit coding uses two 8-bit bytes to make a 16-bit byte.
TP-Failure-Cause (TP-FCS): It's a 1-byte (octet) parameter in SMS-SUBMIT-REPORT and SMS-DELIVER-REPORT messages. It contains the reason for error including unsuccess delivery or processing.
TP-Parameter-Indicator (TP-PI): According to (ETSI, 2010) published in 2010, it's a 1-byte (octet) parameter but can change to an arbitrary number of bytes. It appears in the SMS-DELIVER-REPORT, SMS-SUBMIT-REPORT, and SMS-STATUS-REPORT messages. Each bit in the first byte defines the existence of the optional parameter after the first byte. These bytes are in order of first byte bits.
TP-Message-Reference (TP-MR): This is a 1-byte (octet) parameter in the SMS-SUBMIT, SMS-STATUS-REPORT, and SMS-COMMAND messages. It contains the reference number of the message that is used in SC. MS increases this number 1 unit after each send and stores it in the Last-Used-TP-MR parameter in the SIM. It can change from 0 to 255. Therefore, using this parameter and TP-RD parameter the error and redundant messages are recognizable.
TP-Recipient-Address (TP-RA): This parameter appears in the SMS-STATUS-REPOR message. It contains an SME address. The address format is according to the addressing rules.
TP-Destination-Address (TP-DA): It appears in the SMS-SUBMIT and SMS-COMMAND messages. It defines the destination address of the message according to the addressing rules. In the SMS-COMMAND message, this parameter contains the address that TP-Command points to it.
TP-Command-Data-Length (TP-CDL): This parameter appears in the SMS-COMMAND message. It defines the number of bytes (octets) in the TP-Command-Data-field.
TP-Command-Data (TP-CD): This parameter appears in the SMS-COMMAND message. It contains data for requesting operation by MS. The TP-Command-Type parameter defines how to use this data.
TP-Validity-Period (TP-VP): This parameter appears in the SMS-SUBMIT message. According to the TP-VPF parameter, it has three types (00 value in the TP-VPF is not defined). These three types are as follows.

- Relative: It's a 1-byte parameter. It defines the validity of the SMS-SUBMIT message after it is delivered to SC.
- Absolut: It's a 7-byte (octet) parameter. It defines the absolute validity time of SMS-SUBMIT. In this type, the time format will be similar to TP-Service-Centre-Time-Stamp.
- Improved format: It's a 7-byte parameter. It contains a time interval, its format, and other options.

TP-User-Data (TP-UD): It appears in all messages except SMS-COMMAND. This parameter has its header and body and is described in the following sections.

[79] Greenwich Mean Time zone

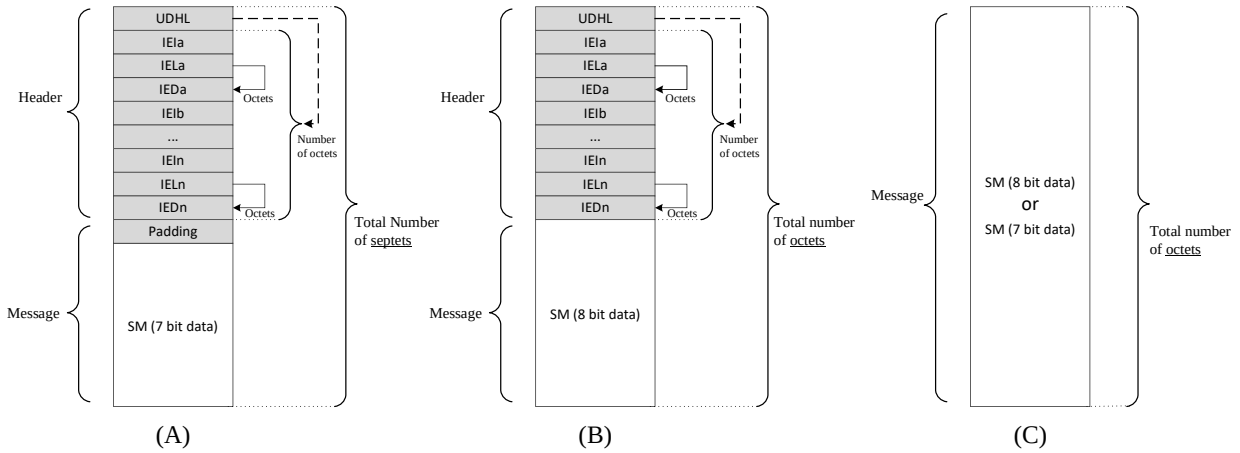

Figure 16: structure of SMS message or TP-UD. A) 7-bit coding, B) 8-bit coding, c) without header

