8.3.19.2 Remote UE context connected

This IE is included in the message by the UE acting as a 5G ProSe layer-3 UE-to-network UE relay to provide the network with newly connected 5G ProSe remote UE information as specified in 3GPP TS 23.304 [6E].

8.3.19.3 Remote UE context disconnected

This IE is included in the message by the UE acting as a 5G ProSe layer-3 UE-to-network UE relay to provide the network with disconnected 5G ProSe remote UE information as specified in 3GPP TS 23.304 [6E].

8.3.20 Remote UE report response

8.3.20.1 Message definition

The REMOTE UE REPORT RESPONSE message is sent by the network to the UE to acknowledge receipt of a remote UE report message. See table 8.3.20.1.

Message type: REMOTE UE REPORT RESPONSE

Significance: dual

Direction: network to UE

Table 8.3.20.1: REMOTE UE REPORT RESPONSE message content

IEI	Information Element	Type/Reference	Presence	Format	Length
	Extended protocol discriminator	Extended protocol discriminator 9.2	M	V	1
	PDU session ID	PDU session identity 9.4	M	V	1
	PTI	Procedure transaction identity 9.6	M	V	1
	Remote UE report response message identity	Message type 9.7	M	V	1

8.3.20.2 Void

8.3.20.3 Void

8.3.20.4 Void

9 General message format and information elements coding

9.1 Overview

9.1.1 NAS message format

Within the protocols defined in the present document, every 5GS NAS message is a standard L3 message as defined in 3GPP TS 24.007 [11]. This means that the message consists of the following parts:

1) if the message is a plain 5GS NAS message:

   a) extended protocol discriminator;

b) security header type associated with a half spare octet or PDU session identity;

c) procedure transaction identity;

d) message type;

e) other information elements, as required.

2) if the message is a security protected 5GS NAS message:

a) extended protocol discriminator;

b) security header type associated with a half spare octet;

c) message authentication code;

d) sequence number;

e) plain 5GS NAS message, as defined in item 1

The organization of a plain 5GS NAS message is illustrated in the example shown in figure 9.1.1.1.

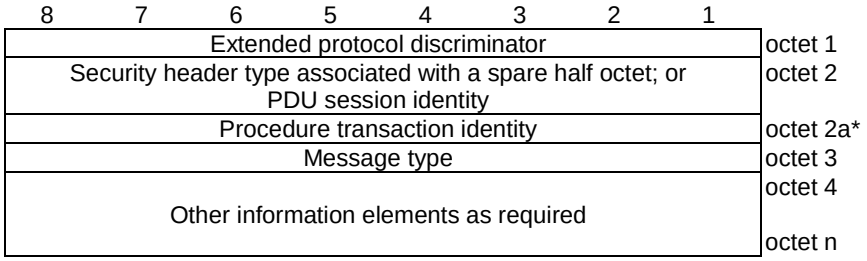


Figure 9.1.1.1: General message organization example for a plain 5GS NAS message

The PDU session identity and the procedure transaction identity are only used in messages with extended protocol discriminator 5GS session management. Octet 2a with the procedure transaction identity shall only be included in these messages.

The organization of a security protected 5GS NAS message is illustrated in the example shown in figure 9.1.1.2.

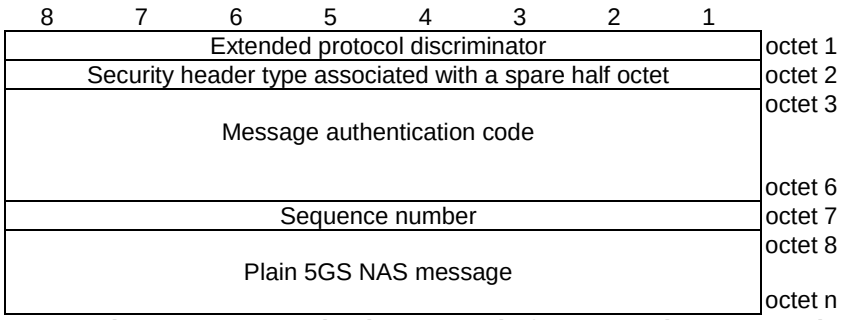


Figure 9.1.1.2: General message organization example for a security protected 5GS NAS message

Unless specified otherwise in the message descriptions of clause 8 and annex D, a particular information element shall not be present more than once in a given message.

9.1.2 Field format and mapping

When a field is contained within a single octet, the lowest numbered bit of the field represents the least significant bit.

When a field extends over more than one octet, the order of bit values progressively decreases as the octet number increases. In that part of the field contained in a given octet, the lowest numbered bit represents the least significant bit.

The most significant bit of the field is represented by the highest numbered bit of the lowest numbered octet of the field. The least significant bit of the field is represented by the lowest numbered bit of the highest numbered octet of the field.

For example, a bit number can be identified as a couple (o, b) where o is the octet number and b is the relative bit number within the octet. Figure 9.1.2.1 illustrates a field that spans from bit (1, 3) to bit (2, 7). The most significant bit of the field is mapped on bit (1, 3) and the least significant bit is mapped on bit (2, 7).

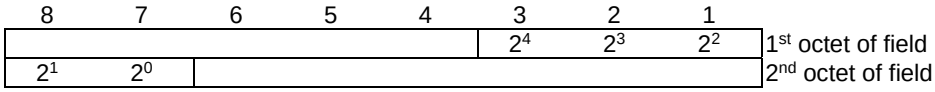


Figure 9.1.2.1: Field mapping convention

9.2 Extended protocol discriminator

Bits 1 to 8 of the first octet of every 5GS NAS message contain the Extended protocol discriminator (EPD) IE. The EPD and its use are defined in 3GPP TS 24.007 [11]. The extended protocol discriminator in the header (see 3GPP TS 24.007 [11]) of a security protected 5GS NAS message is encoded as "5GS mobility management messages".

9.3 Security header type

Bits 1 to 4 of the second octet of every 5GMM message contain the Security header type IE. This IE includes control information related to the security protection of a 5GMM message. The total size of the Security header type IE is 4 bits.

The Security header type IE can take the values shown in table 9.3.1.

Table 9.3.1: Security header type

Security header type (octet 1)				
Bits				
4	**3**	**2**	**1**	
0	0	0	0	Plain 5GS NAS message, not security protected
				Security protected 5GS NAS message:
0	0	0	1	Integrity protected
0	0	1	0	Integrity protected and ciphered
0	0	1	1	Integrity protected with new 5G NAS security context (NOTE 1)
0	1	0	0	Integrity protected and ciphered with new 5G NAS security context (NOTE 2)
All other values are reserved.				

NOTE 1:	This codepoint may be used only for a SECURITY MODE COMMAND message.
NOTE 2:	This codepoint may be used only for a SECURITY MODE COMPLETE message.

A 5GMM message received with the security header type encoded as 0000 shall be treated as not security protected, plain 5GS NAS message. A protocol entity sending a not security protected 5GMM message shall send the message as plain 5GS NAS message and encode the security header type as 0000.

9.4 PDU session identity

Bits 1 to 8 of the second octet of every 5GSM message contain the PDU session identity IE. The PDU session identity and its use to identify a message flow are defined in 3GPP TS 24.007 [11].

9.5 Spare half octet

This element is used in the description of 5GMM and 5GSM messages when an odd number of half octet type 1 information elements are used. This element is filled with spare bits set to zero and is placed in bits 5 to 8 of the octet unless otherwise specified.

9.6 Procedure transaction identity

Bits 1 to 8 of the third octet of every 5GSM message contain the procedure transaction identity. Bits 1 to 8 of the first octet of every UE policy delivery message contain the procedure transaction identity. The procedure transaction identity and its use are defined in 3GPP TS 24.007 [11].

9.7 Message type

The Message type IE and its use are defined in 3GPP TS 24.007 [11]. Tables 9.7.1 and 9.7.2 define the value part of the message type IE used in the 5GS mobility management protocol and 5GS session management protocol.

Table 9.7.1: Message types for 5GS mobility management

Bits 8	7	6	5	4	3	2	1	
0	1	-	-	-	-	-	-	5GS mobility management messages
0	1	0	0	0	0	0	1	Registration request
0	1	0	0	0	0	1	0	Registration accept
0	1	0	0	0	0	1	1	Registration complete
0	1	0	0	0	1	0	0	Registration reject
0	1	0	0	0	1	0	1	Deregistration request (UE originating)
0	1	0	0	0	1	1	0	Deregistration accept (UE originating)
0	1	0	0	0	1	1	1	Deregistration request (UE terminated)
0	1	0	0	1	0	0	0	Deregistration accept (UE terminated)
0	1	0	0	1	1	0	0	Service request
0	1	0	0	1	1	0	1	Service reject
0	1	0	0	1	1	1	0	Service accept
0	1	0	0	1	1	1	1	Control plane service request
0	1	0	1	0	0	0	0	Network slice-specific authentication command
0	1	0	1	0	0	0	1	Network slice-specific authentication complete
0	1	0	1	0	0	1	0	Network slice-specific authentication result
0	1	0	1	0	1	0	0	Configuration update command
0	1	0	1	0	1	0	1	Configuration update complete
0	1	0	1	0	1	1	0	Authentication request
0	1	0	1	0	1	1	1	Authentication response
0	1	0	1	1	0	0	0	Authentication reject
0	1	0	1	1	0	0	1	Authentication failure
0	1	0	1	1	0	1	0	Authentication result
0	1	0	1	1	0	1	1	Identity request
0	1	0	1	1	1	0	0	Identity response
0	1	0	1	1	1	0	1	Security mode command
0	1	0	1	1	1	1	0	Security mode complete
0	1	0	1	1	1	1	1	Security mode reject
0	1	1	0	0	1	0	0	5GMM status
0	1	1	0	0	1	0	1	Notification
0	1	1	0	0	1	1	0	Notification response
0	1	1	0	0	1	1	1	UL NAS transport
0	1	1	0	1	0	0	0	DL NAS transport
0	1	1	0	1	0	0	1	Relay key request
0	1	1	0	1	0	1	0	Relay key accept
0	1	1	0	1	0	1	1	Relay key reject
0	1	1	0	1	1	0	0	Relay authentication request
0	1	1	0	1	1	0	1	Relay authentication response

Table 9.7.2: Message types for 5GS session management

Bits 8	7	6	5	4	3	2	1	
1	1	-	-	-	-	-	-	5GS session management messages
1	1	0	0	0	0	0	1	PDU session establishment request
1	1	0	0	0	0	1	0	PDU session establishment accept
1	1	0	0	0	0	1	1	PDU session establishment reject
1	1	0	0	0	1	0	1	PDU session authentication command
1	1	0	0	0	1	1	0	PDU session authentication complete
1	1	0	0	0	1	1	1	PDU session authentication result
1	1	0	0	1	0	0	1	PDU session modification request
1	1	0	0	1	0	1	0	PDU session modification reject
1	1	0	0	1	0	1	1	PDU session modification command
1	1	0	0	1	1	0	0	PDU session modification complete
1	1	0	0	1	1	0	1	PDU session modification command reject
1	1	0	1	0	0	0	1	PDU session release request
1	1	0	1	0	0	1	0	PDU session release reject
1	1	0	1	0	0	1	1	PDU session release command
1	1	0	1	0	1	0	0	PDU session release complete
1	1	0	1	0	1	1	0	5GSM status
1	1	0	1	1	0	0	0	Service-level authentication command
1	1	0	1	1	0	0	1	Service-level authentication complete
1	1	0	1	1	0	1	0	Remote UE report
1	1	0	1	1	0	1	1	Remote UE report response

9.8 Message authentication code

The message authentication code (MAC) information element contains the integrity protection information for the message. The MAC IE shall be included in the SECURITY PROTECTED 5GS NAS MESSAGE message if a valid 5G NAS security context exists and security functions are started.

The message authentication code (MAC) is also included in the Intra N1 mode NAS transparent container IE and in the S1 mode to N1 mode NAS transparent container IE.

The usage of MAC is specified in subclause 4.4.3.3.

9.9 Plain 5GS NAS message

This IE includes a complete plain 5GS NAS message as specified in subclauses 8.2 and 8.3. The SECURITY PROTECTED 5GS NAS MESSAGE (see subclause 8.2.28) includes a complete plain 5GS NAS message as specified in subclauses 8.2. The SECURITY PROTECTED 5GS NAS MESSAGE message (see subclause 8.2.28) is not plain 5GS NAS messages and shall not be included in this IE.

9.10 Sequence number

This IE includes the NAS message sequence number (SN) which consists of the eight least significant bits of the NAS COUNT for a SECURITY PROTECTED 5GS NAS MESSAGE message.

The NAS message sequence number (SN) with the eight least significant bits of the NAS COUNT is also included in the Intra N1 mode NAS transparent container IE and in the N1 mode to S1 mode NAS transparent container IE.

The usage of SN is specified in subclause 4.4.3.

9.11 Other information elements

9.11.1 General

The different formats (V, LV, T, TV, TLV, LV-E, TLV-E) and the five categories of information elements (type 1, 2, 3, 4 and 6) are defined in 3GPP TS 24.007 [11].

The first octet of an information element in the non-imperative part contains the IEI of the information element. If this octet does not correspond to an IEI known in the message, the receiver shall determine whether this IE is of type 1 or 2 (i.e. it is an information element of one octet length) or an IE of type 4 or 6 (i.e. that the next octet is the length indicator or, for a type 6 IE, the next 2 octets are the length indicator indicating the length of the remaining of the information element) (see 3GPP TS 24.007 [11]).

NOTE: This requirement for the receiver is not applicable for information elements included in a Type 6 IE container information element. Any IE in the Type 6 IE container information element is of type 6 with format TLV-E; therefore, the rules for the IEI value encoding defined in 3GPP TS 24.007 [11], subclause 11.2.4, are not applicable.

This allows the receiver to jump over unknown information elements and to analyse any following information elements of a particular message.

The definitions of information elements which are:

a) common for the 5GMM and 5GSM protocols;

b) used by access stratum protocols; or

c) sent to upper layers

are described in subclause 9.11.2.

The information elements of the 5GMM or 5GSM protocols can be defined by reference to an appropriate specification which provides the definition of the information element, e.g., "see subclause 10.5.6.3A in 3GPP TS 24.008 [12]".

9.11.2 Common information elements

9.11.2.1 Additional information

The purpose of the Additional information information element is to provide additional information to upper layers in relation to the NAS transport mechanism.

The Additional information information element is coded as shown in figure 9.11.2.1.1 and table 9.11.2.1.1.

The Additional information is a type 4 information element with a minimum length of 3 octets.

8	7	6	5	4	3	2	1	
Additional information IEI								octet 1
Additional information length								octet 2
Additional information value								octets 3-n

Figure 9.11.2.1.1: Additional information information element

Table 9.11.2.1.1 : Additional information information element

Additional information value (octet 3 to octet n) The coding of the additional information value is dependent on the LCS application.

9.11.2.1A Access type

The purpose of the access type information element is to indicate the access type over which the signalling or user data is pending to be sent to the UE.

The access type is a type 1 information element.

The access type information element is coded as shown in figure 9.11.2.1A.1 and table 9.11.2.1A.1.

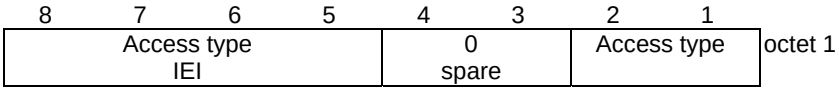


Figure 9.11.2.1A.1: Access type information element

Table 9.11.2.1A.1: Access type information element

Access type value (octet 1, bit 1 to bit 2) Bits **2 1** 0 1 3GPP access 1 0 Non-3GPP access All other values are reserved.

9.11.2.1B DNN

The purpose of the DNN information element is to identify the data network.

The DNN information element is coded as shown in figure 9.11.2.1B.1.

The DNN is a type 4 information element with a minimum length of 3 octets and a maximum length of 102 octets.

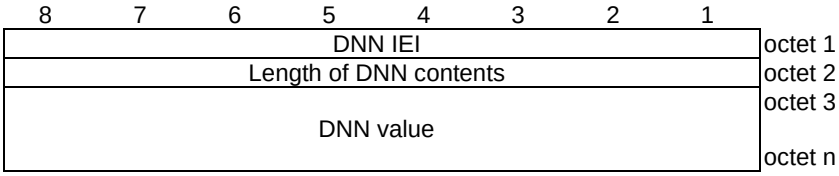


Figure 9.11.2.1B.1: DNN information element

A DNN value field contains an APN as defined in 3GPP TS 23.003 [4].

9.11.2.2 EAP message

The purpose of the EAP message information element is to transport an EAP message as specified in IETF RFC 3748 [34].

The EAP message information element is coded as shown in figure 9.11.2.2.1 and table 9.11.2.2.1.

The EAP message is a type 6 information element with minimum length of 7 octets and maximum length of 1503 octets.

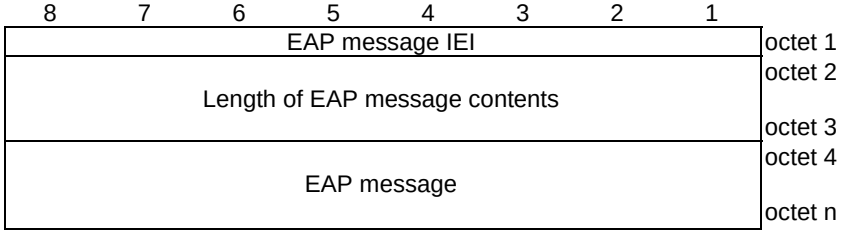


Figure 9.11.2.2.1: EAP message information element

Table 9.11.2.2.1: EAP message information element

EAP message (octet 4 to n) An EAP message as specified in IETF RFC 3748 [34].

9.11.2.3 GPRS timer

See subclause 10.5.7.3 in 3GPP TS 24.008 [12].

9.11.2.4 GPRS timer 2

See subclause 10.5.7.4 in 3GPP TS 24.008 [12].

9.11.2.5 GPRS timer 3

See subclause 10.5.7.4a in 3GPP TS 24.008 [12].

9.11.2.6 Intra N1 mode NAS transparent container

The purpose of the Intra N1 mode NAS transparent container information element is to provide the UE with parameters that enable the UE to handle the 5G NAS security context after N1 mode to N1 mode handover.

The Intra N1 mode NAS transparent container information element is coded as shown in figure 9.11.2.6.1 and table 9.11.2.6.1.

The Intra N1 mode NAS transparent container is a type 4 information element with a length of 9 octets.

The value part of the Intra N1 mode NAS transparent container information element is included in specific information elements within some RRC messages sent to the UE.

NOTE: For these cases the coding of the information element identifier and length information of RRC is defined in 3GPP TS 38.331 [30].

8	7	6	5	4	3	2	1	
Intra N1 mode NAS transparent container IEI								octet 1
Length of Intra N1 mode NAS transparent container contents								octet 2
Message authentication code								octet 3 octet 6
Type of ciphering algorithm				Type of integrity protection algorithm				octet 7
0	0	0	KACF	TSC	Key set identifier in 5G			octet 8
Spare								
Sequence number								octet 9

Figure 9.11.2.6.1: Intra N1 mode NAS transparent container information element

Table 9.11.2.6.1: Intra N1 mode NAS transparent container information element

Message authentication code (octet 3 to 6) This field is coded as the Message authentication code information element (see subclause 9.8). Type of integrity protection algorithm (octet 7, bit 1 to 4) and type of ciphering algorithm (octet 7, bit 5 to 8) These fields are coded as the type of integrity protection algorithm and type of ciphering algorithm in the NAS security algorithms information element (see subclause 9.11.3.34). K_AMF_change_flag (KACF) (octet 8, bit 5) Bit **5** 0 a new K_{AMF} has not been calculated by the network 1 a new K_{AMF} has been calculated by the network Key set identifier in 5G (octet 8, bit 1 to 3) and Type of security context flag (TSC) (octet 8, bit 4) These fields are coded as the NAS key set identifier and type of security context flag in the NAS key set identifier information element (see subclause 9.11.3.32). Sequence number (octet 9) This field is coded as the Sequence number information element (see subclause 9.10)

9.11.2.7 N1 mode to S1 mode NAS transparent container

The purpose of the N1 mode to S1 mode NAS transparent container information element is to provide the UE with information that enables the UE to create a mapped EPS security context.

The N1 mode to S1 mode NAS transparent container information element is coded as shown in figure 9.11.2.7.1 and table 9.11.2.7.1.

The N1 mode to S1 mode NAS transparent container is a type 3 information element with a length of 2 octets.

The value part of the N1 mode to S1 mode NAS transparent container information element is included in specific information elements within some RRC messages sent to the UE; see 3GPP TS 38.331 [30]. For these cases the coding of the information element identifier and length information is defined in 3GPP TS 38.331 [30].

8	7	6	5	4	3	2	1	
N1 mode to S1 mode NAS transparent container IEI								octet 1
Sequence number								octet 2

Figure 9.11.2.7.1: N1 mode to S1 mode NAS transparent container information element

Table 9.11.2.7.1: N1 mode to S1 mode NAS transparent container information element

Sequence number (octet 2) This field is coded as the Sequence number information element (see subclause 9.10).

9.11.2.8 S-NSSAI

The purpose of the S-NSSAI information element is to identify a network slice.

The S-NSSAI information element is coded as shown in figure 9.11.2.8.1 and table 9.11.2.8.1.

The S-NSSAI is a type 4 information element with a minimum length of 3 octets and a maximum length of 10 octets.

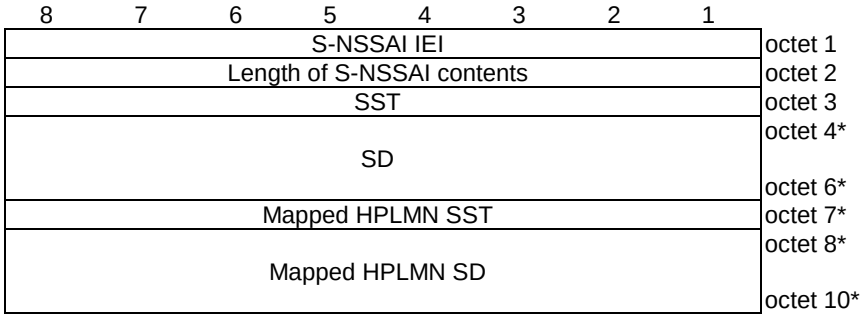


Figure 9.11.2.8.1: S-NSSAI information element

Table 9.11.2.8.1: S-NSSAI information element

Length of S-NSSAI contents (octet 2)

This field indicates the length of the included S-NSSAI contents, and it can have the following values. Depending on the value of the length field the following S-NSSAI contents are included:

Bits 8	7	6	5	4	3	2	1	
0	0	0	0	0	0	0	1	SST
0	0	0	0	0	0	1	0	SST and mapped HPLMN SST
0	0	0	0	0	1	0	0	SST and SD
0	0	0	0	0	1	0	1	SST, SD and mapped HPLMN SST
0	0	0	0	1	0	0	0	SST, SD, mapped HPLMN SST and mapped HPLMN SD

All other values are reserved.

Slice/service type (SST) (octet 3)

This field contains the 8 bit SST value. The coding of the SST value part is defined in 3GPP TS 23.003 [4]. If this IE is included during the network slice-specific authentication and authorization procedure, this field contains the 8 bit SST value of an S-NSSAI in the S-NSSAI(s) of the HPLMN or the RSNPN.

Slice differentiator (SD) (octet 4 to octet 6)

This field contains the 24 bit SD value. The coding of the SD value part is defined in 3GPP TS 23.003 [4]. If this IE is included during the network slice-specific authentication and authorization procedure, this field contains the 24 bit SD value of an S-NSSAI in the S-NSSAI(s) of the HPLMN or the RSNPN.

If the SST encoded in octet 3 is not associated with a valid SD value, and the sender needs to include a mapped HPLMN SST (octet 7) and a mapped HPLMN SD (octets 8 to 10), then the sender shall set the SD value (octets 4 to 6) to "no SD value associated with the SST".

mapped HPLMN Slice/service type (SST) (octet 7)

This field contains the 8 bit SST value of an S-NSSAI in the S-NSSAI(s) of the HPLMN to which the SST value is mapped. The coding of the SST value part is defined in 3GPP TS 23.003 [4].

mapped HPLMN Slice differentiator (SD) (octet 8 to octet 10)

This field contains the 24 bit SD value of an S-NSSAI in the S-NSSAI(s) of the HPLMN to which the SD value is mapped. The coding of the SD value part is defined in 3GPP TS 23.003 [4].

NOTE 1: Octet 3 shall always be included.
NOTE 2: If the octet 4 is included, then octet 5 and octet 6 shall be included.
NOTE 3: If the octet 7 is included, then octets 8, 9, and 10 may be included.
NOTE 4: If the octet 8 is included, then octet 9 and octet 10 shall be included.
NOTE 5: If only HPLMN S-NSSAI or subscribed SNPN S-NSSAI is included, then octets 7 to 10 shall not be included.

9.11.2.9 S1 mode to N1 mode NAS transparent container

The purpose of the S1 mode to N1 mode NAS transparent container information element is to provide the UE with parameters that enable the UE to create a mapped 5G NAS security context and take this context into use after inter-system change to N1 mode in 5GMM-CONNECTED mode.

The S1 mode to N1 mode NAS transparent container information element is coded as shown in figure 9.11.2.9.1 and table 9.11.2.9.1.

The S1 mode to N1 mode NAS transparent container is a type 4 information element with a length of 10 octets.

The value part of the S1 mode to N1 mode NAS transparent container information element is included in specific information elements within some RRC messages sent to the UE.

NOTE: For these cases the coding of the information element identifier and length information of RRC is defined in 3GPP TS 38.331 [30].

8	7	6	5	4	3	2	1	
S1 mode to N1 mode NAS transparent container IEI								octet 1
Length of S1 mode to N1 mode NAS transparent container contents								octet 2
Message authentication code								octet 3 octet 6
Type of ciphering algorithm				Type of integrity protection algorithm				octet 7
0 Spare	NCC			TSC	Key set identifier in 5G			octet 8
0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	octet 9
0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	octet 10

Figure 9.11.2.9.1: S1 mode to N1 mode NAS transparent container information element

Table 9.11.2.9.1: S1 mode to N1 mode NAS transparent container information element

Message authentication code (octet 3 to 6) This field is coded as the Message authentication code information element (see subclause 9.8). Type of integrity protection algorithm (octet 7, bit 1 to 4) and type of ciphering algorithm (octet 7, bit 5 to 8) These fields are coded as the type of integrity protection algorithm and type of ciphering algorithm in the NAS security algorithms information element (see subclause 9.11.3.34). NCC (octet 8, bits 5 to 7) This field contains the 3 bit Next hop chaining counter (see 3GPP TS 33.501 [24]) Key set identifier in 5G (octet 8, bit 1 to 3) and type of security context flag (TSC) (octet 8, bit 4) These fields are coded as the NAS key set identifier and type of security context flag in the NAS key set identifier information element (see subclause 9.11.3.32). Octets 9 and 10 are spare and shall be coded as zero.
NOTE: In earlier versions of this protocol, octets 9 and 10 can have any value. In this version of the protocol, octets 9 and 10 can always be ignored by the UE.

9.11.2.10 Service-level-AA container

The purpose of the Service-level-AA container information element is to transfer upper layer information for authentication and authorization between the UE and the network.

The Service-level-AA container information element is coded as shown in figure 9.11.2.10.1, figure 9.11.2.10.2, figure 9.11.2.10.3, figure 9.11.2.10.4 and table 9.11.2.10.1.

The Service-level-AA container information element is a type 6 information element with a minimum length of 4 octets and a maximum length of 65538 octets.

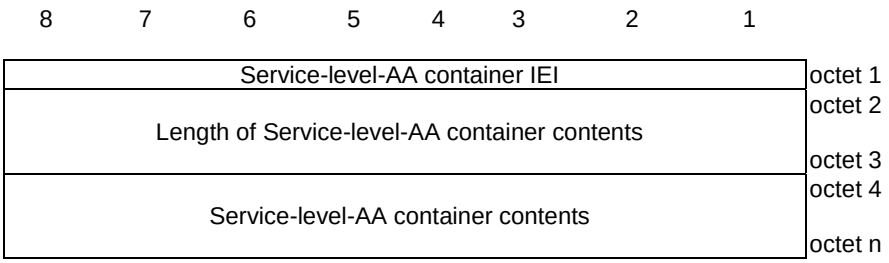


Figure 9.11.2.10.1: Service-level-AA container information element

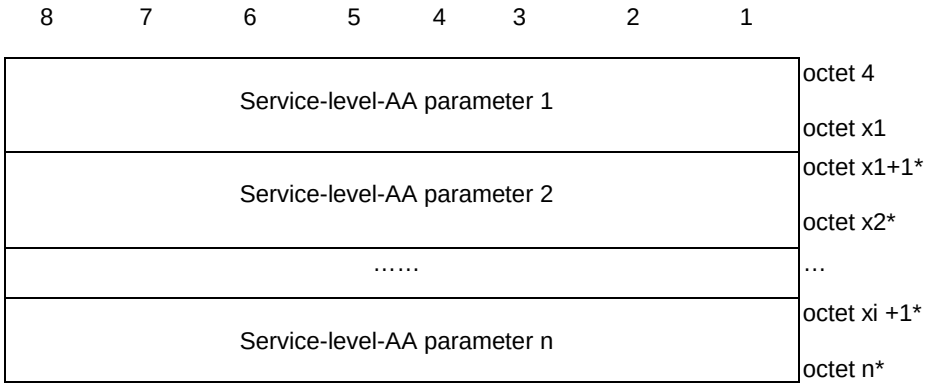


Figure 9.11.2.10.2: Service-level-AA container contents

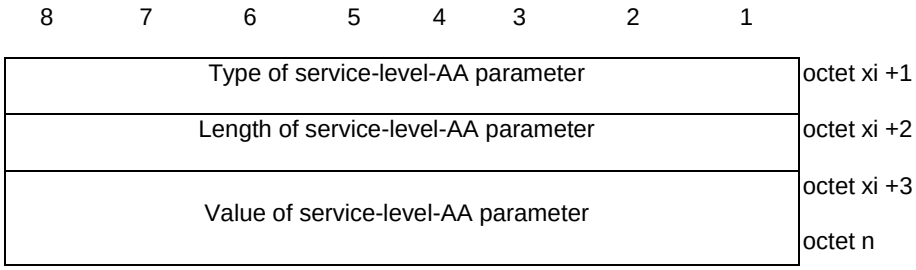


Figure 9.11.2.10.3: Service-level-AA parameter (when the type of service-level-AA parameter field contains an IEI of a type 4 information element as specified in 3GPP TS 24.007 [11])

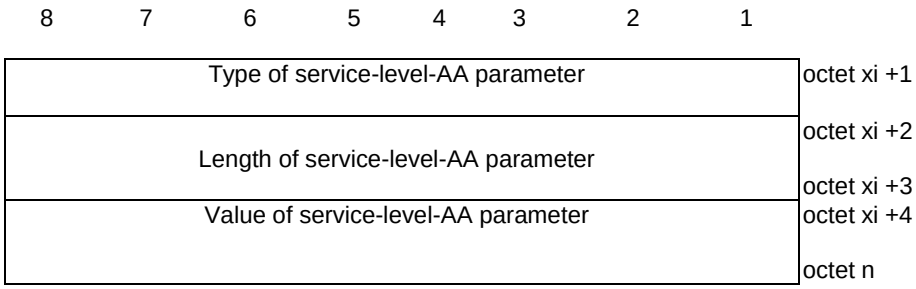


Figure 9.11.2.10.4: Service-level-AA parameter (when the type of service-level-AA parameter field contains an IEI of a type 6 information element as specified in 3GPP TS 24.007 [11])

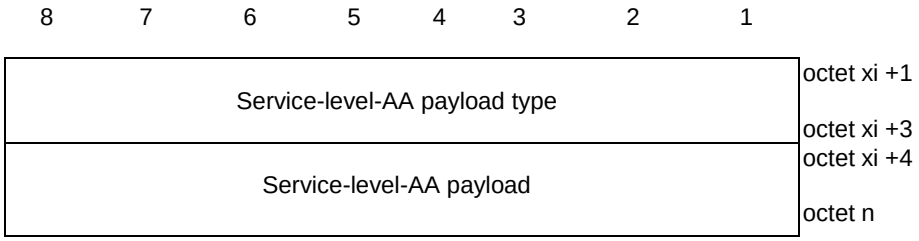


Figure 9.11.2.10.5: Service-level-AA parameter (when Service-level-AA payload type and its associated Service-level-AA payload are included in the Service-level-AA container contents)

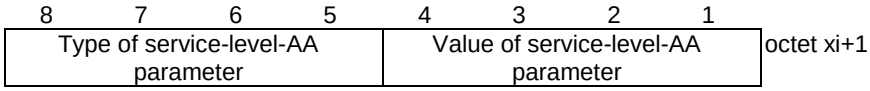


Figure 9.11.2.10.6: Service-level-AA parameter (when the type of service-level-AA parameter field contains an IEI of a type 1 information element as specified in 3GPP TS 24.007 [11])

Table 9.11.2.10.1: Service-level-AA container information element

Service-level-AA container contents (octet 4 to octet n); max value of 65535 octets

The error handlings for service-level-AA parameters specified in subclauses 7.6.1, 7.6.3 and 7.7.1 shall apply to the service-level-AA parameters included in the service-level-AA container contents.

Service-level-AA parameters
Type of service-level-AA parameter (octet xi +1)
This field contains the IEI of the service-level-AA parameter.

Length of service-level-AA parameter
This field indicates binary coded length of the value of the service-level-AA parameter.

Value of service-level-AA parameter
This field contains the value of the service-level-AA parameter with the value part of the referred information element based on following service-level-AA parameter reference.

The receiving entity shall ignore service-level-AA parameter with type of service-level-AA parameter field containing an unknown IEI.

IEI (hexadecimal)	Service-level-AA parameter name	Service-level-AA parameter reference
10	Service-level device ID	Service-level device ID (see subclause 9.11.2.11)
20	Service-level-AA server address	Service-level-AA server address (see subclause 9.11.2.12)
30	Service-level-AA response	Service-level-AA response (see subclause 9.11.2.14)
40	Service-level-AA payload type	Service-level-AA payload type (see subclause 9.11.2.15) (NOTE)
70	Service-level-AA payload	Service-level-AA payload (see subclause 9.11.2.13)
A-	Service-level-AA pending indication	Service-level-AA pending indication (see subclause 9.11.2.17)
50	Service-level-AA service status indication	Service-level-AA service status indication (see subclause 9.11.2.18)

NOTE: A service-level-AA payload type is always followed by the associated service-level-AA payload as shown in figure 9.11.2.10.5.

9.11.2.11 Service-level device ID

The purpose of the Service-level device ID information element is to carry the necessary identity for authentication and authorization by the external DN.

The Service-level device ID information element is coded as shown in figure 9.11.2.11.1 and table 9.11.2.11.1.

The Service-level device ID information element is a type 4 information element with minimum length of 3 octets and maximum length of 257 octets.

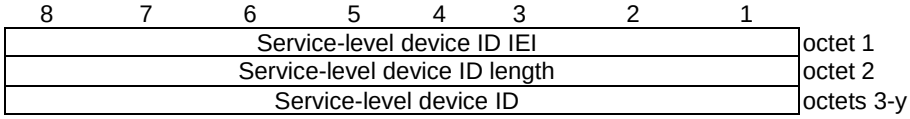


Figure 9.11.2.11.1: Service-level device ID information element

Table 9.11.2.11.1: Service-level device ID information element

Service-level device ID (octet 3 to octet y) A service-level device ID encoded as UTF-8 string.

9.11.2.12 Service-level-AA server address

The purpose of the Service-level-AA server address information element is to carry the address of the service level authentication and authorization server.

The Service-level-AA server address information element is coded as shown in figure 9.11.2.12.1 and table 9.11.2.12.1.

The Service-level-AA server address information element is a type 4 information element with minimum length of 4 octets and maximum length of 257 octets.

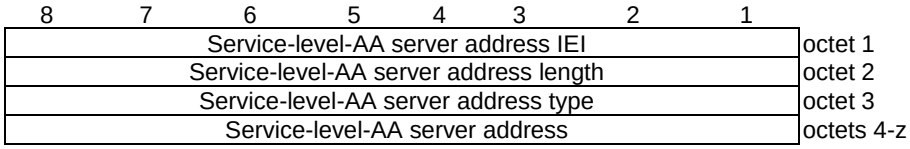


Figure 9.11.2.12.1: Service-level-AA server address information element

Table 9.11.2.12.1: Service-level-AA server address information element

Service-level-AA server address type (octet 3):
Bits

8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	
0	0	0	0	0	0	0	1	IPv4
0	0	0	0	0	0	1	0	IPv6
0	0	0	0	0	0	1	1	IPv4v6
0	0	0	0	0	1	0	0	FQDN

All other values are spare. If received they shall be ignored.

If the service-level-AA server address type indicates IPv4, then the service-level-AA server address field contains an IPv4 address in octet 4 to octet 7.

If the service-level-AA server address type indicates IPv6, then the service-level-AA server address field contains an IPv6 address in octet 4 to octet 19.

If the service-level-AA server address type indicates IPv4v6, then the service-level-AA server address field contains two IP addresses. The first IP address is an IPv4 address in octet 4 to octet 7. The second IP address is an IPv6 address in octet 8 to octet 23.

If the service-level-AA server address type indicates FQDN, octet 4 to octet z is encoded as defined in subclause 19.4.2.1 in 3GPP TS 23.003 [4].

9.11.2.13 Service-level-AA payload

The purpose of the Service-level-AA payload information element is to carry the upper layer payload for authentication and authorization between the UE and the service-level-AA server.

The Service-level-AA payload information element is coded as shown in figure 9.11.2.13.1 and table 9.11.2.13.1.

The Service-level-AA payload information element is a type 6 information element with minimum length of 4 octets and maximum length of 65538 octets.

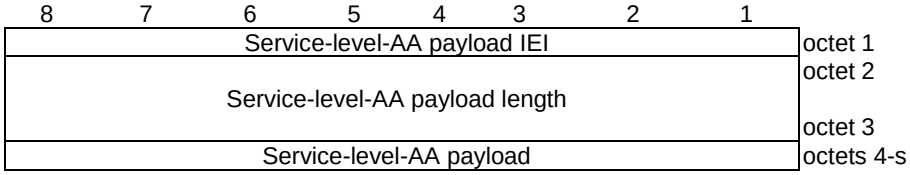


Figure 9.11.2.13.1: Service-level-AA payload information element

Table 9.11.2.13.1: Service-level-AA payload information element

Service-level-AA payload (octet 4 to octet s) A payload for authentication and authorization transparently transported and which is provided from/to the upper layers.

9.11.2.14 Service-level-AA response

The purpose of the Service-level-AA response information element is to provide information regarding the service level authentication and authorization request, e.g. to indicate that the authentication and authorization request to the service level authentication server was successful, or to notify that service level authorization is revoked.

The Service-level-AA response information element is coded as shown in figure 9.11.2.14.1 and table 9.11.2.14.1.

The Service-level-AA response information element is a type 4 information element with length of 3 octets.

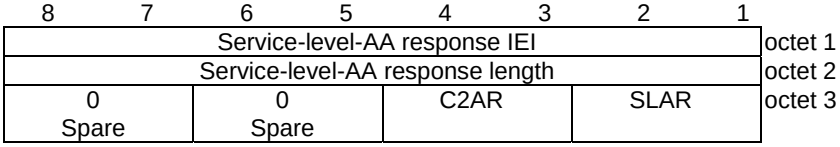


Figure 9.11.2.14.1: Service-level-AA response information element

Table 9.11.2.14.1: Service-level-AA response information element

Service-level-AA result field (SLAR) (octet 3, bits 1 and 2) Bits **1 2** 0 0 No information 0 1 Service level authentication and authorization was successful. 1 0 Service level authentication and authorization was not successful or service level authorization is revoked. 1 1 Reserved C2 authorization result field (C2AR) (octet 3, bits 3 and 4) Bits **3 4** 0 0 No information 0 1 C2 authorization was successful. 1 0 C2 authorization was not successful or C2 authorization is revoked. 1 1 Reserved Bits 5 to 8 of octet 3 are spare and shall be coded as zero.

9.11.2.15 Service-level-AA payload type

The purpose of the Service-level-AA payload type information element is to indicates type of payload included in the Service-level-AA payload information element.

The Service-level-AA payload type information element is coded as shown in figure 9.11.2.15.1 and table 9.11.2.15.1.

The Service-level-AA payload type information element is a type 4 information element with length of 3 octets.

8	7	6	5	4	3	2	1	
Service-level-AA payload type IEI								octet 1
Service-level-AA payload type length								octet 2
Service-level-AA payload type								octet 3

Figure 9.11.2.15.1: Service-level-AA payload type information element

Table 9.11.2.15.1: Service-level-AA payload type information element

Service-level-AA payload type (octet 3):								
Bits								
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	
0	0	0	0	0	0	0	1	UUAA payload (see NOTE 1)
0	0	0	0	0	0	1	0	C2 authorization payload (see NOTE 2)
All other values are spare, and the receiving entity shall ignore the service-level-AA payload type value set to a spare value.								

NOTE 1: If the service-level-AA payload type indicates UUAA payload, the field for the service-level-AA payload of the Service-level AA payload information element is an application layer payload for UUAA procedure between the UE supporting UAS services and the USS.

NOTE 2: If the service-level-AA payload type indicates C2 authorization payload, the field for the service-level-AA payload of the Service-level-AA payload information element is an application layer payload for C2 authorization procedure between the UE supporting UAS services and the USS.

9.11.2.16 Void

9.11.2.17 Service-level-AA pending indication

The purpose of the Service-level-AA pending indication information element is to provide an indication that the service level authentication and authorization procedure is to be performed.

The Service-level-AA pending indication information element is coded as shown in figure 9.11.2.17.1 and table 9.11.2.17.1.

The Service-level-AA pending indication information element is a type 1 information element.

8	7	6	5	4	3	2	1	
Service-level-AA pending indication IEI				0 Spare	0 Spare	0 Spare	SLAPI	octet 1

Figure 9.11.2.17.1: Service-level-AA pending indication

Table 9.11.2.17.1: Service-level-AA pending indication

Service-level-AA pending indication (SLAPI) (octet 1, bit 1)	
Bit	
1	
0	reserved
1	Service-level-AA procedure is to be performed

9.11.2.18 Service-level-AA service status indication

The purpose of the Service-level-AA service status indication information element is to provide an indication of the service availability to the UE.

The Service-level-AA service status indication information element is coded as shown in figure 9.11.2.18.1 and table 9.11.2.18.1.

The Service-level-AA service status indication information element is a type 4 information element with a length of 3 octets.

8	7	6	5	4	3	2	1	
Service-level-AA service status indication IEI								octet 1
Length of Service-level-AA service status indication								octet 2
0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	UAS	octet 3

Figure 9.11.2.18.1: Service-level-AA-service-status indication information element

Table 9.11.2.18.1: Service-level-AA-service-status indication information element

UAS (octet 3, bit 1) Bit **1** 0 UAS services not enabled 1 UAS services enabled Bits 2 to 8 of octet 3 are spare and shall be encoded as zero.

9.11.2.19 Time duration

See subclause 9.9.3.68 in 3GPP TS 24.301 [15].

9.11.2.20 Unavailability information

See subclause 9.9.3.69 in 3GPP TS 24.301 [15].

9.11.2.21 Unavailability configuration

See subclause 9.9.3.70 in 3GPP TS 24.301 [15].

9.11.3 5GS mobility management (5GMM) information elements

9.11.3.1 5GMM capability

The purpose of the 5GMM capability information element is to provide the network with information concerning aspects of the UE related to the 5GCN or interworking with the EPS. The contents might affect the manner in which the network handles the operation of the UE.

The 5GMM capability information element is coded as shown in figure 9.11.3.1.1 and table 9.11.3.1.1.

The 5GMM capability is a type 4 information element with a minimum length of 3 octets and a maximum length of 15 octets.

8	7	6	5	4	3	2	1	
5GMM capability IEI								octet 1
Length of 5GMM capability contents								octet 2
SGC	5G-IPHC-CP CIoT	N3 data	5G-CP CIoT	Restrict tEC	LPP	HO attach	S1 mode	octet 3
RACS	NSSAA	5G-LCS	V2XC NPC5	V2XC EPC5	V2X	5G-UP CIoT	5GSR VCC	octet 4*
5G ProSe-l2relay	5G ProSe-dc	5G ProSe-dd	ER-NSSAI	5G-EHC-CP CIoT	multipleUP	WUSA	CAG	octet 5*
PR	RPR	PIV	NCR	NR-PSSI	5G ProSe-l3rmt	5G ProSe-l2rmt	5G ProSe-l3relay	octet 6*
MPSIU	UAS	NSAG	Ex-CAG	SSNPNSI	Event Notification	MINT	NSSRG	octet 7*
SBTS	NSR	LADN-DS	RAN timing	ECI	ESI	RCMAN	RCMAP	octet 8*
5G ProSe-l2end	5G ProSe-l3U2U relay	5G ProSe-l2U2U relay	RSLPS	SBNS	UN-PER	A2XNPC5	A2XEPC5	octet 9*
A2X-Uu	SLVI	TempNS	SUPL	LCS-UPP	PNS	RSLP	5G ProSe-l3end	octet 10*
0 spare	0 spare	0 spare	0 spare	NSUC	RSLPL	NVL-SATNR	MCSIU	octet 11*
0	0	0	0	0	0	0	0	octet 12*-15*
Spare								

Figure 9.11.3.1.1: 5GMM capability information element

Table 9.11.3.1.1: 5GMM capability information element

EPC NAS supported (S1 mode) (octet 3, bit 1)
Bit
1
0 S1 mode not supported
1 S1 mode supported

ATTACH REQUEST message containing PDN CONNECTIVITY REQUEST message for handover support (HO attach) (octet 3, bit 2)
Bit
2
0 ATTACH REQUEST message containing PDN CONNECTIVITY REQUEST message with request type set to "handover" or "handover of emergency bearer services" to transfer PDU session from N1 mode to S1 mode not supported
1 ATTACH REQUEST message containing PDN CONNECTIVITY REQUEST message with request type set to "handover" or "handover of emergency bearer services" to transfer PDU session from N1 mode to S1 mode supported

LTE Positioning Protocol (LPP) capability (octet 3, bit 3)
This bit indicates the capability to support LTE Positioning Protocol (LPP) (see 3GPP TS 37.355 [26]).
Bit
3
0 LPP in N1 mode not supported
1 LPP in N1 mode supported

Restriction on use of enhanced coverage support (RestrictEC) (octet 3, bit 4)
This bit indicates the capability to support restriction on use of enhanced coverage.
Bit
4
0 Restriction on use of enhanced coverage not supported
1 Restriction on use of enhanced coverage supported

Control plane CIoT 5GS optimization (5G-CP CIoT) (octet 3, bit 5)
This bit indicates the capability for control plane CIoT 5GS optimization.
Bit
5
0 Control plane CIoT 5GS optimization not supported
1 Control plane CIoT 5GS optimization supported

N3 data transfer (N3 data) (octet 3, bit 6)
This bit indicates the capability for N3 data transfer.
Bit
6
0 N3 data transfer supported
1 N3 data transfer not supported

IP header compression for control plane CIoT 5GS optimization (5G-IPHC-CP CIoT) (octet 3, bit 7)
This bit indicates the capability for IP header compression for control plane CIoT 5GS optimization.
Bit
7
0 IP header compression for control plane CIoT 5GS optimization not supported
1 IP header compression for control plane CIoT 5GS optimization supported

Service gap control (SGC) (octet 3, bit 8)
Bit
8
0 service gap control not supported
1 service gap control supported

5G-SRVCC from NG-RAN to UTRAN (5GSRVCC) capability (octet 4, bit 1)
This bit indicates the capability for 5G-SRVCC from NG-RAN to UTRAN (5GSRVCC) (see 3GPP TS 23.216 [6A]).
Bit
1
0 5G-SRVCC from NG-RAN to UTRAN not supported
1 5G-SRVCC from NG-RAN to UTRAN supported

User plane CIoT 5GS optimization (5G-UP CIoT) (octet 4, bit 2)
This bit indicates the capability for user plane CIoT 5GS optimization.