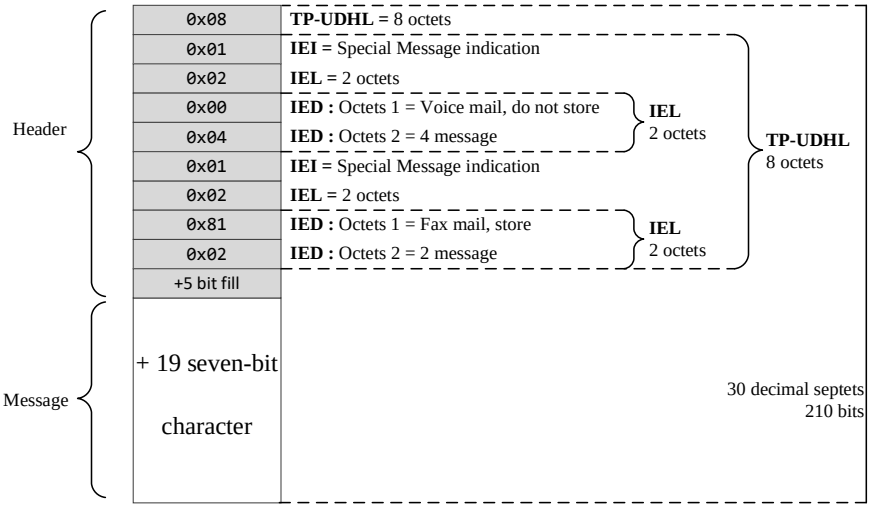

Figure 17: an example of a message with multiple special message indication headers

8 Structure of TP-UD (SMS) in the TP-AL[80] layer

According to 3GPP TS 23.040 (ETSI, 2020b), the structure of an SMS (i.e a text composed by a user) that call TP-UD in this layer is illustrated in Figure 16. Figure 16 parts (A) and (B) show messages with a header but (A) is the 7-bit message and B 8-bit message. Figure 16 part (C) shows a message without a header, it's all user text. All message types showed in Figure 16 are TP-UD. The TP-UD is the same date that goes from one MS to another MS.

The length of the message is limit to 140 bytes (octets) (ETSI, 1998). The lower layer shows if the TP-UD has a header or not. Each header in Figure 16 parts (A) and (B) has variable length and has many parts that describe as follows.

User Data Header Length (UDHL): It's a byte (octet). It defines the length of the header in bytes (octets) without counting itself and the padding bits. Padding bits will be described later.

Information Element Identifier (IEI): It's a 1-byte (octet) parameter. It defines the data element after IEL[81]. For example, any of the following can be set in this parameter. In this paper we used Hex, any Hex number begins with `0x` characters. The two Hex digit is equal with 8 bit or 1 byte.

`0x00` → Concatenated short messages

[80] Short Message-Application Layer

[81] Information Element Length

`0x01` → Special SMS Message Indication
`0x02` → Reserved
`0x70` - `0x7F` → SIM Toolkit Security Headers
…
Information Element Length (IEL): It's a 1-byte (octet) parameter. It defines the number of bytes (octets) used for IED[82] right after itself. It does not count itself.
Information Element Data (IED): It's a data element with different bytes (octets). Its length depends on its type.
Padding: if MS used 7-bit coding scheme, several bits would add at the end of the header to make all header's bits a complete factor of 8. It makes the TP-UD readable to new and old devices.
The body of TP-UD is the user's text. It can be 7-bit, 8-bit, or UCS2 19-bit data. Each TP-UD can have multiple headers as described in the following example.

8.1.1 An example of SMS with multiple special message indication headers

As illustrated in Figure 17, this message has multiple IEI headers. All headers types are Special Message Indication. This type of SMS is called message waiting and has 3 levels. In level 3, the message contains information about the number and types of Message Waiting in the PLMN. This kind of message will store different in the different devices. Also, an SC can add an old data coding scheme in parallel to support old devices.

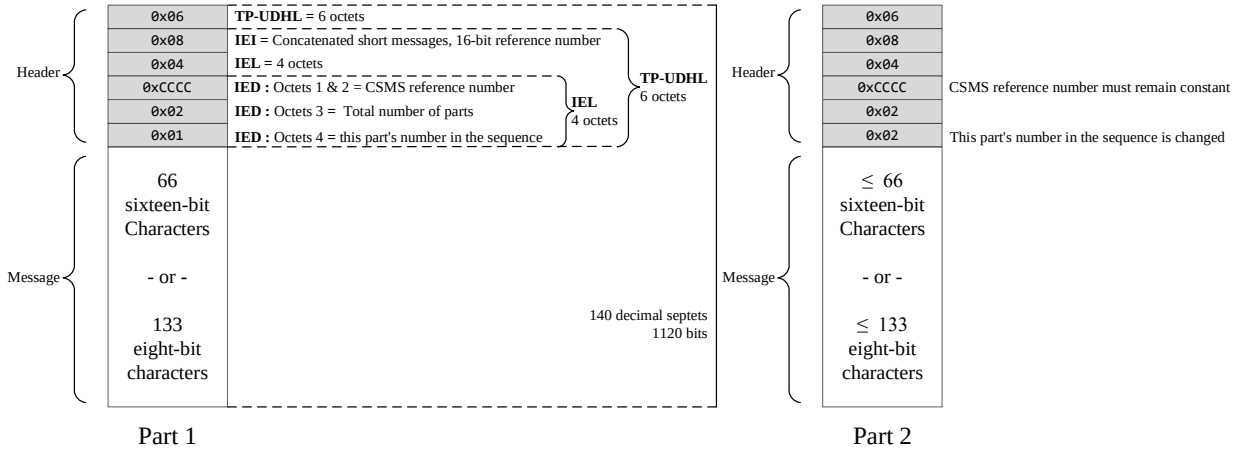

Figure 18: structure of two messages of a set of concatenated messages with a 16-bit reference number. Part 1 is the first message of the set and part 2 is the second message.

8.1.2 Example of concatenated SMS

This feature is used to send a text longer than an SMS. The recipient MS can attach all parts and make a complete message. For this purpose, the value of IEI can be (Hex) `00` or `08` that are used for the 8-bit and 16-bit Reference Number respectively (ETSI, 2010). The IED parameter has the following three parts (ETSI, 1998, 2010):
IED Part 1: the Reference Number, is an 8-bit or 16-bit value that is constant in all concatenated messages. It is taken from a counter that MS must assign each number a set of concatenated messages. The combination of this number, originator address, and SC address make a unique ID for each set of concatenated messages.
IED Part 2: it's a 1-byte (octet) value that defines the number of all messages in a current set of concatenated messages. It's limited between 1 to 255. If the value was 0, the data element would completely be ignored.

[82] Information Element Data

IED Part 3: it's an 8-bit value that defines the sequence of the current message in the set. Its interval is 1 to 255. If it is 0 or more than part 2, it will completely be ignored.
Figure 18 shows two messages of a set of concatenated messages. IEI headers contain a value for a 16-bit reference number. The length of each header is 7 bytes (octets). Therefore, the body can carry 133 8-bit characters or 66 16-bit characters.
In Figure 18, the first byte (octet) has the value `0x06` (Hex) that defines the header length without counting itself. Therefore, there must be 6 bytes (octet) after it in the header. The next byte (octet) called IEI that defines the type of IED the data after the next byte (IEL). It has the value `0x08` which means the IED is a 16-bit reference number. The value of the next byte or IEL is `0x04` which means the IED is 4 bytes which also means there are 4 bytes after this byte. The next two bytes or the first two bytes of IED are the Reference Number. The next byte or the third byte of IED defines the number of all messages in the set. It has the value `0x02` which means there are two messages in the set. The next byte or the fourth byte of the IED defines the sequence of the current message in the set. Its value in the first message is `0x0`1 and in the second message is `0x02` which is obvious. The 16-bit Reference number must support by the MS device. This sample with an 8-bit reference number is showed in Figure 19.