Bit 2	
0	User plane CIoT 5GS optimization not supported
1	User plane CIoT 5GS optimization supported

V2X capability (V2X) (octet 4, bit 3)
This bit indicates the capability for V2X, as specified in 3GPP TS 24.587 [19B].

Bit 3	
0	V2X not supported
1	V2X supported

V2X communication over E-UTRA-PC5 capability (V2XCEPC5) (octet 4, bit 4)
This bit indicates the capability for V2X communication over E-UTRA-PC5, as specified in 3GPP TS 24.587 [19B].

Bit 4	
0	V2X communication over E-UTRA-PC5 not supported
1	V2X communication over E-UTRA-PC5 supported

V2X communication over NR-PC5 capability (V2XCNPC5) (octet 4, bit 5)
This bit indicates the capability for V2X communication over NR-PC5, as specified in 3GPP TS 24.587 [19B].

Bit 5	
0	V2X communication over NR-PC5 not supported
1	V2X communication over NR-PC5 supported

Location Services (5G-LCS) notification mechanisms capability (octet 4, bit 6)
This bit indicates the capability to support Location Services (5G-LCS) notification mechanisms (see 3GPP TS 23.273 [6B]).

Bit 6	
0	LCS notification mechanisms not supported
1	LCS notification mechanisms supported

Network slice-specific authentication and authorization (NSSAA) (octet 4, bit 7)
This bit indicates the capability to support network slice-specific authentication and authorization.

Bit 7	
0	Network slice-specific authentication and authorization not supported
1	Network slice-specific authentication and authorization supported

Radio capability signalling optimisation (RACS) capability (octet 4, bit 8)

Bit 8	
0	RACS not supported
1	RACS supported

Closed Access Group (CAG) capability (octet 5, bit 1)

Bit 1	
0	CAG not supported
1	CAG supported

WUS assistance (WUSA) information reception capability (octet 5, bit 2)

Bit 2	
0	WUS assistance information reception not supported
1	WUS assistance information reception supported

Multiple user-plane resources support (multipleUP) (octet 5, bit 3)
This bit indicates the capability to support multiple user-plane resources in NB-N1 mode.

Bit 3	
0	Multiple user-plane resources not supported
1	Multiple user-plane resources supported

Ethernet header compression for control plane CIoT 5GS optimization (5G-EHC-CP CIoT) (octet 5, bit 4)
Bit
4
0 Ethernet header compression for control plane CIoT 5GS optimization not supported
1 Ethernet header compression for control plane CIoT 5GS optimization supported

Extended rejected NSSAI support (ER-NSSAI) (octet 5, bit 5)
This bit indicates the capability to support extended rejected NSSAI.
Bit
5
0 Extended rejected NSSAI not supported
1 Extended rejected NSSAI supported

5G ProSe direct discovery (5G ProSe-dd) (octet 5, bit 6)
This bit indicates the capability for 5G ProSe direct discovery.
Bit
6
0 5G ProSe direct discovery not supported
1 5G ProSe direct discovery supported

5G ProSe direct communication (5G ProSe-dc) (octet 5, bit 7)
This bit indicates the capability for 5G ProSe direct communication.
Bit
7
0 5G ProSe direct communication not supported
1 5G ProSe direct communication supported

5G ProSe layer-2 UE-to-network-relay (5G ProSe-l2relay) (octet 5, bit 8)
This bit indicates the capability to act as a 5G ProSe layer-2 UE-to-network relay UE.
Bit
8
0 Acting as a 5G ProSe layer-2 UE-to-network relay UE not supported
1 Acting as a 5G ProSe layer-2 UE-to-network relay UE supported

5G ProSe layer-3 UE-to-network-relay (5G ProSe-l3relay) (octet 6, bit 1)
This bit indicates the capability to act as a 5G ProSe layer-3 UE-to-network relay UE
Bit
1
0 Acting as a 5G ProSe layer-3 UE-to-network relay UE not supported
1 Acting as a 5G ProSe layer-3 UE-to-network relay UE supported

5G ProSe layer-2 UE-to-network-remote (5G ProSe-l2rmt) (octet 6, bit 2)
This bit indicates the capability to act as a 5G ProSe layer-2 UE-to-network remote UE
Bit
2
0 Acting as a 5G ProSe layer-2 UE-to-network remote UE not supported
1 Acting as a 5G ProSe layer-2 UE-to-network remote UE supported

5G ProSe layer-3 UE-to-network-remote (5G ProSe-l3rmt) (octet 6, bit 3)
This bit indicates the capability to act as a 5G ProSe layer-3 UE-to-network remote UE
Bit
3
0 Acting as a 5G ProSe layer-3 UE-to-network remote UE not supported
1 Acting as a 5G ProSe layer-3 UE-to-network remote UE supported

NR paging subgroup support indication (NR-PSSI) (octet 6, bit 4)
This bit indicates the capability to support NR paging subgrouping
Bit
4
0 NR paging subgrouping not supported
1 NR paging subgrouping supported

N1 NAS signalling connection release (NCR) (octet 6, bit 5)
This bit indicates whether N1 NAS signalling connection release is supported.

Bit
5
0 N1 NAS signalling connection release not supported
1 N1 NAS signalling connection release supported

Paging indication for voice services (PIV) (octet 6, bit 6)
This bit indicates whether paging indication for voice services is supported.
Bit
6
0 paging indication for voice services not supported
1 paging indication for voice services supported

Reject paging request (RPR) (octet 6, bit 7)
This bit indicates whether reject paging request is supported.
Bit
7
0 reject paging request not supported
1 reject paging request supported

Paging restriction (PR) (octet 6, bit 8)
This bit indicates whether paging restriction is supported.
Bit
8
0 paging restriction not supported
1 paging restriction supported

NSSRG (octet 7, bit 1)
This bit indicates the capability to support the NSSRG.
Bit
1
0 NSSRG not supported
1 NSSRG supported

Minimization of service interruption (MINT) (octet 7, bit 2)
This bit indicates the capability to support Minimization of service interruption (MINT)
Bit
2
0 MINT not supported
1 MINT supported

Event notification (EventNotification) (octet 7, bit 3)
This bit indicates the capability to support event notification for upper layers
Bit
3
0 Event notification not supported
1 Event notification supported

SOR-SNPN-SI (SOR SNPN SI) (octet 7, bit 4)
This bit indicates the capability to support SOR-SNPN-SI.
Bit
4
0 SOR-SNPN-SI not supported
1 SOR-SNPN-SI supported

Extended CAG information list support (Ex-CAG) (octet 7, bit 5)
This bit indicates the capability to support extended CAG information list.
Bit
5
0 Extended CAG information list not supported
1 Extended CAG information list supported

NSAG (octet 7, bit 6)
This bit indicates the capability to support NSAG.
Bit
76
0 NSAG not supported
1 NSAG supported

UAS (octet 7, bit 7)

This bit indicates the capability to support UAS services.
Bit
7
0 UAS services not supported
1 UAS services supported

MPS indicator update (MPSIU) (octet 7, bit 8)
This bit indicates the capability to support MPS indicator update via the UE configuration update procedure.
Bit
8
0 MPS indicator update not supported
1 MPS indicator update supported

Registration complete message for acknowledging negotiated PEIPS assistance information (RCMAP) (octet 8, bit 1)
This bit indicates the capability for sending REGISTRATION COMPLETE message when Negotiated PEIPS assistance information IE is included in the REGISTRATION ACCEPT message.
Bit
1
0 Sending of REGISTRATION COMPLETE message for negotiated PEIPS assistance information not supported
1 Sending of REGISTRATION COMPLETE message for negotiated PEIPS assistance information supported

Registration complete message for acknowledging NSAG information (RCMAN) (octet 8, bit 2)
This bit indicates the capability for sending REGISTRATION COMPLETE message when NSAG information IE is included in the REGISTRATION ACCEPT message.
Bit
2
0 Sending of REGISTRATION COMPLETE message for NSAG information not supported
1 Sending of REGISTRATION COMPLETE message for NSAG information supported

Equivalent SNPNs indicator (ESI) (octet 8, bit 3)
This bit indicates the capability to support equivalent SNPNs.
Bit
3
0 Equivalent SNPNs not supported
1 Equivalent SNPNs supported

Enhanced CAG information (ECI) (octet 8, bit 4)
This bit indicates the capability to support enhanced CAG information.
Bit
4
0 Enhanced CAG information not supported
1 Enhanced CAG information supported

Reconnection to the network due to RAN timing synchronization status change (RANtiming) (octet 8, bit 5)
This bit indicates the capability to support Reconnection to the network due to RAN timing synchronization status change.
Bit
5
0 Reconnection to the network due to RAN timing synchronization status change not supported
1 Reconnection to the network due to RAN timing synchronization status change supported

LADN per DNN and S-NSSAI support (LADN-DS) (octet 8, bit 6)
This bit indicates the capability to support LADN per DNN and S-NSSAI.
Bit
6
0 LADN per DNN and S-NSSAI not supported
1 LADN per DNN and S-NSSAI supported

Network slice replacement (NSR) (octet 8, bit 7)
This bit indicates the capability to support network slice replacement.
Bit
7
0 Network slice replacement not supported
1 Network slice replacement supported

Slice-based TNGF selection support (SBTS) (octet 8, bit 8)
This bit indicates the capability to support slice-based TNGF selection.
Bit
8
0 Slice-based TNGF selection not supported
1 Slice-based TNGF selection supported

A2X over E-UTRA-PC5 (A2XEPC5) (octet 9, bit 1)
This bit indicates the capability for A2X over E-UTRA-PC5, as specified in 3GPP TS 24.577 [60].
Bit
1
0 A2X over E-UTRA-PC5 not supported
1 A2X over E-UTRA-PC5 supported

A2X over NR-PC5 (A2XNPC5) (octet 9, bit 2)
This bit indicates the capability for A2X over NR-PC5, as specified in 3GPP TS 24.577 [60].
Bit
2
0 A2X over NR-PC5 not supported
1 A2X over NR-PC5 supported

Unavailability period (UN-PER) (octet 9, bit 3)
This bit indicates the capability to support unavailability period.
Bit
3
0 Unavailability period not supported
1 Unavailability period supported

Slice-based N3IWFselection support (SBNS) (octet 9, bit 4)
This bit indicates the capability to support slide-based N3IWF selection
Bit
4
0 Slice-based N3IWF selection not supported
1 Slice-based N3IWF selection supported

SL positioning server UE (RSLPS) (octet 9, bit 5)
This bit indicates the capability for SL positioning server UE, as specified in
3GPP TS 24.586 [ts23586].
Bit
5
0 Ranging and sidelink positioning for SL positioning server UE not supported
1 Ranging and sidelink positioning for SL positioning server UE supported

5G ProSe layer-2 UE-to-UE relay (5G ProSe-l2U2U relay) (octet 9, bit 6)
This bit indicates the capability to act as a 5G ProSe layer-2 UE-to-UE relay UE.
Bit
6
0 Acting as a 5G ProSe layer-2 UE-to-UE relay UE not supported
1 Acting as a 5G ProSe layer-2 UE-to-UE relay UE supported

5G ProSe layer-3 UE-to-UE relay (5G ProSe-l3U2U relay) (octet 9, bit 7)
This bit indicates the capability to act as a 5G ProSe layer-3 UE-to-UE relay UE.
Bit
7
0 Acting as a 5G ProSe layer-3 UE-to-UE relay UE not supported
1 Acting as a 5G ProSe layer-3 UE-to-UE relay UE supported

5G ProSe layer-2 end UE (5G ProSe-l2end) (octet 9, bit 8)
This bit indicates the capability to act as a 5G ProSe layer-2 end UE.
Bit
8
0 Acting as a 5G ProSe layer-23 UE-to-UE relayend UE not supported

1 Acting as a 5G ProSe layer-23 UE-to-UE relayend UE supported

5G ProSe layer-3 end UE (5G ProSe-l3end) (octet 10, bit 1)
This bit indicates the capability to act as a 5G ProSe layer-3 end UE.
Bit
1
0 Acting as a 5G ProSe layer-3 end UE not supported
1 Acting as a 5G ProSe layer-3 end UE supported

Ranging and sidelink positioning support (RSLP) (octet 10, bit 2)
Bit
2
0 Ranging and sidelink positioning not supported
1 Ranging and sidelink positioning supported

Partial network slice (PNS) (octet 10, bit 3)
This bit indicates whether the UE support partial network slice in the registration area.
Bit
3
0 Partial network slice not supported
1 Partial network slice supported

LCS-UPP user plane positioning (LCS-UPP) (octet 10, bit 4)
This bit indicates the capability to support LCS-UPP user plane positioning (see 3GPP TS 23.273 [6B]).
Bit
4
0 User plane positioning using LCS-UPP not supported
1 User plane positioning using LCS-UPP supported

SUPL user plane positioning (SUPL) (octet 10, bit 5)
This bit indicates the capability to support SUPL user plane positioning (see 3GPP TS 38.305 [67] and 3GPP TS 23.271 [68]).
Bit
5
0 User plane positioning using SUPL not supported
1 User plane positioning using SUPL supported

S-NSSAI time validity information (TempNS) (octet 10, bit 6)
This bit indicates the capability to support the S-NSSAI time validity information.
Bit
6
0 S-NSSAI time validity information not supported
1 S-NSSAI time validity information supported

S-NSSAI location validity information (SLVI) (octet 10, bit 7)
This bit indicates the capability to support S-NSSAI location validity information.
Bit
7
0 S-NSSAI location validity information not supported
1 S-NSSAI location validity information supported

A2X over Uu capability (A2X-Uu) (octet 10, bit 8)
This bit indicates the capability for A2X over Uu, as specified in 3GPP TS 24.577 [60].
Bit
8
0 A2X over Uu not supported
1 A2X over Uu supported

MCS indicator update (MCSIU) (octet 11, bit 1)
This bit indicates the capability to support MCS indicator update via the UE configuration update procedure.
Bit
1
0 MCS indicator update not supported
1 MCS indicator update supported

Network verified UE location over satellite NG-RAN (NVL-SATNR) (octet 11, bit 2)

This bit indicates the capability to support network verified UE location over satellite NG-RAN as specified in 3GPP TS 23.501 [8].
Bit
2
0 Network verified UE location over satellite NG-RAN not supported
1 Network verified UE location over satellite NG-RAN supported

Ranging and sidelink positioning over PC5 for located UE support (RSLPL) (octet 11, bit 3)
This bit indicates the capability to support ranging and sidelink positioning over PC5 for located UE support.
Bit
3
0 Ranging and sidelink positioning for located UE not supported
1 Ranging and sidelink positioning for located UE supported

Network slice usage control (NSUC) (octet 11, bit 4)
This bit indicates the capability to support network slice usage control.
Bit
4
0 Network slice usage control not supported
1 Network slice usage control supported

Bits 5 to 8 in octet 11 and bits in octets 12 to 15 are spare and shall be coded as zero, if the respective octet is included in the information element.

9.11.3.2 5GMM cause

The purpose of the 5GMM cause information element is to indicate the reason why a 5GMM request is rejected.

The 5GMM cause information element is coded as shown in figure 9.11.3.2.1 and table 9.11.3.2.1.

The 5GMM cause is a type 3 information element with length of 2 octets.

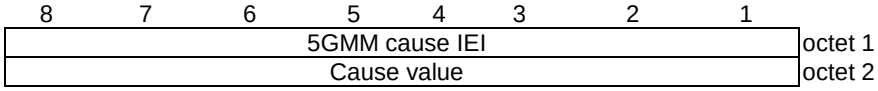


Figure 9.11.3.2.1: 5GMM cause information element

Table 9.11.3.2.1: 5GMM cause information element

Cause value (octet 2)

Bits

8	7	6	5	4	3	2	1	
0	0	0	0	0	0	1	1	Illegal UE
0	0	0	0	0	1	0	1	PEI not accepted
0	0	0	0	0	1	1	0	Illegal ME
0	0	0	0	0	1	1	1	5GS services not allowed
0	0	0	0	1	0	0	1	UE identity cannot be derived by the network
0	0	0	0	1	0	1	0	Implicitly de-registered
0	0	0	0	1	0	1	1	PLMN not allowed
0	0	0	0	1	1	0	0	Tracking area not allowed
0	0	0	0	1	1	0	1	Roaming not allowed in this tracking area
0	0	0	0	1	1	1	1	No suitable cells in tracking area
0	0	0	1	0	1	0	0	MAC failure
0	0	0	1	0	1	0	1	Synch failure
0	0	0	1	0	1	1	0	Congestion
0	0	0	1	0	1	1	1	UE security capabilities mismatch
0	0	0	1	1	0	0	0	Security mode rejected, unspecified
0	0	0	1	1	0	1	0	Non-5G authentication unacceptable
0	0	0	1	1	0	1	1	N1 mode not allowed
0	0	0	1	1	1	0	0	Restricted service area
0	0	0	1	1	1	1	1	Redirection to EPC required
0	0	1	0	0	1	0	0	IAB-node operation not authorized
0	0	1	0	1	0	1	1	LADN not available
0	0	1	1	1	1	1	0	No network slices available
0	1	0	0	0	0	0	1	Maximum number of PDU sessions reached
0	1	0	0	0	0	1	1	Insufficient resources for specific slice and DNN
0	1	0	0	0	1	0	1	Insufficient resources for specific slice
0	1	0	0	0	1	1	1	ngKSI already in use
0	1	0	0	1	0	0	0	Non-3GPP access to 5GCN not allowed
0	1	0	0	1	0	0	1	Serving network not authorized
0	1	0	0	1	0	1	0	Temporarily not authorized for this SNPN
0	1	0	0	1	0	1	1	Permanently not authorized for this SNPN
0	1	0	0	1	1	0	0	Not authorized for this CAG or authorized for CAG cells only
0	1	0	0	1	1	0	1	Wireline access area not allowed
0	1	0	0	1	1	1	0	PLMN not allowed to operate at the present UE location
0	1	0	0	1	1	1	1	UAS services not allowed
0	1	0	1	0	0	0	0	Disaster roaming for the determined PLMN with disaster condition not allowed
0	1	0	1	0	0	0	1	Selected N3IWF is not compatible with the allowed NSSAI
0	1	0	1	0	0	1	0	Selected TNGF is not compatible with the allowed NSSAI
0	1	0	1	1	0	1	0	Payload was not forwarded
0	1	0	1	1	0	1	1	DNN not supported or not subscribed in the slice
0	1	0	1	1	1	0	0	Insufficient user-plane resources for the PDU session
0	1	0	1	1	1	0	1	Onboarding services terminated
0	1	0	1	1	1	1	0	User plane positioning not authorized
0	1	0	1	1	1	1	1	Semantically incorrect message
0	1	1	0	0	0	0	0	Invalid mandatory information
0	1	1	0	0	0	0	1	Message type non-existent or not implemented
0	1	1	0	0	0	1	0	Message type not compatible with the protocol state
0	1	1	0	0	0	1	1	Information element non-existent or not implemented
0	1	1	0	0	1	0	0	Conditional IE error
0	1	1	0	0	1	0	1	Message not compatible with the protocol state
0	1	1	0	1	1	1	1	Protocol error, unspecified

Any other value received by the mobile station shall be treated as 0110 1111, "protocol error, unspecified". Any other value received by the network shall be treated as 0110 1111, "protocol error, unspecified".

9.11.3.2A 5GS DRX parameters

The purpose of the 5GS DRX parameters information element is to indicate that the UE wants to use DRX and for the network to indicate the DRX cycle value to be used at paging.

The 5GS DRX parameters is a type 4 information element with a length of 3 octets.

The 5GS DRX parameters information element is coded as shown in figure 9.11.3.2A.1 and table 9.11.3.2A.1.

The value part of a DRX parameter information element is coded as shown in table 9.11.3.2A.1.

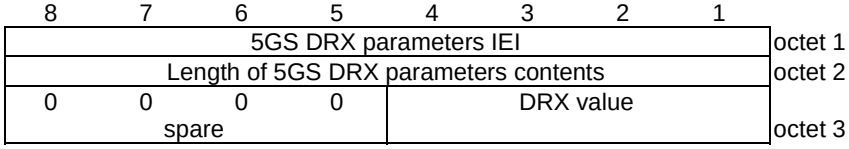


Figure 9.11.3.2A.1: 5GS DRX parameters information element

Table 9.11.3.2A.1: 5GS DRX parameters information element

DRX value (bits 4 to 1 of octet 3)

This field represents the DRX cycle parameter 'T' as defined in 3GPP TS 38.304 [28] or 3GPP TS 36.304 [25C].

Bits

4	**3**	**2**	**1**	
0	0	0	0	DRX value not specified
0	0	0	1	DRX cycle parameter T = 32
0	0	1	0	DRX cycle parameter T = 64
0	0	1	1	DRX cycle parameter T = 128
0	1	0	0	DRX cycle parameter T = 256

All other values shall be interpreted as "DRX value not specified" by this version of the protocol.

Bits 5 to 8 of octet 3 are spare and shall be coded as zero.

9.11.3.3 5GS identity type

The purpose of the 5GS identity type information element is to specify which identity is requested.

The 5GS identity type is a type 1 information element.

The 5GS identity type information element is coded as shown in figure 9.11.3.3.1 and table 9.11.3.3.1.

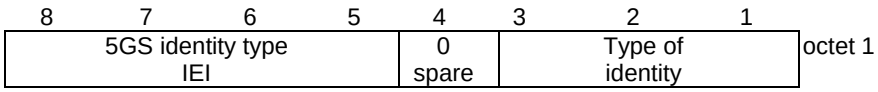


Figure 9.11.3.3.1: 5GS identity type information element

Table 9.11.3.3.1: 5GS identity type information element

Type of identity (octet 1) Bits **3 2 1**	
0 0 1	SUCI
0 1 0	5G-GUTI
0 1 1	IMEI
1 0 0	5G-S-TMSI
1 0 1	IMEISV
1 1 0	MAC address
1 1 1	EUI-64
All other values are unused and shall be interpreted as "SUCI", if received by the UE.	

9.11.3.4 5GS mobile identity

The purpose of the 5GS mobile identity information element is to provide either the SUCI, the 5G-GUTI, the IMEI, the IMEISV, the 5G-S-TMSI, the MAC address or the EUI-64.

The 5GS mobile identity information element is coded as shown in figures 9.11.3.4.1, 9.11.3.4.2, 9.11.3.4.3, 9.11.3.4.4, 9.11.3.4.5, 9.11.3.4.6, 9.11.3.4.8 and 9.11.3.4.7, and table 9.11.3.4.1.

The 5GS mobile identity is a type 6 information element with a minimum length of 4.

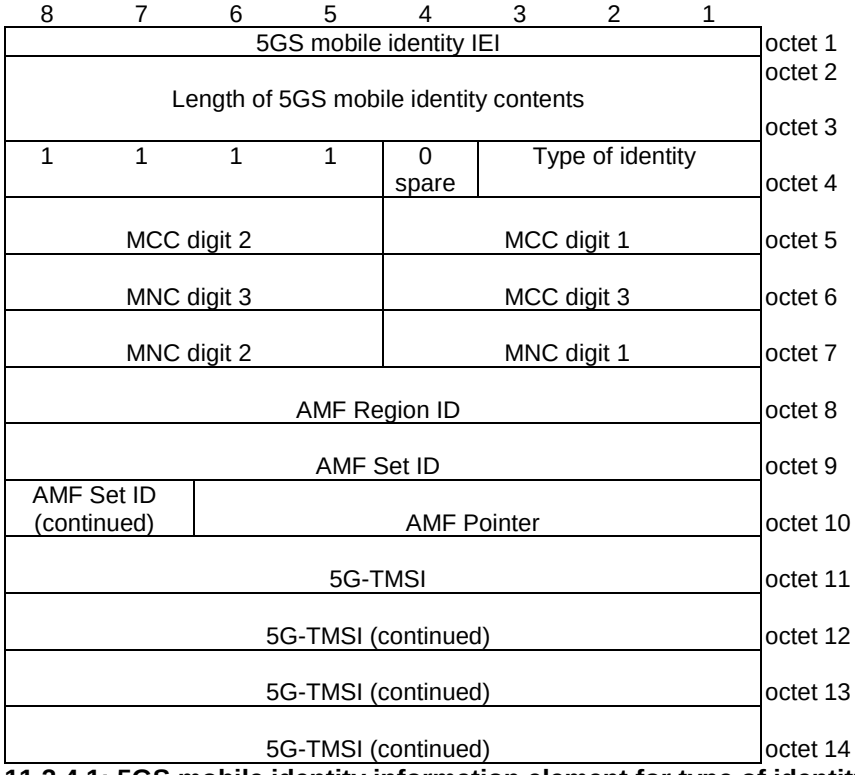


Figure 9.11.3.4.1: 5GS mobile identity information element for type of identity "5G-GUTI"

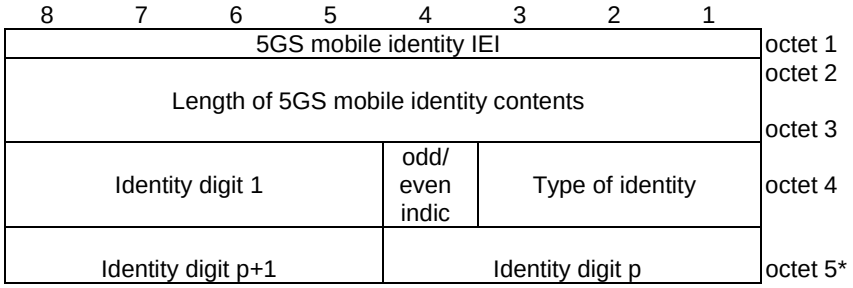


Figure 9.11.3.4.2: 5GS mobile identity information element for type of identity "IMEI" or "IMEISV"

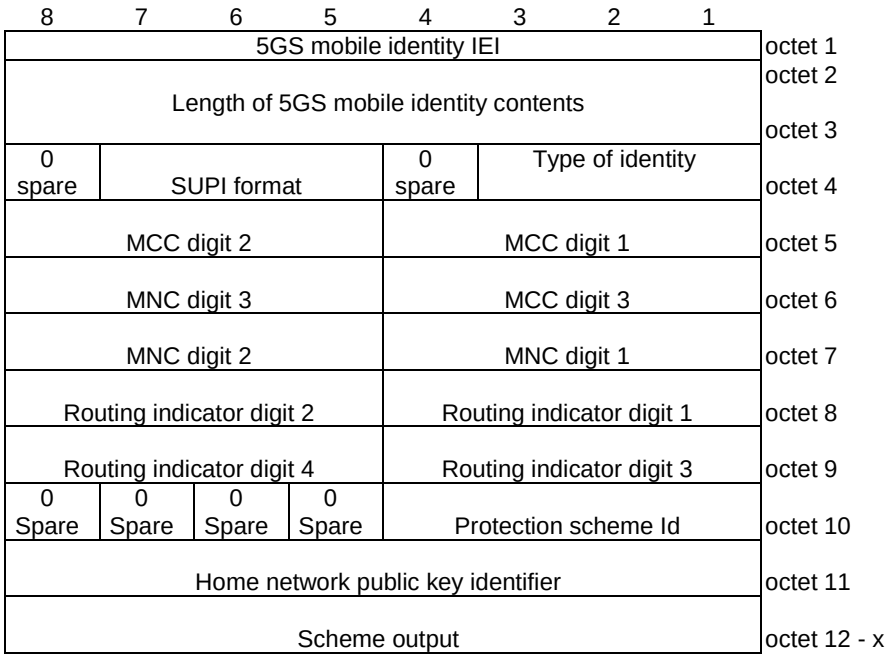


Figure 9.11.3.4.3: 5GS mobile identity information element for type of identity "SUCI" and SUPI format "IMSI"

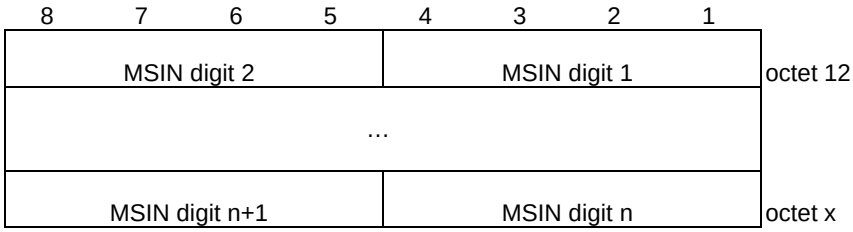


Figure 9.11.3.4.3a: Scheme output for type of identity "SUCI", SUPI format "IMSI" and Protection scheme Id "Null scheme"

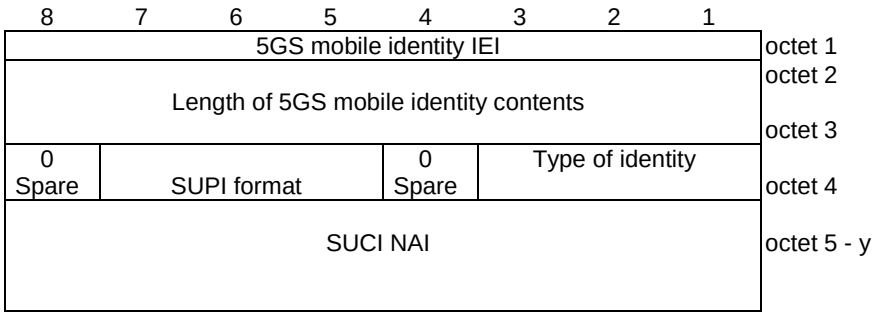


Figure 9.11.3.4.4: 5GS mobile identity information element for type of identity "SUCI" and SUPI format "Network specific identifier", "GCI" or "GLI"

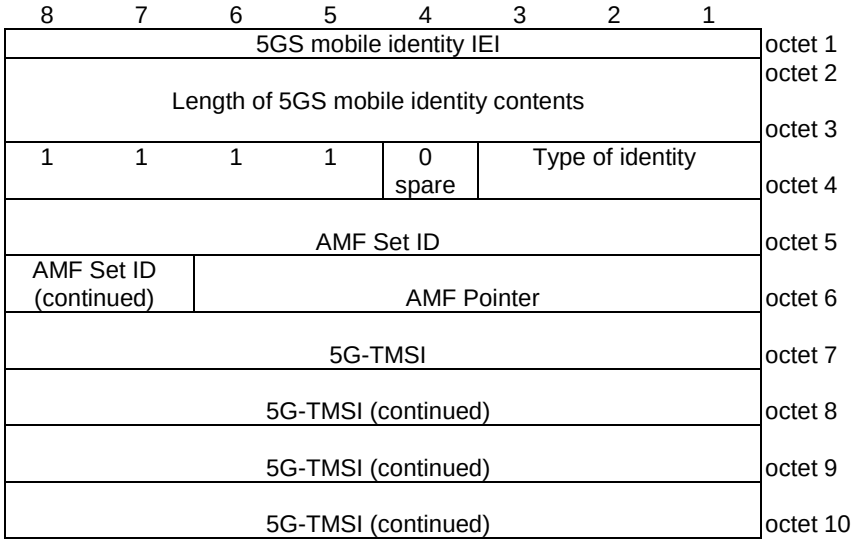


Figure 9.11.3.4.5: 5GS mobile identity information element for type of identity "5G-S-TMSI"

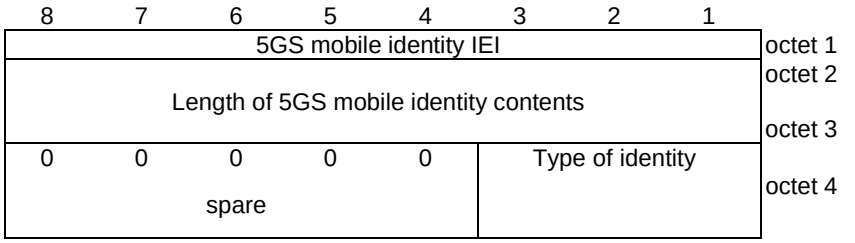


Figure 9.11.3.4.6: 5GS mobile identity information element for type of identity "No identity"

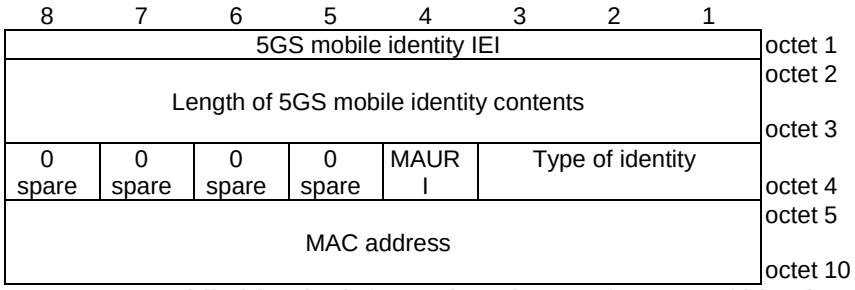


Figure 9.11.3.4.7: 5GS mobile identity information element for type of identity "MAC address"

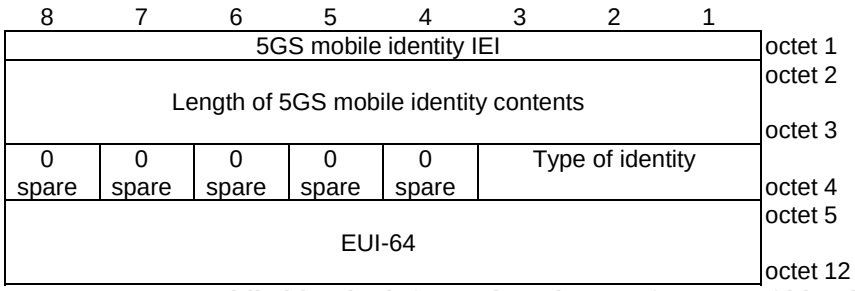


Figure 9.11.3.4.8: 5GS mobile identity information element for type of identity "EUI-64"

Table 9.11.3.4.1: 5GS mobile identity information element

Type of identity (octet 4)
Bits

3	2	1	
0	0	0	No identity (see NOTE 1)
0	0	1	SUCI
0	1	0	5G-GUTI
0	1	1	IMEI
1	0	0	5G-S-TMSI
1	0	1	IMEISV
1	1	0	MAC address
1	1	1	EUI-64

All other values are reserved.

Odd/even indication (octet 4)
Bit

4	
0	even number of identity digits
1	odd number of identity digits

For the 5G-GUTI, then bits 5 to 8 of octet 4 are coded as "1111", octet 5 through 7 contain the MCC and MNC values as specified below, octet 8 through 10 contain the AMF Region ID, the AMF Set ID and the AMF Pointer values and octet 11 through 14 contain the 5G-TMSI as defined in 3GPP TS 23.003 [4].

MCC, Mobile country code (octet 5, octet 6 bits 1 to 4)

The MCC field is coded as in ITU-T Recommendation E.212 [42], annex A.

MNC, Mobile network code (octet 6 bits 5 to 8, octet 7)

The coding of this field is the responsibility of each administration but BCD coding shall be used. The MNC shall consist of 2 or 3 digits. If a network operator decides to use only two digits in the MNC, bits 5 to 8 of octet 6 shall be coded as "1111".

The MCC and MNC digits are coded as octets 6 to 8 of the Temporary mobile group identity IE in figure 10.5.154 of 3GPP TS 24.008 [12].

AMF Region ID (octet 8)
This field contains the binary encoding of the AMF Region ID. Bit 8 of octet 7 is the most significant bit and bit 1 of octet 7 is the least significant bit.

AMF Set ID (octet 9, octet 10 bits 7 to 8)
This field contains the binary encoding of the AMF Set ID. Bit 8 of octet 9 is the most significant bit and bit 7 of octet 10 is the least significant bit.

AMF Pointer (octet 10 bits 1 to 6)
This field contains the binary encoding of the AMF Pointer. Bit 6 of octet 9 is the most significant bit and bit 1 of octet 9 is the least significant bit.

5G-TMSI (octet 11 to 14)
Bit 8 of octet 11 is the most significant bit and bit 1 of octet 14 is the least significant bit.

Identity digit (octet 4 bits 5 to 8, octet 5 etc.)

For the IMEI, Identity digit field is coded using BCD coding. If the number of identity digits is even then bits 5 to 8 of the last octet shall be filled with an end mark coded as "1111". The format of the IMEI is described in 3GPP TS 23.003 [4].

For the IMEISV, Identity digit field is coded using BCD coding. Bits 5 to 8 of the last octet shall be filled with an end mark coded as "1111". The format of the IMEISV is described in 3GPP TS 23.003 [4].

For the SUCI, bit 8 of octet 4 is spare and shall be coded as zero. Bits 5-7 of octet 4 contain the SUPI format and are coded as shown below.

SUPI format (octet 4, bits 5-7)
Bits

7	6	5	
0	0	0	IMSI
0	0	1	Network specific identifier
0	1	0	GCI
0	1	1	GLI

All other values are interpreted as IMSI by this version of the protocol.

For the SUCI with SUPI format "IMSI", octets 5 through 7 contain the MCC and MNC values as specified below. For subsequent fields, bit 8 of octet 8 is the most significant bit and bit 1 of the last octet the least significant bit. The required fields for the SUCI are as defined in 3GPP TS 23.003 [4].

MCC, Mobile country code (octet 5, octet 6 bits 1 to 4)

The MCC field is coded as in ITU-T Recommendation E.212 [42], annex A.

MNC, Mobile network code (octet 6 bits 5 to 8, octet 7)

The coding of this field is the responsibility of each administration but BCD coding shall be used. The MNC shall consist of 2 or 3 digits. If a network operator decides to use only two digits in the MNC, bits 5 to 8 of octet 6 shall be coded as "1111".

The MCC and MNC digits are coded as octets 6 to 8 of the Temporary mobile group identity IE in figure 10.5.154 of 3GPP TS 24.008 [12].

Routing indicator (octets 8-9)

Routing Indicator shall consist of 1 to 4 digits. The coding of this field is the responsibility of home network operator but BCD coding shall be used. If a network operator decides to assign less than 4 digits to Routing Indicator, the remaining digits shall be coded as "1111" to fill the 4 digits coding of Routing Indicator (see NOTE 2). If no Routing Indicator is configured in the USIM or the ME, the UE shall code bits 1 to 4 of octet 8 of the Routing Indicator as "0000" and the remaining digits as "1111".

Protection scheme identifier (octet 10 bits 1 to 4)
Bits

4	3	2	1	
0	0	0	0	Null scheme
0	0	0	1	ECIES scheme profile A
0	0	1	0	ECIES scheme profile B
0	0	1	1	
	to			Reserved
1	0	1	1	
1	1	0	0	
	to			Operator-specific protection scheme
1	1	1	1	

Bits 5-8 of octet 10 are spare and shall be coded as zero.

Home network public key identifier (octet 11)

The Home network public key identifier (PKI) field is coded as defined in 3GPP TS 23.003 [4]. Home network public key identifier shall be coded as "00000000" when Protection scheme identifier is set to "0000" (i.e. Null scheme).
Bits

8	7	6	5	4	3	2	1	
0	0	0	0	0	0	0	0	Home network PKI value 0
0	0	0	0	0	0	0	1	
			to					Home network PKI value (1-254)
1	1	1	1	1	1	1	0	
1	1	1	1	1	1	1	1	Reserved

Scheme output (octets 12 to x)

The Scheme output field consists of a string of characters with a variable length or hexadecimal digits as specified in 3GPP TS 23.003 [4]. If Protection scheme identifier is set to "0000" (i.e. Null scheme), then the Scheme output consists of the MSIN and is coded using BCD coding with each digit of the MSIN coded over 4 bits. If the MSIN includes an odd number of digits, bits 5 to 8 of octet x shall be coded as "1111". If Protection scheme identifier is not "0000" (i.e. ECIES scheme profile A, ECIES scheme profile B or Operator-specific protection scheme), then Scheme output is coded as hexadecimal digits.

For the SUCI with SUPI format set to "Network specific identifier", the SUCI NAI field contains an NAI constructed as specified in subclause 28.7.3 of 3GPP TS 23.003 [4] and encoded as UTF-8 string.

For the SUCI with SUPI format set to "GCI", the SUCI NAI field contains an NAI constructed as specified in subclause 28.15.5 of 3GPP TS 23.003 [4] and encoded as UTF-8 string.

For the SUCI with SUPI format set to "GLI", the SUCI NAI field contains an NAI constructed as specified in subclause 28.16.5 of 3GPP TS 23.003 [4] and encoded as UTF-8 string.

For the 5G-S-TMSI, bits 5 to 8 of octet 4 are coded as "1111". The coding of the 5G-S-TMSI is left open for each administration.

AMF Set ID (octet 5, octet 6 bits 7 to 8)
This field contains the binary encoding of the AMF Set ID. Bit 8 of octet 5 is the most significant bit and bit 7 of octet 6 is the least significant bit.

AMF Pointer (octet 6 bits 1 to 6)
This field contains the binary encoding of the AMF Pointer. Bit 6 of octet 6 is the most significant bit and bit 1 of octet 6 is the least significant bit.

5G-TMSI (octet 7 to 10)
Bit 8 of octet 7 is the most significant bit and bit 1 of octet 10 is the least significant bit.

For Type of identity "No identity", the length of mobile identity contents parameter shall be set to 1 and the bits 4-8 of octet 4 are spare and shall be coded as zero.

MAC address usage restriction indication (MAURI) (octet 4 bit 4)

Bit **4**	
0	No restrictions
1	MAC address is not usable as an equipment identifier

MAC address (octets 5 to 10)
This field contains the MAC address as defined in subclause 8 of IEEE Std 802 [43].
Bit 8 of octet 5 is the most significant bit and bit 1 of octet 10 is the least significant bit.

EUI-64 (octets 5 to 12)
This field contains an EUI-64 as defined in [48].
Bit 8 of octet 5 is the most significant bit and bit 1 of octet 12 is the least significant bit.

NOTE 1: This can be used when the requested identity is not available at the UE during the identification procedure.
NOTE 2: For a 3-digit Routing Indicator, e.g "567", bits 1 to 4 of octet 8 are coded as "0101", bits 5 to 8 of octet 8 are coded as "0110", bits 1 to 4 of octet 9 are coded as "0111", bits 5 to 8 of octet 9 are coded as "1111".

9.11.3.5 5GS network feature support

The purpose of the 5GS network feature support information element is to indicate whether certain features are supported by the network.

The 5GS network feature support information element is coded as shown in figure 9.11.3.5.1 and table 9.11.3.5.1.

The 5GS network feature support is a type 4 information element with a minimum length of 3 octets and a maximum length of 6 octets.

If:

- the length of 5GS network feature support contents field is set to one, then the UE shall interpret this as a receipt of an information element with all bits of octet 4, octet 5 and octet 6 coded as zero.
- the length of 5GS network feature support contents field is set to two, the UE shall interpret this as a receipt of an information element with all bits of octet 5 and octet 6 coded as zero.
- the length of 5GS network feature support contents field is set to three, the UE shall interpret this as a receipt of an information element with all bits of octet 6 coded as zero.

8	7	6	5	4	3	2	1	
5GS network feature support IEI								octet 1
Length of 5GS network feature support contents								octet 2
MPSI	IWK N26	EMF		EMC		IMS-VoPS-N3GPP	IMS-VoPS-3GPP	octet 3
5G-UP CIoT	5G-IPHC-CP CIoT	N3 data	5G-CP CIoT	RestrictEC		MCSI	EMCN3	octet 4*
UN-PER	PR	RPR	PIV	NCR	5G-EHC-CP CIoT	ATS-IND	5G-LCS	octet 5*
0 spare	0 spare	0 spare	0 spare	RSLP	SUPL	LCS-UPP	NAPS	octet 6*

Figure 9.11.3.5.1: 5GS network feature support information element

Table 9.11.3.5.1: 5GS network feature support information element

IMS voice over PS session over 3GPP access indicator (IMS-VoPS-3GPP) (octet 3, bit 1)
This bit indicates the support of IMS voice over PS session over 3GPP access (see NOTE 1).
Bit
1
0 IMS voice over PS session not supported over 3GPP access
1 IMS voice over PS session supported over 3GPP access

IMS voice over PS session over non-3GPP access indicator (IMS-VoPS-N3GPP) (octet 3, bit 2)
This bit indicates the support of IMS voice over PS session over non-3GPP access.
Bit
2
0 IMS voice over PS session not supported over non-3GPP access
1 IMS voice over PS session supported over non-3GPP access

Emergency service support indicator for 3GPP access (EMC) (octet 3, bit 3 and bit 4)
These bits indicate the support of emergency services in 5GS for 3GPP access (see NOTE 1).
Bits
4 3
0 0 Emergency services not supported
0 1 Emergency services supported in NR connected to 5GCN only
1 0 Emergency services supported in E-UTRA connected to 5GCN only
1 1 Emergency services supported in NR connected to 5GCN and E-UTRA connected to 5GCN

Emergency services fallback indicator for 3GPP access (EMF) (octet 3, bit 5 and bit 6)
These bits indicate the support of emergency services fallback for 3GPP access (see NOTE 1).
Bits
6 5
0 0 Emergency services fallback not supported
0 1 Emergency services fallback supported in NR connected to 5GCN only
1 0 Emergency services fallback supported in E-UTRA connected to 5GCN only
1 1 Emergency services fallback supported in NR connected to 5GCN and E-UTRA connected to 5GCN

Interworking without N26 interface indicator (IWK N26) (octet 3, bit 7)
This bit indicates whether interworking without N26 interface is supported.
Bit
7
0 Interworking without N26 interface not supported
1 Interworking without N26 interface supported

MPS indicator (MPSI) (octet 3, bit 8)
This bit indicates the validity of MPS.
Bit
8
0 Access identity 1 not valid
1 Access identity 1 valid

Emergency service support for non-3GPP access indicator (EMCN3) (octet 4, bit 1)
This bit indicates the support of emergency services in 5GS for non-3GPP access.
Bit (see NOTE 2)
1
0 Emergency services not supported over non-3GPP access
1 Emergency services supported over non-3GPP access

MCS indicator (MCSI) (octet 4, bit 2)
This bit indicates the validity of MCS.
Bit
2
0 Access identity 2 not valid
1 Access identity 2 valid

Restriction on enhanced coverage (RestrictEC) (octet 4, bit 3 and bit 4)
These bits indicate enhanced coverage restricted information.
In WB-N1 mode these bits are set as follows:
Bits

4	**3**	
0	0	Both CE mode A and CE mode B are not restricted
0	1	Both CE mode A and CE mode B are restricted
1	0	CE mode B is restricted
1	1	Reserved

In NB-N1 mode these bits are set as follows
Bits

4	**3**	
0	0	Use of enhanced coverage is not restricted
0	1	Use of enhanced coverage is restricted
1	0	Reserved
1	1	Reserved

Control plane CIoT 5GS optimization (5G-CP CIoT) (octet 4, bit 5)
This bit indicates the capability for control plane CIoT 5GS optimization.
Bit

5	
0	Control plane CIoT 5GS optimization not supported
1	Control plane CIoT 5GS optimization supported

N3 data transfer (N3 data) (octet 4, bit 6)
This bit indicates the capability for N3 data transfer.
Bit

6	
0	N3 data transfer supported
1	N3 data transfer not supported

IP header compression for control plane CIoT 5GS optimization (5G-IPHC-CP CIoT) (octet 4, bit 7)
This bit indicates the capability for IP header compression for control plane CIoT 5GS optimization.
Bit

7	
0	IP header compression for control plane CIoT 5GS optimization not supported
1	IP header compression for control plane CIoT 5GS optimization supported

User plane CIoT 5GS optimization (5G-UP CIoT) (octet 4, bit 8)
This bit indicates the capability for user plane CIoT 5GS optimization.
Bit

8	
0	User plane CIoT 5GS optimization not supported
1	User plane CIoT 5GS optimization supported

Location Services indicator in 5GC (5G-LCS) (octet 5, bit 1)
Bit

1	
0	Location services via 5GC not supported
1	Location services via 5GC supported

ATSSS support indicator (ATS-IND) (octet 5, bit 2)
This bit indicates the network support for ATSSS.
Bit

2	
0	ATSSS not supported
1	ATSSS supported

Ethernet header compression for control plane CIoT 5GS optimization (5G-EHC-CP CIoT) (octet 5, bit 3)
This bit indicates the capability for Ethernet header compression for control plane CIoT 5GS optimization
Bit

3

0	Ethernet header compression for control plane CIoT 5GS optimization not supported
1	Ethernet header compression for control plane CIoT 5GS optimization supported

N1 NAS signalling connection release (NCR) (octet 5, bit 4)
This bit indicates whether N1 NAS signalling connection release is supported.