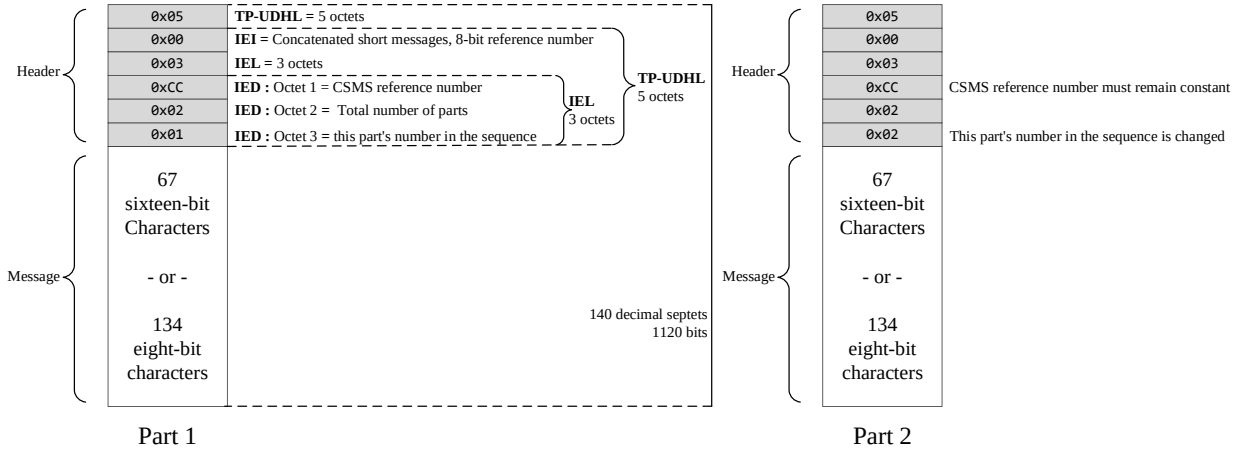

Figure 19: structure of two messages of a set of concatenated messages with an 8-bit reference number. Part 1 is the first message of the set and part 2 is the second message.

If a 7-bit character is used in this sample, padding bits will be necessary at the end of the header. Therefore the messages structures will be as illustrated in Figure 20 and Figure 21. The values in the fill bits are binary not Hex. The value of each bit is zero. The number of added bits in Figure 20 is zero, so it has no padding. But in Figure 21 one bit is added. The maximum number of bits in the padding is 6 bits.

Table 9: Number of possible characters in the concatenated message according to the type of header and coding

	8-bit Reference Number		16-bit Reference Number	
	1 message	All messages	1 message	All messages
7-bit coding	153	39015	152	38760
8-bit coding	134	34170	133	33915
16-bit coding	67	17085	66	16830

In brief, the maximum length of a message in the set for each coding scheme is in Table 9. Also, concerning the maximum number of messages in one set which is 255, the maximum number of characters in all concatenated messages is calculated. It is called concatenated message length.

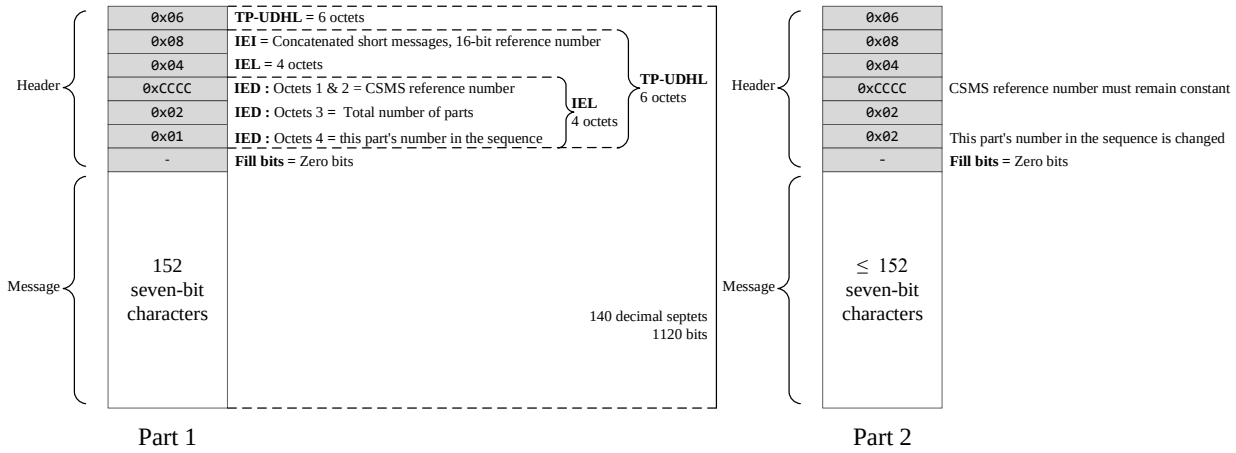

Figure 20: structure of two messages of a set of concatenated messages with a 16-bit reference number and 7-bit body. Part 1 is the first message of the set and part 2 is the second message.

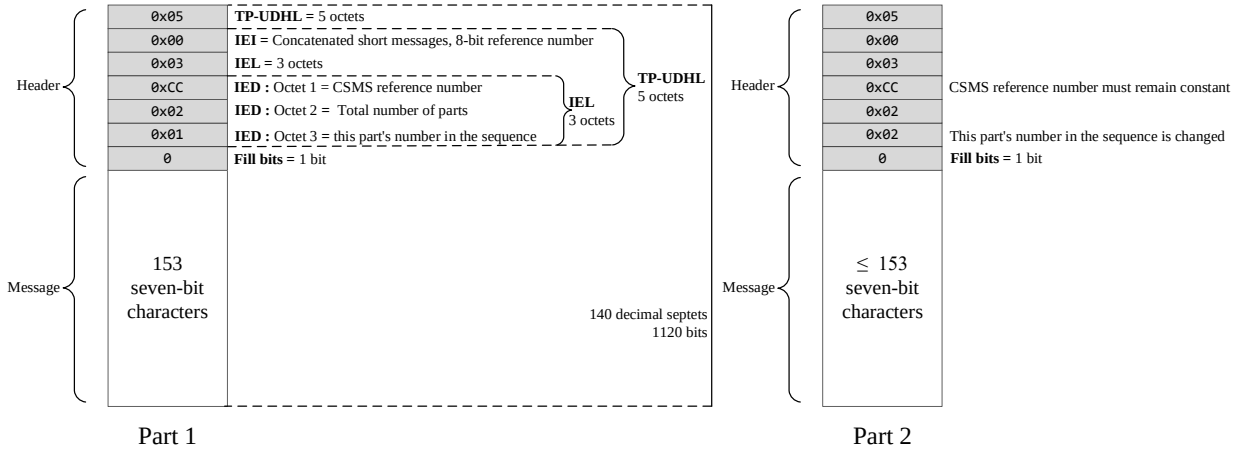

Figure 21: structure of two messages of a set of concatenated messages with an 8-bit reference number and 7-bit body. Part 1 is the first message of the set and part 2 is the second message.

Different values of IEI defines by ETSI and it also has some reserved values (ETSI, 2010). As an example, some defined IEI values are as follows.

`0x00`: It defines a concatenated message with the 8-bit reference number. It is described in the above sections completely.

`0x01`: It's a special message indication

`0x04`: Address of the 8-bit application port. It is like the TCP/IP port determine a specific program to read it.

`0x05`: It is like the `0x05` value but for a 16-bit application.

`0x06`: It's a control header by SC. It is used to inform SC or requesting a procedure related to a message status report.

`0x07`: It is the indication of UDH security.

`0x08`: It defines a concatenated message with the 16-bit reference number. It is described in the above sections completely.

`0x09`: It's a wireless control message protocol. It is used to inform the originator of an error in the recipient.

`0x0A`: It's a text format. It's used to define the text style like font size, left align, right align, etc.

`0x0B`: It's a predefined sound. It defines a sound to play after a character.
`0x0C`: It's a user-defined sound. The IED of this header is a string with 128 bytes (octet) length and its name is iMelody. Also, it defines the location of the character that after it the sound will play.
`0x0D`: It's a predefined animation. It defines an animation to play after a character.
`0x0E`: It's a big animation like `0x0D`.
`0x0F`: It's a small animation like `0x0D`.

9 SECURITY ANALYSIS

There are more details than what is described above. We tried to give the reader a complete insight into the system with minimum and mandatory details. An important dilemma of a communication system is security that even the paper form of the messaging system was involved with it. A secure messaging system has many aspects that each aspect was explained by D'Angelo et. al. in comparison to the paper-based messaging system (D'Angelo, et al., 1994). In the following sections, the SMS protocol will be evaluated from these aspects using the information in the previous sections.