Bit **4**	
0	N1-NAS signalling connection release not supported
1	N1-NAS signalling connection release supported

Paging indication for voice services (PIV) (octet 5, bit 5)
This bit indicates whether paging indication for voice services is supported.

Bit **5**	
0	paging indication for voice services not supported
1	paging indication for voice services supported

Reject paging request (RPR) (octet 5, bit 6)
This bit indicates whether reject paging request is supported.

Bit **6**	
0	reject paging request not supported
1	reject paging request supported

Paging restriction (PR) (octet 5, bit 7)
This bit indicates whether paging restriction is supported.

Bit **7**	
0	paging restriction not supported
1	paging restriction supported

UN-PER (octet 5, bit 8)
This bit indicates the capability to support Unavailability period

Bit 8	
0	unavailability period not supported
1	unavailability period supported

Non-3GPP access path switching (NAPS) (octet 6, bit 1)
This bit indicates whether non-3GPP access path switching is supported.

Bit **1**	
0	non-3GPP access path switching not supported
1	non-3GPP access path switching supported

LCS-UPP user plane positioning (LCS-UPP) (octet 6, bit 2)
This bit indicates the capability to support LCS-UPP user plane positioning (see 3GPP TS 23.273 [6B]).

Bit **2**	
0	User plane positioning using LCS-UPP not supported
1	User plane positioning using LCS-UPP supported

SUPL user plane positioning (SUPL) (octet 6, bit 3)
This bit indicates the capability to support SUPL user plane positioning (see 3GPP TS 38.305 [67] and 3GPP TS 23.271 [68]).

Bit **3**	
0	User plane positioning using SUPL not supported
1	User plane positioning using SUPL supported

Ranging and sidelink positioning support (RSLP) (octet 6, bit 4)

This bit indicates the capability to support ranging and sidelink positioning.
Bit
4
0 Ranging and sidelink positioning not supported
1 Ranging and sidelink positioning supported

Bits 5 to 8 of octet 6 are spare and shall be coded as zero.

NOTE 1: For a registration procedure over non-3GPP access, bit 1 of octet 3 and bits 3 to 7 of octet 3 are ignored.
NOTE 2: For a registration procedure over 3GPP access, bit 2 of octet 3 and bit 1 of octet 4 are ignored.

9.11.3.6 5GS registration result

The purpose of the 5GS registration result information element is to specify the result of a registration procedure.

The 5GS registration result information element is coded as shown in figure 9.11.3.6.1 and table 9.11.3.6.1.

The 5GS registration result is a type 4 information element with a length of 3 octets.

8	7	6	5	4	3	2	1	
5GS registration result IEI								octet 1
Length of 5GS registration result contents								octet 2
0 Spare	Disaster roaming registration result value	Emergency registered	NSSAA Performed	SMS allowed	5GS registration result value			octet 3

Figure 9.11.3.6.1: 5GS registration result information element

Table 9.11.3.6.1: 5GS registration result information element

5GS registration result value (octet 3, bits 1 to 3) (NOTE)

Bits 3	2	1	
0	0	1	3GPP access
0	1	0	Non-3GPP access
0	1	1	3GPP access and non-3GPP access
1	1	1	reserved

All other values are unused and shall be treated as "3GPP access", if received by the UE.

SMS over NAS transport allowed (SMS allowed) (octet 3, bit 4) (NOTE)

Bit 4	
0	SMS over NAS not allowed
1	SMS over NAS allowed

Network slice-specific authentication and authorization is to be performed (NSSAA to be performed) (octet 3, bit 5) (NOTE)

Bit 5	
0	Network slice-specific authentication and authorization is not to be performed
1	Network slice-specific authentication and authorization is to be performed

Emergency registered (octet 3, bit 6)

Bit 6	
0	Not registered for emergency services
1	Registered for emergency services

Disaster roaming registration result value (octet 3, bit 7) (NOTE)

Bit 7	
0	No additional information
1	Request for registration for disaster roaming service accepted as registration not for disaster roaming service

Bit 8 of octet 3 is spare and shall be coded as zero.

NOTE: All bits other than bit 6 in octet 3 shall be ignored by the UE when the 5GS registration result IE is received in the CONFIGURATION UPDATE COMMAND message

9.11.3.7 5GS registration type

The purpose of the 5GS registration type information element is to indicate the type of the requested registration.

The 5GS registration type information element is coded as shown in figure 9.11.3.7.1 and table 9.11.3.7.1.

The 5GS registration type is a type 1 information element with a length of 1 octet.

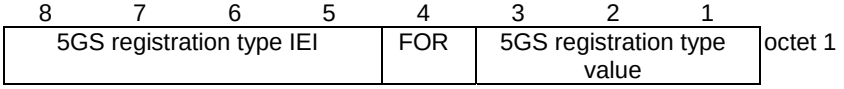


Figure 9.11.3.7.1: 5GS registration type information element

Table 9.11.3.7.1: 5GS registration type information element

5GS registration type value (octet 1, bits 1 to 3)			
Bits			
3	**2**	**1**	
0	0	1	initial registration
0	1	0	mobility registration updating
0	1	1	periodic registration updating
1	0	0	emergency registration
1	0	1	SNPN onboarding registration
1	1	0	disaster roaming mobility registration updating
1	1	1	disaster roaming initial registration
All other values are unused and shall be interpreted as "initial registration", if received by the network.			
Follow-on request bit (FOR) (octet 1, bit 4)			
Bit			
4			
0			No follow-on request pending
1			Follow-on request pending

9.11.3.8 5GS tracking area identity

The purpose of the 5GS tracking area identity information element is to provide an unambiguous identification of tracking areas within the area covered by the 5GS.

The 5GS tracking area identity information element is coded as shown in figure 9.11.3.8.1 and table 9.11.3.8.1.

The 5GS tracking area identity is a type 3 information element with a length of 7 octets.

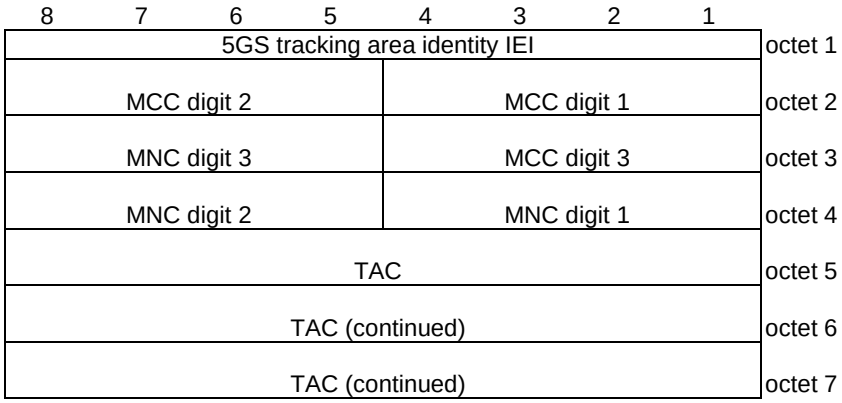


Figure 9.11.3.8.1: 5GS tracking area identity information element

Table 9.11.3.8.1: 5GS tracking area identity information element

MCC, Mobile country code (octets 2 and 3)
The MCC field is coded as in ITU-T Recommendation E212 [42], annex A.

If the TAI is deleted the MCC and MNC shall take the value from the deleted TAI.

In abnormal cases, the MCC stored in the UE can contain elements not in the set {0, 1 ... 9}. In such cases the UE should transmit the stored values using full hexadecimal encoding. When receiving such an MCC, the network shall treat the TAI as deleted.

MNC, Mobile network code (octet 3 bits 5 to 8, octet 4)
The coding of this field is the responsibility of each administration, but BCD coding shall be used. The MNC shall consist of 2 or 3 digits. For PCS 1900 for NA, Federal regulation mandates that a 3-digit MNC shall be used. However, a network operator may decide to use only two digits in the MNC in the TAI over the radio interface. In this case, bits 5 to 8 of octet 3 shall be coded as "1111". Mobile equipment shall accept a TAI coded in such a way.

In abnormal cases, the MNC stored in the UE can have:
- digit 1 or 2 not in the set {0, 1 ... 9}, or
- digit 3 not in the set {0, 1 ... 9, F} hex.

In such cases the UE shall transmit the stored values using full hexadecimal encoding. When receiving such an MNC, the network shall treat the TAI as deleted.

The same handling shall apply for the network, if a 3-digit MNC is sent by the UE to a network using only a 2-digit MNC.

TAC, Tracking area code (octets 5 to 7)
In the TAC field bit 8 of octet 5 is the most significant bit and bit 1 of octet 7 the least significant bit.
The coding of the tracking area code is the responsibility of each administration except that two values are used to mark the TAC, and hence the TAI, as deleted. Coding using full hexadecimal representation may be used. The tracking area code consists of 3 octets.
If a TAI has to be deleted, then all bits of the tracking area code shall be set to one with the exception of the least significant bit which shall be set to zero. If a USIM is inserted in a mobile equipment with the tracking area code containing all zeros, then the mobile equipment shall recognise this TAC as part of a deleted TAI.

9.11.3.9 5GS tracking area identity list

The purpose of the 5GS tracking area identity list information element is to transfer a list of tracking areas from the network to the UE.

The coding of the information element allows combining different types of lists. The lists of type "00" and "01" allow a more compact encoding, when the different TAIs are sharing the PLMN identity.

The 5GS tracking area identity list information element is coded as shown in figure 9.11.3.8.1, figure 9.11.3.8.2, figure 9.11.3.9.3, figure 9.11.3.9.4 and table 9.11.3.9.1.

The 5GS tracking area identity list is a type 4 information element, with a minimum length of 9 octets and a maximum length of 114 octets. The list can contain a maximum of 16 different tracking area identities.

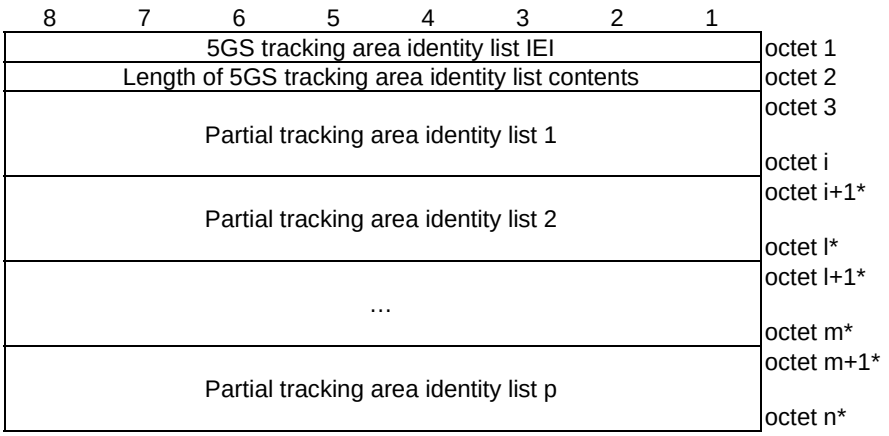


Figure 9.11.3.9.1: 5GS tracking area identity list information element

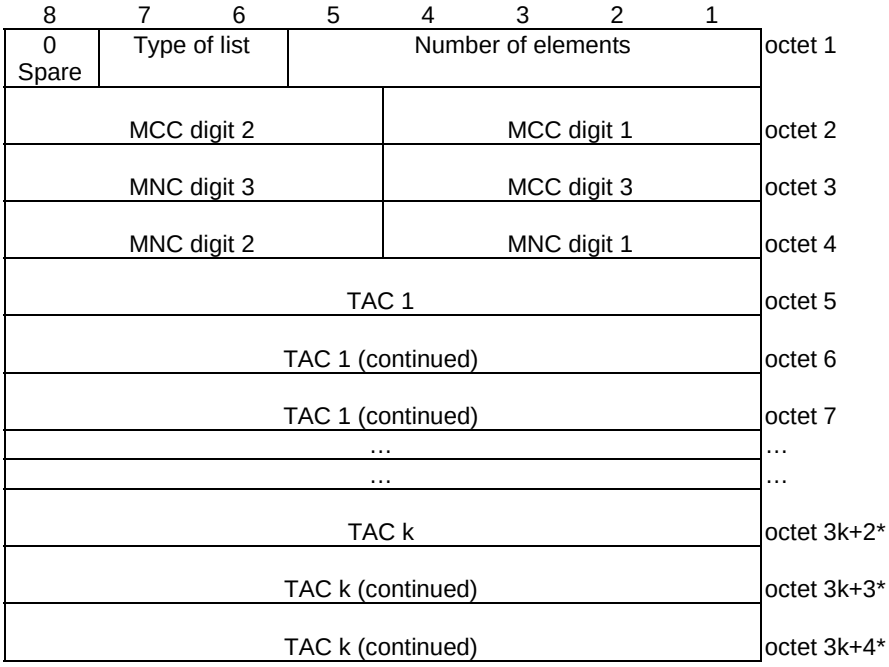


Figure 9.11.3.9.2: Partial tracking area identity list – type of list = "00"

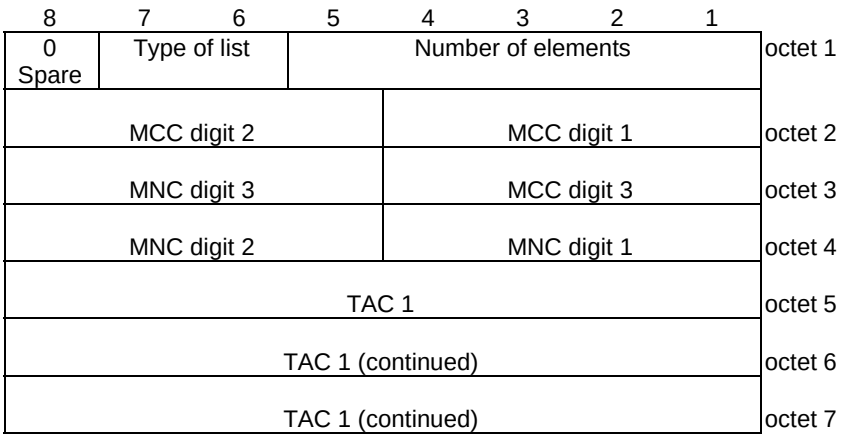


Figure 9.11.3.9.3: Partial tracking area identity list – type of list = "01"

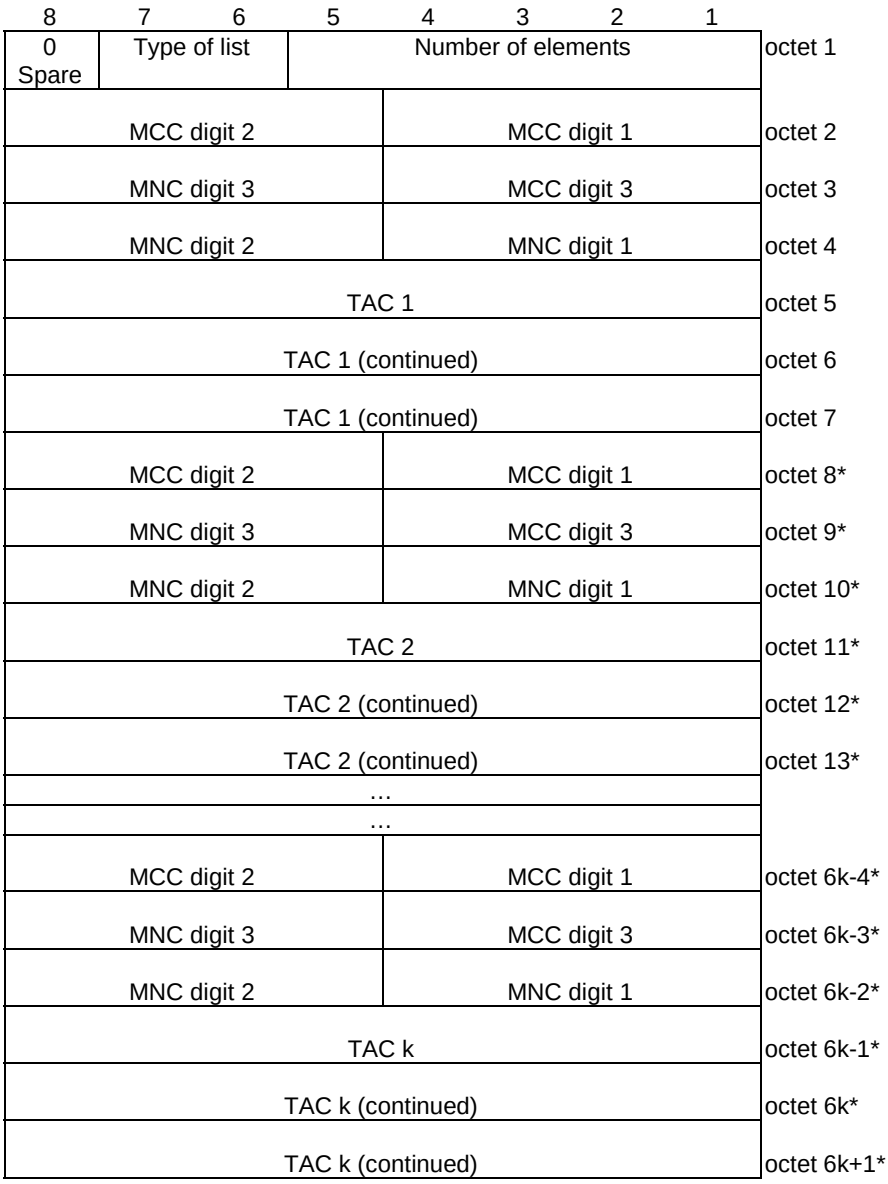


Figure 9.11.3.9.4: Partial tracking area identity list – type of list = "10"

Table 9.11.3.9.1: Tracking area identity list information element

Value part of the Tracking area identity list information element (octets 3 to n)

The value part of the Tracking area identity list information element consists of one or several partial tracking area identity lists. The length of each partial tracking area identity list can be determined from the 'type of list' field and the 'number of elements' field in the first octet of the partial tracking area identity list.
The UE shall store the complete list received. If more than 16 TAIs are included in this information element, the UE shall store the first 16 TAIs and ignore the remaining octets of the information element.

Partial tracking area identity list:

Type of list (octet 1)
Bits

7	**6**	
0	0	list of TACs belonging to one PLMN or SNPN, with non-consecutive TAC values
0	1	list of TACs belonging to one PLMN or SNPN, with consecutive TAC values
1	0	list of TAIs belonging to different PLMNs (see NOTE)

All other values are reserved.

Number of elements (octet 1)
Bits

5	**4**	**3**	**2**	**1**	
0	0	0	0	0	1 element
0	0	0	0	1	2 elements
0	0	0	1	0	3 elements
		…			
0	1	1	0	1	14 elements
0	1	1	1	0	15 elements
0	1	1	1	1	16 elements

All other values are unused and shall be interpreted as 16, if received by the UE.

Bit 8 of octet 1 is spare and shall be coded as zero.

For type of list = "00" and number of elements = k:

octet 2 to 4 contain the MCC+MNC, and
for j = 1, …, k:
octets 3j+2 to 3j+4 contain the TAC of the j-th TAI belonging to the partial list,

For type of list = "01" and number of elements = k:

octet 2 to 4 contain the MCC+MNC, and
octets 5 to 7 contain the TAC of the first TAI belonging to the partial list.
The TAC values of the other k-1 TAIs are TAC+1, TAC+2, …, TAC+k-1.

For type of list = "10" and number of elements = k:

for j = 1, …, k.
octets 6j-4 to 6j-2 contain the MCC+MNC, and
octets 6j-1 to 6j+1 contain the TAC of the j-th TAI belonging to the partial list.

MCC, Mobile country code

The MCC field is coded as in ITU-T Recommendation E.212 [42], annex A.

MNC, Mobile network code

The coding of this field is the responsibility of each administration but BCD coding shall be used. The MNC shall consist of 2 or 3 digits. If a network operator decides to use only two digits in the MNC, MNC digit 3 shall be coded as "1111".

TAC, Tracking area code

In the TAC field bit 8 of the first octet is the most significant bit and bit 1 of third octet the least significant bit. The coding of the tracking area code is the responsibility of each administration. Coding using full hexadecimal representation may be used. The tracking area code consists of 3 octets.
NOTE: If the "list of TAIs belonging to different PLMNs" is used, the PLMNs included in the list need to be present in the list of "equivalent PLMNs". This type of list is not applicable in an SNPN.

9.11.3.9A 5GS update type

The purpose of the 5GS update type IE is to allow the UE to provide additional information to the network when performing a registration procedure.

The 5GS update type information element is coded as shown in figure 9.11.3.9A.1 and table 9.11.3.9A.1.

The 5GS update type is a type 4 information element with a length of 3 octects.

8	7	6	5	4	3	2	1	
5GS update type IEI								octet 1
Length of 5GS update type								octet 2
0 Spare	0 Spare	EPS- PNB-CIoT		5GS-PNB-CIoT		NG-RAN-RCU	SMS requested	octet 3

Figure 9.11.3.9A.1: 5GS update type information element

Table 9.11.3.9A.1: 5GS update type information element

SMS over NAS transport requested (SMS requested) (octet 3, bit 1) Bit **1** 0 SMS over NAS not supported 1 SMS over NAS supported NG-RAN Radio Capability Update (NG-RAN-RCU) (octet 3, bit 2) Bit **2** 0 UE radio capability update not needed 1 UE radio capability update needed For a list of RATs for which a radio capability update can be triggered by means of this indication see subclause 5.5.1.3.2, case n). 5GS Preferred CIoT network behaviour (5GS PNB-CIoT) (octet 3, bits 3 and 4) Bits **4 3** 0 0 no additional information 0 1 control plane CIoT 5GS optimization 1 0 user plane CIoT 5GS optimization 1 1 reserved EPS Preferred CIoT network behaviour (EPS-PNB-CIoT) (octet 3, bits 5 and 6) Bits **6 5** 0 0 no additional information 0 1 control plane CIoT EPS optimization 1 0 user plane CIoT EPS optimization 1 1 reserved Bits 7 to 8 of octet 3 are spare and shall be coded as zero.

9.11.3.10 ABBA

The purpose of the ABBA information element is to enable the bidding down protection of security features.

The ABBA information element is coded as shown in figure 9.11.3.10.1 and table 9.11.3.10.1.

The ABBA is a type 4 information element with a minimum length of 4 octets and maximum length of 257 octets.

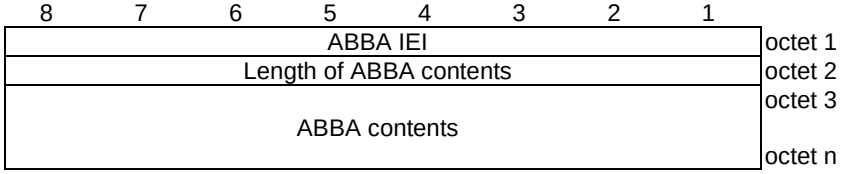


Figure 9.11.3.10.1: ABBA information element

Table 9.11.3.10.1: ABBA information element

ABBA contents (octet 3-n): indicate set of security features defined for 5GS as described in 3GPP TS 33.501 [24].
NOTE 1: If the UE receives the ABBA IE with a length that is set to a value of 2 and with a value of 0000H, the UE shall use the length and the contents of the ABBA IE as received from the network. NOTE 2: If the UE receives the ABBA IE with a length that is set to a value larger than 2 or with a value that is different from 0000H, the UE shall use the length and the contents of the ABBA IE as received from the network.

9.11.3.11 Void

9.11.3.12 Additional 5G security information

The purpose of the Additional 5G security information information element is to provide the UE with additional security parameters (e.g. horizontal derivation parameter) or to request the UE to retransmit an initial NAS message during a security mode control procedure as defined in 3GPP TS 33.501 [24]. The UE uses these parameters for completion of security mode control procedure.

The Additional 5G security information information element is coded as shown in figure 9.11.3.12.1 and table 9.11.3.12.1.

The Additional 5G security information is a type 4 information element with a length of 3 octets.

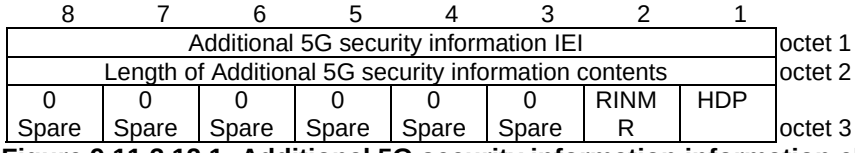


Figure 9.11.3.12.1: Additional 5G security information information element

Table 9.11.3.12.1: Additional 5G security information information element

Horizontal derivation parameter (HDP) (octet 3, bit 1) 0 K_{AMF} derivation is not required 1 K_{AMF} derivation is required Retransmission of initial NAS message request (octet 3, bit 2) 0 Retransmission of the initial NAS message not requested 1 Retransmission of the initial NAS message requested Bits 3 to 8 of octet 3 are spare and shall be coded as zero.

9.11.3.12A Additional information requested

The purpose of the Additional information requested information element is to enable the UE to request ciphering keys for deciphering of ciphered broadcast assistance data.

The Additional information requested information element is coded as shown in figure 9.11.3.12A.1 and table 9.11.3.12A.1.

The Additional information requested is a type 4 information element with a length of 3 octets.

8	7	6	5	4	3	2	1	
Additional information requested IEI								octet 1
Length of additional information requested contents								octet 2
0	0	0	0	0	0	0	Cipher Key	octet 3
Spare								

Figure 9.11.3.12A.1: Additional information requested information element

Table 9.11.3.12A.1: Additional information requested information element

Ciphering keys for ciphered broadcast assistance data (CipherKey) (octet 3, bit 1)	
Bit	
1	
0	ciphering keys for ciphered broadcast assistance data not requested
1	ciphering keys for ciphered broadcast assistance data requested
Bits 8 to 2 of octet 3 are spare and shall be coded as zero.	

9.11.3.13 Allowed PDU session status

The purpose of the Allowed PDU session status information element is to indicate to the network user-plane resources of PDU sessions associated with non-3GPP access that are allowed to be re-established over 3GPP access or if there is no PDU session(s) for which the UE allows the user-plane resources to be re-established over 3GPP access.

NOTE: Allowed PDU session status IE is not applicable for MA PDU session(s) in this release of specification.

The Allowed PDU session status information element is coded as shown in figure 9.11.3.13.1 and table 9.11.3.13.1.

The Allowed PDU session status is a type 4 information element with minimum length of 4 octets and maximum length of 34 octets.

8	7	6	5	4	3	2	1	
Allowed PDU session status IEI								octet 1
Length of Allowed PDU session status contents								octet 2
PSI (7)	PSI (6)	PSI (5)	PSI (4)	PSI (3)	PSI (2)	PSI (1)	PSI (0)	octet 3
PSI (15)	PSI (14)	PSI (13)	PSI (12)	PSI (11)	PSI (10)	PSI (9)	PSI (8)	octet 4
0	0	0	0	0	0	0	0	
Spare								octet 5* -34*

Figure 9.11.3.13.1: Allowed PDU session status information element

Table 9.11.3.13.1: Allowed PDU session status information element

PSI(x) shall be coded as follows: PSI(0): Bit 1 octet 3 is spare and shall be coded as zero. PSI(1) – PSI(15): 0 indicates that the user-plane resources of corresponding PDU session is not allowed to be re-established over 3GPP access. 1 indicates that the user-plane resources of corresponding PDU session can be re-established over 3GPP access. If there is no PDU session for which the user-plane resources can be re-established over 3GPP access, all bits in PSI(1) – PSI(15) shall be coded as zero. All bits in octet 5 to 34 are spare and shall be coded as zero, if the respective octet is included in the information element.

9.11.3.14 Authentication failure parameter

See subclause 10.5.3.2.2 in 3GPP TS 24.008 [12].

9.11.3.15 Authentication parameter AUTN

See subclause 10.5.3.1.1 in 3GPP TS 24.008 [12].

9.11.3.16 Authentication parameter RAND

See subclause 10.5.3.1 in 3GPP TS 24.008 [12].

9.11.3.17 Authentication response parameter

See subclause 9.9.3.4 in 3GPP TS 24.301 [15].

9.11.3.18 Configuration update indication

The purpose of the Configuration update indication information element is to indicate the additional information associated with the generic UE configuration update procedure.

The Configuration update indication information element is coded as shown in figure 9.11.3.18.1 and table 9.11.3.18.1.

The Configuration update indication is a type 1 information element.

8	7	6	5	4	3	2	1	
Configuration update indication IEI				0 Spare	0 Spare	RED	ACK	octet 1

Figure 9.11.3.18.1: Configuration update indication

Table 9.11.3.18.1: Configuration update indication

Acknowledgement (ACK) (octet 1, bit 1) Bit **1** 0 acknowledgement not requested 1 acknowledgement requested Registration requested (RED) (octet 1, bit 2) Bit **2** 0 registration not requested 1 registration requested Bits 3 and 4 are spare and shall be coded as zero,

9.11.3.18A CAG information list

The purpose of the CAG information list information element is to provide "CAG information list" or to delete the "CAG information list" at the UE.

The CAG information list information element is coded as shown in figures 9.11.3.18A.1 and 9.11.3.18A.2 and table 9.11.3.18A.1.

The CAG information list is a type 6 information element, with a minimum length of 3 octets.

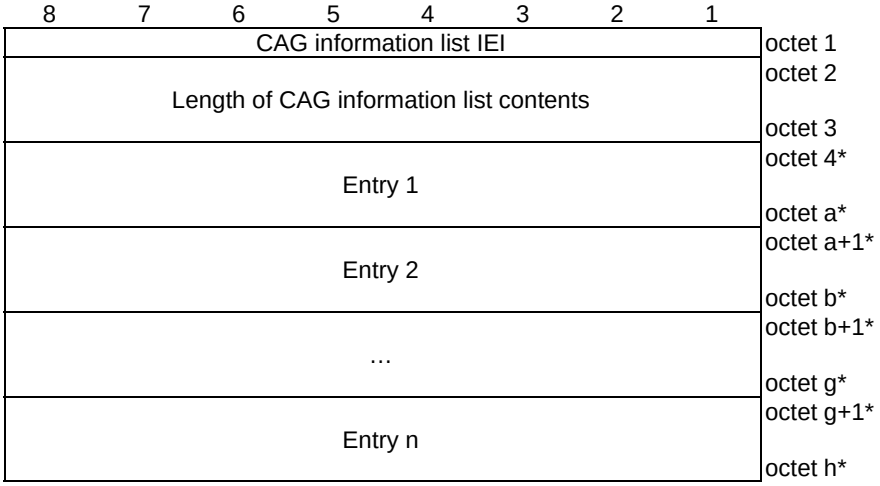


Figure 9.11.3.18A.1: CAG information list information element

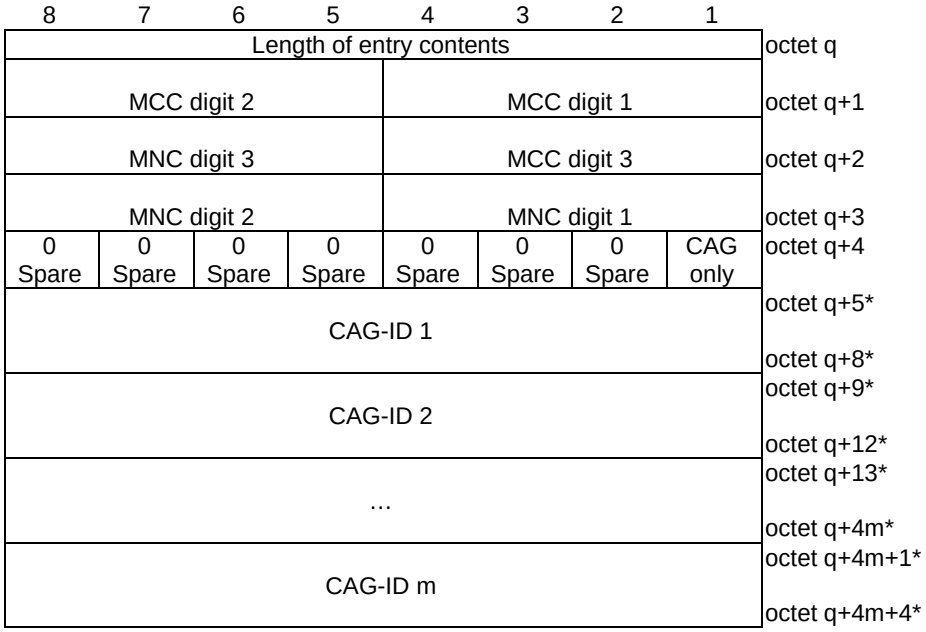


Figure 9.11.3.18A.2: Entry n

Table 9.11.3.18A.1: CAG information list information element

MCC, Mobile country code (octet q+1 and bits 1 to 4 octet q+2)
The MCC field is coded as in ITU-T Recommendation E.212 [42], annex A.

MNC, Mobile network code (bits 5 to 8 of octet q+2 and octet q+3)
The coding of this field is the responsibility of each administration, but BCD coding shall be used. The MNC shall consist of 2 or 3 digits. If a network operator decides to use only two digits in the MNC, bits 5 to 8 of octet q+2 shall be coded as "1111".

The MCC and MNC digits are coded as octets 6 to 8 of the Temporary mobile group identity IE in figure 10.5.154 of 3GPP TS 24.008 [12].

Indication that the UE is only allowed to access 5GS via CAG cells (CAGonly) (bit 1 of octet q+4)
Bit
1
0 "Indication that the UE is only allowed to access 5GS via CAG cells" is not set (i.e., the UE is allowed to access 5GS via non-CAG cells)
1 "Indication that the UE is only allowed to access 5GS via CAG cells" is set (i.e., the UE is not allowed to access 5GS via non-CAG cells)

CAG-ID m (octet q+4m+1 to octet q+4m+4)
This field contains the 32 bit CAG-ID. The coding of the CAG-ID is defined as the CAG-Identifier in 3GPP TS 23.003 [4].

NOTE 1: The Length of CAG information list contents shall be 0 if no subscription data for CAG information list exists.
NOTE 2: The Length of entry contents shall be 4 if there is no allowed CAG-ID for the PLMN.
NOTE 3: Bit 2 in octet q+4 may be set to 1 in the USIM (see 3GPP TS 31.102 [22]).
NOTE 4: For a given PLMN ID, there shall be up to one Entry containing the MCC value and the MNC value of the PLMN ID.

9.11.3.18B CIoT small data container

This information element is used to encapsulate the CIoT user data, SMS, or location services message with a size that is not more than 254 octets between the UE and the AMF when the UE is using control plane CIoT 5GS optimization. The CIoT small data container information element is coded as shown in figure 9.11.3.18B.1, figure 9.11.3.18B.2, figure 9.11.3.18B.3, figure 9.11.3.18B.4 and table 9.11.3.18B.1.

The CIoT small data container is a type 4 information element with a minimum length of 4 octets and a maximum length of 257 octets.

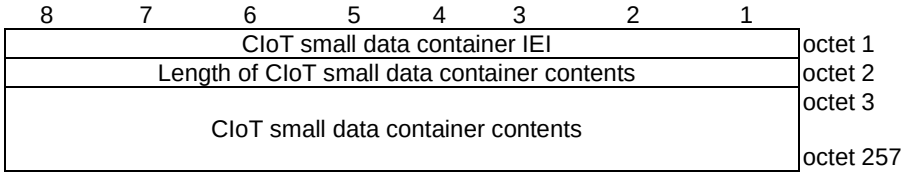


Figure 9.11.3.18B.1: CIoT small data container information element

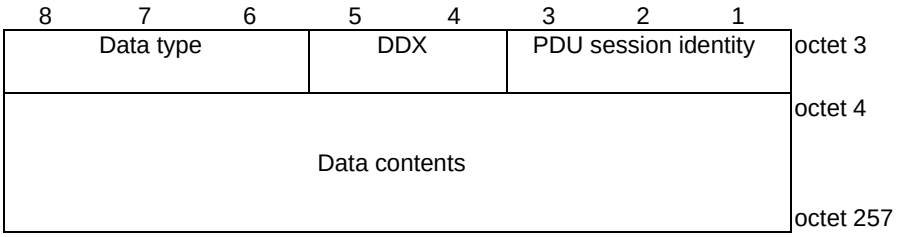


Figure 9.11.3.18B.2: CIoT small data container contents for Data type "Control plane user data"

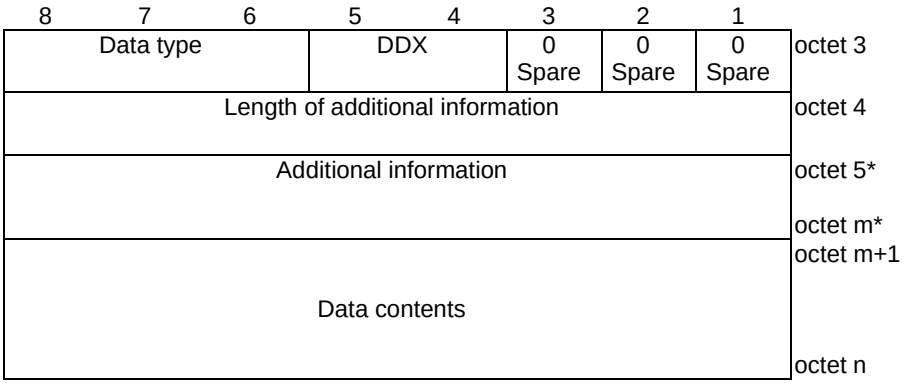


Figure 9.11.3.18B.3: CIoT small data container contents for Data type "Location services message container"

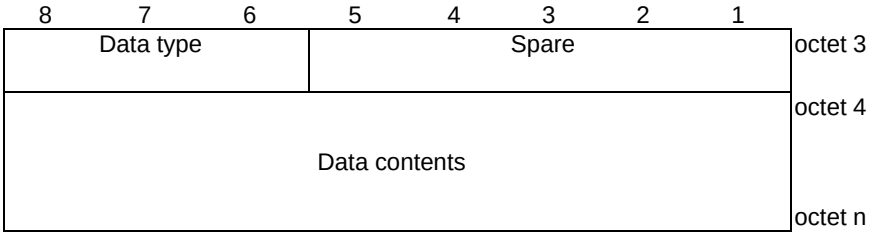


Figure 9.11.3.18B.4: CIoT small data container contents for Data type "SMS"

Table 9.11.3.18B.1: CIoT small data container information element

CIoT small data container contents (octet 3 to octet 257)

These octets include user data to be delivered between UE and AMF.

Data type (octet 3, bits 6 to 8)
Bits

8	7	6	
0	0	0	Control plane user data
0	0	1	SMS
0	1	0	Location services message container

All other values are spare. If received they shall be ignored.

When the Data type is "Control plane user data ", the PDU session identity and Downlink data expected (DDX) fields are encoded as follows:

PDU session identity (octet 3, bits 1 to 4)
Bit

3	2	1	
0	0	0	No PDU session identity assigned
0	0	1	PDU session identity value 1
0	1	0	PDU session identity value 2
0	1	1	PDU session identity value 3
1	0	0	PDU session identity value 4
1	0	1	PDU session identity value 5
1	1	0	PDU session identity value 6
1	1	1	PDU session identity value 7

Downlink data expected (DDX) (octet 3, bits 5 to 6)
Bits

5	4	
0	0	No information available
0	1	No further uplink and no further downlink data transmission subsequent to the uplink data transmission is expected
1	0	Only a single downlink data transmission and no further uplink data transmission subsequent to the uplink data transmission is expected
1	1	reserved

NOTE: The DDX field is only used in the UE to network direction.

Data contents (octet 4 to octet 257)
This field contains the control plane user data.

When the Data type is "SMS", Bits 1 to 5 of octet 3 are spare and shall be coded as zero.
Data contents (octet 4 to octet 257)
This field contains an SMS message.

When the Data type is "Location services message container":

Downlink data expected (DDX) (octet 3, bits 5 to 4)
This field is encoded as described above for the case when the Data type is "Control plane user data".

Bits 3 to 1 of octet 3 are spare and shall be encoded as zero.

Length of Additional information (octet 4) (see NOTE)
Indicates the length, in octets, of the Additional information field.

Additional information (octets 5 to m)
Contains additional information if provided by the upper layer location services application.

Data contents (octets m+1 to n)
Contains the location services message payload.

NOTE: The Length of Additional information shall be set to zero if the upper layer location service application does not provide routing information.

9.11.3.18C Ciphering key data

The purpose of the Ciphering key data information element is to transfer a list of ciphering data sets from the network to the UE for deciphering of ciphered assistance data.

The Ciphering key data information element is coded as shown in figure 9.11.3.18C.1, figure 9.11.3.18C.2 and table 9.11.3.18C.1.

The Ciphering key data is a type 6 information element, with a minimum length of 34 octets and a maximum length of 2675 octets. The list can contain a maximum of 16 ciphering data sets.

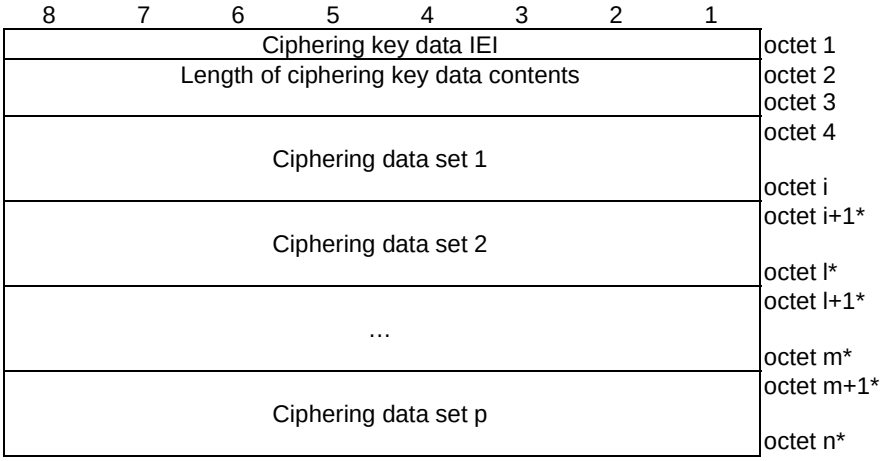


Figure 9.11.3.18C.1: Ciphering key data information element

Figure 9.11.3.18C.2: Ciphering data set

Table 9.11.3.18C.1: Ciphering key data information element

Value part of the Ciphering key data information element (octets 4 to n)

The value part of the Ciphering key data information element consists of one or several ciphering data sets.
The UE shall store the complete list received. If more than 16 ciphering data sets are included in this information element, the UE shall store the first 16 ciphering data sets and ignore the remaining octets of the information element.

Ciphering data set:

Ciphering set ID (octets 1 to 2)

This field contains the binary encoding of the ID identifying the ciphering set.

Ciphering key (octets 3 to octet 18)

This field contains the 128 bit ciphering key.

c0 length (octet 19, bits 5 to 1)

This field contains the binary encoding of the length, in octets, of the c0 counter. The maximum value for the length of the c0 counter is 16 octets.

Bits 8 to 6 of octect 19 are spare and shall be coded as zero.

c0 (octets 20 to k)

This field contains the binary encoding of the c0 counter.

E-UTRA posSIB length (octet k+1, bits 4 to 1)

This field contains the length in octets of the E -UTRA Positioning SIB types. A length of zero means E -UTRA Positioning SIB types are not included (see NOTE).

E-UTRA Positioning SIB types for which the ciphering data set is applicable (octets k+2 to p). Unassigned bits shall be ignored by a UE. Non-included bits shall be assumed to be zero by a UE.

Ciphering data set applicable for positioning SIB type 1-1 (octet k+2, bit 8)
0 Ciphering data set not applicable to positioning SIB type 1-1
1 Ciphering data set applicable to positioning SIB type 1-1

Ciphering data set applicable for positioning SIB type 1-2 (octet k+2, bit 7)
0 Ciphering data set not applicable to positioning SIB type 1-2
1 Ciphering data set applicable to positioning SIB type 1-2

Ciphering data set applicable for positioning SIB type 1-3 (octet k+2, bit 6)
0 Ciphering data set not applicable to positioning SIB type 1-3
1 Ciphering data set applicable to positioning SIB type 1-3

Ciphering data set applicable for positioning SIB type 1-4 (octet k+2, bit 5)
0 Ciphering data set not applicable to positioning SIB type 1-4
1 Ciphering data set applicable to positioning SIB type 1-4

Ciphering data set applicable for positioning SIB type 1-5 (octet k+2, bit 4)
0 Ciphering data set not applicable to positioning SIB type 1-5
1 Ciphering data set applicable to positioning SIB type 1-5

Ciphering data set applicable for positioning SIB type 1-6 (octet k+2, bit 3)
0 Ciphering data set not applicable to positioning SIB type 1-6
1 Ciphering data set applicable to positioning SIB type 1-6

Ciphering data set applicable for positioning SIB type 1-7 (octet k+2, bit 2)
0 Ciphering data set not applicable to positioning SIB type 1-7
1 Ciphering data set applicable to positioning SIB type 1-7

Ciphering data set applicable for positioning SIB type 1-8 (octet k+2, bit 1)
0 Ciphering data set not applicable to positioning SIB type 1-8
1 Ciphering data set applicable to positioning SIB type 1-8

Ciphering data set applicable for positioning SIB type 2-1 (octet k+3, bit 8)
0 Ciphering data set not applicable to positioning SIB type 2-1
1 Ciphering data set applicable to positioning SIB type 2-1

Ciphering data set applicable for positioning SIB type 2-2 (octet k+3, bit 7)
0 Ciphering data set not applicable to positioning SIB type 2-2
1 Ciphering data set applicable to positioning SIB type 2-2

Ciphering data set applicable for positioning SIB type 2-3 (octet k+3, bit 6)
0 Ciphering data set not applicable to positioning SIB type 2-3
1 Ciphering data set applicable to positioning SIB type 2-3

Ciphering data set applicable for positioning SIB type 2-4 (octet k+3, bit 5)
0 Ciphering data set not applicable to positioning SIB type 2-4
1 Ciphering data set applicable to positioning SIB type 2-4

Ciphering data set applicable for positioning SIB type 2-5 (octet k+3, bit 4)
0 Ciphering data set not applicable to positioning SIB type 2-5
1 Ciphering data set applicable to positioning SIB type 2-5

Ciphering data set applicable for positioning SIB type 2-6 (octet k+3, bit 3)
0 Ciphering data set not applicable to positioning SIB type 2-6
1 Ciphering data set applicable to positioning SIB type 2-6

Ciphering data set applicable for positioning SIB type 2-7 (octet k+3, bit 2)
0 Ciphering data set not applicable to positioning SIB type 2-7
1 Ciphering data set applicable to positioning SIB type 2-7

Ciphering data set applicable for positioning SIB type 2-8 (octet k+3, bit 1)
0 Ciphering data set not applicable to positioning SIB type 2-8
1 Ciphering data set applicable to positioning SIB type 2-8

Ciphering data set applicable for positioning SIB type 2-9 (octet k+4, bit 8)
0 Ciphering data set not applicable to positioning SIB type 2-9
1 Ciphering data set applicable to positioning SIB type 2-9

Ciphering data set applicable for positioning SIB type 2-10 (octet k+4, bit 7)
0 Ciphering data set not applicable to positioning SIB type 2-10
1 Ciphering data set applicable to positioning SIB type 2-10

Ciphering data set applicable for positioning SIB type 2-11 (octet k+4, bit 6)
0 Ciphering data set not applicable to positioning SIB type 2-11
1 Ciphering data set applicable to positioning SIB type 2-11

Ciphering data set applicable for positioning SIB type 2-12 (octet k+4, bit 5)
0 Ciphering data set not applicable to positioning SIB type 2-12
1 Ciphering data set applicable to positioning SIB type 2-12

Ciphering data set applicable for positioning SIB type 2-13 (octet k+4, bit 4)
0 Ciphering data set not applicable to positioning SIB type 2-13
1 Ciphering data set applicable to positioning SIB type 2-13

Ciphering data set applicable for positioning SIB type 2-14 (octet k+4, bit 3)
0 Ciphering data set not applicable to positioning SIB type 2-14
1 Ciphering data set applicable to positioning SIB type 2-14

Ciphering data set applicable for positioning SIB type 2-15 (octet k+4, bit 2)
0 Ciphering data set not applicable to positioning SIB type 2-15
1 Ciphering data set applicable to positioning SIB type 2-15

Ciphering data set applicable for positioning SIB type 2-16 (octet k+4, bit 1)
0 Ciphering data set not applicable to positioning SIB type 2-16

1	Ciphering data set applicable to positioning SIB type 2-16
Ciphering data set applicable for positioning SIB type 2-17 (octet k+5, bit 8)	
0	Ciphering data set not applicable to positioning SIB type 2-17
1	Ciphering data set applicable to positioning SIB type 2-17
Ciphering data set applicable for positioning SIB type 2-18 (octet k+5, bit 7)	
0	Ciphering data set not applicable to positioning SIB type 2-18
1	Ciphering data set applicable to positioning SIB type 2-18
Ciphering data set applicable for positioning SIB type 2-19 (octet k+5, bit 6)	
0	Ciphering data set not applicable to positioning SIB type 2-19
1	Ciphering data set applicable to positioning SIB type 2-19
Ciphering data set applicable for positioning SIB type 2-20 (octet k+5, bit 5)	
0	Ciphering data set not applicable to positioning SIB type 2-20
1	Ciphering data set applicable to positioning SIB type 2-20
Ciphering data set applicable for positioning SIB type 2-21 (octet k+5, bit 4)	
0	Ciphering data set not applicable to positioning SIB type 2-21
1	Ciphering data set applicable to positioning SIB type 2-21
Ciphering data set applicable for positioning SIB type 2-22 (octet k+5, bit 3)	
0	Ciphering data set not applicable to positioning SIB type 2-22
1	Ciphering data set applicable to positioning SIB type 2-22
Ciphering data set applicable for positioning SIB type 2-23 (octet k+5, bit 2)	
0	Ciphering data set not applicable to positioning SIB type 2-23
1	Ciphering data set applicable to positioning SIB type 2-23
Ciphering data set applicable for positioning SIB type 2-24 (octet k+5, bit 1)	
0	Ciphering data set not applicable to positioning SIB type 2-24
1	Ciphering data set applicable to positioning SIB type 2-24
Ciphering data set applicable for positioning SIB type 2-25 (octet k+6, bit 8)	
0	Ciphering data set not applicable to positioning SIB type 2-25
1	Ciphering data set applicable to positioning SIB type 2-25
Ciphering data set applicable for positioning SIB type 3-1 (octet k+6, bit 7)	
0	Ciphering data set not applicable to positioning SIB type 3-1
1	Ciphering data set applicable to positioning SIB type 3-1
Ciphering data set applicable for positioning SIB type 4-1 (octet k+6, bit 6)	
0	Ciphering data set not applicable to positioning SIB type 4-1
1	Ciphering data set applicable to positioning SIB type 4-1
Ciphering data set applicable for positioning SIB type 5-1 (octet k+6, bit 5)	
0	Ciphering data set not applicable to positioning SIB type 5-1
1	Ciphering data set applicable to positioning SIB type 5-1
Ciphering data set applicable for positioning SIB type 1-9 (octet k+6, bit 4)	
0	Ciphering data set not applicable to positioning SIB type 1-9
1	Ciphering data set applicable to positioning SIB type 1-9
Ciphering data set applicable for positioning SIB type 1-10 (octet k+6, bit 3)>	
0	Ciphering data set not applicable to positioning SIB type 1-10
1	Ciphering data set applicable to positioning SIB type 1-10
Ciphering data set applicable for positioning SIB type 2-17a (octet k+6, bit 2)	
0	Ciphering data set not applicable to positioning SIB type 2-17a
1	Ciphering data set applicable to positioning SIB type 2-17a
Ciphering data set applicable for positioning SIB type 2-18a (octet k+6, bit 1)	
0	Ciphering data set not applicable to positioning SIB type 2-18a
1	Ciphering data set applicable to positioning SIB type 2-18a
Ciphering data set applicable for positioning SIB type 2-20a (octet k+7, bit 8)	
0	Ciphering data set not applicable to positioning SIB type 2-20a

1 Ciphering data set applicable to positioning SIB type 2-20a

Ciphering data set applicable for positioning SIB type 2-26 (octet k+7, bit 7)
0 Ciphering data set not applicable to positioning SIB type 2-26
1 Ciphering data set applicable to positioning SIB type 2-26

Ciphering data set applicable for positioning SIB type 2-27 (octet k+7, bit 6)
0 Ciphering data set not applicable to positioning SIB type 2-27
1 Ciphering data set applicable to positioning SIB type 2-27

Ciphering data set applicable for positioning SIB type 1-11 (octet k+7, bit 5)
0 Ciphering data set not applicable to positioning SIB type 1-11
1 Ciphering data set applicable to positioning SIB type 1-11

Ciphering data set applicable for positioning SIB type 1-12 (octet k+7, bit 4)
0 Ciphering data set not applicable to positioning SIB type 1-12
1 Ciphering data set applicable to positioning SIB type 1-12

Any unassigned bits shall be coded as zero.

NR posSIB length (octet p+1, bits 4 to 1)
This field contains the length in octets of the NR Positioning SIB types. A length of zero means NR Positioning SIB types are not included (see NOTE).

NR Positioning SIB types for which the ciphering data set is applicable (octets p+2 to q).
Unassigned bits shall be ignored. Non-included bits shall be assumed to be zero.

Ciphering data set applicable for positioning SIB type 1-1 (octet p+2, bit 8)
0 Ciphering data set not applicable to positioning SIB type 1-1
1 Ciphering data set applicable to positioning SIB type 1-1

Ciphering data set applicable for positioning SIB type 1-2 (octet p+2, bit 7)
0 Ciphering data set not applicable to positioning SIB type 1-2
1 Ciphering data set applicable to positioning SIB type 1-2

Ciphering data set applicable for positioning SIB type 1-3 (octet p+2, bit 6)
0 Ciphering data set not applicable to positioning SIB type 1-3
1 Ciphering data set applicable to positioning SIB type 1-3

Ciphering data set applicable for positioning SIB type 1-4 (octet p+2, bit 5)
0 Ciphering data set not applicable to positioning SIB type 1-4
1 Ciphering data set applicable to positioning SIB type 1-4

Ciphering data set applicable for positioning SIB type 1-5 (octet p+2, bit 4)
0 Ciphering data set not applicable to positioning SIB type 1-5
1 Ciphering data set applicable to positioning SIB type 1-5

Ciphering data set applicable for positioning SIB type 1-6 (octet p+2, bit 3)
0 Ciphering data set not applicable to positioning SIB type 1-6
1 Ciphering data set applicable to positioning SIB type 1-6

Ciphering data set applicable for positioning SIB type 1-7 (octet p+2, bit 2)
0 Ciphering data set not applicable to positioning SIB type 1-7
1 Ciphering data set applicable to positioning SIB type 1-7

Ciphering data set applicable for positioning SIB type 1-8 (octet p+2, bit 1)
0 Ciphering data set not applicable to positioning SIB type 1-8
1 Ciphering data set applicable to positioning SIB type 1-8

Ciphering data set applicable for positioning SIB type 2-1 (octet p+3, bit 8)
0 Ciphering data set not applicable to positioning SIB type 2-1
1 Ciphering data set applicable to positioning SIB type 2-1

Ciphering data set applicable for positioning SIB type 2-2 (octet p+3, bit 7)
0 Ciphering data set not applicable to positioning SIB type 2-2
1 Ciphering data set applicable to positioning SIB type 2-2

Ciphering data set applicable for positioning SIB type 2-3 (octet p+3, bit 6)
0 Ciphering data set not applicable to positioning SIB type 2-3
1 Ciphering data set applicable to positioning SIB type 2-3

Ciphering data set applicable for positioning SIB type 2-4 (octet p+3, bit 5)
0 Ciphering data set not applicable to positioning SIB type 2-4
1 Ciphering data set applicable to positioning SIB type 2-4

Ciphering data set applicable for positioning SIB type 2-5 (octet p+3, bit 4)
0 Ciphering data set not applicable to positioning SIB type 2-5
1 Ciphering data set applicable to positioning SIB type 2-5

Ciphering data set applicable for positioning SIB type 2-6 (octet p+3, bit 3)
0 Ciphering data set not applicable to positioning SIB type 2-6
1 Ciphering data set applicable to positioning SIB type 2-6

Ciphering data set applicable for positioning SIB type 2-7 (octet p+3, bit 2)
0 Ciphering data set not applicable to positioning SIB type 2-7
1 Ciphering data set applicable to positioning SIB type 2-7

Ciphering data set applicable for positioning SIB type 2-8 (octet p+3, bit 1)
0 Ciphering data set not applicable to positioning SIB type 2-8
1 Ciphering data set applicable to positioning SIB type 2-8

Ciphering data set applicable for positioning SIB type 2-9 (octet p+4, bit 8)
0 Ciphering data set not applicable to positioning SIB type 2-9
1 Ciphering data set applicable to positioning SIB type 2-9

Ciphering data set applicable for positioning SIB type 2-10 (octet p+4, bit 7)
0 Ciphering data set not applicable to positioning SIB type 2-10
1 Ciphering data set applicable to positioning SIB type 2-10

Ciphering data set applicable for positioning SIB type 2-11 (octet p+4, bit 6)
0 Ciphering data set not applicable to positioning SIB type 2-11
1 Ciphering data set applicable to positioning SIB type 2-11

Ciphering data set applicable for positioning SIB type 2-12 (octet p+4, bit 5)
0 Ciphering data set not applicable to positioning SIB type 2-12
1 Ciphering data set applicable to positioning SIB type 2-12

Ciphering data set applicable for positioning SIB type 2-13 (octet p+4, bit 4)
0 Ciphering data set not applicable to positioning SIB type 2-13
1 Ciphering data set applicable to positioning SIB type 2-13

Ciphering data set applicable for positioning SIB type 2-14 (octet p+4, bit 3)
0 Ciphering data set not applicable to positioning SIB type 2-14
1 Ciphering data set applicable to positioning SIB type 2-14

Ciphering data set applicable for positioning SIB type 2-15 (octet p+4, bit 2)
0 Ciphering data set not applicable to positioning SIB type 2-15
1 Ciphering data set applicable to positioning SIB type 2-15

Ciphering data set applicable for positioning SIB type 2-16 (octet p+4, bit 1)
0 Ciphering data set not applicable to positioning SIB type 2-16
1 Ciphering data set applicable to positioning SIB type 2-16

Ciphering data set applicable for positioning SIB type 2-17 (octet p+5, bit 8)
0 Ciphering data set not applicable to positioning SIB type 2-17
1 Ciphering data set applicable to positioning SIB type 2-17

Ciphering data set applicable for positioning SIB type 2-18 (octet p+5, bit 7)
0 Ciphering data set not applicable to positioning SIB type 2-18
1 Ciphering data set applicable to positioning SIB type 2-18

Ciphering data set applicable for positioning SIB type 2-19 (octet p+5, bit 6)
0 Ciphering data set not applicable to positioning SIB type 2-19
1 Ciphering data set applicable to positioning SIB type 2-19

Ciphering data set applicable for positioning SIB type 2-20 (octet p+5, bit 5)
0 Ciphering data set not applicable to positioning SIB type 2-20
1 Ciphering data set applicable to positioning SIB type 2-20

Ciphering data set applicable for positioning SIB type 2-21 (octet p+5, bit 4)
0 Ciphering data set not applicable to positioning SIB type 2-21
1 Ciphering data set applicable to positioning SIB type 2-21

Ciphering data set applicable for positioning SIB type 2-22 (octet p+5, bit 3)
0 Ciphering data set not applicable to positioning SIB type 2-22
1 Ciphering data set applicable to positioning SIB type 2-22

Ciphering data set applicable for positioning SIB type 2-23 (octet p+5, bit 2)
0 Ciphering data set not applicable to positioning SIB type 2-23
1 Ciphering data set applicable to positioning SIB type 2-23

Ciphering data set applicable for positioning SIB type 3-1 (octet p+5, bit 1)
0 Ciphering data set not applicable to positioning SIB type 3-1
1 Ciphering data set applicable to positioning SIB type 3-1

Ciphering data set applicable for positioning SIB type 4-1 (octet p+6, bit 8)
0 Ciphering data set not applicable to positioning SIB type 4-1
1 Ciphering data set applicable to positioning SIB type 4-1

Ciphering data set applicable for positioning SIB type 5-1 (octet p+6, bit 7)
0 Ciphering data set not applicable to positioning SIB type 5-1
1 Ciphering data set applicable to positioning SIB type 5-1

Ciphering data set applicable for positioning SIB type 6-1 (octet p+6, bit 6)
0 Ciphering data set not applicable to positioning SIB type 6-1
1 Ciphering data set applicable to positioning SIB type 6-1

Ciphering data set applicable for positioning SIB type 6-2 (octet p+6, bit 5)
0 Ciphering data set not applicable to positioning SIB type 6-2
1 Ciphering data set applicable to positioning SIB type 6-2

Ciphering data set applicable for positioning SIB type 6-3 (octet p+6, bit 4)
0 Ciphering data set not applicable to positioning SIB type 6-3
1 Ciphering data set applicable to positioning SIB type 6-3

Ciphering data set applicable for positioning SIB type 6-4 (octet p+6, bit 3)
0 Ciphering data set not applicable to positioning SIB type 6-4
1 Ciphering data set applicable to positioning SIB type 6-4

Ciphering data set applicable for positioning SIB type 6-5 (octet p+6, bit 2)
0 Ciphering data set not applicable to positioning SIB type 6-5
1 Ciphering data set applicable to positioning SIB type 6-5

Ciphering data set applicable for positioning SIB type 6-6 (octet p+6, bit 1)
0 Ciphering data set not applicable to positioning SIB type 6-6
1 Ciphering data set applicable to positioning SIB type 6-6

Ciphering data set applicable for positioning SIB type 1-9 (octet p+7, bit 8)
0 Ciphering data set not applicable to positioning SIB type 1-9
1 Ciphering data set applicable to positioning SIB type 1-9

Ciphering data set applicable for positioning SIB type 1-10 (octet p+7, bit 7)
0 Ciphering data set not applicable to positioning SIB type 1-10
1 Ciphering data set applicable to positioning SIB type 1-10

Ciphering data set applicable for positioning SIB type 2-24 (octet p+7, bit 6)

0 Ciphering data set not applicable to positioning SIB type 2-24
1 Ciphering data set applicable to positioning SIB type 2-24

Ciphering data set applicable for positioning SIB type 2-25 (octet p+7, bit 5)
0 Ciphering data set not applicable to positioning SIB type 2-25
1 Ciphering data set applicable to positioning SIB type 2-25

Ciphering data set applicable for positioning SIB type 2-17a (octet p+7, bit 4)
0 Ciphering data set not applicable to positioning SIB type 2-17a
1 Ciphering data set applicable to positioning SIB type 2-17a

Ciphering data set applicable for positioning SIB type 2-18a (octet p+7, bit 3)
0 Ciphering data set not applicable to positioning SIB type 2-18a
1 Ciphering data set applicable to positioning SIB type 2-18a

Ciphering data set applicable for positioning SIB type 2-20a (octet p+7, bit 2)
0 Ciphering data set not applicable to positioning SIB type 2-20a
1 Ciphering data set applicable to positioning SIB type 2-20a

Ciphering data set applicable for positioning SIB type 2-26 (octet p+7, bit 1)
0 Ciphering data set not applicable to positioning SIB type 2-26
1 Ciphering data set applicable to positioning SIB type 2-26

Ciphering data set applicable for positioning SIB type 2-27 (octet p+8, bit 8)
0 Ciphering data set not applicable to positioning SIB type 2-27
1 Ciphering data set applicable to positioning SIB type 2-27

Ciphering data set applicable for positioning SIB type 1-11 (octet p+8, bit 7)
0 Ciphering data set not applicable to positioning SIB type 1-11
1 Ciphering data set applicable to positioning SIB type 1-11

Ciphering data set applicable for positioning SIB type 1-12 (octet p+8, bit 6)
0 Ciphering data set not applicable to positioning SIB type 1-12
1 Ciphering data set applicable to positioning SIB type 1-12

Ciphering data set applicable for positioning SIB type 6-7 (octet p+8, bit 5)
0 Ciphering data set not applicable to positioning SIB type 6-7
1 Ciphering data set applicable to positioning SIB type 6-7

Ciphering data set applicable for positioning SIB type 7-1 (octet p+8, bit 4)
0 Ciphering data set not applicable to positioning SIB type 7-1
1 Ciphering data set applicable to positioning SIB type 7-1

Ciphering data set applicable for positioning SIB type 7-2 (octet p+8, bit 3)
0 Ciphering data set not applicable to positioning SIB type 7-2
1 Ciphering data set applicable to positioning SIB type 7-2

Ciphering data set applicable for positioning SIB type 7-3 (octet p+8, bit 2)
0 Ciphering data set not applicable to positioning SIB type 7-3
1 Ciphering data set applicable to positioning SIB type 7-3

Ciphering data set applicable for positioning SIB type 7-4 (octet p+8, bit 1)
0 Ciphering data set not applicable to positioning SIB type 7-4
1 Ciphering data set applicable to positioning SIB type 7-4

Any unassigned bits shall be coded as zero.

Validity start time (octets q+1 to q+5)
This field contains the UTC time when the ciphering data set becomes valid, encoded as octets 2 to 6 of the Time zone and time IE specified in 3GPP TS 24.008 [12].

Validity duration (octets q+6 to q+7)
This field contains the duration for which the ciphering data set is valid after the validity start time, in units of minutes.

TAIs list (octets q+8 to r)
This field contains the list of tracking areas for which the ciphering data set is applicable, encoded as octets 2 to n of the Tracking area identity list IE as specified in subclause 9.11.3.9. If the TAIs list is empty (as indicated by a zero length), the ciphering data set is applicable to the entire serving PLMN.

NOTE: The ciphering data set is always applicable to at least one of the E -UTRA Positioning SIB types or the NR Positioning SIB types.

9.11.3.18D Control plane service type

The purpose of the Control plane service type information element is to specify the purpose of the CONTROL PLANE SERVICE REQUEST message.

The Control plane service type information element is coded as shown in figure 9.11.3.18D.1 and table 9.11.3.18D.1.

The Control plane service type is a type 1 information element.

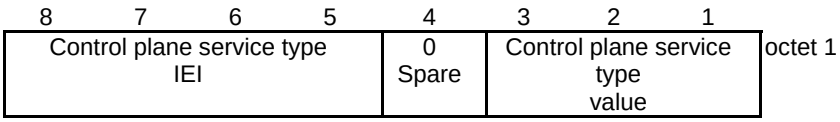


Figure 9.9.3.18D.1: Control plane service type information element

Table 9.9.3.18D.1: Control plane service type information element

Control plane service type value (octet 1, bit 1 to 3)			
Bits			
3	**2**	**1**	
0	0	0	mobile originating request
0	0	1	mobile terminating request
0	1	0	emergency services
0	1	1	emergency services fallback
1	0	0	
	to		unused; shall be interpreted as " mobile originating request", if received by the network.
1	1	1	

9.11.3.19 Daylight saving time

See subclause 10.5.3.12 in 3GPP TS 24.008 [12].

9.11.3.20 De-registration type

The purpose of the De-registration type information element is to indicate the type of de-registration.

The De-registration type information element is coded as shown in figure 9.11.3.20.1 and table 9.11.3.20.1.

The De-registration type is a type 1 information element.

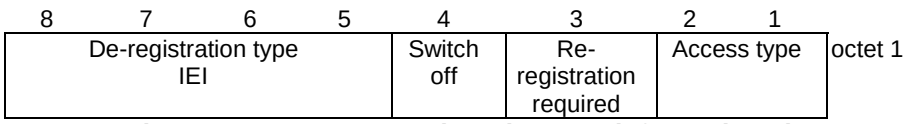


Figure 9.11.3.20.1: Deregistration type information element

Table 9.11.3.20.1: Deregistration type information element

Switch off (octet 1, bit 4)

In the UE to network direction:
Bit
4
0 Normal de-registration
1 Switch off

In the network to UE direction bit 4 is spare. The network shall set this bit to zero.

Re-registration required (octet 1, bit 3)

In the network to UE direction:
Bit
3
0 re-registration not required
1 re-registration required

In the UE to network direction bit 3 is spare. The UE shall set this bit to zero.

Access type (octet 1,bit 2, bit 1)
Bit
2 1
0 1 3GPP access
1 0 Non-3GPP access
1 1 3GPP access and non-3GPP access

All other values are reserved.

9.11.3.21 Void

9.11.3.22 Void

9.11.3.23 Emergency number list

See subclause 10.5.3.13 in 3GPP TS 24.008 [12].

9.11.3.23A EPS bearer context status

See subclause 9.9.2.1 in 3GPP TS 24.301 [15].

9.11.3.24 EPS NAS message container

The purpose of the EPS NAS message container information element is to transport an EPS NAS message as specified in 3GPP TS 24.301 [15].

The EPS NAS message container information element is coded as shown in figure 9.11.3.24.1 and table 9.11.3.24.1.

The EPS NAS message container is a type 6 information element.

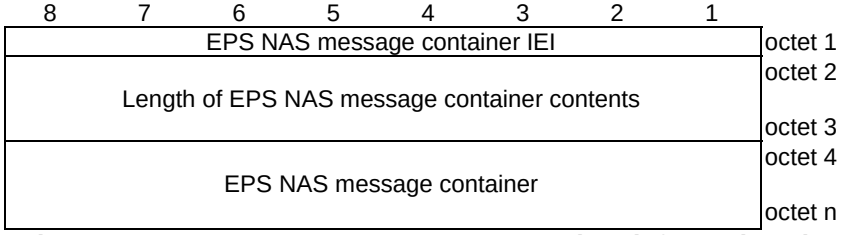


Figure 9.11.3.24.1: EPS NAS message container information element

Table 9.11.3.24.1: EPS NAS message container information element

EPS NAS message container (octet 4 to n) An EPS NAS message as specified in 3GPP TS 24.301 [15].

9.11.3.25 EPS NAS security algorithms

See subclause 9.9.3.23 in 3GPP TS 24.301 [15].

9.11.3.26 Extended emergency number list

See subclause 9.9.3.37A in 3GPP TS 24.301 [15].

9.11.3.26A Extended DRX parameters

See subclause 10.5.5.32 in 3GPP TS 24.008 [12].

9.11.3.27 Void

9.11.3.28 IMEISV request

See subclause 10.5.5.10 in 3GPP TS 24.008 [12].

9.11.3.29 LADN indication

The purpose of the LADN indication information element is to request the network for LADN information for specific LADN DNN(s) or to indicate a request for LADN information.

The LADN indication information element is coded as shown in figure 9.11.3.29.1 and table 9.11.3.29.1.

The LADN indication is a type 6 information element with a minimum length of 3 octets and a maximum length of 811 octets.

The LADN indication information element can contain a minimum of 0 and a maximum of 8 different LADN DNN values.

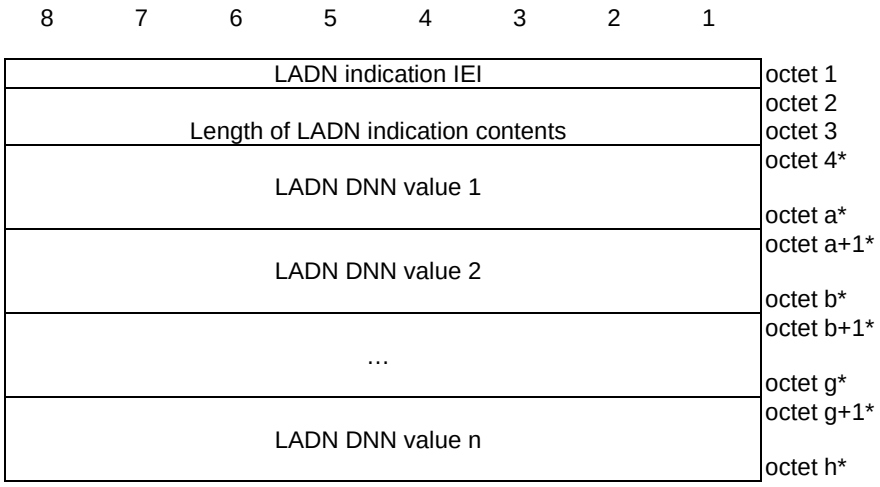


Figure 9.11.3.29.1: LADN indication information element

Table 9.11.3.29.1: LADN indication information element

Value part of the LADN indication information element (octet 4 to h): The value part of the LADN indication information element consists of zero or more LADN DNN values. If the LADN indication information element conveys more than 8 LADN DNN values in this information element, the network shall consider the first 8 LADN DNN values and ignore the remaining octets of the information element. LADN DNN value: LADN DNN value is coded as the length and value part of DNN information element as specified in subclause 9.11.2.1B starting with the second octet.

9.11.3.30 LADN information

The purpose of the LADN information information element is to provide the UE with the LADN service area for each available LADN in the current registration area or to delete the LADN information at the UE.

The LADN information information element is coded as shown in figure 9.11.3.30.1, figure 9.11.3.30.2 and table 9.11.3.30.1.

The LADN information is a type 6 information element with a minimum length of 3 octets and a maximum length of 1715 octets.

The LADN information information element can contain a minimum of 0 and a maximum of 8 different LADNs each including a DNN and a 5GS tracking area identity list.

8	7	6	5	4	3	2	1	
LADN information IEI								octet 1
Length of LADN information contents								octet 2 octet 3
LADN 1								octet 4 octet a
LADN 2								octet a+1* octet b*
…								octet b+1* octet g*
LADN n								octet g+1* octet h*

Figure 9.11.3.30.1: LADN information information element

8	7	6	5	4	3	2	1	
Length of DNN value								octet 4
DNN value								octet 5 octet m
5GS tracking area identity list								octet m+1 octet a

Figure 9.11.3.30.2: LADN

Table 9.11.3.30.1: LADN information information element

Value part of the LADN information information element (octet 4 to octet h) The value part of the LADN information information element consists of one or several LADNs. Each LADN (e.g. octet 4 to octet a) consists one DNN value and one 5GS tracking area identity list. The length of each LADN is determined by the length of DNN value field and the length of 5GS tracking area identity list field. The UE shall store the complete list as received. If more than 8 LADNs are included in this information element, the UE shall store the first 8 LADNs and ignore the remaining octets of the information element. DNN value (octet 5 to octet m): DNN value field is coded as DNN value part of DNN information element as specified in subclause 9.11.2.1B starting with the third octet. 5GS tracking area identity list (octet m+1 to octet a): 5GS tracking area identity list field is coded as the length and the value part of the 5GS Tracking area identity list information element as specified in subclause 9.11.3.9 starting with the second octet.

9.11.3.31 MICO indication

The purpose of the MICO indication information element is to indicate the use of MICO mode or the re-negotiation of MICO mode.

The MICO indication information element is coded as shown in figure 9.11.3.31.1 and table 9.11.3.31.1.

The MICO indication is a type 1 information element.

8	7	6	5	4	3	2	1	
MICO indication IEI				0 Spare	0 Spare	SPRTI	RAAI	octet 1

Figure 9.11.3.31.1: MICO indication

Table 9.11.3.31.1: MICO indication

Registration Area Allocation Indication (RAAI) (octet 1, bit 1) In the network to UE direction: Bit **1** 0 all PLMN registration area not allocated 1 all PLMN registration area allocated In the UE to network direction bit 1 is spare. The UE shall set this bit to zero. Strictly Periodic Registration Timer Indication (SPRTI) (octet 1, bit 2) In the network to UE and the UE to network direction: Bit **2** 0 strictly periodic registration timer not supported 1 strictly periodic registration timer supported Bits 3 and 4 are spare and shall be coded as zero. NOTE: In the network to UE direction in the CONFIGURATION UPDATE COMMAND message, bits 1 and 2 shall be coded as zero.

9.11.3.31A MA PDU session information

The purpose of the MA PDU session information information element is to convey the MA-related information for the PDU session.

The MA PDU session information information element is coded as shown in figure 9.11.3.31A.1 and table 9.11.3.31A.1.

The MA PDU session information is a type 1 information element.

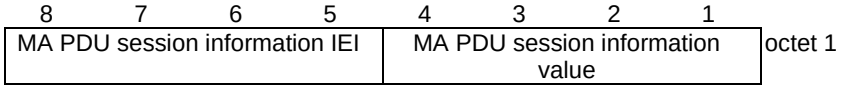


Figure 9.11.3.31A.1: MA PDU session information information element

Table 9.11.3.31A.1: MA PDU session information information element

MA PDU session information value (octet 1, bit 1 to bit 4)
Bits 4 3 2 1 0 0 0 0 No additional information 0 0 0 1 MA PDU session network upgrade is allowed All other values are spare. If received they shall be ignored.

9.11.3.31B Mapped NSSAI

The purpose of the Mapped NSSAI information element is to transfer S-NSSAI(s) applicable in the HPLMN to the visited PLMN.

The Mapped NSSAI information element is coded as shown in figure 9.11.3.31B.1, figure 9.11.3.31B.2 and table 9.11.3.31B.1.

The Mapped NSSAI is a type 4 information element with a minimum length of 4 octets and a maximum length of 42 octets.

NOTE 1: The total number of S-NSSAI values in a requested mapped NSSAI cannot exceed eight.

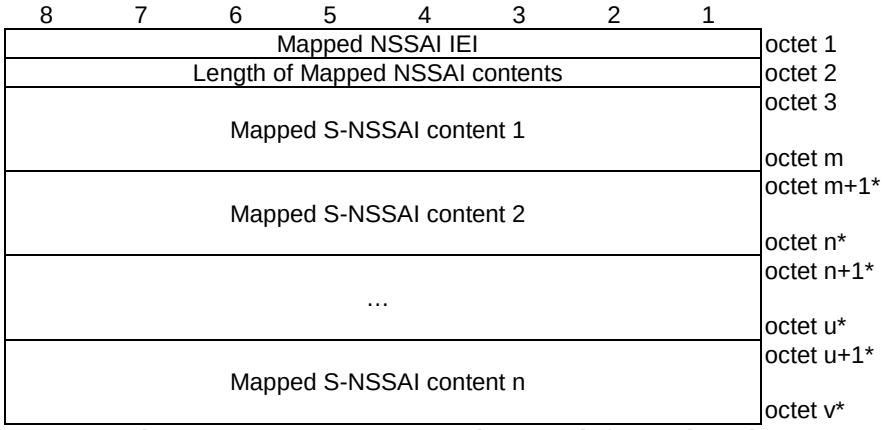


Figure 9.11.3.31B.1: Mapped NSSAI information element

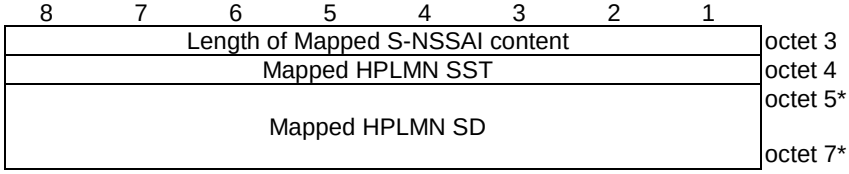


Figure 9.11.3.31B.2: Mapped S-NSSAI content

Table 9.11.3.31B.1: Mapped NSSAI information element

Value part of the Mapped NSSAI information element (octet 3 to v) The value part of the Mapped NSSAI information element consists of one or more mapped S-NSSAI contents. Mapped S-NSSAI content: Length of S-NSSAI contents (octet 3) Mapped HPLMN Slice/service type (SST) (octet 4) This field contains the 8 bit SST value of an S-NSSAI in the S-NSSAI(s) of the HPLMN to which the SST value is mapped. The coding of the SST value part is defined in 3GPP TS 23.003 [4]. NOTE 1: Octet 4 (i.e. mapped HPLMN SST) shall always be included. Mapped HPLMN Slice differentiator (SD) (octet 5 to octet 7) This field contains a 24-bit SD value of an S-NSSAI in the S-NSSAI(s) of the HPLMN to which the SD value is mapped. The coding of the SD value part is defined in 3GPP TS 23.003 [4]. NOTE 2: If the octet 5 is included, then octet 6 and octet 7 shall be included.

9.11.3.31C Mobile station classmark 2

See subclause 10.5.1.6 in 3GPP TS 24.008 [12].

9.11.3.32 NAS key set identifier

The NAS key set identifier is allocated by the network.

The NAS key set identifier information element is coded as shown in figure 9.11.3.32.1 and table 9.11.3.32.1.

The NAS key set identifier is a type 1 information element.

8	7	6	5	4	3	2	1	
NAS key set identifier IEI				TSC	NAS key set identifier			octet 1

Figure 9.11.3.32.1: NAS key set identifier information element

Table 9.11.3.32.1: NAS key set identifier information element

Type of security context flag (TSC) (octet 1) Bit **4** 0 native security context (for KSI_{AMF}) 1 mapped security context (for KSI_{ASME}) TSC does not apply for NAS key set identifier value "111". NAS key set identifier (octet 1) Bits **3 2 1** 0 0 0 through possible values for the NAS key set identifier 1 1 0 1 1 1 no key is available (UE to network); reserved (network to UE)			

9.11.3.33 NAS message container

The purpose of the NAS message container IE is to encapsulate a plain 5GS NAS REGISTRATION REQUEST, DEREGISTRATION REQUEST, or SERVICE REQUEST message, or to encapsulate non-cleartext IEs of a CONTROL PLANE SERVICE REQUEST message.

The NAS message container information element is coded as shown in figure 9.11.3.33.1 and table 9.11.3.33.1.

The NAS message container is a type 6 information element.

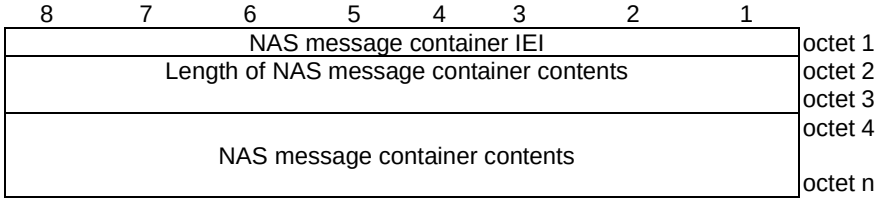


Figure 9.11.3.33.1: NAS message container information element

Table 9.11.3.33.1: NAS message container information element

NAS message container contents (octet 4 to octet n); Max value of 65535 octets This IE can contain a REGISTRATION REQUEST message as defined in subclause 5.5.1, DEREGISTRATION REQUEST message as defined in subclause 5.5.2.2.1, or a SERVICE REQUEST message as defined in subclause 5.6.1, or non-cleartext IEs of a CONTROL PLANE SERVICE REQUEST message as defined in subclause 5.6.1.

9.11.3.34 NAS security algorithms

The purpose of the NAS security algorithms information element is to indicate the 5G algorithms to be used for ciphering and integrity protection.

The NAS security algorithms information element is coded as shown in figure 9.11.3.34.1 and table 9.11.3.34.1.

The NAS security algorithms is a type 3 information element with a length of 2 octets.

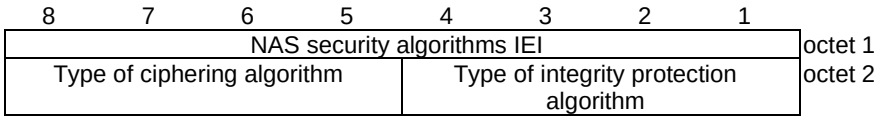


Figure 9.11.3.34.1: NAS security algorithms information element

Table 9.11.3.34.1: NAS security algorithms information element

Type of integrity protection algorithm (octet 2, bit 1 to 3)				
Bits				
4	**3**	**2**	**1**	
0	0	0	0	5G integrity algorithm 5G-IA0 (null integrity protection algorithm)
0	0	0	1	5G integrity algorithm 128-5G-IA1
0	0	1	0	5G integrity algorithm 128-5G-IA2
0	0	1	1	5G integrity algorithm 128-5G-IA3
0	1	0	0	5G integrity algorithm 5G-IA4
0	1	0	1	5G integrity algorithm 5G-IA5
0	1	1	0	5G integrity algorithm 5G-IA6
0	1	1	1	5G integrity algorithm 5G-IA7
All other values are reserved.				
Type of ciphering algorithm (octet 2, bit 5 to 7)				
Bits				
8	**7**	**6**	**5**	
0	0	0	0	5G encryption algorithm 5G-EA0 (null ciphering algorithm)
0	0	0	1	5G encryption algorithm 128-5G-EA1
0	0	1	0	5G encryption algorithm 128-5G-EA2
0	0	1	1	5G encryption algorithm 128-5G-EA3
0	1	0	0	5G encryption algorithm 5G-EA4
0	1	0	1	5G encryption algorithm 5G-EA5
0	1	1	0	5G encryption algorithm 5G-EA6
0	1	1	1	5G encryption algorithm 5G-EA7
All other values are reserved.				

9.11.3.35 Network name

See subclause 10.5.3.5a in 3GPP TS 24.008 [12].

9.11.3.36 Network slicing indication

The purpose of the Network slicing indication information element is to indicate additional information associated with network slicing in the generic UE configuration update procedure and the registration procedure, other than the user's configured NSSAI, allowed NSSAI, pending NSSAI and rejected NSSAI information.

The Network slicing indication information element is coded as shown in figure 9.11.3.36.1 and table 9.11.3.36.1.

The Network slicing indication is a type 1 information element.

8	7	6	5	4	3	2	1	
Network slicing indication IEI				0 Spare	0 Spare	DCNI	NSSCI	octet 1

Figure 9.11.3.36.1: Network slicing indication

Table 9.11.3.36.1: Network slicing indication

Network slicing subscription change indication (NSSCI) (octet 1, bit 1) Bit **1** 0 Network slicing subscription not changed 1 Network slicing subscription changed Default configured NSSAI indication (DCNI) (octet 1, bit 2) Bit **2** 0 Requested NSSAI not created from default configured NSSAI 1 Requested NSSAI created from default configured NSSAI In the UE to network direction bit 1 is spare. The UE shall set this bit to zero. In the network to UE direction bit 2 is spare. The network shall set this bit to zero. Bits 3 and 4 are spare and shall be coded as zero.

9.11.3.36A Non-3GPP NW provided policies

See subclause 10.5.5.37 in 3GPP TS 24.008 [12].

9.11.3.37 NSSAI

The purpose of the NSSAI information element is to identify a collection of S-NSSAIs

The NSSAI information element is coded as shown in figure 9.11.3.37.1 and table 9.11.3.37.1.

The NSSAI is a type 4 information element with a minimum length of 4 octets and a maximum length of 146 octets.

NOTE: More than one S-NSSAIs in an NSSAI can have the same SST values, and optionally same SD values, which are associated with different mapped HPLMN SST values and optionally mapped HPLMN SD values.

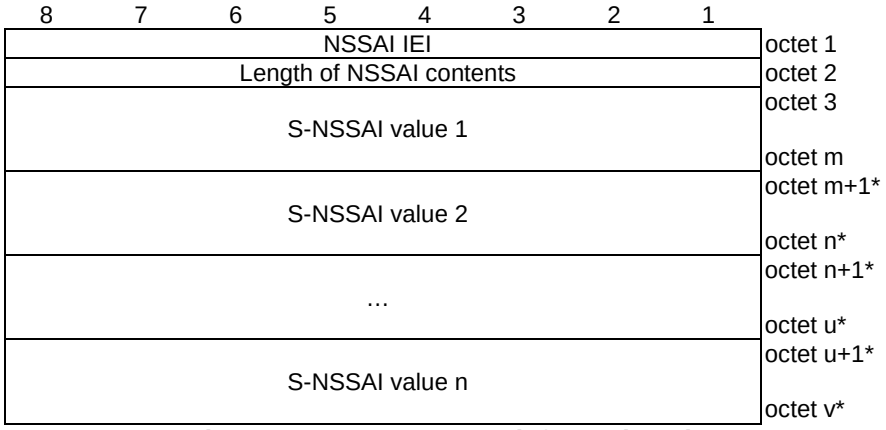


Figure 9.11.3.37.1: NSSAI information element

Table 9.11.3.37.1: NSSAI information element

Value part of the NSSAI information element (octet 3 to v) The value part of the NSSAI information element consists of one or more S-NSSAI values. Each S-NSSAI value consists of one S-NSSAI and optionally one mapped S-NSSAI. The recipient of this information element shall store the complete list received (NOTE 1, NOTE 2, NOTE 3). If the NSSAI information element conveys an allowed NSSAI and more than 8 S-NSSAI values are included in this information element, the UE shall store the first 8 S-NSSAI values and ignore the remaining octets of the information element. If the NSSAI information element conveys a configured NSSAI (including the default configured NSSAI) or pending NSSAI and more than 16 S-NSSAI values are included in this information element, the UE shall store the first 16 S-NSSAI values and ignore the remaining octets of the information element. S-NSSAI value: S-NSSAI value is coded as the length and value part of S-NSSAI information element as specified in subclause 9.11.2.8 starting with the second octet.
NOTE 1: The total number of S-NSSAI values in a requested NSSAI shall not exceed eight. NOTE 2: The number of S-NSSAI values in an allowed NSSAI shall not exceed eight. NOTE 3: The number of S-NSSAI values in a configured NSSAI (including the default configured NSSAI) or pending NSSAI shall not exceed sixteen.

9.11.3.37A NSSAI inclusion mode

The purpose of the NSSAI inclusion mode information element is to indicate the NSSAI inclusion mode in which the UE shall operate.

The NSSAI inclusion mode is a type 1 information element.

The NSSAI inclusion mode information element is coded as shown in figure 9.11.3.37A.1 and table 9.11.3.37A.1.

8	7	6	5	4	3	2	1	
NSSAI inclusion mode IEI				0 spare	0 spare	NSSAI inclusion mode		octet 1

Figure 9.11.3.37A.1: NSSAI inclusion mode information element

Table 9.11.3.37A.1: NSSAI inclusion mode information element

NSSAI inclusion mode (octet 1, bit 1 to bit 2)		
Bits		
2	**1**	
0	0	NSSAI inclusion mode A
0	1	NSSAI inclusion mode B
1	0	NSSAI inclusion mode C
1	1	NSSAI inclusion mode D

9.11.3.38 Operator-defined access category definitions

The purpose of the Operator-defined access category definitions information element is to provide the UE with the operator-defined access category definitions or to delete the operator-defined access category definitions at the UE.

The Operator-defined access category definitions information element is coded as shown in figure 9.11.3.38.1, figure 9.11.3.38.2 and table 9.11.3.38.1.

The Operator-defined access category definitions is a type 6 information element with a minimum length of 3 octets, and maximum length of 8323 octets.

8	7	6	5	4	3	2	1	
Operator-defined access category definitions IEI								octet 1
Length of operator-defined access category definitions contents								octet 2 octet 3
Operator-defined access category definition 1								octet 4* octet a*
Operator-defined access category definition 2								octet a+1* octet b*
…								octet b+1* octet g*
Operator-defined access category definition n								octet g+1* octet h*

Figure 9.11.3.38.1: Operator-defined access category definitions information element

8	7	6	5	4	3	2	1	
Length of operator-defined access category definition contents								octet 4
Precedence value								octet 5
PSAC	0 Spare	0 Spare	Operator-defined access category number					octet 6
Length of criteria								octet 7
Criteria								octet 8 octet a-1
0 Spare	0 Spare	0 Spare	Standardized access category					octet a*

Figure 9.11.3.38.2: Operator-defined access category definition

Table 9.11.3.38.1: Operator-defined access category definitions information element

Value part of the Operator-defined access category definitions information element (octet 4 to h)
The value part of the Operator-defined access category definitions information element consists of zero or no more than 32 operator-defined access category definition fields. Each operator-defined access category definition field is coded as described in figure 9.11.3.38.2. The length of each operator-defined access category definition field is determined by the length of operator-defined access category definition contents field.

Operator-defined access category definition (octet 4 to octet a):

Length of operator-defined access category definition contents (octet 4)
Length of operator-defined access category definition contents indicates binary coded length of the operator-defined access category definition value field (octet 5 to octet a).

Precedence value (octet 5)
Bits

8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	
0	0	0	0	0	0	0	0	Precedence value 0
				to				
1	1	1	1	1	1	1	1	Precedence value 255

Operator-defined access category number (bits 5 to 1 of octet 6)
Bits

5	**4**	**3**	**2**	**1**	
0	0	0	0	0	Access category number 32
		to			
1	1	1	1	1	Access category number 63

Presence of standardized access category (PSAC) (bit 8 of octet 6)
PSAC field indicates whether the standardized access category field is present or absent.
Bit

8	
0	Standardized access category field is not included
1	Standardized access category field is included

Length of criteria (octet 7)
Length of criteria field indicates binary coded length of the criteria field.

Criteria (octets 8 to octet a-1)
The criteria field contains one or more criteria components fields. Each criteria component field shall be encoded as a sequence of a one octet criteria type field and zero or more octets criteria value field. The criteria type field shall be transmitted first.

Criteria type
Bits

8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	
0	0	0	0	0	0	0	0	DNN type
0	0	0	0	0	0	0	1	OS id + OS App Id type
0	0	0	0	0	0	1	0	S-NSSAI type

All other values are reserved.

For "DNN type", the criteria value field shall be encoded as a sequence of one octet DNN length-value pair count field and one or more DNN length-value pair fields. The DNN length-value pair count field indicates the number of included DNN length-value pair fields. Each DNN length-value pair field is coded as a sequence of one octet DNN value length field and a DNN value field. The DNN value length field indicates the length in octets of the DNN value field. The DNN value field contains an APN as specified in 3GPP TS 23.003 [4].

For "OS Id + OS App Id type", the criteria value field shall be encoded as a sequence of one octet app id value count field and one or more app id value fields. The app id value count field indicates the number of included app id value fields. Each app id value field is coded as a sequence of a sixteen octet OS id value field, one octet OS app id value length field and an OS app id value field. The OS app id value length field indicates the length in octets of the OS app id value field. The OS id value field contains a Universally Unique IDentifier (UUID) as specified in IETF RFC 4122 [35A]. The OS app id value field contains an OS specific application identifier. Coding of the OS app id value field is outside the scope of the present document.

For "S-NSSAI type", the criteria value field shall be encoded as a sequence of one octet S-NSSAI length-value pair count field and one or more S-NSSAI length-value value fields. The S-NSSAI length-value pair count field indicates the number of included S-NSSAI length-value pair fields. Each S-NSSAI length-value pair field is coded as a sequence of one octet S-NSSAI value length field and an S-NSSAI value field. The S-NSSAI value length field indicates the length in octets of the S-NSSAI value field. The S-NSSAI value field contains one octet SST field optionally followed by three octets SD field. The SST field contains a SST. The SD field contains an SD. SST and SD are specified in 3GPP TS 23.003 [4].

Standardized access category (bits 5 to 1 of octet a)
Standardized access category field indicates the access category number of the standardized access category that is used in combination with the access identities to determine the establishment cause.

Bits					
5	**4**	**3**	**2**	**1**	
0	0	0	0	0	Access category number 0
		to			
0	0	1	1	1	Access category number 7
0	1	0	0	1	Access category number 9
0	1	0	1	0	Access category number 10

All other values are reserved.