9.1 Identification

Identification of the message originator in a messaging system is very important. According to section 6.2. The RP-SMEA parameter in the mobile terminated (RP-MT-DATA) messages in the SM-RL layer defines the originator identity. This parameter is independent of the originator. Also, in the transfer layer (SM-TL), the message originates in an MS and then goes to SC. The SC reproduces the message and then adds the originator address then sends it to the MS. According to section 7.1, in this layer (SM-TL) the parameter TP-OA in the mobile terminated (SMS-DELIVER) message contains the originator address that was added by SC. The address format is defined in the (ETSI, 2001), MS will show the address as sender number. Since TP-OA is a plain text and independent from its lower layer addressing also can be edited by SC. Therefore, it is a weakness and any hack into the SC or SM-RL devices can endanger true identification of a sender.

9.2 Authentication

The authentication process is needed to be sure about the sender's identity. Each MS is authenticated using a subscriber identity module (SIM) in the SM-LL layer. Furthermore, according to section 6.2, in the RP-MT-DATA message, the RP-SMEA parameter is added and is independent of the message originator. In this layer, the MSC entity is connected to MS and this parameter is added by MSC. Also, in the above layer (SM-TL), the MS is connected to SC. According to section 7.1, in this layer, the TP-OA parameter in the SMS-DELIVER contains the originator address (i.e. sender number). This parameter is added by SC and is independent of the originator. In this protocol, authentication is based on trust to SC. SC checks sender identity through lower layers devices. But other entities like SMS-IWMSC can trick SC. Therefore, The authentication based on lower layer devices and based on a physical connection is not secure without using a strong cryptographic techniques.

9.3 Integrity

Integrity is referring to change the message between originator and recipient. The messaging system has the weak integrity feature. In the SMS, the layer SM-AL, SM-TL, and SM-RL have no parameter to ensure integrity. According to section 7, the SMS protocol limits the length of the message, and each message is called Data Unit and the originator must receive an RP-ACK packet for each Data Unit to acknowledge about message status. This method prevents from the message change by an error. According to the variety of mobile devices and their processing power, it is impossible to use the cryptographic method to ensure end-to-end integrity. The integrity is sacrificed for availability.

9.4 Nonrepudiation

Nonrepudiation means a message originator must unable to deny its message. According to sections 6.2 and 7.1, the MSC in the SM-RL layer and SC in the SM-TL layer guarantees the originator identity. If the MSC and SC are trusted the message is undeniable. But, again its upon the physical link an also a weak trust on SC.

9.5 Confidentiality

Confidentiality is a concept that refers to prevention of eavesdropping. According to section 5.4, in the LLC sublayer, there is a method to encrypt data over the radio link and prevent eavesdropping. Also, according to section 5.8, in the EMM sublayer, there is a method to private the MS identity over the physical link. But the MSC, SMS router and SC can read the message content. Also, the MSC and SC can read the originator MS and recipient MS identity. In case of compromised MSC, SMS router and SC the entire communication will be exposed.

9.6 Availability

It's an important issue for a messaging system. Because a most secure messaging system with hard accessibility is useless. Availability means the system is accessible everywhere and at any time. Also, if a part of the system is destroyed, the other part must be fully functional and still deliver the messages. SMS has its physical infrastructure, also, it can be used on a wide range of devices from black and white LCD mobile phones to advanced smartphones and GSM modules on personal computers. Therefore, it is accessible in all covered areas of the cellular network. Also, if one or more (but not all) BTS, MSC, or even PLMN is destroyed, other BTSs and MSCs of a PLMN and other PLMNs still can serve to an MS. It may cause offline some users but others still can communicate. Therefore, SMS has the availability feature in the best way because, it's a *federative* messaging protocol.

10. CONCLUSION

All the Identification, Authentication, Integrity, Nonrepudiation, Confidentiality, and Availability features are addressed in the previous sections as well as the SMS protocol. These features are listed in Table 10 briefly. SMS is a federative protocol, so, it helps the system grow faster but it has lacks some security features. In brief, SMS is not secure but the most available messaging system. Due to its availability, it's more popular and is used as a part of the authentication mechanism for other services.