9.11.3.39 Payload container

The purpose of the Payload container information element is to transport one or multiple payloads. If multiple payloads are transported, the associated information of each payload are also transported together with the payload.

The Payload container information element is coded as shown in figure 9.11.3.39.1, figure 9.11.3.39.1A, figure 9.11.3.39.1B, figure 9.11.3.39.2, figure 9.11.3.39.3, figure 9.11.3.39.4 and table 9.11.3.39.1.

The Payload container information element is a type 6 information element with a minimum length of 4 octets and a maximum length of 65538 octets.

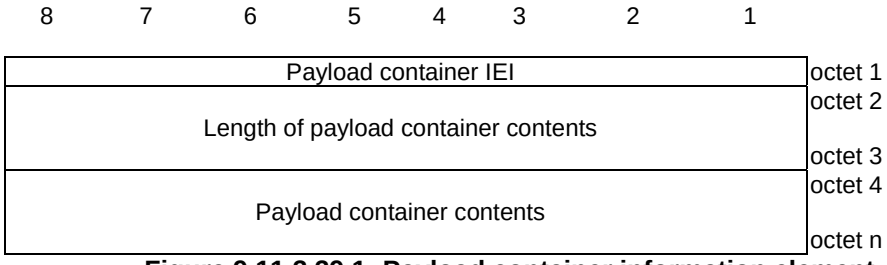


Figure 9.11.3.39.1: Payload container information element

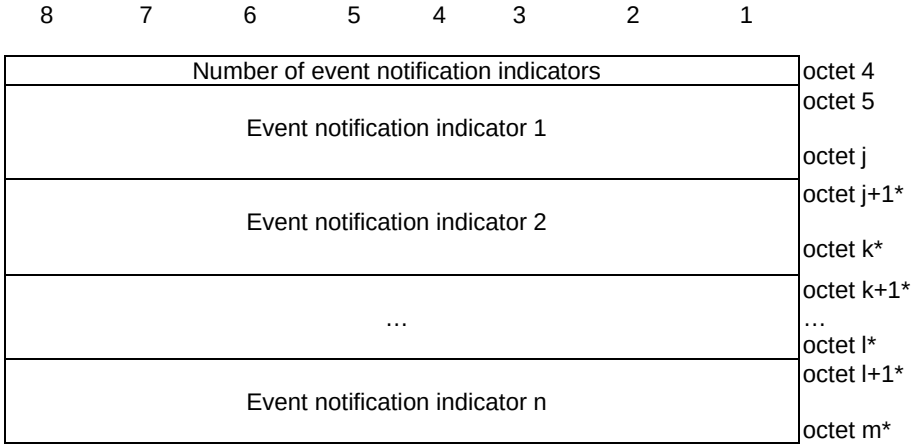


Figure 9.11.3.39.1A: Payload container contents with Payload container type "Event notification"

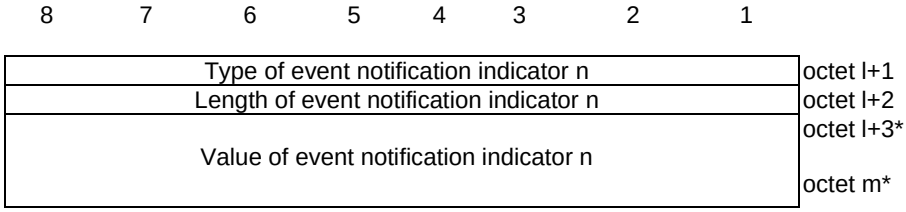


Figure 9.11.3.39.1B: Even notification indicator n

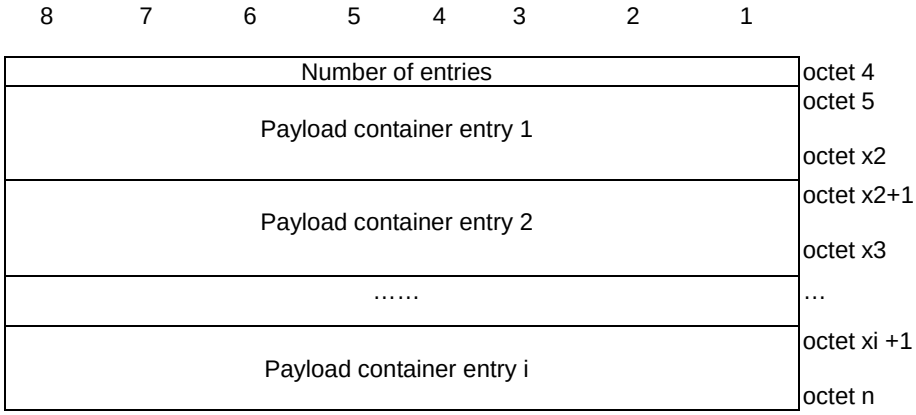


Figure 9.11.3.39.2: Payload container contents with Payload container type "Multiple payloads"

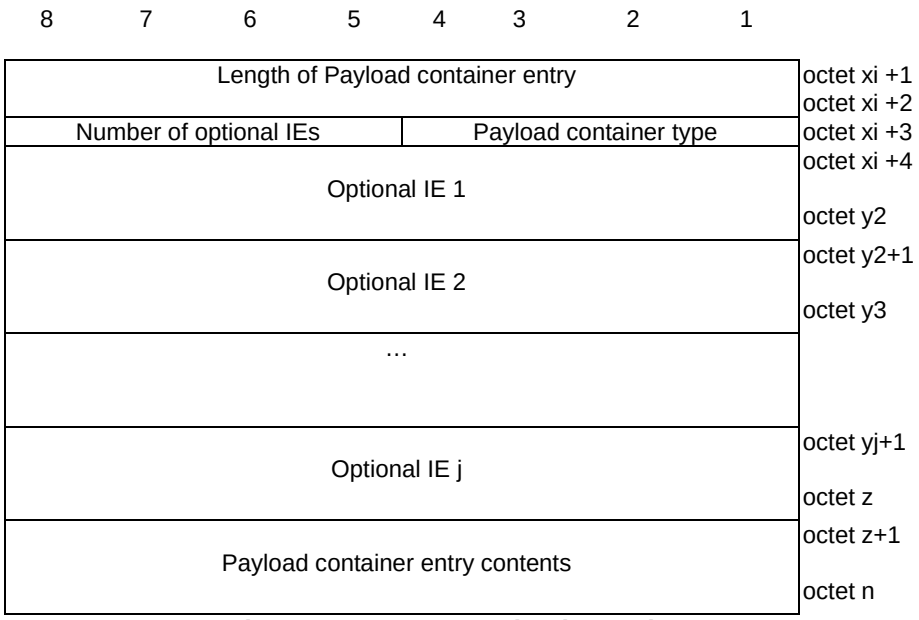


Figure 9.11.3.39.3: Payload container entry

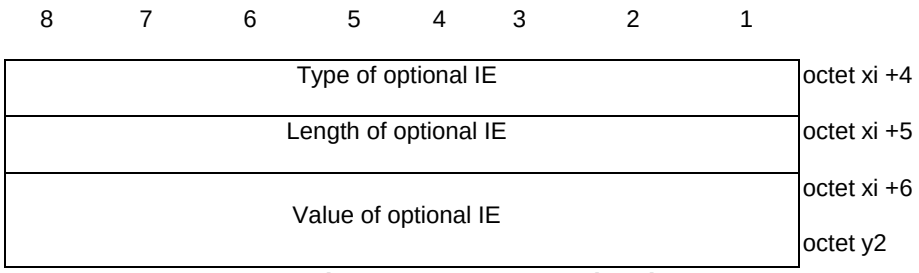


Figure 9.11.3.39.4: Optional IE

Table 9.11.3.39.1: Payload container information element

Payload container contents (octet 4 to octet n); max value of 65535 octets

If the payload container type is set to "N1 SM information" and is included in the UL NAS TRANSPORT or DL NAS TRANSPORT message, the payload container contents contain a 5GSM message as defined in subclause 8.3.

If the payload container type is set to "SOR transparent container" and is included in the DL NAS TRANSPORT message, the payload container contents are coded the same way as the contents of the SOR transparent container IE (see subclause 9.11.3.51) for SOR data type is set to value "0" except that the first three octets are not included.

If the payload container type is set to "SOR transparent container" and is included in the UL NAS TRANSPORT message, the payload container contents are coded the same way as the contents of the SOR transparent container IE (see subclause 9.11.3.51) for SOR data type is set to value "1" except that the first three octets are not included.

If the payload container type is set to "UE policy container" and is included in the DL NAS TRANSPORT, UL NAS TRANSPORT or REGISTRATION REQUEST message, the payload container contents are coded as defined in subclause Annex D.

If the payload container type is set to "UE parameters update transparent container" and is included in the DL NAS TRANSPORT message, the payload container contents are coded the same way as the contents of the UE parameters update transparent container IE (see subclause 9.11.3.53A) for UE parameters update data type is set to value "0" except that the first three octets are not included.

If the payload container type is set to "UE parameters update transparent container" and is included in the UL NAS TRANSPORT message, the payload container contents are coded the same way as the contents of the UE parameters update transparent container IE (see subclause 9.11.3.53A) for UE parameters update data type is set to value "1" except that the first three octets are not included.

If the payload container type is set to "SMS" and is included in the UL NAS TRANSPORT or DL NAS TRANSPORT message, the payload container contents contain an SMS message (i.e. CP-DATA, CP-ACK or CP-ERROR) as defined in subclause 7.2 in 3GPP TS 24.011 [13].

If the payload container type is set to "CIoT user data container" and is included in the UL NAS TRANSPORT, DL NAS TRANSPORT or CONTROL PLANE SERVICE REQUEST message, the payload container contents are coded the same way as the contents of the user data container IE (see subclause 9.9.4.24 in 3GPP TS 24.301 [15]) except that the first three octets are not included.

If the payload container type is set to "SMS" and is included in the CONTROL PLANE SERVICE REQUEST message, the payload container contents are coded the same way as the contents of the NAS message container IE (see subclause 9.9.3.22 in 3GPP TS 24.301 [15]) except that the first two octets are not included.

If the payload container type is set to "Location services message container" and is included in the UL NAS TRANSPORT, DL NAS TRANSPORT or CONTROL PLANE SERVICE REQUEST message, the payload container contents include location services message payload.

If the payload container type is set to "LTE Positioning Protocol (LPP) message container" and is included in the UL NAS TRANSPORT or DL NAS TRANSPORT message, the payload container contents include LPP message payload.

If the payload container type is set to "SLPP message container" and is included in the UL NAS TRANSPORT or DL NAS TRANSPORT message, the payload container contents include SLPP message payload.

If the payload container type is set to "Service-level-AA container" and is included in the UL NAS TRANSPORT or DL NAS TRANSPORT message, the payload container contents are coded the same way as the contents of service-level-AA container (see subclause 9.11.2.10).

If the payload container type is set to "Event notification", the payload container contents include one or more event notification indicators.

Type of event notification indicator n (octet l+1)
Bits

8	7	6	5	4	3	2	1	
0	0	0	0	0	0	0	0	"SRVCC handover cancelled, IMS session re-establishment required" indicator
0	0	0	0	0	0	0	1	
				to				Unused, shall be ignored if received by the UE
1	1	1	1	1	1	1	1	

If the type of an event notification indicator is set to "SRVCC handover cancelled, IMS session re-establishment required" indicator, the value of the event notification indicator shall not be included.

If the payload container type is set to "UPP-CMI container" and is included in the UL NAS TRANSPORT or DL NAS TRANSPORT message, the payload container contents include UPP-CMI messages as specified in 3GPP TS 24.572 [64].

If the payload container type is set to "Multiple payloads", the number of entries field represents the total number of payload container entries, and the payload container entry contents field is coded as a list of payload container entry according to figure 9.11.3.39.2, with each payload container entry is coded according to figure 9.11.3.39.3 and figure 9.11.3.39.4.

The coding of Payload container contents is dependent on the particular application.

Payload container entry

For each payload container entry, the payload container type field represents the payload container type value as described in subclause 9.11.3.40, the coding of payload container contents field is dependent on the particular application, and the number of optional IEs field represents the total number of optional IEs associated with the payload container entry contents field in the payload container entry. The error handlings for optional IEs specified in subclauses 7.6.3 and 7.7.1 shall apply to the optional IEs included in the payload container entry.

The receiving entity shall ignore Optional IEs with type of optinal IE parameter field containing an unknown IEI.

Optional IEs

Type of optional IE (octet xi +4)
This field contains the IEI of the optional IE.

Length of optional IE (octet xi+5)
This field indicates binary coded length of the value of the optional IE entry.

Value of optional IE (octet xi+6 to octet y2)
This field contains the value of the optional IE entry with the value part of the referred information element based on following optional IE reference. If the Request type is included, the value part of the Request type shall be encoded in the bits 1 to 4 and bits 5 to 8 shall be coded as zero. If the Release assistance indication is included, the value part of the Release assistance indication shall be encoded in the bits 1 to 4 and bits 5 to 8 shall be coded as zero. If the MA PDU session information is included, the value part of the MA PDU session information shall be encoded in the bits 1 to 4 and bits 5 to 8 shall be coded as zero.

IEI	Optional IE name	Optional IE reference
12	PDU session ID	PDU session identity 2 (see subclause 9.11.3.41)
24	Additional information	Additional information (see subclause 9.11.2.1)
58	5GMM cause	5GMM cause (see subclause 9.11.3.2)
37	Back-off timer value	GPRS timer 3 (see subclause 9.11.2.5)
59	Old PDU session ID	PDU session identity 2 (see subclause 9.11.3.41)
80	Request type	Request type (see subclause 9.11.3.47)
22	S-NSSAI	S-NSSAI (see subclause 9.11.2.8)
25	DNN	DNN (see subclause 9.11.2.1B)
F0	Release assistance indication	Release assistance indication (see subclause 9.11.3.46A)

A0	MA PDU session information	MA PDU session information (see subclause 9.11.3.31A)

9.11.3.40 Payload container type

The purpose of the Payload container type information element indicates type of payload included in the payload container information element.

The Payload container type information element is coded as shown in figure 9.11.3.40.1 and table 9.11.3.40.1.

The Payload container type information element is a type 1 information element.

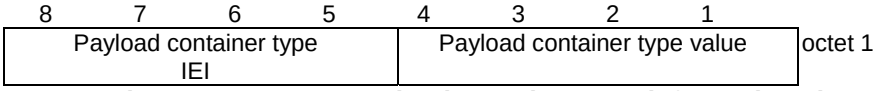


Figure 9.11.3.40.1: Payload container type information element

Table 9.11.3.40.1: Payload container type information element

Payload container type value (octet 1)				
Bits				
4	**3**	**2**	**1**	
0	0	0	1	N1 SM information
0	0	1	0	SMS
0	0	1	1	LTE Positioning Protocol (LPP) message container
0	1	0	0	SOR transparent container
0	1	0	1	UE policy container
0	1	1	0	UE parameters update transparent container
0	1	1	1	Location services message container (see 3GPP TS 23.273 [6B])
1	0	0	0	CIoT user data container
1	0	0	1	Service-level-AA container
1	0	1	0	Event notification
1	0	1	1	UPP-CMI container
1	1	0	0	SLPP message container
1	1	1	1	Multiple payloads
All other values are reserved.				
NOTE: The value "Multiple payloads" is only used when the Payload container contents in figure 9.11.3.39.1 contains multiple payloads as shown in figure 9.11.3.39.2.				

9.11.3.41 PDU session identity 2

The purpose of the PDU session identity 2 information element is to indicate the identity of a PDU session in a 5GMM message.

The PDU session identity 2 information element is coded as shown in figure 9.11.3.41.1 and table 9.11.3.41.1.

The PDU session identity 2 is a type 3 information element with a length of 2 octets .

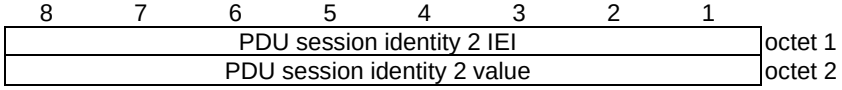


Figure 9.11.3.41.1: PDU session identity 2 information element

Table 9.11.3.41.1: PDU session identity 2 information element

PDU session identity 2 value (octet 2)
The coding of the PDU session identity 2 value is identical to the coding of the PDU session identity value as defined in 3GPP TS 24.007 [11] .

9.11.3.42 PDU session reactivation result

The purpose of the PDU session reactivation result information element is to indicate the result of establishments of user-plane resources of PDU sessions.

The PDU session reactivation result information element is coded as shown in figure 9.11.3.42.1 and table 9.11.3.42.1.

The PDU session reactivation result is a type 4 information element with minimum length of 4 octets and maximum length of 34 octets.

8	7	6	5	4	3	2	1	
PDU session reactivation result IEI								octet 1
Length of PDU session reactivation result								octet 2
PSI (7)	PSI (6)	PSI (5)	PSI (4)	PSI (3)	PSI (2)	PSI (1)	PSI (0)	octet 3
PSI (15)	PSI (14)	PSI (13)	PSI (12)	PSI (11)	PSI (10)	PSI (9)	PSI (8)	octet 4
0	0	0	0	0	0	0	0	octet 5* -34*
Spare								

Figure 9.11.3.42.1: PDU session reactivation result information element

Table 9.11.3.42.1: PDU session reactivation result information element

PSI(x) shall be coded as follows: PSI(0): Bit 1 of octet 3 is spare and shall be coded as zero. PSI(1) – PSI(15): 0 indicates establishment of user-plane resources of the PDU session was not requested in the Uplink data status IE or establishment of user-plane resources of the PDU session was not allowed in the Allowed PDU session status IE or establishment of user-plane resource of the PDU session is successful. 1 indicates either establishment of user-plane resources of the PDU session was requested in the Uplink data status IE but establishment of user-plane resource of the PDU session is not successful or indicates establishment of user-plane resources of the PDU session was allowed in the Allowed PDU session status IE but establishment of user-plane resource of the PDU session is either not performed or not successful. All bits in octet 5 to 34 are spare and shall be coded as zero, if the respective octet is included in the information element.

9.11.3.43 PDU session reactivation result error cause

The purpose of the PDU session reactivation result error cause information element is to indicate error causes for PDU session ID(s) where there was a failure to establish the user-plane resources.

The PDU session reactivation result error cause information element is coded as shown in figure 9.11.3.43.1 and table 9.11.3.43.1.

The PDU session reactivation result error cause is a type 6 information element with a minimum length of 5 octets and a maximum length of 515 octets.

8	7	6	5	4	3	2	1	
PDU session reactivation result error cause IEI								octet 1
Length of PDU session reactivation result error cause								octet 2 octet 3
PDU session ID								octet 4
cause value								octet 5
….								
PDU session ID								octet 514*
cause value								octet 515*

Figure 9.11.3.43.1: PDU session reactivation result error cause information element

Table 9.11.3.43.1: PDU session reactivation result error cause information element

PDU session ID is coded same as PDU session ID IE (see subclause 9.4). The cause value is coded same as second octet of 5GMM cause information element (see subclause 9.11.3.2).

9.11.3.44 PDU session status

The purpose of the PDU session status information element is to indicate the state of each PDU session that can be identified by a PDU session identity.

The PDU session status information element is coded as shown in figure 9.11.3.44.1 and table 9.11.3.44.1.

The PDU session status information element is a type 4 information element with minimum length of 4 octets and a maximum length of 34 octets.

8	7	6	5	4	3	2	1	
PDU session status IEI								octet 1
Length of PDU session status contents								octet 2
PSI (7)	PSI (6)	PSI (5)	PSI (4)	PSI (3)	PSI (2)	PSI (1)	PSI (0)	octet 3
PSI (15)	PSI (14)	PSI (13)	PSI (12)	PSI (11)	PSI (10)	PSI (9)	PSI (8)	octet 4
0	0	0	0	0	0	0	0	octet 5*-34*
spare								

Figure 9.11.3.44.1: PDU session status information element

Table 9.11.3.44.1: PDU session status information element

PSI(x) shall be coded as follows: PSI(0): Bit 1 of octet 3 is spare and shall be coded as zero. PSI(1) – PSI(15): 0 indicates that the 5GSM state of the corresponding PDU session is PDU SESSION INACTIVE. 1 indicates that the 5GSM state of the corresponding PDU session is not PDU SESSION INACTIVE All bits in octet 5 to 34 are spare and shall be coded as zero, if the respective octet is included in the information element.

9.11.3.45 PLMN list

See subclause 10.5.1.13 in 3GPP TS 24.008 [12].

9.11.3.46 Rejected NSSAI

The purpose of the Rejected NSSAI information element is to identify a collection of rejected S-NSSAIs.

The Rejected NSSAI information element is coded as shown in figure 9.11.3.46.1, figure 9.11.3.46.2 and table 9.11.3.46.1.

The Rejected NSSAI is a type 4 information element with a minimum length of 4 octets and a maximum length of 42 octets.

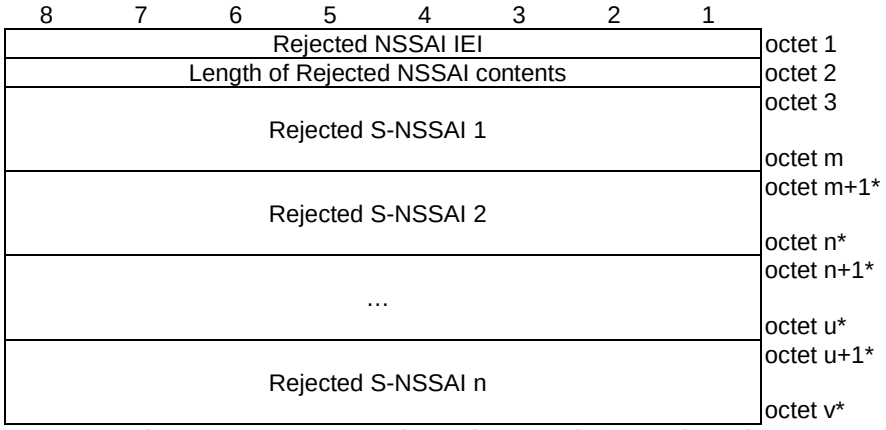


Figure 9.11.3.46.1: Rejected NSSAI information element

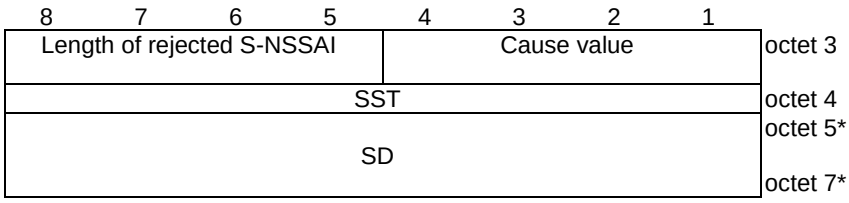


Figure 9.11.3.46.2: Rejected S-NSSAI

Table 9.11.3.46.1: Rejected NSSAI information element

Value part of the Rejected NSSAI information element (octet 3 to v)

The value part of the Rejected NSSAI information element consists of one or more rejected S-NSSAIs. Each rejected S-NSSAI consists of one S-NSSAI and an associated cause value. The length of each rejected S-NSSAI can be determined by the 'length of rejected S-NSSAI' field in the first octet of the rejected S-NSSAI.
The UE shall store the complete list received (NOTE 0). If more than 8 rejected S-NSSAIs are included in this information element, the UE shall store the first 8 rejected S-NSSAIs and ignore the remaining octets of the information element.

Rejected S-NSSAI:

Cause value (octet 3)
Bits

4	**3**	**2**	**1**	
0	0	0	0	S-NSSAI not available in the current PLMN or SNPN
0	0	0	1	S-NSSAI not available in the current registration area
0	0	1	0	S-NSSAI not available due to the failed or revoked network slice-specific authentication and authorization

All other values are reserved.

Slice/service type (SST) (octet 4)
This field contains the 8 bit SST value. The coding of the SST value part is defined in 3GPP TS 23.003 [4]. (NOTE 2)

Slice differentiator (SD) (octet 5 to octet 7)
This field contains the 24 bit SD value. The coding of the SD value part is defined in 3GPP TS 23.003 [4]. (NOTE 3)

NOTE 0: The number of rejected S-NSSAI(s) shall not exceed eight.
NOTE 1: If octet 5 is included, then octet 6 and octet 7 shall be included.
NOTE 2: If the Cause value is "S-NSSAI not available due to the failed or revoked network slice-specific authentication and authorization", this field shall contain the 8 bit SST value of an S-NSSAI in the S-NSSAI(s) of the HPLMN.
NOTE 3: If the Cause value is "S-NSSAI not available due to the failed or revoked network slice-specific authentication and authorization", this field, if included, shall contain the 24 bit SD value of an S-NSSAI in the S-NSSAI(s) of the HPLMN.

9.11.3.46A Release assistance indication

See subclause 9.9.4.25 in 3GPP TS 24.301 [15].

9.11.3.47 Request type

The purpose of the Request type information element is to indicate the type of the 5GSM message.

The Request type information element is coded as shown in figure 9.11.3.47.1 and table 9.11.3.47.1.

The Request type is a type 1 information element.

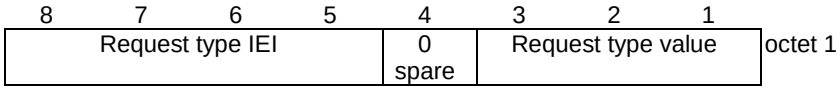


Figure 9.11.3.47.1: Request type information element

Table 9.11.3.47.1: Request type information element

Request type value (octet 1, bit 1 to bit 4) Bits 3 2 1 0 0 1 initial request 0 1 0 existing PDU session 0 1 1 initial emergency request 1 0 0 existing emergency PDU session 1 0 1 modification request 1 1 0 MA PDU request (NOTE) 1 1 1 reserved All other values are unused and shall be interpreted as "initial request", if received by the network.
NOTE: This value shall be interpreted as "initial request", if received by a network not supporting MA PDU sessions.

9.11.3.48 S1 UE network capability

See subclause 9.9.3.34 in 3GPP TS 24.301 [15].

9.11.3.48A S1 UE security capability

See subclause 9.9.3.36 in 3GPP TS 24.301 [15].

9.11.3.49 Service area list

The purpose of the Service area list information element is to transfer a list of allowed tracking areas for an allowed area or a list of non-allowed tracking areas for a non-allowed area from the network to the UE.

The coding of the information element allows combining different types of lists. The lists of type "00" and "01" allow a more compact encoding, when the different TAIs are sharing the PLMN identity. The lists of type "11" indicate all TAIs of the PLMNs in the registration area are allowed area.

The Service area list information element is coded as shown in figure 9.11.3.49.1, figure 9.11.3.49.2, figure 9.11.3.49.3, figure 9.11.3.49.4, figure 9.11.3.49.5 and table 9.11.3.49.1.

The Service area list is a type 4 information element with a minimum length of 6 octets and a maximum length of 114 octets. The list can contain a maximum of 16 different tracking area identities.

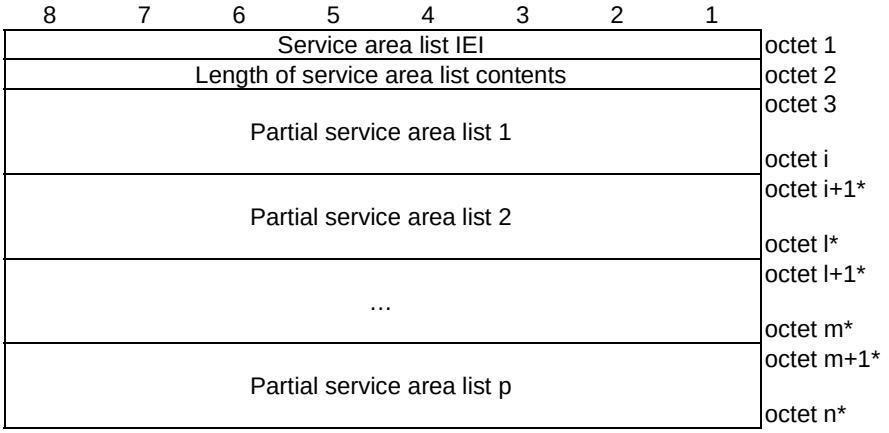


Figure 9.11.3.49.1: Service area list information element

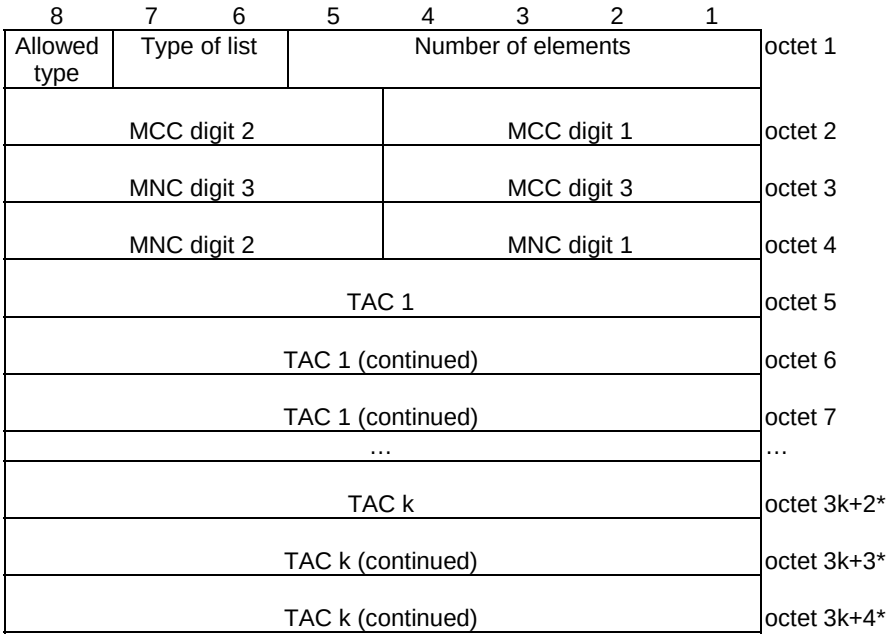


Figure 9.11.3.49.2: Partial service area list – type of list = "00"

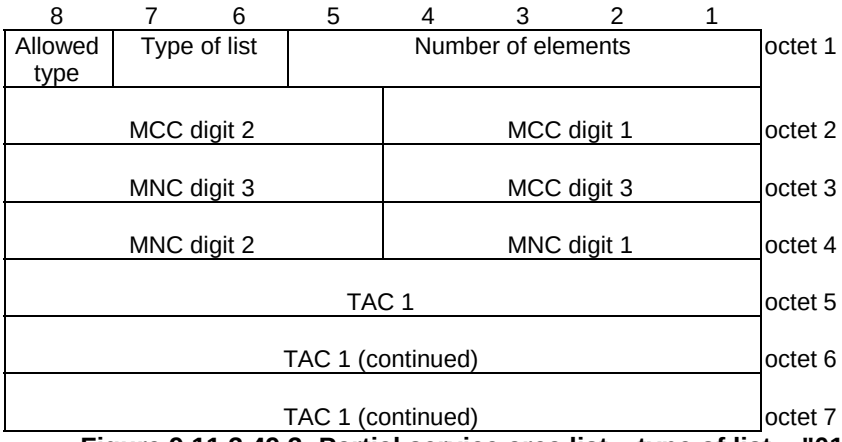


Figure 9.11.3.49.3: Partial service area list – type of list = "01"

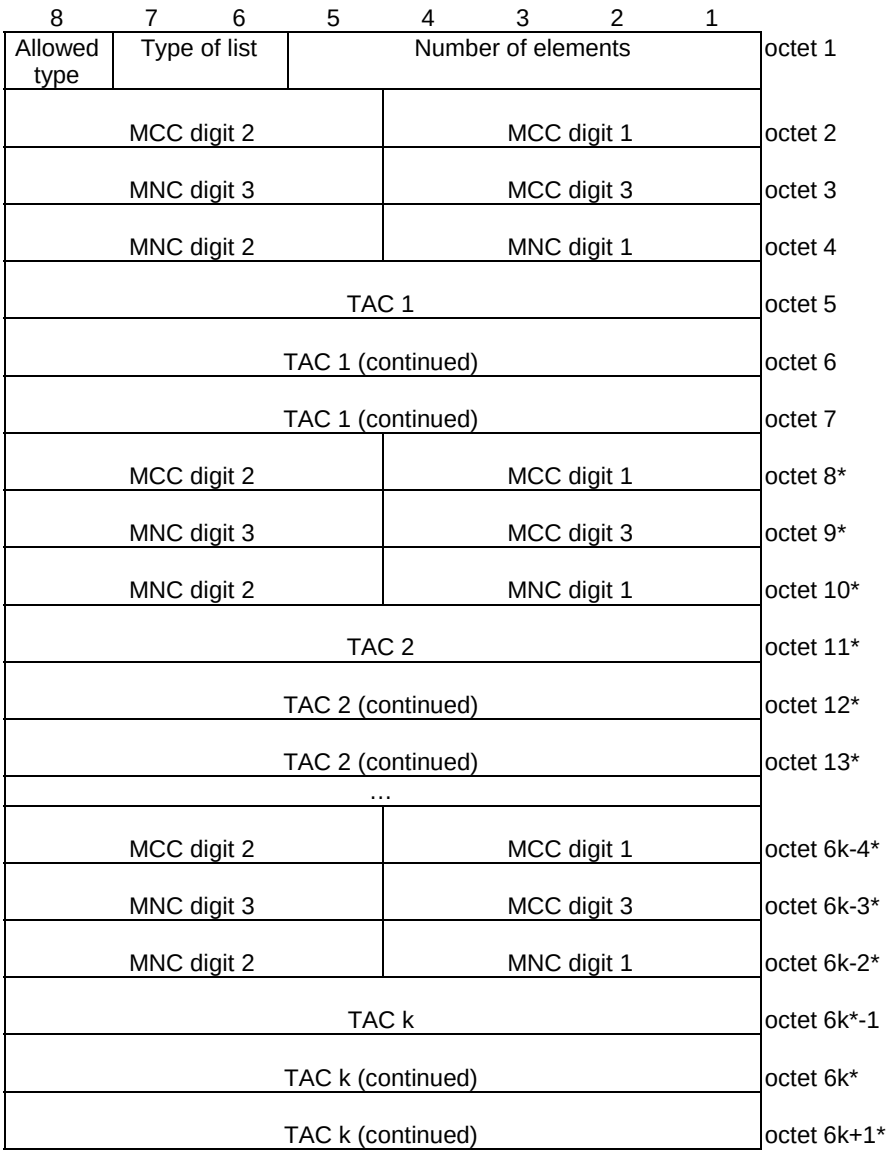


Figure 9.11.3.49.4: Partial service area list – type of list = "10"

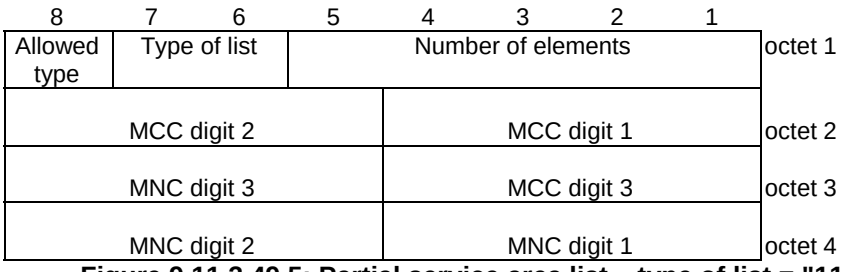


Figure 9.11.3.49.5: Partial service area list – type of list = "11"

Table 9.11.3.49.1: Service area list information element

Value part of the Service area list information element (octets 3 to n)

The value part of the Service area list information element consists of one or several partial service area lists. The length of each partial service area list can be determined from the 'type of list' field and the 'number of elements' field in the first octet of the partial service area list.
The "Allowed type" fields in all the partial service area lists shall have the same value. For allowed type "0", TAIs contained in all partial service area lists are in the allowed area. For allowed type "1", TAIs contained in all partial service area lists are in the non-allowed area.
The UE shall store the complete list received. If more than 16 TAIs are included in this information element, the UE shall store the first 16 TAIs and ignore the remaining octets of the information element.

Partial service area list:

Allowed type (octet 1)
Bit
8
0 TAIs in the list are in the allowed area
1 TAIs in the list are in the non-allowed area

Type of list (octet 1)
Bits
7 6
0 0 list of TACs belonging to one PLMN, with non-consecutive TAC values
0 1 list of TACs belonging to one PLMN, with consecutive TAC values
1 0 list of TAIs belonging to different PLMNs (see NOTE)
1 1 All TAIs belonging to the PLMNs in the registration area are in the allowed area

Number of elements (octet 1)
Bits

5	**4**	**3**	**2**	**1**	
0	0	0	0	0	1 element
0	0	0	0	1	2 elements
0	0	0	1	0	3 elements
		to			
0	1	1	0	1	14 elements
0	1	1	1	0	15 elements
0	1	1	1	1	16 elements

All other values are unused and shall be interpreted as 16, if received by the UE.

For type of list = "00" and number of elements = k:

octets 2 to 4 contain the MCC+MNC, and
for j = 1, …, k:
octets 3j+2 to 3j+4 contain the TAC of the j-th TAI belonging to the partial list,

For type of list = "01" and number of elements = k:

octets 2 to 4 contain the MCC+MNC, and
octets 5 to 7 contain the TAC of the first TAI belonging to the partial list.
The TAC values of the other k-1 TAIs are TAC+1, TAC+2, …, TAC+k-1.

For type of list = "10" and number of elements = k:

for j = 1, …, k.
octets 6j-4 to 6j-2 contain the MCC+MNC, and
octets 6j-1 to 6j+1 contain the TAC of the j-th TAI belonging to the partial list.

For type of list = "11":

Allowed type shall be coded as "0" and number of elements shall be ignored, and octets 2 to 4 containing the MCC+MNC can be ignored.
If allowed type is coded as "1", it shall be interpreted as "0".

MCC, Mobile country code

The MCC field is coded as in ITU-T Recommendation E.212 [42], annex A.

MNC, Mobile network code

The coding of this field is the responsibility of each administration but BCD coding shall be used. The MNC shall consist of 2 or 3 digits. If a network operator decides to use only two digits in the MNC, MNC digit 3 shall be coded as "1111".

TAC, Tracking area code

In the TAC field bit 8 of the first octet is the most significant bit and bit 1 of the third octet the least significant bit.
The coding of the tracking area code is the responsibility of each administration. Coding using full hexadecimal representation may be used. The tracking area code consists of 3 octets.

NOTE: If the "list of TAIs belonging to different PLMNs" is used, the PLMNs included in the list need to be present in the list of equivalent PLMNs. This type is not applicable in an SNPN.

9.11.3.50 Service type

The purpose of the service type information element is to specify the purpose of the service request procedure.

The service type is a type 1 information element.

The service type information element is coded as shown in figure 9.11.3.50.1 and table 9.11.3.50.1.

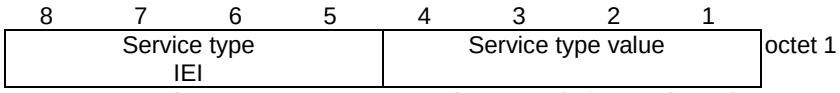


Figure 9.11.3.50.1: Service type information element

Table 9.11.3.50.1: Service type information element

Service type value (octet 1)

Service type value
Bits

4	3	2	1	
0	0	0	0	signalling
0	0	0	1	data
0	0	1	0	mobile terminated services
0	0	1	1	emergency services
0	1	0	0	emergency services fallback
0	1	0	1	high priority access
0	1	1	0	elevated signalling
0	1	1	1	unused; shall be interpreted as "signalling", if received by the network
1	0	0	0	unused; shall be interpreted as "signalling", if received by the network
1	0	0	1	unused; shall be interpreted as "data", if received by the network
1	0	1	0	unused; shall be interpreted as "data", if received by the network
1	0	1	1	unused; shall be interpreted as "data", if received by the network

All other values are reserved.

9.11.3.50A SMS indication

The purpose of the SMS indication information element is to indicate that the ability for the UE to use SMS over NAS has changed.

The SMS indication information element is coded as shown in figure 9.11.3.50A.1 and table 9.11.3.50A.1.

The SMS indication is a type 1 information element.

8	7	6	5	4	3	2	1	
SMS indication IEI				0 Spare	0 Spare	0 Spare	SAI	octet 1

Figure 9.11.3.50A.1: SMS indication

Table 9.11.3.50A.1: SMS indication

SMS availability indication (SAI) (octet 1) Bit 1 0 SMS over NAS not available 1 SMS over NAS available Bits 2, 3 and 4 are spare and shall be coded as zero,

9.11.3.51 SOR transparent container

The purpose of the SOR transparent container information element in the REGISTRATION ACCEPT message is to provide the list of preferred PLMN/access technology combinations (or HPLMN indication that 'no change of the "Operator Controlled PLMN Selector with Access Technology" list stored in the UE is needed and thus no list of preferred PLMN/access technology combinations is provided'), or a secured packet (see 3GPP TS 23.122 [5] annex C) and optional indication of an acknowledgement request, SOR-CMCI, request the storage of the received SOR-CMCI in the ME, SOR-SNPN-SI (or subscribed SNPN or HPLMN indication that 'no change of the SOR-SNPN-SI stored in the UE is needed and thus no SOR-SNPN-SI is provided'), and SOR-SNPN-SI-LS. The purpose of the SOR transparent container information element in the REGISTRATION COMPLETE message is to indicate the UE acknowledgement of successful reception of the SOR transparent container IE in the REGISTRATION ACCEPT message as well as to indicate the ME support of SOR-CMCI, the ME support of SOR-SNPN-SI and the ME support of SOR-SNPN-SI-LS.

NOTE 1: When used in NAS transport procedure, the contents of the SOR transparent container information element in the Payload container IE of the DL NAS TRANSPORT message are used to provide the list of preferred PLMN/access technology combinations and optional indication of an acknowledgement request, SOR-CMCI, request the storage of the received SOR-CMCI in the ME, SOR-SNPN-SI, and SOR-SNPN-SI-LS. The contents of the SOR transparent container information element in the Payload container IE of the UL NAS TRANSPORT message are used to indicate the UE acknowledgement of successful reception of the SOR transparent container IE in the DL NAS TRANSPORT message as well as to indicate the ME support of SOR-CMCI, the ME support of SOR-SNPN-SI and the ME support of SOR-SNPN-SI-LS.

NOTE 2: The "Operator controlled signal threshold per access technology" content to update the USIM file EF_{OCST} (see 3GPP TS 31.102 [22]) can be included in the secured packet of the SOR transparent container.

The SOR transparent container information element is coded as shown in figure 9.11.3.51.1, figure 9.11.3.51.2, figure 9.11.3.51.3, figure 9.11.3.51.4, figure 9.11.3.51.5, figure 9.11.3.51.6, figure 9.11.3.51.7, figure 9.11.3.51.8, figure 9.11.3.51.9, figure 9.11.3.51.9A, figure 9.11.3.51.10, figure 9.11.3.51.11, figure 9.11.3.51.11A, figure 9.11.3.51.11B, figure 9.11.3.51.11C, figure 9.11.3.51.11D, figure 9.11.3.51.11E, figure 9.11.3.51.11F, figure 9.11.3.51.11G, figure 9.11.3.51.11H, figure 9.11.3.51.11I, figure 9.11.3.51.12, figure 9.11.3.51.13, table 9.11.3.51.1, table 9.11.3.51.2, table 9.11.3.51.3, table 9.11.3.51.4, table 9.11.3.51.4A, table 9.11.3.51.5 and table 9.11.3.51.6.

The SOR transparent container is a type 6 information element with a minimum length of 20 octets.

8	7	6	5	4	3	2	1	
SOR transparent container IEI								octet 1
Length of SOR transparent container contents								octet 2 octet 3
SOR header								octet 4
SOR-MAC-I_{AUSF}								octet 5-20
$Counter_{SOR}$								octet 21-22
Secured packet								octet 23* - n*

Figure 9.11.3.51.1: SOR transparent container information element for list type with value "0" and SOR data type with value "0"

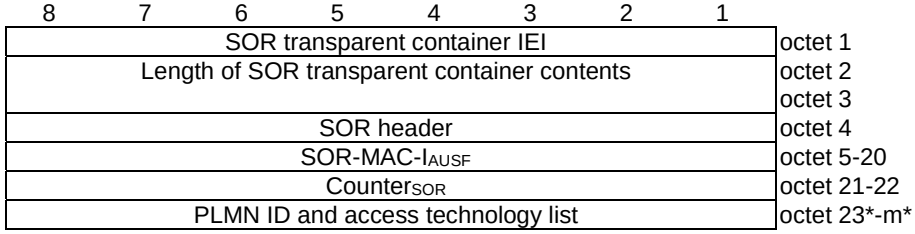


Figure 9.11.3.51.2: SOR transparent container information element for list type with value "1", SOR data type with value "0", and additional parameters with value "0"

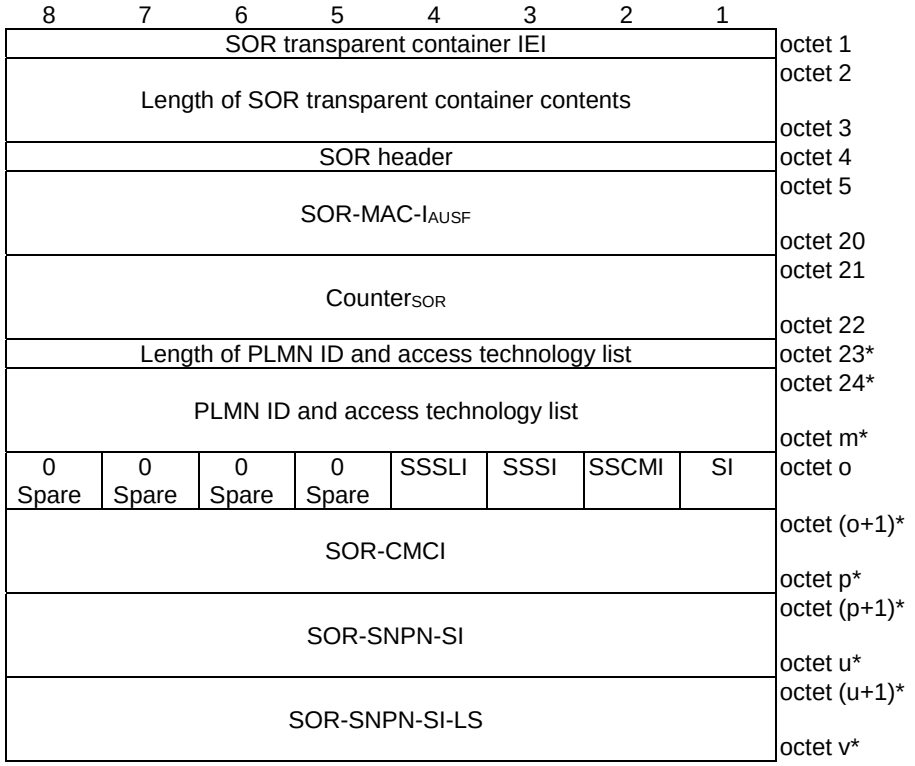


Figure 9.11.3.51.2A: SOR transparent container information element for list type with value "1", SOR data type with value "0", additional parameters with value "1"

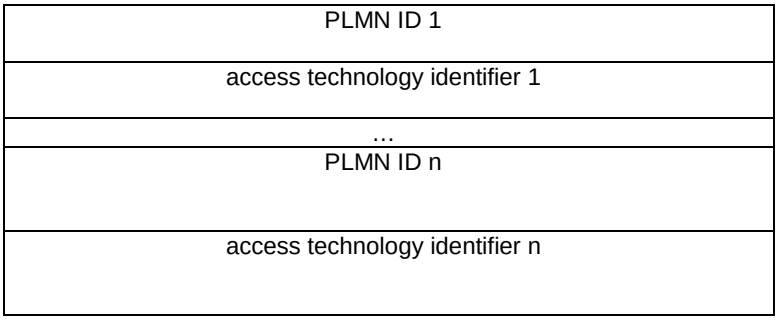


Figure 9.11.3.51.3: PLMN ID and access technology list (m=22+5*n)

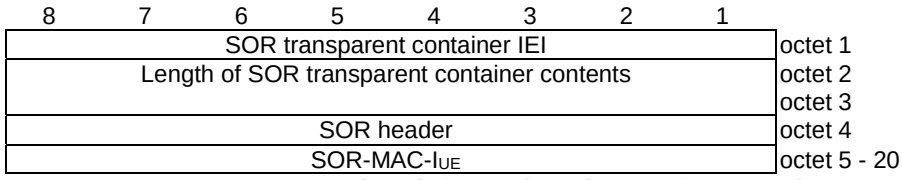


Figure 9.11.3.51.4: SOR transparent container information element for SOR data type with value "1"

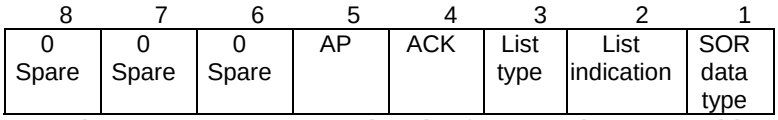


Figure 9.11.3.51.5: SOR header for SOR data type with value "0"

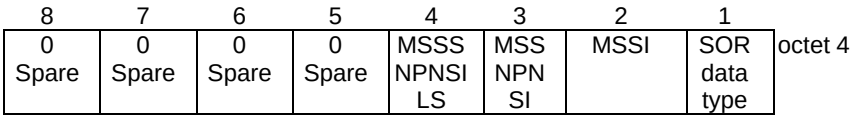


Figure 9.11.3.51.6: SOR header for SOR data type with value "1"

Table 9.11.3.51.1: SOR transparent container information element

SOR-MAC-I_{AUSF} (see NOTE 1), SOR-MAC-I_{UE} (see NOTE 2) and $Counter_{SOR}$ (see NOTE 1) are coded as specified in 3GPP TS 33.501 [24].

SOR data type (octet 4, bit 1)
0 The SOR transparent container carries steering of roaming information.
1 The SOR transparent container carries acknowledgement of successful reception of the steering of roaming information.

List indication (octet 4, bit 2) (see NOTE 1 and NOTE 5)
0 HPLMN indication that 'no change of the "Operator Controlled PLMN Selector with Access Technology" list stored in the UE is needed and thus no list of preferred PLMN/access technology combinations is provided'
1 list of preferred PLMN/access technology combinations is provided

List type (octet 4, bit 3) (see NOTE 1)
0 The list type is a secured packet.
1 The list type is a "PLMN ID and access technology list".

Acknowledgement (ACK) value (octet 4, bit 4) (see NOTE 1)
0 acknowledgement not requested
1 acknowledgement requested

Additional parameters (AP) value (octet 4, bit 5)
Bit
5
0 Additional parameters not included
1 Additional parameters included (see NOTE 3)

If the SOR data type is set to value "0", the list type bit is set to value "1", and the additional parameters bit is set to value "1" then:
- the octet o is present.
- if the list indication bit is set to "0" then the PLMN ID and access technology list field and the length of PLMN ID and access technology list field are absent.
- if the list indication bit is set to "1" then the PLMN ID and access technology list field and the length of PLMN ID and access technology list field are present.

The secure packet is coded as specified in 3GPP TS 31.115 [22B]. (see NOTE 1)

The PLMN ID and access technology list consists of PLMN ID and access technology identifier and are coded as specified in 3GPP TS 31.102 [22] subclause 4.2.5. The PLMN ID and access technology identifier are provided in decreasing order of priority, i.e. PLMN ID 1 indicates highest priority and PLMN ID n indicates lowest priority. The PLMN ID and access technology list contains at minimum zero and at maximum 16 (decimal) PLMN IDs and access technology identifiers. (see NOTE 1)

ME support of SOR-CMCI indicator (MSSI) value (octet 4, bit 2) (see NOTE 2, NOTE 4)
0 SOR-CMCI not supported by the ME
1 SOR-CMCI supported by the ME
ME support of SOR-SNPN-SI indicator (MSSNPNSI) value (octet 4, bit 3) (see NOTE 2, NOTE 6)
0 SOR-SNPN-SI not supported by the ME
1 SOR-SNPN-SI supported by the ME

MS support of SOR-SNPN-SI-LS indicator (MSSNPNSILS) value (octet 4, bit 4) (see NOTE 2)
Bit
4
0 SOR-SNPN-SI-LS not supported by the ME
1 SOR-SNPN-SI-LS supported by the ME

SOR-CMCI indicator (SI) value (octet o, bit 1)
Bit
1
0 SOR-CMCI absent
1 SOR-CMCI present

If the SOR-CMCI indicator bit is set to "SOR-CMCI present", the SOR-CMCI field is present. If the SI bit is set to "SOR-CMCI absent", the SOR-CMCI field is absent.

Store SOR-CMCI in ME indicator (SSCMI) value (octet o, bit 2)
Bit
2
0 Do not store SOR-CMCI in ME
1 Store SOR-CMCI in ME

SOR-CMCI (octet o+1 to octet p)
The SOR-CMCI field is coded according to figure 9.11.3.51.7 and table 9.11.3.51.2.

SOR-SNPN-SI indicator (SSSI) value (octet o, bit 3)
Bit
3
0 subscribed SNPN or HPLMN indication that 'no change of the SOR-SNPN-SI stored in the UE is needed and thus no SOR-SNPN-SI is provided'
1 SOR-SNPN-SI present

If the SSSI bit is set to "SOR-SNPN-SI present", the SOR-SNPN-SI field is present. If the SSSI bit is set to "subscribed SNPN or HPLMN indication that 'no change of the SOR-SNPN-SI stored in the UE is needed and thus no SOR-SNPN-SI is provided'", the SOR-SNPN-SI is absent.

SOR-SNPN-SI-LS indicator (SSSLI) value (octet o, bit 4)
Bit
4
0 SOR-SNPN-SI-LS absent
1 SOR-SNPN-SI-LS present

If the SSSLI bit is set to "SOR-SNPN-SI-LS present", the SOR-SNPN-SI-LS field is present. If the SSSLI bit is set to "SOR-SNPN-SI-LS absent", the SOR-SNPN-SI-LS is absent.

NOTE 1: This bit or field applies for SOR header with SOR data type with value "0".
NOTE 2: This bit or field applies for SOR header with SOR data type with value "1".
NOTE 3: Additional parameters can be set to value "1" only when the ME supports SOR-CMCI, SOR-SNPN-SI or SOR-SNPN-SI-LS, and the list type bit is set to value "1". The ME supporting SOR-SNPN-SI-LS supports SOR-SNPN-SI as specified in 3GPP TS 23.122 [5].
NOTE 4: The "SOR-CMCI supported by the ME" is not set by a UE compliant to an earlier release of the specification.
NOTE 5: This bit or field applies for SOR header with list type with value "1".
NOTE 6: The "SOR-SNPN-SI supported by the ME" may only be set by a UE which supports access to an SNPN using credentials from a credentials holder and which is not operating in SNPN access operation mode.

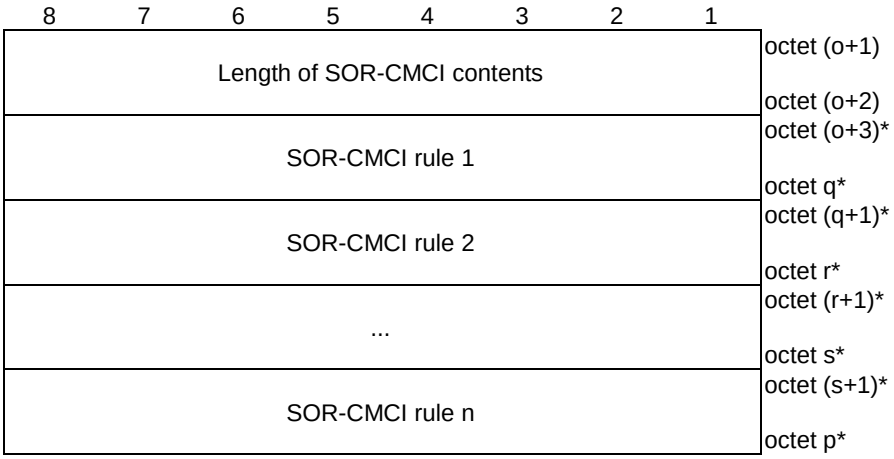


Figure 9.11.3.51.7: SOR-CMCI

Table 9.11.3.51.2: SOR-CMCI

SOR-CMCI rule: The SOR-CMCI rule is coded according to figure 9.11.3.51.8 and table 9.11.3.51.3. If the length of SOR-CMCI contents field indicates a length bigger than indicated in figure 9.11.3.51.7, receiving entity shall ignore any superfluous octets located at the end of the SOR-CMCI.

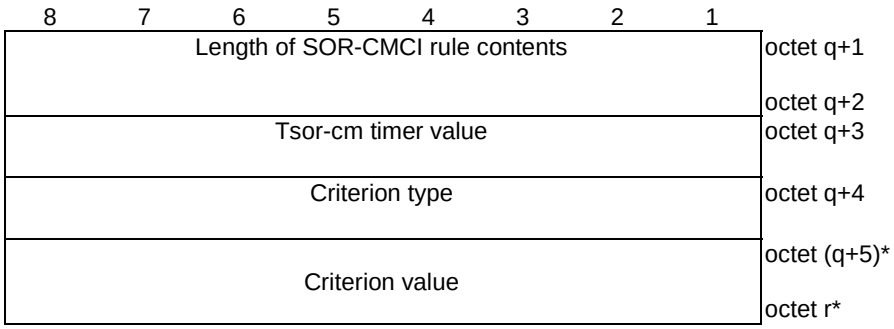


Figure 9.11.3.51.8: SOR-CMCI rule

Table 9.11.3.51.3: SOR-CMCI rule

Tsor-cm timer value
The Tsor-cm timer value field is coded according to octet 2 of the GPRS timer information element as specified in 3GPP TS 24.008 [12] subclause 10.5.7.3 and indicates the Tsor-cm timer value. When the unit field of the Tsor-cm timer value field indicates that the timer is deactivated, the receiving entity shall consider that Tsor-cm timer value is set to the infinity value.

Criterion type
Bits
8 7 6 5 4 3 2 1

0 0 0 0 0 0 0 1	DNN
0 0 0 0 0 0 1 0	S-NSSAI SST
0 0 0 0 0 0 1 1	S-NSSAI SST and SD
0 0 0 0 0 1 0 0	IMS registration related signalling
0 0 0 0 0 1 0 1	MMTEL voice call
0 0 0 0 0 1 1 0	MMTEL video call
0 0 0 0 0 1 1 1	SMS over NAS or SMSoIP
0 0 0 0 1 0 0 0	SOR security check not successful
1 1 1 1 1 1 1 1	match all

All other values are spare.

The receiving entity shall ignore SOR-CMCI rule with criterion of criterion type set to a spare value.

For "DNN", the criterion value field shall be encoded as a DNN length-value pair field.

For "S-NSSAI SST", the criterion value field shall be encoded as one octet SST field.

For "S-NSSAI SST and SD", the criterion value field shall be encoded as a sequence of one octet SST field and three octets SD field. The SST field shall be transmitted first.

The DNN length-value pair field shall be encoded as a sequence of one octet DNN value length field and a DNN value field. The DNN value length field shall be transmitted first. The DNN value length field indicates the length in octets of the DNN value field. The DNN value field contains an APN as specified in 3GPP TS 23.003 [4].

The SST field contains SST of HPLMN's S-NSSAI.

The SD field contains SD of HPLMN's S-NSSAI.

For "match all", "SOR security check not successful", "IMS registration related signalling", "MMTEL voice call", "MMTEL video call", and "SMS over NAS or SMSoIP", the criterion value field is zero octets long.

If the length of SOR-CMCI rule contents field indicates a length bigger than indicated in figure 9.11.3.51.8, receiving entity shll ignore any superfluous octets located at the end of the SOR-CMCI rule.

The UE applies SOR-CMCI rules as described in 3GPP TS 23.122 [5] annex C.

8	7	6	5	4	3	2	1	
Length of SOR-SNPN-SI contents								octet (p+1) octet (p+2)
0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	CLGI	CLSI	octet (p+3)
CH controlled prioritized list of preferred SNPNs								octet (p+4)* octet t*
CH controlled prioritized list of GINs								octet (t+1)* octet u*

Figure 9.11.3.51.9: SOR-SNPN-SI

Table 9.11.3.51.4: SOR-SNPN-SI

CH controlled prioritized list of preferred SNPNs indicator (CLSI) value (octet p+3, bit 1)
Bit
1
0 CH controlled prioritized list of preferred SNPNs absent
1 CH controlled prioritized list of preferred SNPNs present

If the CLSI bit is set to "CH controlled prioritized list of preferred SNPNs present", the CH controlled prioritized list of preferred SNPNs field is present. If the CLSI bit is set to "CH controlled prioritized list of preferred SNPNs absent", the CH controlled prioritized list of preferred SNPNs field is absent.

CH controlled prioritized list of GINs indicator (CLGI) value (octet p+3, bit 2)
Bit
2
0 CH controlled prioritized list of GINs absent
1 CH controlled prioritized list of GINs present

If the CLGI bit is set to "CH controlled prioritized list of GINs present", the CH controlled prioritized list of GINs field is present. If the CLGI bit is set to "CH controlled prioritized list of GINs absent", the CH controlled prioritized list of GINs field is absent.

If the length of SOR-SNPN-SI contents field indicates a length bigger than indicated in figure 9.11.3.51.9, receiving entity shall ignore any superfluous octets located at the end of the SOR-SNPN-SI.

8	7	6	5	4	3	2	1	
Length of SOR-SNPN-SI-LS contents								octet (u+1) octet (u+2)
0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	CLGLSI	CLSLSI	octet (u+3)
CH controlled prioritized list of preferred SNPNs for access for localized services in SNPN								octet (w+1)* octet x*
CH controlled prioritized list of preferred GINs for access for localized services in SNPN								octet (x+1)* octet v*

Figure 9.11.3.51.9A: SOR-SNPN-SI-LS

Table 9.11.3.51.4A: SOR-SNPN-SI-LS

CH controlled prioritized list of preferred SNPNs for access for localized services in SNPN indicator (CLSLSI) value (octet u+3, bit 1)
Bit
1
0 CH controlled prioritized list of preferred SNPNs for access for localized services in SNPN absent
1 CH controlled prioritized list of preferred SNPNs for access for localized services in SNPN present

If the CLSLSI bit is set to " CH controlled prioritized list of preferred SNPNs for access for localized services in SNPN present", the CH controlled prioritized list of preferred SNPNs for access for localized services in SNPN field is present. If the CLSLSI bit is set to " CH controlled prioritized list of preferred SNPNs for access for localized services in SNPN absent", the CH controlled prioritized list of preferred SNPNs for access for localized services in SNPN field is absent.

CH controlled prioritized list of preferred GINs for access for localized services in SNPN indicator (CLGLSI) value (octet u+3, bit 2)
Bit
2
0 CH controlled prioritized list of preferred GINs for access for localized services in SNPN absent
1 CH controlled prioritized list of preferred GINs for access for localized services in SNPN present

If the CLGLSI bit is set to " CH controlled prioritized list of preferred GINs for access for localized services in SNPN present", the CH controlled prioritized list of preferred GINs for access for localized services in SNPN field is present. If the CLGLSI bit is set to " CH controlled prioritized list of preferred GINs for access for localized services in SNPN absent", the CH controlled prioritized list of preferred GINs for access for localized services in SNPN field is absent.

If the length of SOR-SNPN-SI-LS contents field indicates a length bigger than indicated in figure 9.11.3.51.9A, receiving entity shall ignore any superfluous octets located at the end of the SOR-SNPN-SI.

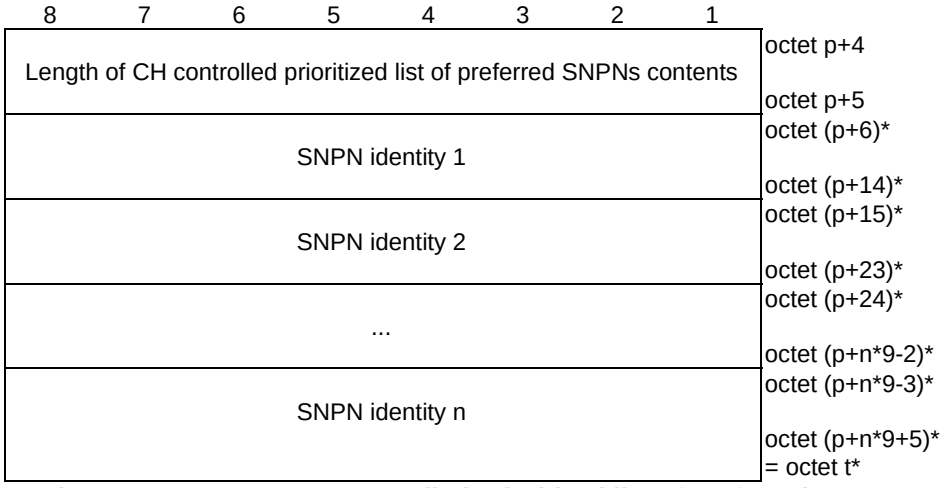


Figure 9.11.3.51.10: CH controlled prioritized list of preferred SNPNs

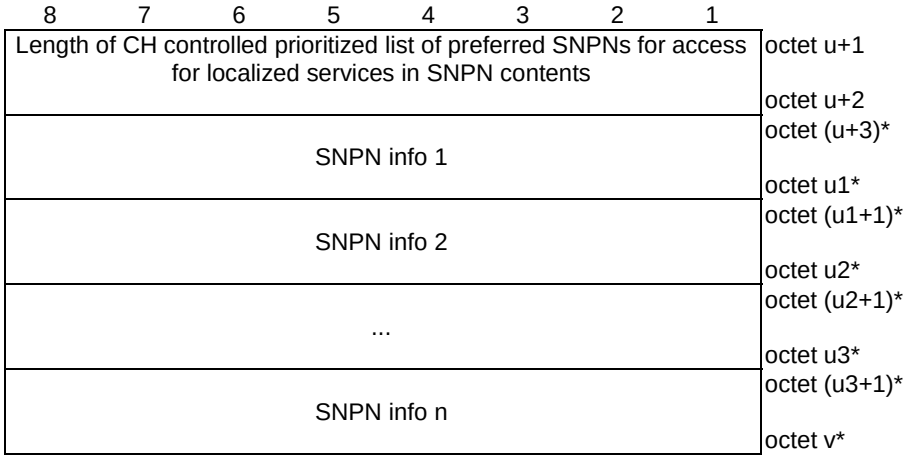


Figure 9.11.3.51.10A: CH controlled prioritized list of preferred SNPNs for access for localized services in SNPN

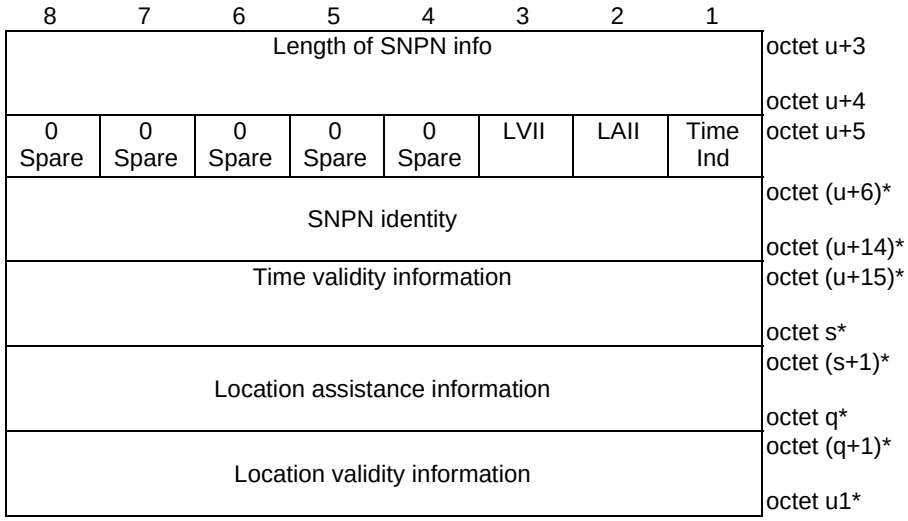


Figure 9.11.3.51.10B: SNPN info

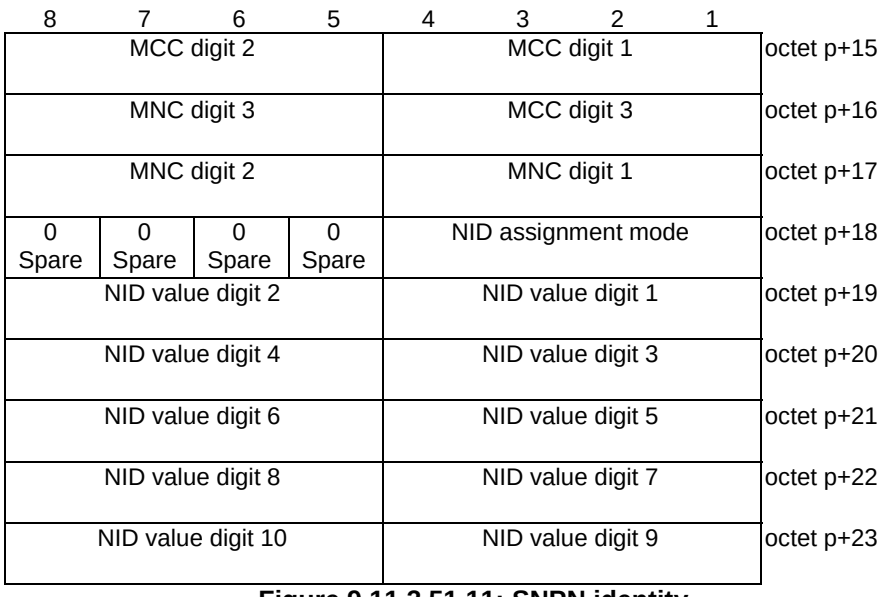


Figure 9.11.3.51.11: SNPN identity

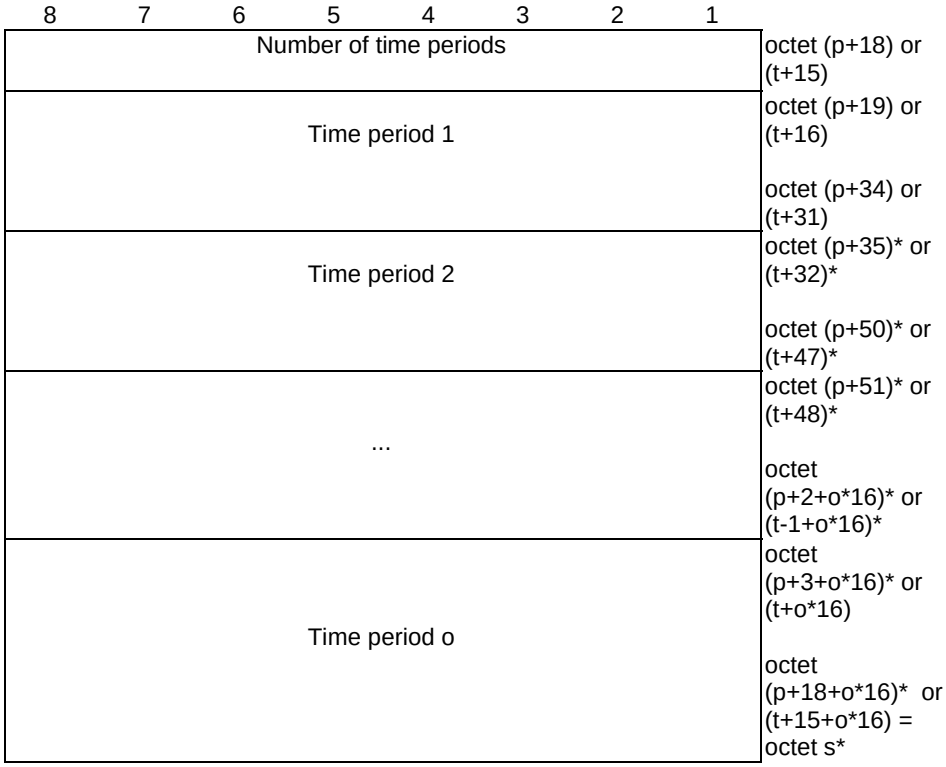


Figure 9.11.3.51.11A: Time validity information

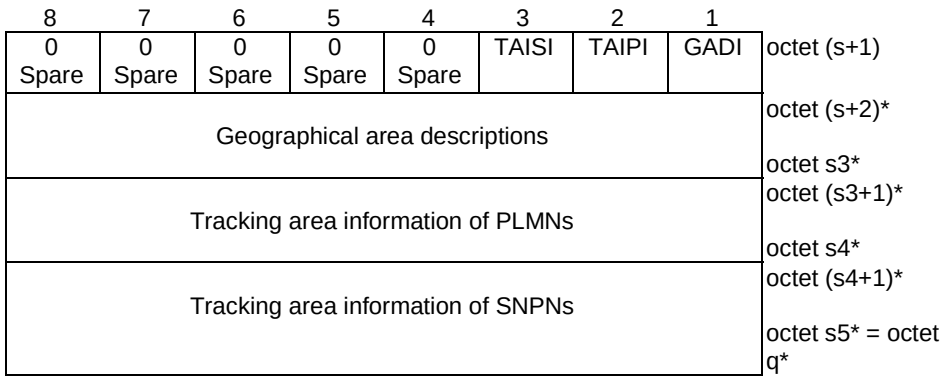


Figure 9.11.3.51.11B: Location assistance information

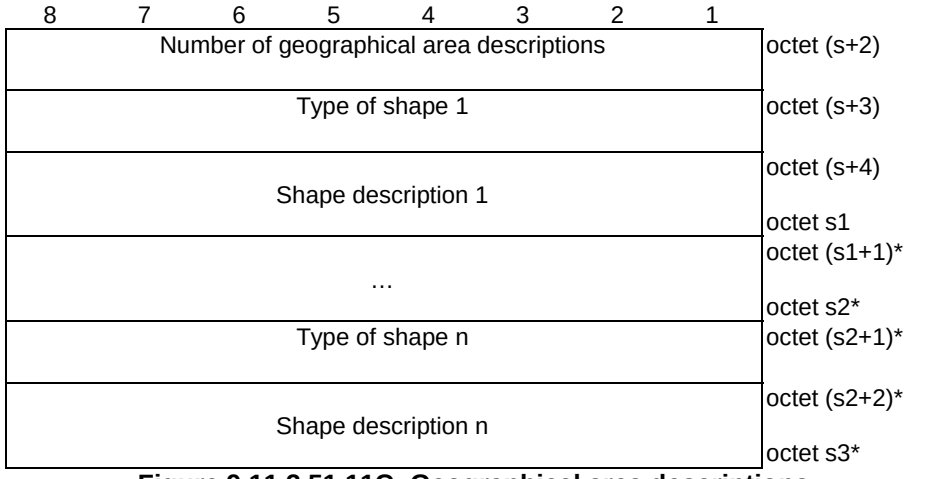


Figure 9.11.3.51.11C: Geographical area descriptions

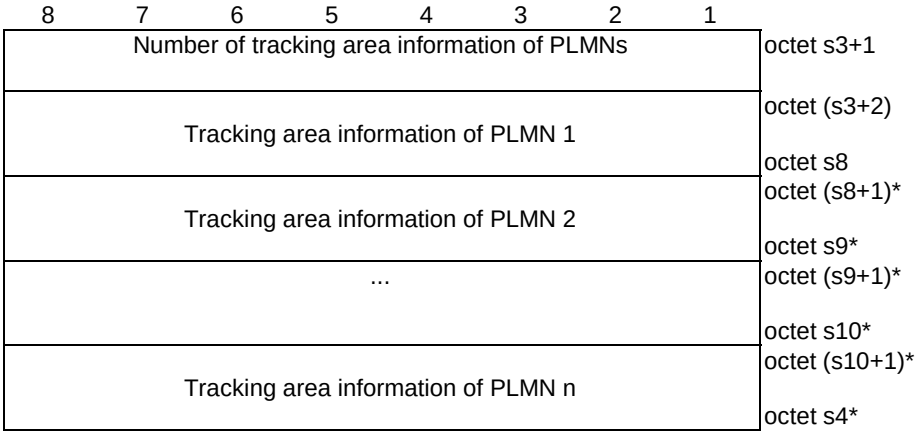


Figure 9.11.3.51.11D: Tracking area information of PLMNs

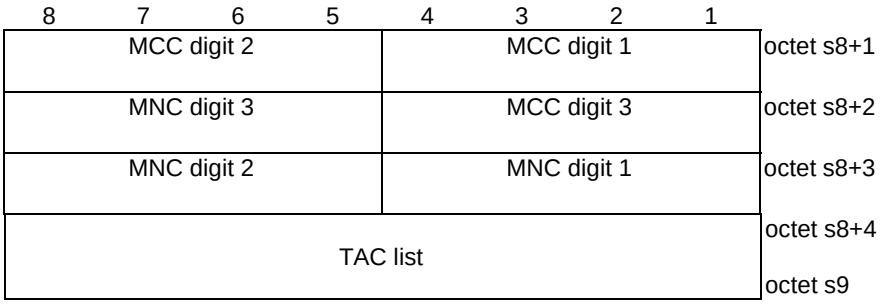


Figure 9.11.3.51.11E: Tracking area information of PLMN

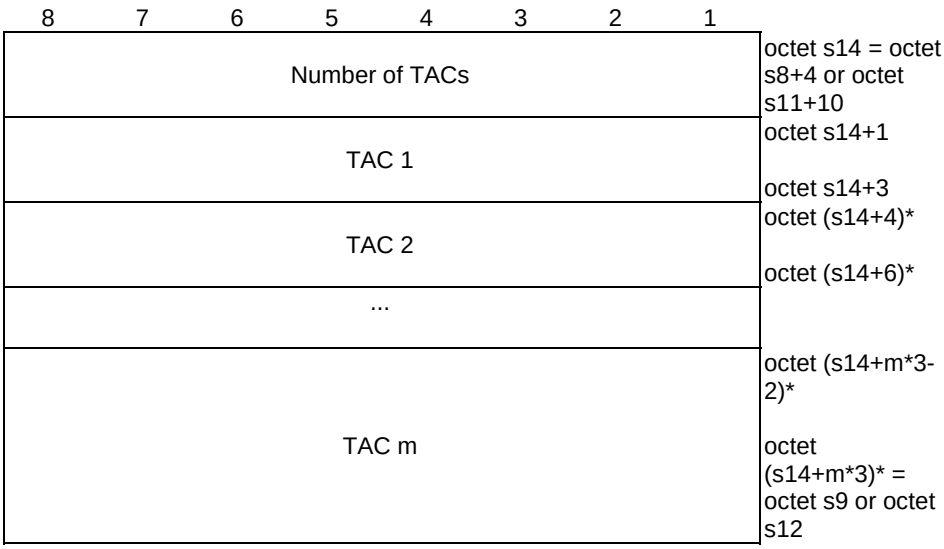


Figure 9.11.3.51.11F: TAC list

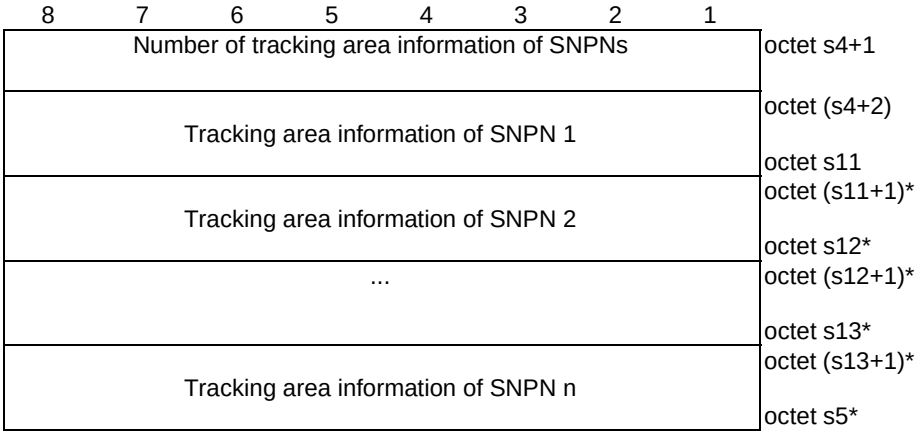


Figure 9.11.3.51.11G: Tracking area information of SNPNs

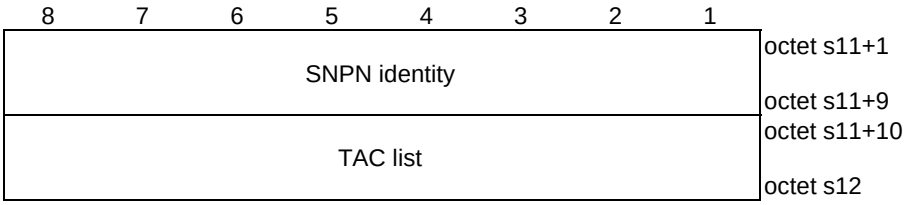


Figure 9.11.3.51.11H: Tracking area information of SNPN

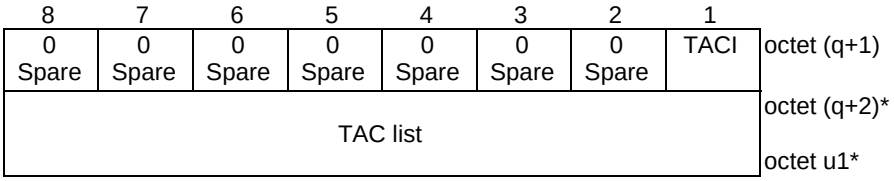


Figure 9.11.3.51.11I: Location validity information

Table 9.11.3.51.5: CH controlled prioritized list of preferred SNPNs and CH controlled prioritized list of preferred SNPNs for access for localized services in SNPN

Mobile country code (MCC):
The MCC field is coded as in ITU-T Recommendation E.212 [42], annex A.

Mobile network code (MNC):
The coding of MNC field is the responsibility of each administration but BCD coding shall be used. The MNC shall consist of 2 or 3 digits. If a network operator decides to use only two digits in the MNC, MNC digit 3 shall be coded as "1111".

NID assignment mode (see NOTE 1)
NID assignment mode is coded as specified in 3GPP TS 23.003 [4].

NID value (see NOTE 1)
NID value is coded as specified in 3GPP TS 23.003 [4].

Time indication (bit1 of octet u+5)
Bit
1
0 Time validity infomation not included
1 Time validity infomationinformation is included

Location assistance information indicator (LAII) (bit 2 of octet u+5)
Bit
2
0 Location assistance information not included
1 Location assistance information included

Location validity information indicator (LVII) (bit 3 of octet u+5)
Bit
3
0 Location validity information not included
1 Location validity information included

Tracking area code list indicator (TACI) (bit 1 of octet q+1) (see NOTE 2)
Bit
2
0 TAC list not included
1 TAC list included

Geographical area descriptions indicator (GADI) (bit 1 of octet s+1)
Bit
1
0 Geographical area descriptions not included
1 Geographical area descriptions included

Tracking area information of PLMNs (TAIPI) (bit 2 of octet s+1)
Bit
2
0 Tracking area information of PLMNs not included
1 Tracking area information of PLMNs included

Tracking area information of SNPNs (TAISI) (bit 3 of octet s+1)
Bit
3
0 Tracking area information of SNPNs not included
1 Tracking area information of SNPNs included

Location assistance information
Location assistance information field contains the geographical area descriptions field, the tracking area information of PLMNs field, the tracking area information of SNPNs field. or any combination of them.

Time period
The time period field is coded as the route selection descriptor component value field for "time window type" specified in 3GPP TS 24.526 [19] table 5.2.1.

Type of shape
Type of shape is coded as specified in Table 2a in 3GPP TS 23.032 [4B].

Shape description
Shape description is coded as specified in subclause 7.3 in 3GPP TS 23.032 [4B].

Tracking area information of PLMNs
Tracking area information of PLMNs field contains one or more tracking area information of PLMN fields.

Tracking area information of PLMN
Tracking area information of PLMN field contains an MCC and MNC of a PLMN identity and a TAC list field containing one or more tracking area code fields, each indicating a TAC of a PLMN identified by the PLMN identity.

Tracking area information of SNPNs
Tracking area information of SNPNs field contains one or more tracking area information of SNPN fields.
If the tracking area information of SNPNs field is included in a location assistance information field of an SNPN info field, the SNPN identity field in each tracking area information of SNPN field of the tracking area information of SNPNs field is different from the SNPN identity field in the SNPN info field.

Tracking area information of SNPN
Tracking area information of SNPN field contains SNPN identity and a TAC list containing one or more tracking area code fields, each indicating a TAC of an SNPN identified by the SNPN identity.

Tracking area code (TAC)
In the TAC field bit 8 of the first octet is the most significant bit and bit 1 of third octet the least significant bit.
The coding of the tracking area code is the responsibility of each administration. Coding using full hexadecimal representation may be used. The tracking area code consists of 3 octets.

NOTE 1: NID coding deviates from coding of value part of NID IE as specified in subclause 9.2.7 of 3GPP TS 24.502 [18], coding of the NID field of the SNPN list IE as specified in subclause 9.11.3.92, and coding of the NID field of the SNPN list with trusted 5G connectivity IE as specified in subclause H.2.4.7 of 3GPP TS 24.302 [16].
NOTE 2: If the location validity information indicator is set to 'Location validity information included' but TAC list indicator is set to 'TAC list not included', the UE shall ignore the location validity information.

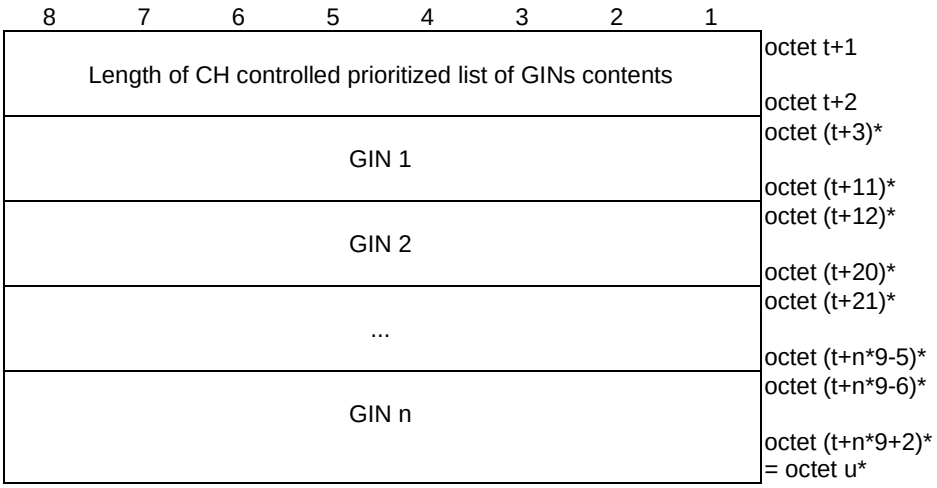


Figure 9.11.3.51.12: CH controlled prioritized list of GINs

8	7	6	5	4	3	2	1	
Length of CH controlled prioritized list of preferred GINs for access for localized services in SNPN contents								octet v+1 octet v+2
GIN info 1								octet (v+3)* octet v1*
GIN info 2								octet (v1+1)* octet v2*
...								octet (v2+1)* octet v3*
GIN info n								octet (v3+1)* octet w*

Figure 9.11.3.51.12A: CH controlled prioritized list of preferred GINs for access for localized services in SNPN

8	7	6	5	4	3	2	1	
Length of GIN info								octet v+3 octet v+4
0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	LVII	LAII	Time Ind	octet v+5
GIN								octet (v+6)* octet (v+14)*
Time validity information								octet (v+15)* octet s*
Location assistance information								octet (s+1)* octet q*
Location validity information								octet (q+1)* octet v1*

Figure 9.11.3.51.12B: GIN info

8	7	6	5	4	3	2	1	
MCC digit 2				MCC digit 1				octet t+12
MNC digit 3				MCC digit 3				octet t+13
MNC digit 2				MNC digit 1				octet t+14
0 Spare	0 Spare	0 Spare	0 Spare	NID assignment mode				octet t+15
NID value digit 2				NID value digit 1				octet t+16
NID value digit 4				NID value digit 3				octet t+17
NID value digit 6				NID value digit 5				octet t+18
NID value digit 8				NID value digit 7				octet t+19
NID value digit 10				NID value digit 9				octet t+20

Figure 9.11.3.51.13: GIN

Table 9.11.3.51.6: CH controlled prioritized list of GINs and CH controlled prioritized list of preferred GINs for access for localized services in SNPN

Mobile country code (MCC): The MCC field is coded as in ITU-T Recommendation E.212 [42], annex A. Mobile network code (MNC): The coding of MNC field is the responsibility of each administration but BCD coding shall be used. The MNC shall consist of 2 or 3 digits. If a network operator decides to use only two digits in the MNC, MNC digit 3 shall be coded as "1111". NID assignment mode (see NOTE) NID assignment mode is coded as specified in 3GPP TS 23.003 [4]. NID value (see NOTE) NID value is coded as specified in 3GPP TS 23.003 [4]. Time indication (bit1 of octet v+5) Bit 1 0 Time validity information not included 1 Time validity information included Location assistance information indicator (LAII) (bit 2 of octet v+5) Bit **2** 0 Location assistance information not included 1 Location assistance information included Location validity information indicator (LVII) (bit 3 of octet v+5) Bit **3** 0 Location validity information not included 1 Location validity information included Time period The time period field is coded as the route selection descriptor component value field for "time window type" specified in 3GPP TS 24.526 [19] table 5.2.1. Location assistance information (oct(s+1)* to (q)*) The Location assistance information is coded according to Figure 9.11.3.51.11B and Table 9.11.3.51.5.
NOTE: NID coding deviates from coding of value part of NID IE as specified in subclause 9.2.7 of 3GPP TS 24.502 [18], coding of the NID field of the SNPN list IE as specified in subclause 9.11.3.92, and coding of the NID field of the SNPN list with trusted 5G connectivity IE as specified in subclause H.2.4.7 of 3GPP TS 24.302 [16].

9.11.3.51A Supported codec list

See subclause 10.5.4.32 in 3GPP TS 24.008 [12].

9.11.3.52 Time zone

See subclause 10.5.3.8 in 3GPP TS 24.008 [12].

9.11.3.53 Time zone and time

See subclause 10.5.3.9 in 3GPP TS 24.008 [12].

9.11.3.53A UE parameters update transparent container

The purpose of the UE parameters update transparent container when sent from the network to the UE is to provide UE parameters update data, optional acknowledgement request and optional re-registration request. The purpose of the UE

parameters update transparent container when sent from the UE to the network is to indicate the UE acknowledgement of successful reception of the UE parameters update transparent container.

The UE parameters update transparent container information element is coded as shown in figure 9.11.3.53A.1, figure 9.11.3.53A.2, figure 9.11.3.53A.3, figure 9.11.3.53A.4, figure 9.11.3.53A.4B, figure 9.11.3.53A.5, figure 9.11.3.53A.6, figure 9.11.3.53A.7 and table 9.11.3.53A.1.

The UE parameters update transparent container is a type 6 information element with a minimum length of 20 octets.

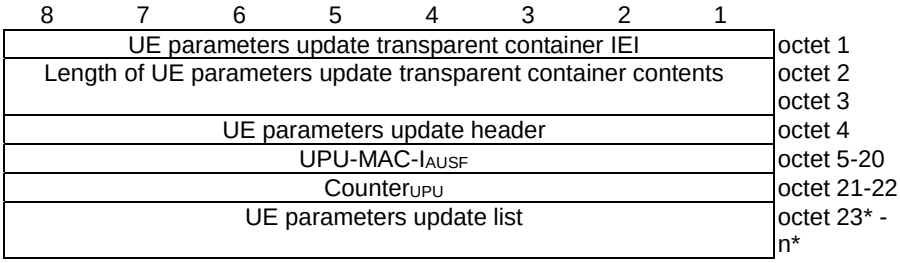


Figure 9.11.3.53A.1: UE parameters update transparent container information element for UE parameters update data type with value "0"

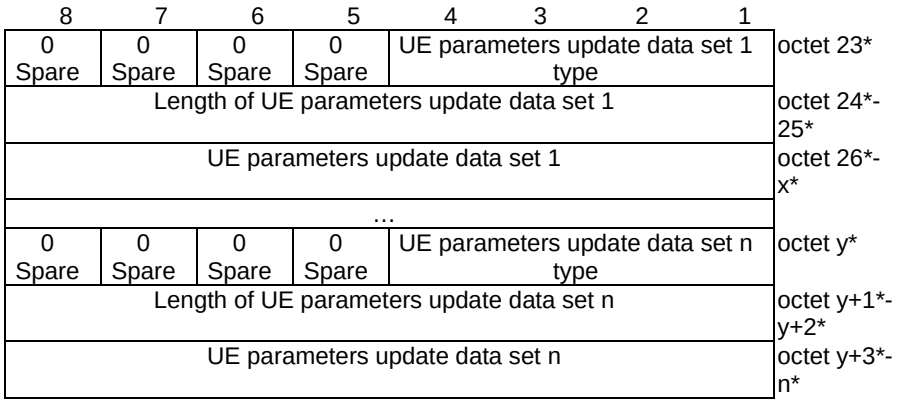


Figure 9.11.3.53A.2: UE parameters update list

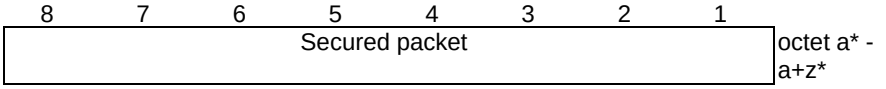


Figure 9.11.3.53A.3: UE parameters update data set for UE parameters update data set type with value "0001"

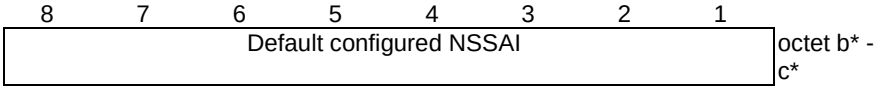


Figure 9.11.3.53A.4: UE parameters update data set for UE parameters update data set type with value "0010"

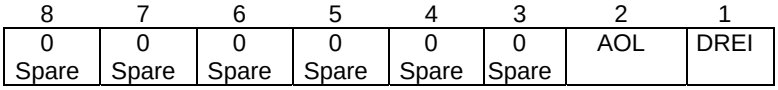


Figure 9.11.3.53A.4A: UE parameters update data set for UE parameters update data set type with value "0011"

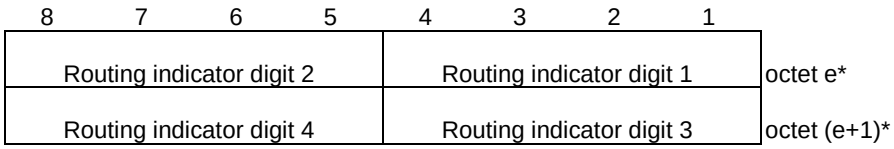


Figure 9.11.3.53A.4B: UE parameters update data set for UE parameters update data set type with value "0100"

UE parameters update transparent container IEI	octet 1
Length of UE parameters update transparent container contents	octet 2 octet 3
UE parameters update header	octet 4
UPU-MAC-I_{UE}	octet 5 - 20

Figure 9.11.3.53A.5: UE parameters update transparent container information element for UE parameters update data type with value "1"

8	7	6	5	4	3	2	1	
0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	REG	ACK	UPU data type	octet 4

Figure 9.11.3.53A.6: UE parameters update header for UE parameters update data type with value "0"

8	7	6	5	4	3	2	1	
0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	UPU data type	octet 4

Figure 9.11.3.53A.7: UE parameters update header for UE parameters update data type with value "1"

Table 9.11.3.53A.1: UE parameters update transparent container information element

UPU-MAC-I_{AUSF}, UPU-MAC-I_{UE} and $Counter_{UPU}$ are coded as specified in 3GPP TS 33.501 [24] UPU data type (octet 4, bit 1) 0 The UE parameters update transparent container carries a UE parameters update list 1 The UE parameters update transparent container carries an acknowledgement of successful reception of a UE parameters update list Acknowledgement (ACK) value (octet 4, bit 2) 0 acknowledgement not requested 1 acknowledgement requested Re-registration (REG) value (octet 4, bit 3) 0 re-registration not requested 1 re-registration requested UE parameters update data set type Bits 4 3 2 1 0 0 0 1 Routing indicator update data 0 0 1 0 Default configured NSSAI update data 0 0 1 1 Disaster roaming information update data 0 1 0 0 ME routing indicator update data All other values are reserved Disaster Roaming Enabled Indication (DREI) value (octet d*, bit 1) 0 Disaster roaming is disabled in the UE 1 Disaster roaming is enabled in the UE Indication of 'applicability of "lists of PLMN(s) to be used in disaster condition" provided by a VPLMN' (AOL) value (octet d*, bit 2) 0 false 1 true The secured packet is coded as specified in 3GPP TS 31.115 [22B]. The default configured NSSAI is encoded as the value part of the NSSAI IE (see subclause 9.11.3.37). Routing indicator Routing indicator is encoded as the routing indicator field of the 5GS mobile identity IE (see subclause 9.11.3.4).
NOTE: When the routing indicator is updated, if the SNPN uses the EAP based primary authentication and key agreement procedure using the EAP-AKA' or the 5G AKA based primary authentication and key agreement procedure, then UE parameter update data set type is set to "routing indicator update data", otherwise, UE parameter update data set type is set to "ME routing indicator update data".