Table 10: SMS protocol at a glance

Protocol	Identification	Authentication	Integrity	Nonrepudiation	Confidentiality	Availability
SMS	Partially	If MSC or SC is trusted	No	No	No	Highly available

One solution to eliminate the security issues is to use the S/MIME standard described in RFC 2633 (Ramsdell, 1999) with a third-party application. But this solution decreases the Availability of SMS and is limited to the application's users. The main problem is to manage all certificates needed in the cryptographic method that many mobile devices cannot support. We are working to solve this problem by light and secure cryptographic methods that have backward compatibility. This is our main topic for future work.

REFERENCES

3GPP. (1999). 3rd Generation Partnership Project; Technical Specification Group Terminals; Alphabets and language-specific information (3G TS 23.038 version 2.0.0) (Technical Specification 3GPP TSG-T#4; 3G TS, p. 20). ETSI. https://www.3gpp.org/ftp/tsg_t/tsg_t/tsgt_04/docs/PDFs/TP-99127.pdf

BBC. (2002, December 3). Frist SMS. http://news.bbc.co.uk/2/hi/uk_news/2538083.stm

D'Angelo, D. M., McNair, B., & Wilkes, J. E. (1994). Security in Electronic Messaging Systems. AT&T Technical Journal, 73(3), 7–13. https://doi.org/10.1002/j.1538-7305.1994.tb00584.x

ETSI. (1998). Digital cellular telecommunications system (Phase 2+); Technical realization of the Short Message Service (SMS); Point-to-Point (PP) (GSM 03.40 version 6.1.0 Release 1997) (Technical Specification DTS/SMG-040340Q6; p. 115). ETSI. https://www.etsi.org/deliver/etsi_ts/100900_100999/100901/06.01.00_60/ts_100901v060100p.pdf

ETSI. (2000). Digital cellular telecommunications system (Phase 2+); Point-to-Point (PP) Short Message Service (SMS) Support on Mobile Radio Interface (3GPP TS 04.11 version 7.1.0 Release 1998) (Technical Specification RTS/TSGN-010411v710; 3GPP TS 04.11, p. 81). ETSI. https://portal.etsi.org/webapp/workprogram/Report_WorkItem.asp?WKI_ID=16869

ETSI. (2001). Digital cellular telecommunications system (Phase 2+); Technical realization of the Short Message Service (SMS) Point-to-Point (PP) (3GPP TS 03.40 version 7.5.0 Release 1998) (Technical Specification RTS/TSGT-020340Q7R3; 3GPP TS 03.40, p. 120). ETSI. https://portal.etsi.org/webapp/workprogram/Report_WorkItem.asp?WKI_ID=16869

ETSI. (2003). Digital cellular telecommunications system (Phase 2+); Mobile radio interface layer 3 specification (3GPP TS 04.08 version 7.21.0 Release 1998) (Technical Specification RTS/TSGN-010408v7l0; 3GPP TS 04.08, p. 625). ETSI. https://portal.etsi.org/webapp/workprogram/Report_WorkItem.asp?WKI_ID=20082

ETSI. (2004). Digital cellular telecommunications system (Phase 2+); Mobile Application Part (MAP) specification (3GPP TS 09.02 version 7.15.0 Release 1998) (Technical Specification RTS/TSGN-040902v7f0; 3GPP TS 09.02, p. 1118). ETSI. https://portal.etsi.org/webapp/workprogram/Report_WorkItem.asp?WKI_ID=20392

ETSI. (2010). Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Technical realization of the Short Message Service (SMS) (3GPP TS 23.040 version 9.3.0 Release 9) (Technical Specification RTS/TSGC-0123040v930; ETSI TS, p. 204). ETSI. https://www.etsi.org/deliver/etsi_ts/123000_123099/123040/09.03.00_60/ts_123040v090300p.pdf

ETSI. (2020a). Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface (3GPP TS 24.011 version 16.0.0 Release 16) (Technical Specification RTS/TSGC-0124011vg00; 3GPP TS 24.011, p. 151). ETSI. https://portal.etsi.org/webapp/workprogram/Report_WorkItem.asp?WKI_ID=60164