9.11.3.54 UE security capability

The UE security capability information element is used by the UE and by the network to indicate which security algorithms are supported by the UE in N1 mode for NAS security as well as which security algorithms are supported over NR and E-UTRA connected to 5GCN for AS security.

The UE security capability information element is coded as shown in figure 9.11.3.54.1 and table 9.11.3.54.1.

The UE security capability is a type 4 information element with a minimum length of 4 octets and a maximum length of 10 octets.

Octets 5 to 10 are optional. If octet 5 is included, then also octet 6 shall be included.

If the UE does not support any security algorithm for AS security over E-UTRA connected to 5GCN, it shall not include octets 5 and 6. The UE shall not include octets 7 to 10.

If the UE does not support any security algorithm for AS security over E-UTRA connected to 5GCN, and if the network includes octets 7 to 10, then the network shall also include octets 5 to 6.

If the network includes octet 7, then it shall include also octet 8. If the network includes octet 9, then it shall include also octet 10.

8	7	6	5	4	3	2	1	
UE security capability IEI								octet 1
Length of UE security capability contents								octet 2
5G-EA0	128-5G-EA1	128-5G-EA2	128-5G-EA3	5G-EA4	5G-EA5	5G-EA6	5G-EA7	octet 3
5G-IA0	128-5G-IA1	128-5G-IA2	128-5G-IA3	5G-IA4	5G-IA5	5G-IA6	5G-IA7	octet 4
EEA0	128-EEA1	128-EEA2	128-EEA3	EEA4	EEA5	EEA6	EEA7	octet 5*
EIA0	128-EIA1	128-EIA2	128-EIA3	EIA4	EIA5	EIA6	EIA7	octet 6*
0	0	0	0	0	0	0	0	
Spare								octet 7* -10*

Figure 9.11.3.54.1: UE security capability information element

Table 9.11.3.54.1: UE security capability information element

5GS encryption algorithms supported (see NOTE 1) (octet 3)

5GS encryption algorithm 5G-EA0 supported (octet 3, bit 8)
0 5GS encryption algorithm 5G-EA0 not supported
1 5GS encryption algorithm 5G-EA0 supported

5GS encryption algorithm 128-5G-EA1 supported (octet 3, bit 7)
0 5GS encryption algorithm 128-5G-EA1 not supported
1 5GS encryption algorithm 128-5G-EA1 supported

5GS encryption algorithm 128-5G-EA2 supported (octet 3, bit 6)
0 5GS encryption algorithm 128-5G-EA2 not supported
1 5GS encryption algorithm 128-5G-EA2 supported

5GS encryption algorithm 128-5G-EA3 supported (octet 3, bit 5)
0 5GS encryption algorithm 128-5G-EA3 not supported
1 5GS encryption algorithm 128-5G-EA3 supported

5GS encryption algorithm 5G-EA4 supported (octet 3, bit 4)
0 5GS encryption algorithm 5G-EA4 not supported
1 5GS encryption algorithm 5G-EA4 supported

5GS encryption algorithm 5G-EA5 supported (octet 3, bit 3)
0 5GS encryption algorithm 5G-EA5 not supported
1 5GS encryption algorithm 5G-EA5 supported

5GS encryption algorithm 5G-EA6 supported (octet 3, bit 2)
0 5GS encryption algorithm 5G-EA6 not supported
1 5GS encryption algorithm 5G-EA6 supported

5GS encryption algorithm 5G-EA7 supported (octet 3, bit 1)
0 5GS encryption algorithm 5G-EA7 not supported
1 5GS encryption algorithm 5G-EA7 supported

5GS integrity algorithms supported (see NOTE 2) (octet 4)

5GS integrity algorithm 5G-IA0 supported (octet 4, bit 8)
0 5GS integrity algorithm 5G-IA0 not supported
1 5GS integrity algorithm 5G-IA0 supported

5GS integrity algorithm 128-5G-IA1 supported (octet 4, bit 7)
0 5GS integrity algorithm 128-5G-IA1 not supported
1 5GS integrity algorithm 128-5G-IA1 supported

5GS integrity algorithm 128-5G-IA2 supported (octet 4, bit 6)
0 5GS integrity algorithm 128-5G-IA2 not supported
1 5GS integrity algorithm 128-5G-IA2 supported

5GS integrity algorithm 128-5G-IA3 supported (octet 4, bit 5)
0 5GS integrity algorithm 128-5G-IA3 not supported
1 5GS integrity algorithm 128-5G-IA3 supported

5GS integrity algorithm 5G-IA4 supported (octet 4, bit 4)
0 5GS integrity algorithm 5G-IA4 not supported
1 5GS integrity algorithm 5G-IA4 supported

5GS integrity algorithm 5G-IA5 supported (octet 4, bit 3)
0 5GS integrity algorithm 5G-IA5 not supported
1 5GS integrity algorithm 5G-IA5 supported

5GS integrity algorithm 5G-IA6supported (octet 4, bit 2)
0 5GS integrity algorithm 5G-IA6 not supported
1 5GS integrity algorithm 5G-IA6 supported

5GS integrity algorithm 5G-IA7 supported (octet 4, bit 1)
0 5GS integrity algorithm 5G-IA7 not supported
1 5GS integrity algorithm 5G-IA7 supported

EPS encryption algorithms supported (see NOTE 3) (octet 5)

EPS encryption algorithm EEA0 supported (octet 5, bit 8)
0 EPS encryption algorithm EEA0 not supported
1 EPS encryption algorithm EEA0 supported

EPS encryption algorithm 128-EEA1 supported (octet 5, bit 7)
0 EPS encryption algorithm 128-EEA1 not supported
1 EPS encryption algorithm 128-EEA1 supported

EPS encryption algorithm 128-EEA2 supported (octet 5, bit 6)
0 EPS encryption algorithm 128-EEA2 not supported
1 EPS encryption algorithm 128-EEA2 supported

EPS encryption algorithm 128-EEA3 supported (octet 5, bit 5)
0 EPS encryption algorithm 128-EEA3 not supported
1 EPS encryption algorithm 128-EEA3 supported

EPS encryption algorithm EEA4 supported (octet 5, bit 4)
0 EPS encryption algorithm EEA4 not supported
1 EPS encryption algorithm EEA4 supported

EPS encryption algorithm EEA5 supported (octet 5, bit 3)
0 EPS encryption algorithm EEA5 not supported
1 EPS encryption algorithm EEA5 supported

EPS encryption algorithm EEA6 supported (octet 5, bit 2)
0 EPS encryption algorithm EEA6 not supported
1 EPS encryption algorithm EEA6 supported

EPS encryption algorithm EEA7 supported (octet 5, bit 1)
0 EPS encryption algorithm EEA7 not supported
1 EPS encryption algorithm EEA7 supported

EPS integrity algorithms supported (see NOTE 4) (octet 6)

EPS integrity algorithm EIA0 supported (octet 6, bit 8)
0 EPS integrity algorithm EIA0 not supported
1 EPS integrity algorithm EIA0 supported

EPS integrity algorithm 128-EIA1 supported (octet 6, bit 7)
0 EPS integrity algorithm 128-EIA1 not supported
1 EPS integrity algorithm 128-EIA1 supported

EPS integrity algorithm 128-EIA2 supported (octet 6, bit 6)
0 EPS integrity algorithm 128-EIA2 not supported
1 EPS integrity algorithm 128-EIA2 supported

EPS integrity algorithm 128-EIA3 supported (octet 6, bit 5)
0 EPS integrity algorithm 128-EIA3 not supported
1 EPS integrity algorithm 128-EIA3 supported

EPS integrity algorithm EIA4 supported (octet 6, bit 4)
0 EPS integrity algorithm EIA4 not supported
1 EPS integrity algorithm EIA4 supported

EPS integrity algorithm EIA5 supported (octet 6, bit 3)
0 EPS integrity algorithm EIA5 not supported
1 EPS integrity algorithm EIA5 supported

EPS integrity algorithm EIA6 supported (octet 6, bit 2)
0 EPS integrity algorithm EIA6 not supported
1 EPS integrity algorithm EIA6 supported

EPS integrity algorithm EIA7 supported (octet 6, bit 1)
0 EPS integrity algorithm EIA7 not supported
1 EPS integrity algorithm EIA7 supported

For the UE not supporting any security algorithm for AS security over E-UTRA connected to 5GCN, all bits in octets 5 to 10 are spare and shall be ignored, if the respective octet is received with the information element.
For the UE supporting at least one security algorithm for AS security over E-UTRA connected to 5GCN all bits in octets 7 to 10 are spare and shall be ignored, if the respective octet is received with the information element.
If the AMF receives any of the octets 7 to 10 (NOTE 5), it shall store the octets as received and include them when sending the UE security capability information element to the UE.

NOTE 1: The code points in octet 3 are used to indicate support for 5GS encryption algorithms for NAS security in N1 mode and support for 5GS encryption algorithms for AS security over NR.
NOTE 2: The code points in octet 4 are used to indicate support for 5GS integrity algorithms for NAS security in N1 mode and support for 5GS integrity algorithms for AS security over NR.
NOTE 3: The code points in octet 5 are used to indicate support for EPS encryption algorithms for AS security over E-UTRA connected to 5GCN.
NOTE 4: The code points in octet 6 are used to indicate support for EPS integrity algorithms for AS security over E-UTRA connected to 5GCN.
NOTE 5: The AMF can receive this information element also from another AMF or MME during N1 mode to N1 mode or S1 mode to N1 mode handover preparation.

9.11.3.55 UE's usage setting

The purpose of the UE's usage setting information element is to provide the network with the UE's usage setting as defined in 3GPP TS 24.301 [15]. The network uses the UE's usage setting to select the RFSP index.

The UE's usage setting information element is coded as shown in figure 9.11.3.55.1 and table 9.11.3.55.1.

The UE's usage setting is a type 4 information element with a length of 3 octets.

8	7	6	5	4	3	2	1	
UE's usage setting IEI								octet 1
Length of UE's usage setting contents								octet 2
0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	UE's usage setting	octet 3

Figure 9.11.3.55.1: UE's usage setting information element

Table 9.11.3.55.1: UE's usage setting information element

UE's usage setting (octet 3, bit 1)	
0	voice centric
1	data centric
All other bits in the octet 3 are spare and shall be coded as zero,	

9.11.3.56 UE status

The purpose of the UE status information element is to provide the network with information concerning aspects of the current UE registration status which is used for interworking with EPS.

The UE status information element is coded as shown in figure 9.11.3.56.1 and table 9.11.3.56.1.

The UE status is a type 4 information element with a length of 3 octets.

8	7	6	5	4	3	2	1	
UE status IEI								octet 1
Length of UE status contents								octet 2
0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	N1 mode reg	S1 mode reg	octet 3

Figure 9.11.3.56.1: UE status information element

Table 9.11.3.56.1: UE status information element

EMM registration status (S1 mode reg) (octet 3, bit 1) 0 UE is not in EMM-REGISTERED state 1 UE is in EMM-REGISTERED state 5GMM registration status (N1 mode reg) (octet 3, bit 2) 0 UE is not in 5GMM-REGISTERED state 1 UE is in 5GMM-REGISTERED state All other bits in the octet 3 are spare and shall be coded as zero.

9.11.3.57 Uplink data status

The purpose of the Uplink data status information element is to indicate to the network which preserved PDU session(s) have uplink data pending or which preserved PDU session(s) are associated with active multicast MBS session(s).

The Uplink data status information element is coded as shown in figure 9.11.3.57.1 and table 9.11.3.57.1.

The Uplink data status information element is a type 4 information element with minimum length of 4 octets a maximum length of 34 octets.

8	7	6	5	4	3	2	1	
Uplink data status IEI								octet 1
Length of uplink data status contents								octet 2
PSI (7)	PSI (6)	PSI (5)	PSI (4)	PSI (3)	PSI (2)	PSI (1)	PSI (0)	octet 3
PSI (15)	PSI (14)	PSI (13)	PSI (12)	PSI (11)	PSI (10)	PSI (9)	PSI (8)	octet 4
0	0	0	0	0	0	0	0	
spare								octet 5* -34*

Figure 9.11.3.57.1: Uplink data status information element

Table 9.11.3.57.1: Uplink data status information element

PSI(x) shall be coded as follows: PSI(0): Bit 1 of octet 3 is spare and shall be coded as zero. PSI(1) – PSI(15): 0 indicates that no uplink data are pending for the corresponding PDU session identity or the PDU session is in PDU SESSION INACTIVE state or is in PDU SESSION ACTIVE state with user-plane resources already established. 1 indicates that uplink data are pending for the corresponding PDU session identity and the user-plane resources for the corresponding PDU session are not established, or the UE has active multicast MBS session(s) associated with the corresponding PDU session. All bits in octet 5 to 34 are spare and shall be coded as zero, if the respective octet is included in the information element.

9.11.3.58 Void

9.11.3.59 Void

9.11.3.60 Void

9.11.3.61 Void

9.11.3.62 Void

9.11.3.63 Void

9.11.3.64 Void

9.11.3.65 Void

9.11.3.66 Void

9.11.3.67 Void

9.11.3.68 UE radio capability ID

The purpose of the UE radio capability ID information element is to carry a UE radio capability ID.

The UE radio capability ID information element is coded as shown in figure 9.11.3.68.1 and table 9.11.3.68.1.

The UE radio capability ID is a type 4 information element with a length of n octets.

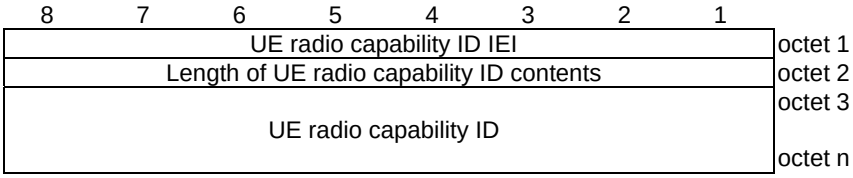


Figure 9.11.3.68.1: UE radio capability ID information element

Table 9.11.3.68.1: UE radio capability ID information element

UE radio capability ID (octets 3 to n) The UE radio capability ID contents contain the UE radio capability ID as specified in 3GPP TS 23.003 [4], with each hexadecimal digit coded over 4 bits, starting with the first hexadecimal digit coded in bits 4 to 1 of octet 3, the second hexadecimal digit coded in bits 8 to 5 of octet 3, and so on. If the UE radio capability ID contains an odd number of hexadecimal digits, bits 8 to 5 of the last octet (octet n) shall be coded as "1111".

9.11.3.69 UE radio capability ID deletion indication

The purpose of the UE radio capability ID deletion indication information element is to indicate to the UE that deletion of UE radio capability IDs is requested.

The UE radio capability ID deletion indication is a type 1 information element.

The UE radio capability ID deletion indication information element is coded as shown in figure 9.11.3.69.1 and table 9.11.3.69.1.

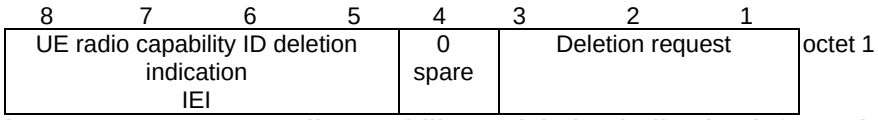


Figure 9.11.3.69.1: UE radio capability ID deletion indication information element

Table 9.11.3.69.1: UE radio capability ID deletion indication information element

Deletion requested (octet 1)			
Bits			
3	**2**	**1**	
0	0	0	UE radio capability ID deletion not requested
0	0	1	Network-assigned UE radio capability IDs deletion requested
All other values are unused and shall be interpreted as "UE radio capability ID deletion not requested", if received by the UE.			

9.11.3.70 Truncated 5G-S-TMSI configuration

The purpose of the Truncated 5G-S-TMSI configuration information element is to provide the size of the components of the truncated 5G-S-TMSI to the UE in NB-N1 mode to create the truncated 5G-S-TMSI.

The Truncated 5G-S-TMSI configuration information element is coded as shown in figure 9.11.3.70.1 and table 9.11.3.70.1.

The Truncated 5G-S-TMSI configuration is a type 4 information element with 3 octets length.

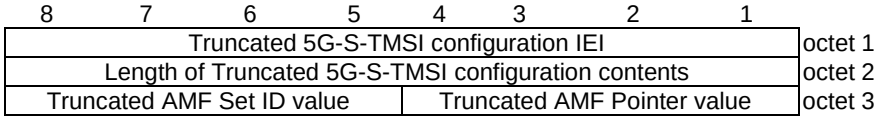


Figure 9.11.3.70.1: Truncated 5G-S-TMSI configuration information element

Table 9.11.3.70.1: Truncated 5G-S-TMSI configuration information element

Truncated AMF Pointer value (bits 4 to 1 of octet 3)

This field represents the size of the least significant bits of the AMF Pointer.

Bits

4	**3**	**2**	**1**	
0	0	0	0	reserved
0	0	0	1	1 least significant bit of the AMF Pointer
0	0	1	0	2 least significant bits of the AMF Pointer
0	0	1	1	3 least significant bits of the AMF Pointer
0	1	0	0	4 least significant bits of the AMF Pointer
0	1	0	1	5 least significant bits of the AMF Pointer
0	1	1	0	6 least significant bits of the AMF Pointer

All other values shall be interpreted as "6 least significant bits of the AMF Pointer" by this version of the protocol.

Truncated AMF Set ID value (bits 8 to 5 of octet 3)

This field represents the size of the least significant bits of the AMF Set ID.

Bits

4	**3**	**2**	**1**	
0	0	0	0	reserved
0	0	0	1	1 least significant bit of the AMF Set ID
0	0	1	0	2 least significant bits of the AMF Set ID
0	0	1	1	3 least significant bits of the AMF Set ID
0	1	0	0	4 least significant bits of the AMF Set ID
0	1	0	1	5 least significant bits of the AMF Set ID
0	1	1	0	6 least significant bits of the AMF Set ID
0	1	1	1	7 least significant bits of the AMF Set ID
1	0	0	0	8 least significant bits of the AMF Set ID
1	0	0	1	9 least significant bits of the AMF Set ID
1	0	1	0	10 least significant bits of the AMF Set ID

All other values shall be interpreted as "10 least significant bits of the AMF Set ID" by this version of the protocol.

NOTE: Total sum of the "Truncated AMF Set ID value" and the "Truncated AMF Pointer value" in the Truncated 5G-S-TMSI configuration IE is specified in 3GPP TS 23.003 [4] and 3GPP TS 36.300 [25B].

9.11.3.71 WUS assistance information

See subclause 9.9.3.62 in 3GPP TS 24.301 [15].

9.11.3.72 N5GC indication

The purpose of the N5GC indication information element is to indicate to the network that the registration request by the W-AGF is on behalf of an N5GC device.

The N5GC indication information element is coded as shown in figure 9.11.3.72.1.

The N5GC indication is a type 1 information element.

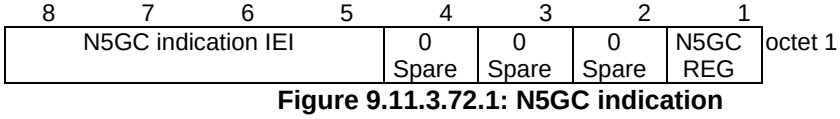


Figure 9.11.3.72.1: N5GC indication

Table 9.11.3.72.1: N5GC indication

N5GC device indication bit (N5GCREG) (octet 1, bit 1) Bit **1** 0 N5GC device registration is not requested 1 N5GC device registration is requested Bits 2 to 4 are spare and shall be coded as zero.

9.11.3.73 NB-N1 mode DRX parameters

The purpose of the NB-N1 mode DRX parameters information element is to indicate that the UE wants to use DRX in NB-N1 mode and for the network to indicate the DRX cycle value to be used at paging in NB-N1 mode.

The NB-N1 mode DRX parameters is a type 4 information element with a length of 3 octets.

The NB-N1 mode DRX parameters information element is coded as shown in figure 9.11.3.73.1 and table 9.11.3.73.1.

The value part of a DRX parameter information element is coded as shown in table 9.11.3.73.1.

8	7	6	5	4	3	2	1	
NB-N1 mode DRX parameters IEI								octet 1
Length of NB-N1 mode DRX parameters contents								octet 2
0	0	0	0	NB-N1 mode DRX value				octet 3
Spare								

Figure 9.11.3.73.1: NB-N1 mode DRX parameters information element

Table 9.11.3.73.1: NB-N1 mode DRX parameters information element

NB-N1 mode DRX value (octet 3, bits 1 to 4) This field represents the DRX cycle parameter 'T', for NB-N1 mode, as defined in 3GPP TS 36.304 [25C]. Bits **4 3 2 1** 0 0 0 0 DRX value not specified 0 0 0 1 DRX cycle parameter T = 32 0 0 1 0 DRX cycle parameter T = 64 0 0 1 1 DRX cycle parameter T = 128 0 1 0 0 DRX cycle parameter T = 256 0 1 0 1 DRX cycle parameter T = 512 0 1 1 1 DRX cycle parameter T = 1024 All other values shall be interpreted as "DRX value not specified" by this version of the protocol. Bits 5 to 8 of octet 3 are spare and shall be coded as zero.

9.11.3.74 Additional configuration indication

The purpose of the Additional configuration indication information element is to indicate additional information associated with the generic UE configuration update procedure.

The Additional configuration indication information element is coded as shown in figure 9.11.3.74.1 and table 9.11.3.74.1.

The Additional configuration indication is a type 1 information element.

8	7	6	5	4	3	2	1	
Additional configuration indication IEI				0 Spare	0 Spare	0 Spare	SCMR	octet 1

Figure 9.11.3.74.1: Additional configuration indication

Table 9.11.3.74.1: Additional configuration indication

Signalling connection maintain request (SCMR) (octet 1, bit 1) Bit **1** 0 no additional information 1 release of N1 NAS signalling connection not required Bits 2 to 4 are spare and shall be coded as zero,

9.11.3.75 Extended rejected NSSAI

The purpose of the Extended rejected NSSAI information element is to identify a collection of rejected S-NSSAIs if UE supports extended rejected NSSAI.

The Extended rejected NSSAI information element is coded as shown in figure 9.11.3.75.1, figure 9.11.3.75.2 and table 9.11.3.75.1.

The Extended rejected NSSAI is a type 4 information element with a minimum length of 5 octets and a maximum length of 90 octets.

8	7	6	5	4	3	2	1	
Extended rejected NSSAI IEI								octet 1
Length of Extended rejected NSSAI contents								octet 2
Partial extended rejected NSSAI list 1								octet 3 octet m
Partial extended rejected NSSAI list 2								octet m+1* octet n*
…								octet n+1* octet u*
Partial extended rejected NSSAI list n								octet u+1* octet v*

Figure 9.11.3.75.1: Extended rejected NSSAI information element

8	7	6	5	4	3	2	1	
spare	Type of list			Number of elements				octet 3
Rejected S-NSSAI 1								octet 4 octet j
Rejected S-NSSAI 2								octet j+1* octet k*
…								octet k+1 octet p*
Rejected S-NSSAI n								octet p+1* octet m*

Figure 9.11.3.75.2: Partial extended rejected NSSAI list – type of list = 000

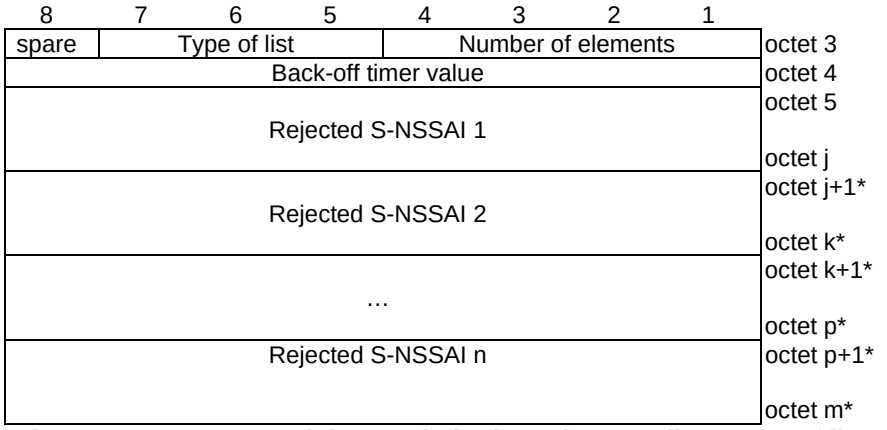


Figure 9.11.3.75.3: Partial extended rejected NSSAI list – type of list = 001

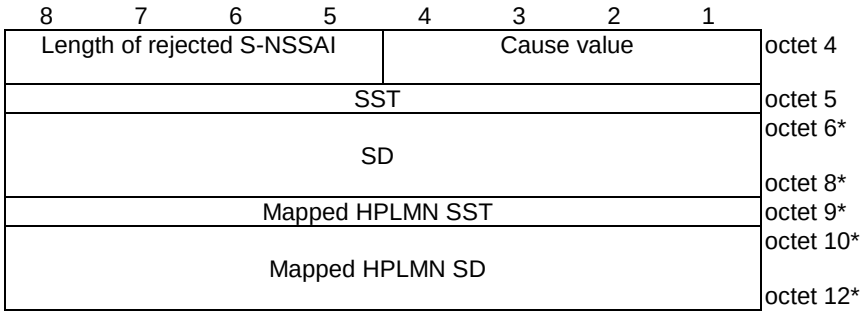


Figure 9.11.3.75.4: Rejected S-NSSAI

Table 9.11.3.75.1: Extended rejected NSSAI information element

Value part of the Extended rejected NSSAI information element (octet 3 to v)

The value part of the Extended rejected NSSAI information element consists of one or more partial extended rejected NSSAI lists. The length of each partial extended rejected NSSAI list can be determined from the 'type of list' field and the 'number of elements' field in the first octet of the partial extended rejected NSSAI list.

Each rejected S-NSSAI consists of one S-NSSAI and an associated cause value. Each rejected S-NSSAI also includes the mapped HPLMN S-NSSAI if available. The length of each rejected S-NSSAI can be determined by the 'length of rejected S-NSSAI' field in the first octet of the rejected S-NSSAI.
The UE shall store the complete list received (NOTE 0). If more than 8 rejected S-NSSAIs are included in this information element, the UE shall store the first 8 rejected S-NSSAIs and ignore the remaining octets of the information element.

Partial extended rejected NSSAI list:

Number of elements (octet 3, bits 1 to 4)
Bits

4	**3**	**2**	**1**	
0	0	0	0	1 element
0	0	0	1	2 element
		…		
0	1	1	0	7 element
0	1	1	1	8 element

All other values are unused and shall be interpreted as 8, if received by the UE.

Type of list (octet 3, bits 5 to 7) (NOTE 7)
Bits

7	**6**	**5**	
0	0	0	list of S-NSSAIs without any associated back-off timer value
0	0	1	list of S-NSSAIs with one associated back-off timer value that applies to all S-NSSAIs in the list

All other values are reserved.

Bit 8 of octet 3 is spare and shall be coded as zero.

Back-off timer value (octet 4):

Back-off timer value is coded as the value part of GPRS timer 3 in subclause 10.5.7.4a in 3GPP TS 24.008 [12].

Rejected S-NSSAI:

Cause value (octet x) (NOTE 8)
Bits

4	**3**	**2**	**1**	
0	0	0	0	S-NSSAI not available in the current PLMN or SNPN
0	0	0	1	S-NSSAI not available in the current registration area
0	0	1	0	S-NSSAI not available due to the failed or revoked network slice-specific authentication and authorization
0	0	1	1	S-NSSAI not available due to maximum number of UEs reached

All other values are reserved.

Slice/service type (SST) (octet x+1)
This field contains the 8 bit SST value. The coding of the SST value part is defined in 3GPP TS 23.003 [4]. (NOTE 5)

Slice differentiator (SD) (octet x+2 to octet x+4)

This field contains the 24 bit SD value. The coding of the SD value part is defined in 3GPP TS 23.003 [4]. (NOTE 6)

If the SST encoded in octet x+1 is not associated with a valid SD value, and the sender needs to include a mapped HPLMN SST (octet x+5) and a mapped HPLMN SD (octets x+6 to x+8), then the sender shall set the SD value (octets x+2 to x+4) to "no SD value associated with the SST".

mapped HPLMN Slice/service type (SST) (octet x+5)

This field contains the 8 bit SST value of an S-NSSAI in the S-NSSAI(s) of the HPLMN to which the SST value is mapped. The coding of the SST value part is defined in 3GPP TS 23.003 [4].

mapped HPLMN Slice differentiator (SD) (octet x+6 to octet x+8)

This field contains the 24 bit SD value of an S-NSSAI in the S-NSSAI(s) of the HPLMN to which the SD value is mapped. The coding of the SD value part is defined in 3GPP TS 23.003 [4].

NOTE 0: The number of rejected S-NSSAI(s) shall not exceed eight.
NOTE 1: Octet x and octet x+1 shall always be included.
NOTE 2: If the octet x+2 is included, then octet x+3 and octet x+4 shall be included.
NOTE 3: If the octet x+5 is included, then octets x+6, x+7, and x+8 may be included.
NOTE 4: If the octet x+6 is included, then octet x+7 and octet x+8 shall be included.
NOTE 5: If the Cause value is "S-NSSAI not available due to the failed or revoked network slice-specific authentication and authorization", this field shall contain the 8 bit SST value of an S-NSSAI in the S-NSSAI(s) of the HPLMN and octets x+5, x+6, x+7, and x+8 shall not be included.
NOTE 6: If the Cause value is "S-NSSAI not available due to the failed or revoked network slice-specific authentication and authorization", this field shall contain the 24 bit SD value of an S-NSSAI in the S-NSSAI(s) of the HPLMN and octets x+5, x+6, x+7, and x+8 shall not be included.
NOTE 7: The partial extended rejected NSSAI with type of list = 001 shall only be used for rejected S-NSSAI(s) with the rejection cause "S-NSSAI not available due to maximum number of UEs reached".
NOTE 8: Octet x can be 4 or 5.

9.11.3.76 UE request type

See subclause 9.9.3.65 in 3GPP TS 24.301 [15].

9.11.3.77 Paging restriction

The purpose of the Paging restriction information element is to request the network to restrict paging.

The Paging restriction information element is coded as shown in figure 9.11.3.77.1, figure 9.11.3.77.2 and table 9.11.3.77.1.

The Paging restriction is a type 4 information element with a minimum length of 3 octets and a maximum length of 35 octets.

8	7	6	5	4	3	2	1	
Paging restriction IEI								octet 1
Length of Paging restriction contents								octet 2
0 Spare	0 Spare	0 Spare	0 Spare	Paging restriction type				octet 3

Figure 9.11.3.77.1: Paging restriction information element for Paging restriction type = "All paging is restricted" and for Paging restriction type = "All paging is restricted except voice"

8	7	6	5	4	3	2	1	
Paging restriction IEI								octet 1
Length of Paging restriction contents								octet 2
0 Spare	0 Spare	0 Spare	0 Spare	Paging restriction type				octet 3
PSI (7)	PSI (6)	PSI (5)	PSI (4)	PSI (3)	PSI (2)	PSI (1)	PSI (0)	octet 4
PSI (15)	PSI (14)	PSI (13)	PSI (12)	PSI (11)	PSI (10)	PSI (9)	PSI (8)	octet 5
0	0	0	0	0	0	0	0	octet 6*-35*
spare								

Figure 9.11.3.77.2: Paging restriction information element for Paging restriction type = "All paging is restricted except for specified PDU session(s)" and for Paging restriction type = "All paging is restricted except for voice service and specified PDU session(s)"

Table 9.11.3.77.1: Paging restriction information element

Paging restriction type (bits 4 to 1 of octet 3)

Bits

4	**3**	**2**	**1**	
0	0	0	0	reserved
0	0	0	1	All paging is restricted
0	0	1	0	All paging is restricted except for voice service
0	0	1	1	All paging is restricted except for specified PDU session(s)
0	1	0	0	All paging is restricted except for voice service and specified PDU session(s)

All other values are reserved.

Bits 5 to 8 of octet 3 are spare and shall be coded as zero.

PSI(x) (bits 8 to 1 of octet 4 and octet 5):
This field indicates the PDU session identity of the PDU session for which paging is restricted.

PSI(0): (bit 1 of octet 4)
Spare and shall be coded as zero.

PSI(1) – PSI(15):
0 indicates that paging is restricted for the PDU session associated with the PDU session identity.
1 indicates that paging is not restricted for the PDU session associated with the PDU session identity.
All bits in octet 6 to 35 are spare and shall be coded as zero, if the respective octet is included in the information element.

9.11.3.78 Void

9.11.3.79 NID

See subclause 9.2.7 in 3GPP TS 24.502 [18].

9.11.3.80 PEIPS assistance information

The purpose of the PEIPS assistance information, information element is to transfer the required assistance information to indicate the paging subgroup used when paging the UE.

The coding of the information element allows combining different types of PEIPS assistance information.

The PEIPS assistance information, information element is coded as shown in figure 9.11.3.80.1, figure 9.11.3.80.2, figure 9.11.3.80.3 and table 9.11.3.80.1.

The PEIPS assistance information is a type 4 information element, with a minimum length of 3 octets.

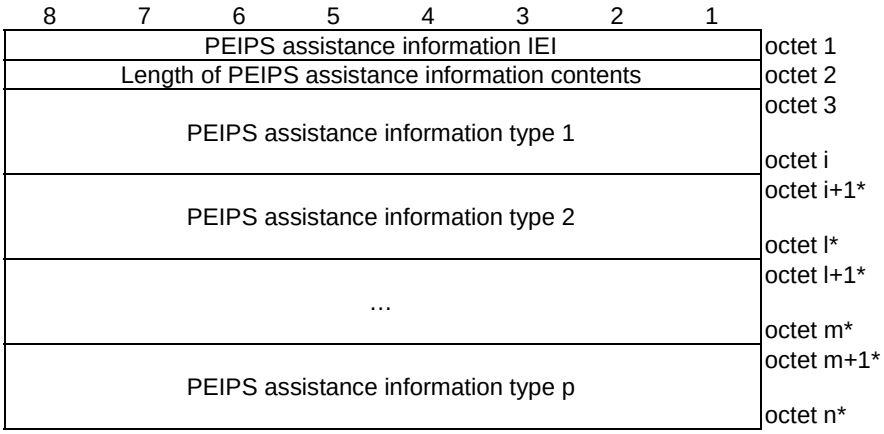


Figure 9.11.3.80.1: PEIPS assistance information information element

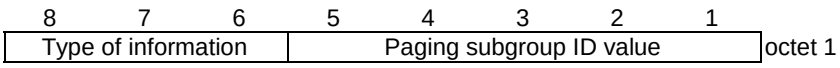


Figure 9.11.3.80.2: PEIPS assistance information type –type of information= "000"

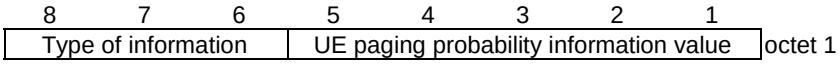


Figure 9.11.3.80.3: PEIPS assistance information type –type of information= "001"

Table 9.11.3.80.1: PEIPS assistance information information element

Value part of the PEIPS assistance information information element (octets 3 to n)

The value part of the PEIPS assistance information information element consists of one or several types of PEIPS assistance information.

PEIPS assistance information type:

Type of information (octet 1)
Bits

8	7	6	
0	0	0	Paging subgroup ID
0	0	1	UE paging probability information

All other values are reserved.

Paging subgroup ID value: (octet 1, bits 1-5)
This field contains the value (in decimal) of paging subgroup ID that is assigned by the AMF for paging the UE. This field has a valid range of values from (0-7). All other values are unused and shall be interpreted as 0 by this version of the protocol.

UE paging probability information value: (octet 1, bits 1-5)
This field contains the value of UE paging probability information provided by the UE to the AMF. It represents the probability of the UE receiving the paging.

Bit

5	4	3	2	1	UE paging probability information value
0	0	0	0	0	p00 (UE calculated paging probability is 0%)
0	0	0	0	1	p05 (UE calculated paging probability > 0% and <= 5%)
0	0	0	1	0	p10 (UE calculated paging probability > 5% and <= 10%)
0	0	0	1	1	p15 (UE calculated paging probability > 10% and <= 15%)
0	0	1	0	0	p20 (UE calculated paging probability > 15% and <= 20%)
0	0	1	0	1	p25 (UE calculated paging probability > 20% and <= 25%)
0	0	1	1	0	p30 (UE calculated paging probability > 25% and <= 30%)
0	0	1	1	1	p35 (UE calculated paging probability > 30% and <= 35%)
0	1	0	0	0	p40 (UE calculated paging probability > 35% and <= 40%)
0	1	0	0	1	p45 (UE calculated paging probability > 40% and <= 45%)
0	1	0	1	0	p50 (UE calculated paging probability > 45% and <= 50%)
0	1	0	1	1	p55 (UE calculated paging probability > 50% and <= 55%)
0	1	1	0	0	p60 (UE calculated paging probability > 55% and <= 60%)
0	1	1	0	1	p65 (UE calculated paging probability > 60% and <= 65%)
0	1	1	1	0	p70 (UE calculated paging probability > 65% and <= 70%)
0	1	1	1	1	p75 (UE calculated paging probability > 70% and <= 75%)
1	0	0	0	0	p80 (UE calculated paging probability > 75% and <= 80%)
1	0	0	0	1	p85 (UE calculated paging probability > 80% and <= 85%)
1	0	0	1	0	p90 (UE calculated paging probability > 85% and <= 90%)
1	0	0	1	1	p95 (UE calculated paging probability > 90% and <= 95%)
1	0	1	0	0	p100 (UE calculated paging probability > 95% and <= 100%)

All other values shall be interpreted as 10100 by this version of the protocol.

9.11.3.81 5GS additional request result

The purpose of the 5GS additional request result information element is to inform the UE about the result of additional request.

The 5GS additional request result information element is coded as shown in figure 9.11.3.81.1 and table 9.11.3.81.1.

The 5GS additional request result is a type 4 information element with a length of 3 octets.

8	7	6	5	4	3	2	1	
5GS additional request result IEI								octet 1
Length of 5GS additional request result contents								octet 2
0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	PRD		octet 3

Figure 9.11.3.81.1: 5GS additional request result information element

Table 9.11.3.81.1: 5GS additional request result information element

Paging restriction decision (PRD) (bits 2 to 1 of octet 3) Bits **2 1** 0 0 no additional information 0 1 paging restriction is accepted 1 0 paging restriction is rejected All other values are reserved. Bits 3 to 8 of octet 3 are spare and shall be coded as zero.

9.11.3.82 NSSRG information

The purpose of the NSSRG information information element is to identify one or more NSSRG values associated with each of the HPLMN S-NSSAIs in a configured NSSAI.

The NSSRG information information element is coded as shown in figure 9.11.3.82.1, figure 9.11.3.82.2 and table 9.11.3.82.1.

The NSSRG information is a type 6 information element with minimum length of 7 octets and maximum length of 4099 octets.

8	7	6	5	4	3	2	1	
NSSRG information IEI								octet 1
Length of NSSRG information contents								octet 2 octet 3
NSSRG values for S-NSSAI 1								octet 4 octet m
NSSRG values for S-NSSAI 2								octet m+1* octet n*
…								octet n+1* octet u*
NSSRG values for S-NSSAI x								octet u+1* octet v*

Figure 9.11.3.82.1: NSSRG information information element

8	7	6	5	4	3	2	1	
Length of NSSRG values for S-NSSAI								octet 4
S-NSSAI value								octet 5 … octet w
NSSRG value 1 for the S-NSSAI								octet w+1
NSSRG value 2 for the S-NSSAI								octet w+2*
…								octet w+3* … octet w+15
NSSRG value y for the S-NSSAI								octet w+16

Figure 9.11.3.82.2: NSSRG values for S-NSSAI

Table 9.11.3.82.1: NSSRG information information element

Value part of the NSSRG information information element (octet 4 to v) The value part of the NSSRG information information element consists of one or more NSSRG values for each S-NSSAI in the Configured NSSAI IE. S-NSSAI value (octet 5 to w) (see NOTE 2) S-NSSAI value is coded as the length and value part of S-NSSAI information element as specified in subclause 9.11.2.8 starting with the second octet. See NOTE 1. NSSRG value for the S-NSSAI (octet w+1) This field contains the 8 bit NSSRG value.
NOTE 1: If a mapped HPLMN SST is included in a S-NSSAI value, then the NSSRG value(s) are associated with the Mapped HPLMN SST, and the Mapped HPLMN SD, if included. NOTE 2: The NSSRG information IE shall contain the complete set of S-NSSAI(s) included in the configured NSSAI. NOTE 3: The number of NSSRG values associated with an S-NSSAI cannot exceed 16. If there are more than 16 NSSRG values for an S-NSSAI in the NSSRG information, then the UE shall retain only the first 16 NSSRG values and ignore the rest.

9.11.3.83 List of PLMNs to be used in disaster condition

The purpose of the list of PLMNs to be used in disaster condition information element is to provide the "list of PLMN(s) to be used in disaster condition" associated with the serving PLMN to the UE.

The list of PLMNs to be used in disaster condition information element is coded as shown in figures 9.11.3.83.1 and 9.11.3.83.2 and table 9.11.3.83.1.

The list of PLMNs to be used in disaster condition is a type 4 information element, with a minimum length of 2 octets.

8	7	6	5	4	3	2	1	
List of PLMNs to be used in disaster condition list IEI								octet 1
Length of list of PLMNs to be used in disaster condition contents								octet 2
PLMN ID 1								octet 3* octet 5*
PLMN ID 2								octet 6* octet 8*
…								octet 9* octet q*
PLMN ID n								octet q+1* octet q+3*

Figure 9.11.3.83.1: List of PLMNs to be used in disaster condition information element

8	7	6	5	4	3	2	1	
MCC digit 2				MCC digit 1				octet q+1
MNC digit 3				MCC digit 3				octet q+2
MNC digit 2				MNC digit 1				octet q+3

Figure 9.11.3.83.2: PLMN ID n

Table 9.11.3.83.1: List of PLMNs to be used in disaster condition information element

MCC, Mobile country code (octet q+1 and bits 1 to 4 octet q+2) The MCC field is coded as in ITU-T Recommendation E.212 [42], annex A. MNC, Mobile network code (bits 5 to 8 of octet q+2 and octet q+3) The coding of this field is the responsibility of each administration but BCD coding shall be used. The MNC shall consist of 2 or 3 digits. If a network operator decides to use only two digits in the MNC, bits 5 to 8 of octet q+2 shall be coded as "1111". The MCC and MNC digits are coded as octets 6 to 8 of the Temporary mobile group identity IE in figure 10.5.154 of 3GPP TS 24.008 [12].
NOTE: The PLMN IDs are provided in decreasing order of priority, i.e. PLMN ID 1 indicates highest priority and PLMN ID n indicates lowest priority.

9.11.3.84 Registration wait range

The purpose of the registration wait range information element is to provide the disaster roaming wait range or the disaster return wait range to the UE.

The registration wait range information element is coded as shown in figure 9.11.3.84.1 and table 9.11.3.84.1.

The registration wait range is a type 4 information element, with a length of 4 octets.

8	7	6	5	4	3	2	1	
Registration wait range IEI								octet 1
Length of registration wait range								octet 2
Minimum registration wait time								octet 3
Maximum registration wait time								octet 4

Figure 9.11.3.84.1: Registration wait range information element

Table 9.11.3.84.1: Registration wait range information element

Minimum registration wait time (octet 3) The minimum registration wait time contains the minimum duration of the registration wait time, encoded as octet 2 of the GPRS timer information element (see 3GPP TS 24.008 [12] subclause 10.5.7.3). Maximum registration wait time (octet 4) The maximum registration wait time contains the maximum duration of the registration wait time, encoded as octet 2 of the GPRS timer information element (see 3GPP TS 24.008 [12] subclause 10.5.7.3).

9.11.3.85 PLMN identity

The purpose of the PLMN identity information element is to provide a PLMN identity.

The PLMN identity information element is coded as shown in figure 9.11.3.85.1, and table 9.11.3.85.1.

The PLMN identity is a type 4 information element.

8	7	6	5	4	3	2	1	
PLMN identity IEI								octet 1
Length of PLMN identity contents								octet 2
MCC digit 2				MCC digit 1				octet 3
MNC digit 3				MCC digit 3				octet 4
MNC digit 2				MNC digit 1				octet 5

Figure 9.11.3.85.1: PLMN identity information element

Table 9.11.3.85.1: PLMN identity information element

MCC, Mobile country code (octet 3, octet 4 bits 1 to 4) The MCC field is coded as in ITU-T Recommendation E.212 [42], annex A. MNC, Mobile network code (octet 4 bits 5 to 8, octet 5) The coding of this field is the responsibility of each administration but BCD coding shall be used. The MNC shall consist of 2 or 3 digits. If a network operator decides to use only two digits in the MNC, bits 5 to 8 of octet 4 shall be coded as "1111". The MCC and MNC digits are coded as octets 6 to 8 of the Temporary mobile group identity IE in figure 10.5.154 of 3GPP TS 24.008 [12].

9.11.3.86 Extended CAG information list

The purpose of the Extended CAG information list information element is to provide "CAG information list" or to delete the "CAG information list" at the UE.

The Extended CAG information list information element is coded as shown in figures 9.11.3.86.1, figure 9.11.3.86.2, figure 9.11.3.86.3, figure 9.11.3.86.4, figure 9.11.3.86.5 and table 9.11.3.86.1.

The Extended CAG information list is a type 6 information element, with a minimum length of 3 octets.