ETSI. (2020b). Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Technical realization of the Short Message Service (SMS) (3GPP TS 23.040 version 16.0.0 Release 16) (Technical Specification RTS/TSGC-0123040vg00; ETSI TS 123 040, p. 220). ETSI. https://portal.etsi.org/webapp/workprogram/Report_WorkItem.asp?WKI_ID=60072

ETSI. (2020c). Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Circuit Switched (CS) fallback in Evolved Packet System (EPS); Stage 2 (3GPP TS 23.272 version 16.0.0 Release 16) (Technical Specification RTS/TSGS-

0223272vg00; 3GPP TS 23.272, p. 107). ETSI. https://portal.etsi.org/webapp/workprogram/Report_WorkItem.asp?WKI_ID=60074

ETSI. (2020d). Digital cellular telecommunications system (Phase 2+) (GSM); Mobile Station—Serving GPRS Support Node (MS-SGSN); Logical Link Control (LLC) Layer Specification (3GPP TS 44.064 version 16.0.0 Release 16) TECHNICAL SPECIFICATION GLOBAL SYSTEM (Technical Specification RTS/TSGC-0144064vg00; 3GPP TS 44.064, p. 71). ETSI. https://portal.etsi.org/webapp/workprogram/Report_WorkItem.asp?WKI_ID=60096

ETSI. (2020e). Universal Mobile Telecommunications System (UMTS); LTE; Mobility Management Entity (MME)—Visitor Location Register (VLR) SGs interface specification (3GPP TS 29.118 version 16.0.0 Release 16) (Technical Specification RTS/TSGC-0129118vg00; 3GPP TS 29.118, p. 79). ETSI. https://portal.etsi.org/webapp/workprogram/Report_WorkItem.asp?WKI_ID=60115

ETSI. (2020f). Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); General Packet Radio Service (GPRS); Service description; Stage 2 (3GPP TS 23.060 version 16.0.0 Release 16) TECHNICAL SPECIFICATION GLOBAL (Technical Specification RTS/TSGS-0223060vg00; 3GPP TS 23.060, p. 373). ETSI. https://portal.etsi.org/webapp/workprogram/Report_WorkItem.asp?WKI_ID=59612

ETSI. (2020g). Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Vocabulary for 3GPP Specifications (3GPP TR 21.905 version 16.0.0 Release 16) (Technical Report RTR/TSGS-0021905vg00; 3GPP TR 21.905, p. 70). ETSI. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=558

ETSI. (2021a). 5G; System architecture for the 5G System (5GS) (3GPP TS 23.501 version 16.7.0 Release 16) (Technical Specification RTS/TSGS-0223501vg70; 3GPP TS 23.501, p. 452). ETSI. https://portal.etsi.org/webapp/workprogram/Report_WorkItem.asp?WKI_ID=62182

ETSI. (2021b). Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Mobile Application Part (MAP) specification (3GPP TS 29.002 version 16.1.0 Release 16) (Technical Specification RTS/TSGC-0429002vg10; 3GPP TS 29.002, p. 1027). ETSI. https://portal.etsi.org/webapp/workprogram/Report_WorkItem.asp?WKI_ID=62061

ETSI. (2021c). Universal Mobile Telecommunications System (UMTS); LTE; 5G; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3 (3GPP TS 24.301 version 16.7.0 Release 16) (Technical Specification RTS/TSGC-0124301vg70; 3GPP TS 24.301, p. 575). ETSI. https://portal.etsi.org/webapp/workprogram/Report_WorkItem.asp?WKI_ID=62197

ETSI. (2021d). 5G; Procedures for the 5G System (5GS) (3GPP TS 23.502 version 16.8.0 Release 16) (Technical Specification RTS/TSGS-0223502vg80; 3GPP TS 23.502, p. 612). ETSI. https://portal.etsi.org/webapp/workprogram/Report_WorkItem.asp?WKI_ID=62708

Huurdeman, A. A. (2003). The worldwide history of telecommunications. John Wiley & Sons.

Peersman, G., Griffiths, P., Spear, H., Cvetkovic, S., & Smythe, C. (2000). A tutorial overview of the short message service within GSM. Computing & Control Engineering Journal, 11(2), 79–89.

Ramsdell, B. (1999). RFC 2633: S/MIME Version 3 Message Specification (Technical Specification RFC 2633; Internet Requests for Comment, p. 31). RFC Editor. https://datatracker.ietf.org/doc/html/rfc2633