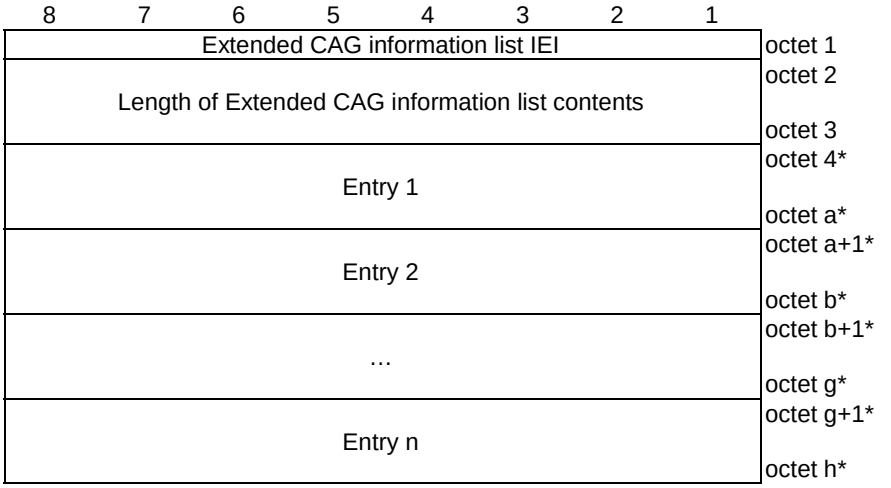
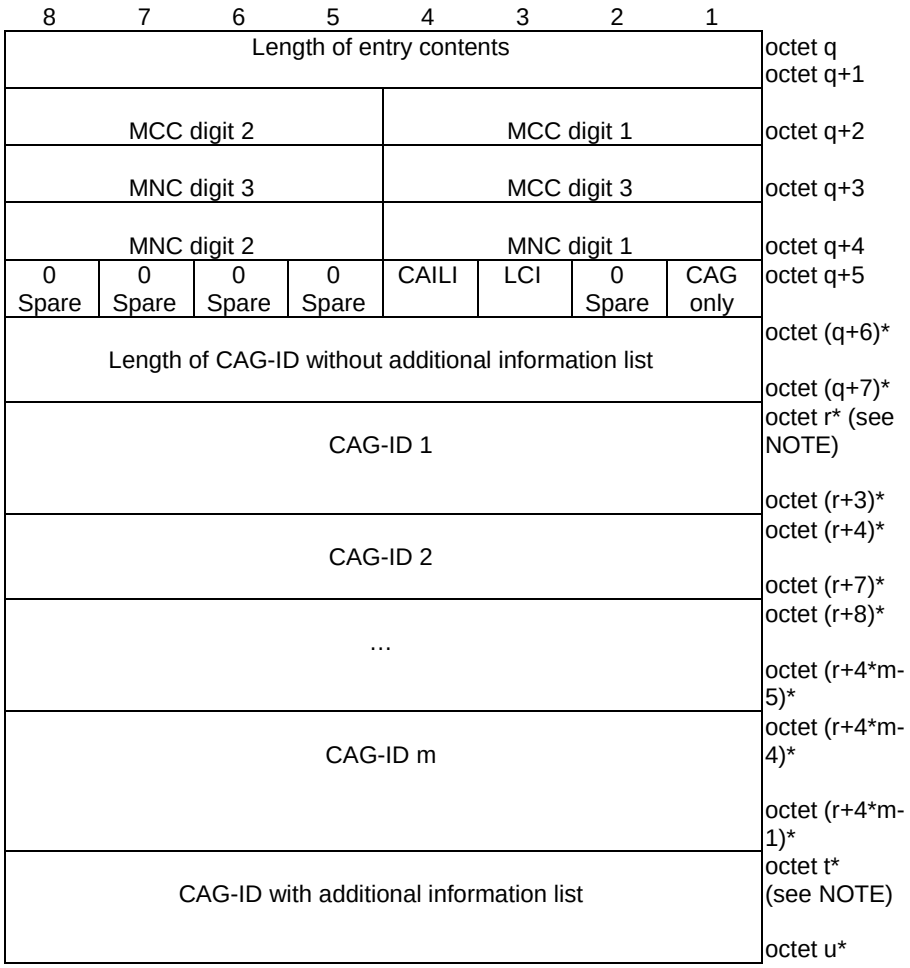


Figure 9.11.3.86.1: Extended CAG information list information element



NOTE: The field is placed immediately after the last present preceding field.

Figure 9.11.3.86.2: Entry n

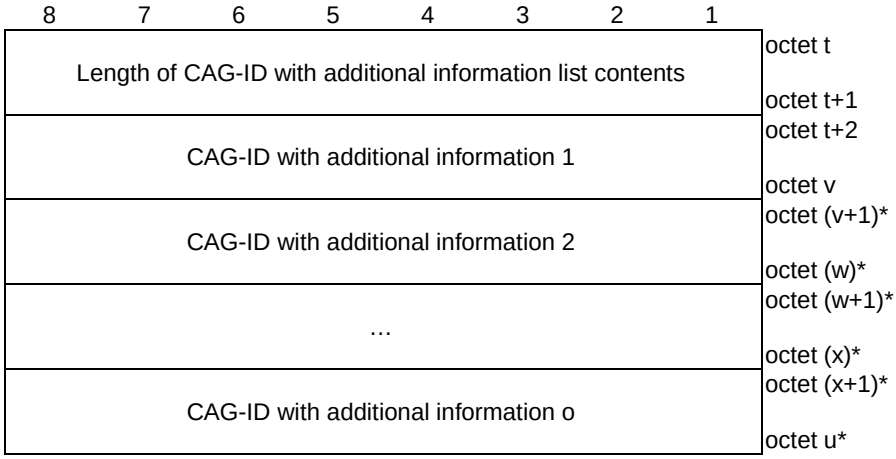
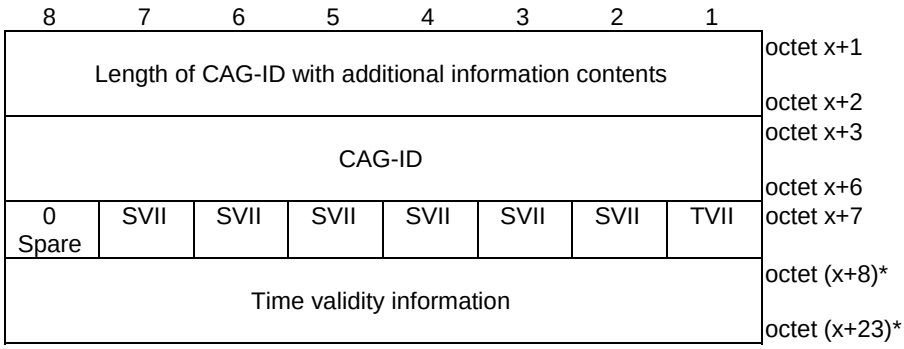


Figure 9.11.3.86.3: CAG-ID with additional information list



NOTE: The field is placed immediately after the last present preceding field.

Figure 9.11.3.86.4: CAG-ID with additional information

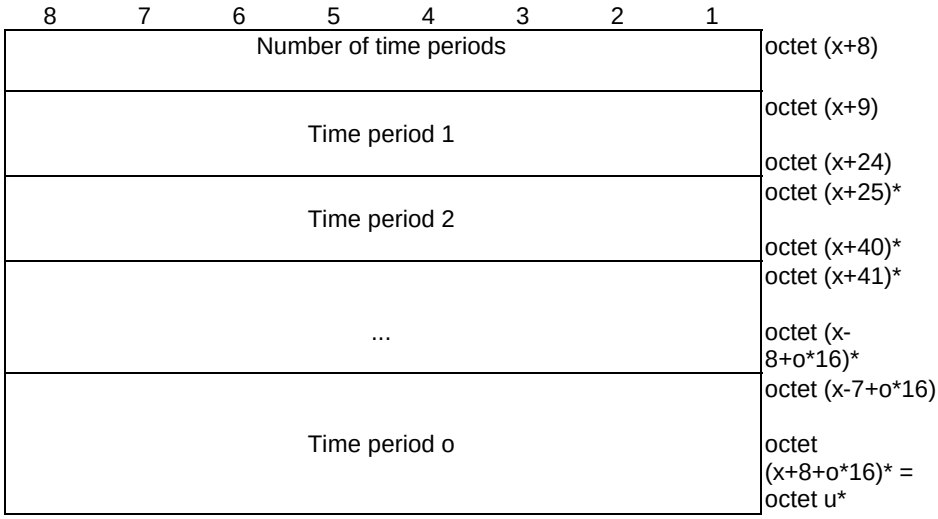


Figure 9.11.3.86.5: Time validity infomation

Table 9.11.3.86.1: Extended CAG information list information element

Value part of the Extended CAG information list information element (octet 4 to h)
The value part of the Extended CAG information list information element consists of one or more entries.

Entry n:

Length of entry contents (octet q and q+1)

MCC, Mobile country code (octet q+2 and bits 1 to 4 octet q+3)
The MCC field is coded as in ITU-T Recommendation E.212 [42], annex A.

MNC, Mobile network code (bits 5 to 8 of octet q+3 and octet q+4)
The coding of this field is the responsibility of each administration, but BCD coding shall be used. The MNC shall consist of 2 or 3 digits. If a network operator decides to use only two digits in the MNC, bits 5 to 8 of octet q+2 shall be coded as "1111".

The MCC and MNC digits are coded as octets 6 to 8 of the Temporary mobile group identity IE in figure 10.5.154 of 3GPP TS 24.008 [12].

Indication that the UE is only allowed to access 5GS via CAG cells (CAGonly) (bit 1 of octet q+5)
Bit
1
0 "Indication that the UE is only allowed to access 5GS via CAG cells" is not set (i.e., the UE is allowed to access 5GS via non-CAG cells)
1 "Indication that the UE is only allowed to access 5GS via CAG cells" is set (i.e., the UE is not allowed to access 5GS via non-CAG cells)

Length of CAG-ID without additional information list indicator (LCI) (bit 3 of octet q+5)
Bit
3
0 Length of CAG-ID without additional information list field is absent
1 Length of CAG-ID without additional information list field is present
If the UE does not support enhanced CAG information, the LCI bit shall be set to "Length of CAG-ID without additional information list field is absent".

CAG-ID with additional information list indicator (CAILI) (bit 4 of octet q+5)
Bit
4
0 CAG-ID with additional information list field is absent
1 CAG-ID with additional information list field is present
If the UE does not support enhanced CAG information or the LCI bit is set to "Length of CAG-ID without additional information list field is absent", the CAILI bit shall be set to "CAG-ID with additional information list field is absent".

Length of CAG-ID without additional information list (octet q+6 to octet q+7)
This field indicates length of CAG-ID fields in octet r to octet (r+4*m-1).

CAG-ID m (octet r+4*m-4 to octet r+4*m-1)
This field contains the 32 bit CAG-ID which is not associated with additional information. The coding of the CAG-ID is defined as the CAG-Identifier in 3GPP TS 23.003 [4]. See NOTE 4.

If the length of entry contents field indicates a length bigger than indicated in figure 9.11.3.86.1, receiving entity shall ignore any superfluous octets located at the end of the entry contents.

CAG-ID (octet x+3 to octet x+6)
This field contains the 32 bit CAG-ID which is associated with additional information. The additional information is indicated in remaining fields of figure 9.11.3.86.4. The coding of the CAG-ID is defined as the CAG-Identifier in 3GPP TS 23.003 [4].

Time validity information indicator (TVII) (bit 1 of octet x+7)
Bit
1
0 Time validity information field is absent
1 Time validity information field is present

Spare validity information indicator (SVII) 0 Spare validity information is absent 1 Spare validity information is present The SVII bit indicates presence of a validity information not specified in the present version of the present document. See NOTE 5. If the SVII bit is set to "Spare validity information is present", the receiving entity shall ignore the CAG-ID with additional information field. Time period (octet x+25 to octet x+40) The time period field is coded as the route selection descriptor component value field for "time window type" specified in 3GPP TS 24.526 [19] table 5.2.1. If the length of CAG-ID with additional information contents field indicates a length bigger than indicated in figure 9.11.3.86.4, receiving entity shall ignore any superfluous octets located at the end of the CAG-ID with additional information contents.
NOTE 1: The length of extended CAG information list contents field shall be 0 if no subscription data for CAG information list exists. NOTE 2: The length of entry contents field shall be 4 if there is no allowed CAG-ID for the PLMN. NOTE 3: For a given PLMN ID, there shall be up to one entry field containing the MCC value and the MNC value of the PLMN ID. NOTE 4: CAG-ID field containing a CAG-ID which is not associated with additional information, can be provided regardless whether the LCI bit is set to "Length of CAG-ID without additional information list field is absent" or "Length of CAG-ID without additional information list field is present". NOTE 5: In a future version of the present document, semantic of this bit can be changed to indicate presence or absence of an additional validity information.

9.11.3.87 NSAG information

The purpose of the NSAG information information element is to provide the NSAG information to the UE.

The NSAG information information element is coded as shown in figures 9.11.3.87.1, 9.11.3.87.2 and 9.11.3.87.3, and table 9.11.3.87.1.

The NSAG information information element can contain a maximum of 32 NSAG entries.

In the NSAG information information element, at most 4 NSAG entries can contain a TAI list.

The NSAG information is a type 6 information element, with a minimum length of 9 octets and a maximum length of 3143 octets.

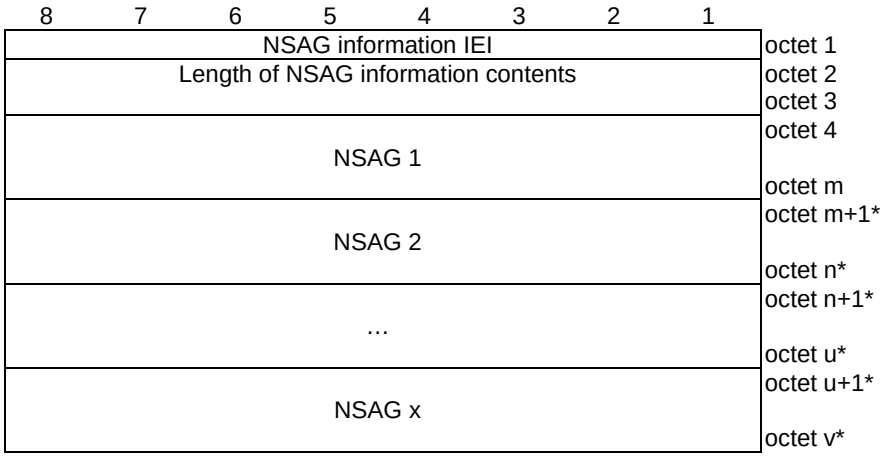


Figure 9.11.3.87.1: NSAG information information element

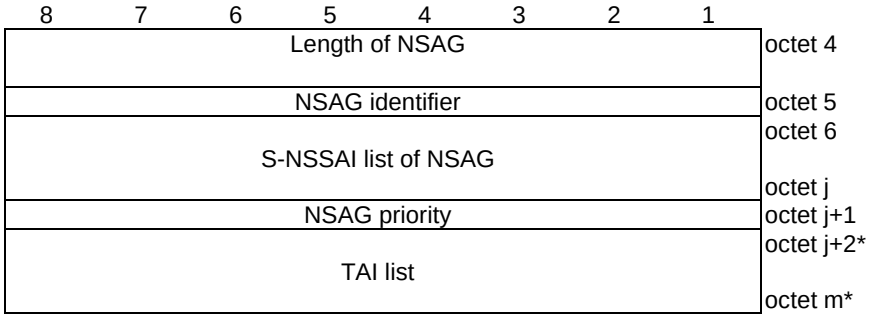


Figure 9.11.3.87.2: NSAG

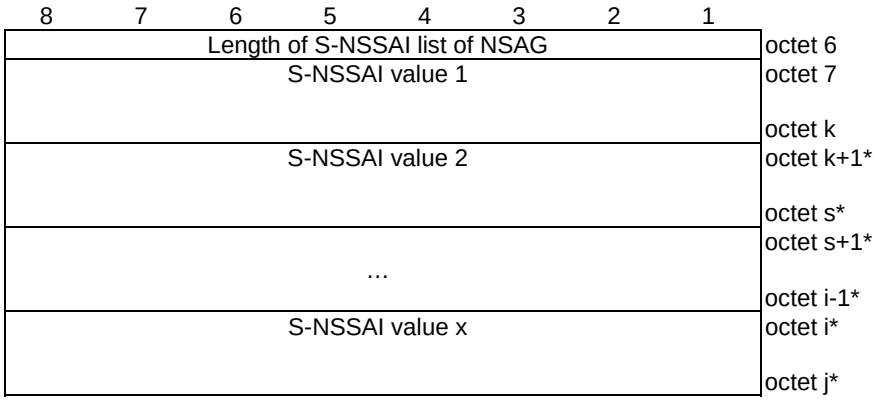


Figure 9.11.3.87.3: S-NSSAI list of NSAG

Table 9.11.3.87.1: NSAG information information element

NSAG part of the NSAG information information element (octet 4 to m) Each entry of the NSAG information information element consists of one NSAG in the NSAG information IE.
NSAG identifier(octet 5) NSAG identifier field contains an 8 bits NSAG ID value. S-NSSAI list of NSAG (octet 6 to j) S-NSSAI list of NSAG field consists of one or more S-NSSAIs in the configured NSSAI. Each S-NSSAI in S-NSSAI list of NSAG field is coded as the length and value part of S-NSSAI information element as specified in subclause 9.11.2.8 starting with the second octet, without the mapped HPLMN SST field and without the mapped HPLMN SD field. NSAG priority (octet j+1) The NSAG priority field represents the binary coded value of NSAG priority for cell reselection (see 3GPP TS 38.304 [28]) and random access (see 3GPP TS 38.321 [58]). The range of the NSAG priority is 0 to 255. A lower value indicates a higher priority, with 0 as the highest priority. TAI list (octet j+2 to m) The TAI list field is coded as the length and value part of the 5GS tracking area identity list IE defined in subclause 9.11.3.9 starting with the second octet.

9.11.3.88 ProSe relay transaction identity

The purpose of the ProSe relay transaction identity (PRTI) information element is to uniquely identify an authentication and key agreement procedure for 5G ProSe UE-to-network relay or 5G ProSe UE-to-UE relay. The PRTI allows distinguishing up to 254 different bi-directional messages.

The ProSe relay transaction identity information element is coded as shown in figure 9.11.3.88.1 and table 9.11.3.88.1.

The ProSe relay transaction identity is a type 3 information element with a length of 2 octets.

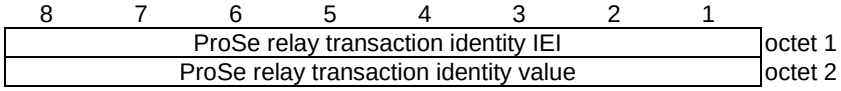


Figure 9.11.3.88.1: ProSe relay transaction identity information element

Table 9.11.3.88.1: ProSe relay transaction identity information element

ProSe relay transaction identity value (octet 2)

Bits								
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	
0	0	0	0	0	0	0	0	No ProSe relay transaction identity assigned
0	0	0	0	0	0	0	1	\
to								} ProSe relay transaction identity value
1	1	1	1	1	1	1	0	/
1	1	1	1	1	1	1	1	Reserved

9.11.3.89 Relay key request parameters

The purpose of the relay key request parameters information element is to transport the parameters of the key request for 5G ProSe UE-to-network relay or 5G ProSe UE-to-UE relay as specified in 3GPP TS 33.503 [56].

The relay key request parameters information element is coded as shown in figure 9.11.3.89.1, figure 9.11.3.89.2 and table 9.11.3.89.1.

The relay key request parameters is a type 6 information element.

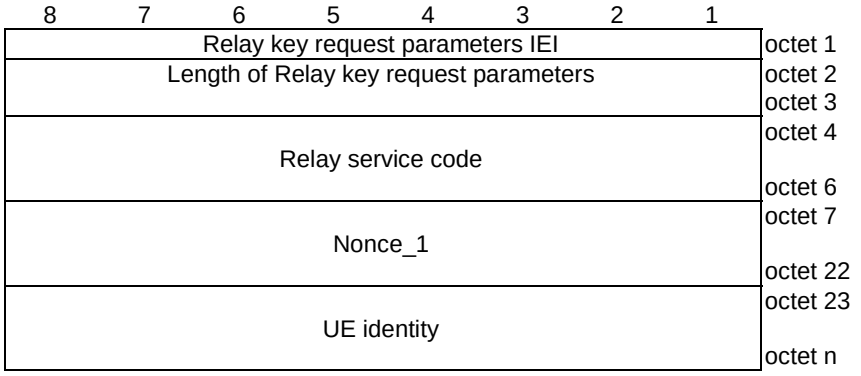


Figure 9.11.3.89.1: Relay key request parameters information element

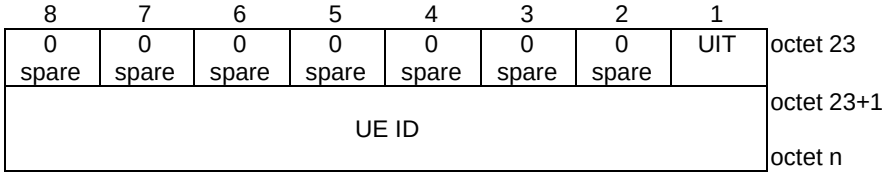


Figure 9.11.3.89.2: UE identity

Table 9.11.3.89.1: Relay key request parameters information element

Relay service code (octet 4 to 6) The relay service code contains 24-bit relay service code as defined in 3GPP TS 24.554 [19E]. Nonce_1 (octet 7 to 22) Nonce_1 is the 128-bit nonce value as defined in 3GPP TS 24.554 [19E]. UE ID type (UIT) (octet 23, bit 1) Bit **1** 0 SUCI 1 CP-PRUK ID UE ID (octet 23+1 to n) UE ID indicates the value of the 5G ProSe remote UE identity or the 5G ProSe end UE identity. If the UE ID type is set to SUCI, the UE ID is coded as 5GS mobile identity IE starting from octet 2 with the Type of identity set to "SUCI" (see subclause 9.11.3.4). If the UE ID type is set to CP-PRUK ID, the UE ID is coded as the CP-PRUK ID as defined in 3GPP TS 33.503 [56].

9.11.3.90 Relay key response parameters

The purpose of the relay key response parameters information element is to transport the parameters of the key response for 5G ProSe UE-to-network relay or 5G ProSe UE-to-UE relay as specified in 3GPP TS 33.503 [56].

The relay key response parameters information element is coded as shown in figure 9.11.3.90.1 and table 9.11.3.90.1.

The relay key response parameters is a type 6 information element.

8	7	6	5	4	3	2	1	
Relay key response parameters IEI								octet 1
Length of Relay key response parameters								octet 2 octet 3
Key K_{NR_ProSe}								octet 4 octet 35
Nonce_2								octet 36 octet 51
CP-PRUK ID								octet 52 octet m

Figure 9.11.3.90.1: Relay key response parameters information element

Table 9.11.3.90.1: Relay key response parameters information element

Key K_{NR_ProSe} (octet 5 to 35) Key K_{NR_ProSe} contains a 256-bit root key that is established between the two entities that communicating using NR PC5 unicast link as defined in 3GPP TS 33.503 [56]. Nonce_2 (octet 36 to 51) Nonce_2 is the 128-bit nonce value as defined in 3GPP TS 24.554 [19E]. CP-PRUK ID (octet 52 to m) The CP-PRUK ID is defined in 3GPP TS 33.503 [56].

9.11.3.91 Priority indicator

The purpose of the Priority indicator information element is to convey a priority indication to the UE.

The Priority indicator information element is coded as shown in figure 9.11.3.91.1 and table 9.11.3.91.1.

The Priority indicator is a type 1 information element.

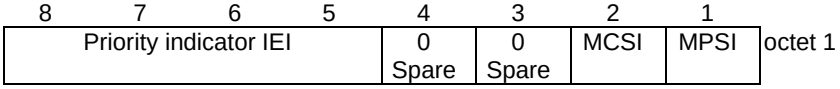


Figure 9.11.3.91.1: Priority indicator

Table 9.11.3.91.1: Priority indicator

MPS indicator (MPSI) (octet 1, bit 1)	
Bit **1**	
0 1	Access identity 1 not valid Access identity 1 valid
MCS indicator (MCSI) (octet 1, bit 2)	
Bit **2**	
0	Access identity 2 not valid
1	Access identity 2 valid
Bits 3, 4 are spare and shall be coded as zero.	

9.11.3.92 SNPN list

The purpose of the SNPN list information element is to provide a list of SNPN identities.

The SNPN list information element is coded as shown in figure 9.11.3.92.1, table 9.11.3.92.1, figure 9.11.3.92.2 and table 9.11.3.92.2.

The SNPN list is a type 4 information element with a minimum length of 11 octets and a maximum length of 137 octets.

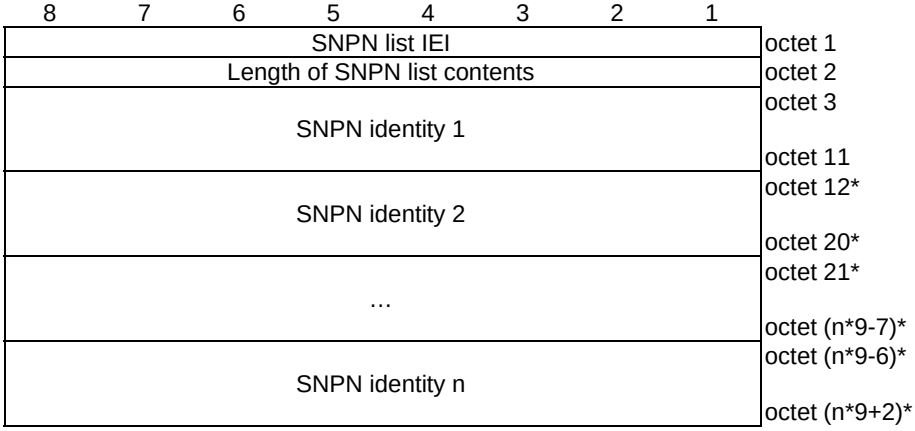


Figure 9.11.3.92.1: SNPN list information element

Table 9.11.3.92.1: SNPN list information element

Each SNPN identity field is coded according to figure 9.11.3.92.2 and table 9.11.3.92.2.

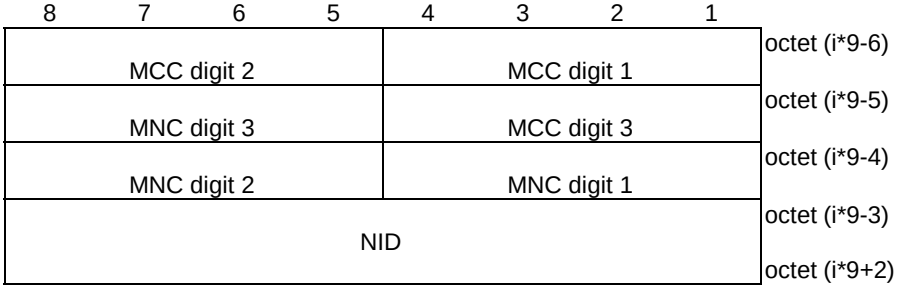


Figure 9.11.3.92.2: SNPN identity i

Table 9.11.3.92.2: SNPN identity i

MCC, Mobile country code (octet (i*9-6), octet (i*9-5) bits 1 to 4) The MCC field is coded as in ITU-T Recommendation E.212 [42], annex A. MNC, Mobile network code (octet (i*9-5) bits 5 to 8, octet (i*9-4)) The coding of this field is the responsibility of each administration but BCD coding shall be used. The MNC shall consist of 2 or 3 digits. If a network operator decides to use only two digits in the MNC, bits 5 to 8 of octet 6 shall be coded as "1111" The MCC and MNC digits are coded as octets 6 to 8 of the Temporary mobile group identity IE in figure 10.5.154 of 3GPP TS 24.008 [12]. NID (octet (i*9-3) to octet (i*9+2)) NID field is coded as the NID field of NID IE as specified in figure 9.2.7-2 and table 9.2.7-2 of 3GPP TS 24.502 [18] starting with the octet 3 and ending with the octet 8.

9.11.3.93 N3IWF identifier

The purpose of the N3IWF identifier information element is to enable the network to assign the UE, a suitable N3IWF for the requested NSSAI.

The N3IWF identifier information element is coded as shown in figure 9.11.3.93.1, figure 9.11.3.93.2, figure 9.11.3.93.3 and table 9.11.3.93.1.

The N3IWF identifier information element is a type 4 information element with a minimum length of 7 octets.

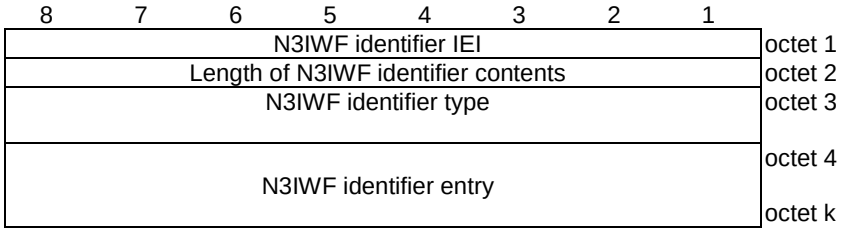


Figure 9.11.3.93.1: N3IWF identifier information element

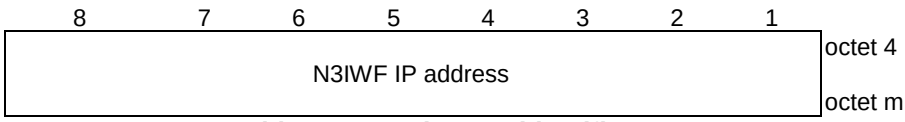


Figure 9.11.3.93.2: N3IWF address entry (N3IWF identifier type = "IPv4", "IPv6" or "IPv4v6")

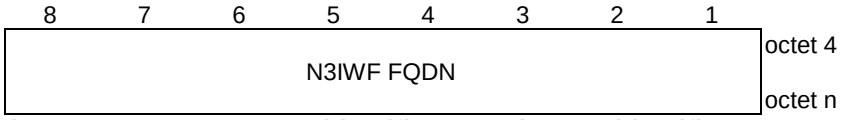


Figure 9.11.3.93.3: N3IWF identifier entry (N3IWF identifiertype ="FQDN")

Table 9.11.3.93.1: N3IWF address entry

N3IWF identifier type (octet 3) is set as follows:								
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	
0	0	0	0	0	0	0	1	IPv4
0	0	0	0	0	0	1	0	IPv6
0	0	0	0	0	0	1	1	IPv4v6
0	0	0	0	0	1	0	0	FQDN
All other values are reserved.								
If the N3IWF identifier type indicates IPv4, then the N3IWF IP address field contains an IPv4 address in octet 4 to octet 7.								
If the N3IWF identifier type indicates IPv6, then the N3IWF IP address field contains an IPv6 address in octet 4 to octet 19.								
If the N3IWF identifier type indicates IPv4v6, then the N3IWF IP address field contains two IP addresses. The first IP address is an IPv4 address in octet 4 to octet 7. The second IP address is an IPv6 address in octet 8 to octet 23.								
If the N3IWF identifier type indicates FQDN, the N3IWF FQDN field in octet 4 to octet n is encoded as defined in subclauses 28.3.2.2.2, 28.3.2.2.3, 28.3.2.2.8 or 28.3.2.2.9 in 3GPP TS 23.003 [4].								

9.11.3.94 TNAN information

The purpose of the TNAN information information element is to enable the network to assign the UE, a suitable TNAN information (SSID and TNGF ID) for the requested NSSAI.

The TNAN information information element is coded as shown in figure 9.11.3.94.1 and table 9.11.3.94.1.

The TNAN information information element is a type 4 information element with a minimum length of 3 octets.

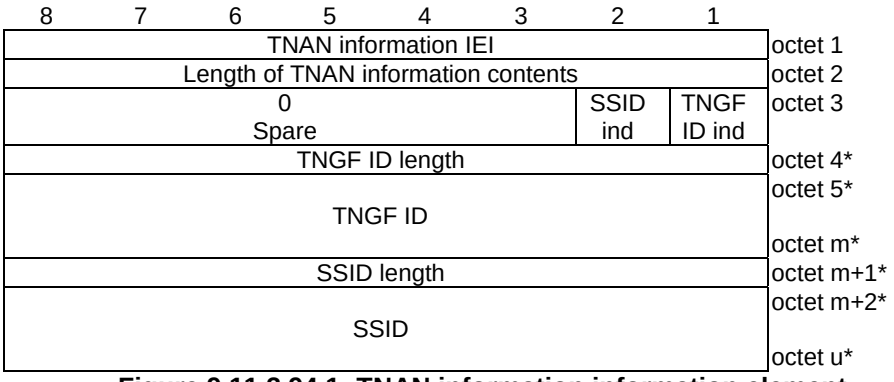


Figure 9.11.3.94.1: TNAN information information element

Table 9.11.3.94.1: TNAN information information element

TNGF ID indication (TNGF ID ind) (bit 1 of octet 3) The TNGF ID ind indicates whether the TNGF ID length field and the TNGF ID field are included in the TNAN information or not. Bit **1** 0 TNGF ID length and TNGF ID not included 1 TNGF ID length and TNGF ID included SSID indication (SSID ind) (bit 2 of octet 3) The SSID ind indicates whether the SSID length field and the SSID field are included in the TNAN information or not. Bit **2** 0 SSID length and SSID not included 1 SSID length and SSID included Bits 3 to 8 of octet 3 are spare and shall be coded as zero TNGF ID length (octet 4) indicates the length of the TNGF ID field. TNGF ID (octets 5 to m) The TNGF ID field is an octet string that indicates the TNGF ID. SSID length (octet m+1) indicates the length of the SSID field. SSID (octets m+2 to u) The SSID field is an octet string which shall have a maximum length of 32 octets (see IEEE Std 802.11 [59]).

9.11.3.95 RAN timing synchronization

The purpose of the RAN timing synchronization IE is to provide information related to the RAN timing synchronization.

The RAN timing synchronization information element is coded as shown in figure 9.11.3.95.1 and table 9.11.3.95.1.

The RAN timing synchronization is a type 4 information element with a length of 3 octets.

8	7	6	5	4	3	2	1	
RAN timing synchronization IEI								octet 1
Length of RAN timing synchronization								octet 2
0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	Rec Req	octet 3

Figure 9.11.3.95.1: RAN timing synchronization information element

Table 9.11.3.95.1: RAN timing synchronization information element

Request to reconnect to the network upon receiving an indication of a change in the RAN timing synchronization status (RecReq) (octet 3, bit 1) Bit **1** 0 Reconnection not requested 1 Reconnection requested Bits 2 to 8 of octet 3 are spare and shall be coded as zero.

9.11.3.96 Extended LADN information

The purpose of the Extended LADN information information element is to provide the UE with the LADN service area for each available LADN associated for an LADN DNN and an S-NSSAI in the current registration area or to delete the Extended LADN information at the UE.

The Extended LADN information information element is coded as shown in figure 9.11.3.96.1, figure 9.11.3.96.2 and table 9.11.3.96.1.

The Extended LADN information is a type 6 information element with a minimum length of 3 octets and a maximum length of 1787 octets.

The Extended LADN information information element can contain a minimum of 0 and a maximum of 8 different LADNs each including a DNN, an S-NSSAI and a 5GS tracking area identity list.

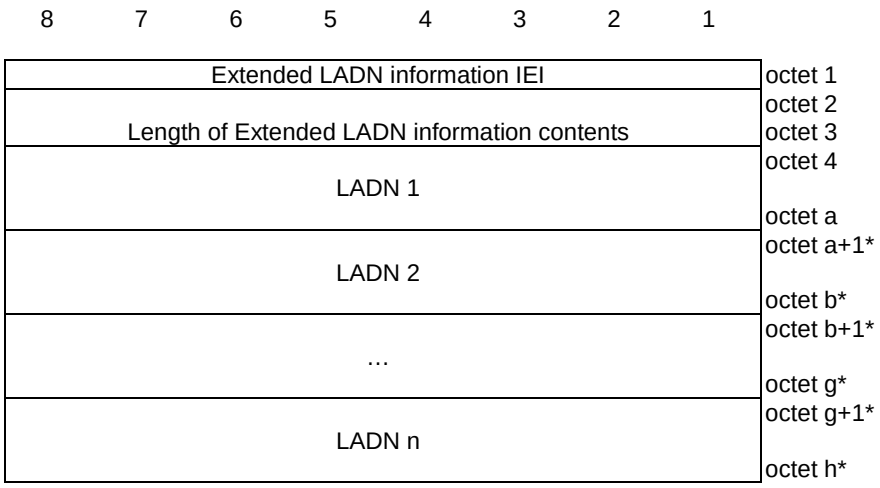


Figure 9.11.3.96.1: Extended LADN information information element

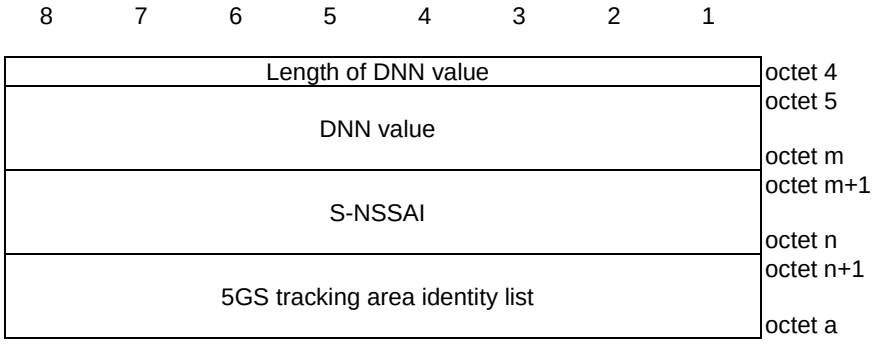


Figure 9.11.3.96.2: LADN

Table 9.11.3.96.1: Extended LADN information information element

Value part of the Extended LADN information information element (octet 4 to octet h) The value part of the Extended LADN information information element consists of one or several LADNs. Each LADN (e.g. octet 4 to octet a) consists of one DNN value, one S-NSSAI and one 5GS tracking area identity list. The length of each LADN is determined by the length of DNN value field, the length of S-NSSAI field and the length of 5GS tracking area identity list field. The UE shall store the complete list as received. If more than 8 LADNs are included in this information element, the UE shall store the first 8 LADNs and ignore the remaining octets of the information element. DNN value (octet 5 to octet m): DNN value field is coded as DNN value part of DNN information element as specified in subclause 9.11.2.1B starting with the third octet. S-NSSAI (octet m+1 to n) (see NOTE 1) S-NSSAI is coded as the length and value part of S-NSSAI information element as specified in subclause 9.11.2.8 starting with the second octet. 5GS tracking area identity list (octet m+1 to octet a): 5GS tracking area identity list field is coded as the length and the value part of the 5GS Tracking area identity list information element as specified in subclause 9.11.3.9 starting with the second octet.
NOTE 1: The S-NSSAI included in the Extended LADN information information element shall be an S-NSSAI from, an allowed NSSAI or an partially allowed NSSAI provided to the UE.

9.11.3.97 Alternative NSSAI

The purpose of the Alternative NSSAI information element is to identify a list of mapping information between the S-NSSAI to be replaced and the alternative S-NSSAI.

The Alternative NSSAI information element is coded as shown in figure 9.11.3.97.1, figure 9.11.3.97.2 and table 9.11.3.97.1.

The Alternative NSSAI is a type 4 information element with minimum length of 2 octets and maximum length of 146 octets.

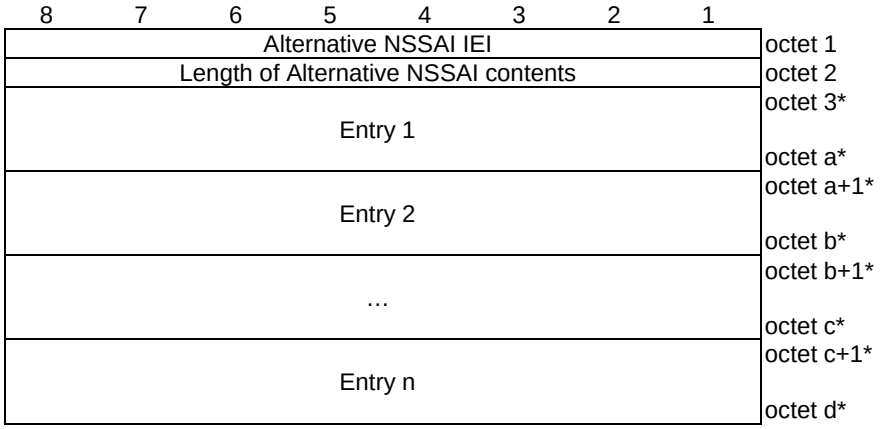


Figure 9.11.3.97.1: Alternative NSSAI information element

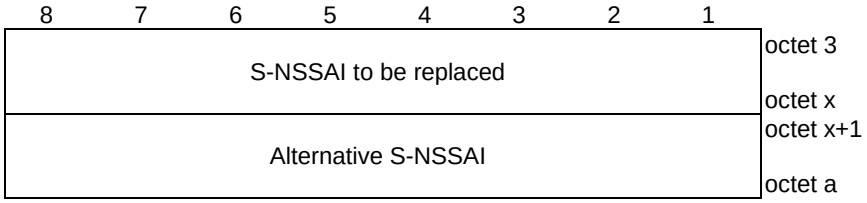


Figure 9.11.3.97.2: Entry

Table 9.11.3.97.1: Alternative NSSAI information element

Value part of the Alternative NSSAI information element (octet 3 to d) The value part of the Alternative NSSAI information element consists of one or more entries, each entry consists of one S-NSSAI to be replaced and one alternative S-NSSAI. The number of entries shall not exceed eight. S-NSSAI to be replaced (octet 3 to x) (see NOTE) S-NSSAI to be replaced is coded as the length and value part of S-NSSAI information element as specified in subclause 9.11.2.8 starting with the second octet. Alternative S-NSSAI (octet x+1 to a) Alternative S-NSSAI is coded as the length and value part of S-NSSAI information element as specified in subclause 9.11.2.8 starting with the second octet.
NOTE: The S-NSSAI to be replaced shall be one S-NSSAI included in the allowed NSSAI.

9.11.3.98 Type 6 IE container

The purpose of the Type 6 IE container information element is to transfer type 6 IEs of format TLV-E explicitly specified for inclusion in this information element for the respective message.

NOTE: Use of this information element is intended only for type 6 IEs added to a message in Rel-18 or later.

The rules for the IEI value encoding specified in 3GPP TS 24.007 [11], subclause 11.2.4, are not applicable for the IEIs of the type 6 IEs within the Type 6 IE container information element. These IEIs can take any value in the range 00 to FF (hexadecimal).

The type 6 IE container information element is coded as shown in figure 9.11.3.98.1, figure 9.11.3.98.2 and table 9.11.3.98.1.

The type 6 IE container is a type 6 information element with a minimum length of 6 octets.

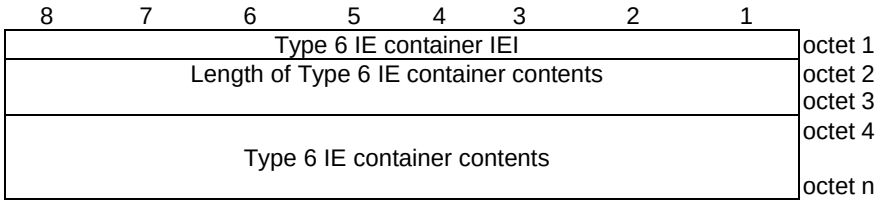


Figure 9.11.3.98.1: Type 6 IE container information element

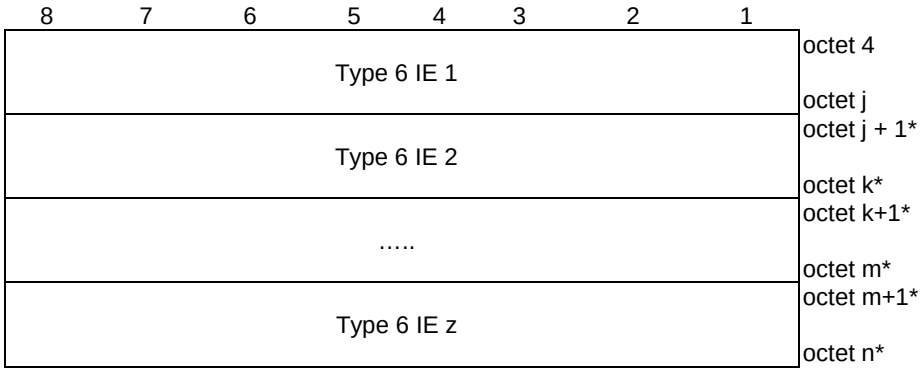


Figure 9.11.3.98.2: Type 6 IE container contents

Table 9.11.3.98.1: Type 6 IE container contents

Type 6 IE container contents (octets 4 to n) The Type 6 IE container is coded according to figure 9.11.3.98.2. The sender of this information element shall encode each type 6 IE included in the contents in format TLV-E. For the coding of each of the type 6 IEs in the type 6 IE container, see the definition of the respective type 6 IE in subclause 9.11

9.11.3.99 Non-3GPP access path switching indication

The purpose of the Non-3GPP access path switching indication information element is to indicate whether the UE supports the non-3GPP access path switching for the PDU session.

The Non-3GPP access path switching indication information element is coded as shown in figure 9.11.3.99.1 and table 9.11.3.99.1.

The Non-3GPP access path switching indication is a type 4 information element with a length of 3 octets.

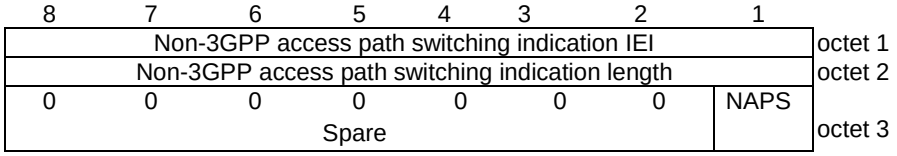


Figure 9.11.3.99.1: Non-3GPP access path switching indication information element

Table 9.11.3.99.1 : Non-3GPP access path switching indication information element

Non-3GPP access path switching (NAPS) (octet 3, bit 1) This bit indicates whether non-3GPP access path switching is supported. Bit **1** 0 non-3GPP access path switching not supported 1 non-3GPP access path switching supported Bits 2 to 8 of octet 3 are spare and shall be coded as zero.

9.11.3.100 S-NSSAI location validity information

The purpose of the S-NSSAI location validity information information element is to provide the S-NSSAI location validity information to the UE.

The S-NSSAI location validity information information element is coded as shown in figures 9.11.3.100.1, 9.11.3.100.2, 9.11.3.100.3, and 9.11.3.100.4 and table 9.11.3.100.1.

The S-NSSAI location validity information information element can contain per-S-NSSAI location validity information for maximum 16 S-NSSAIs.

The S-NSSAI location validity information information is a type 6 information element with a minimum length of 17 octets and a maximum length of 38611 octets.

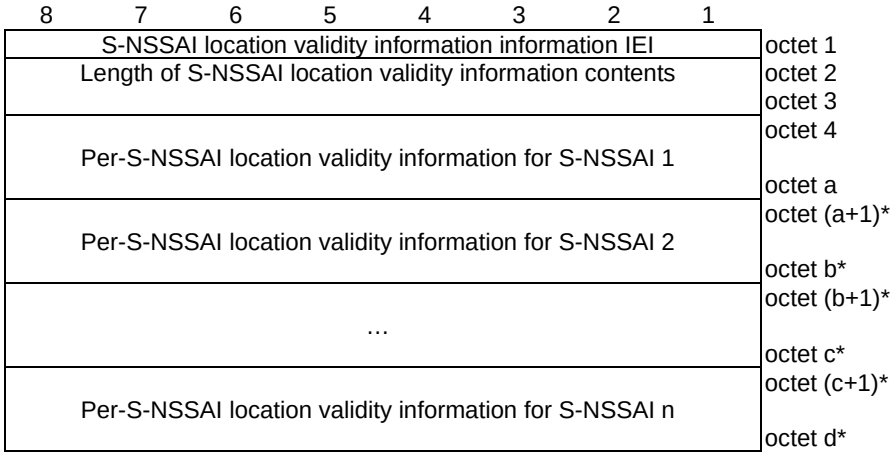


Figure 9.11.3.100.1: S-NSSAI location validity information information element

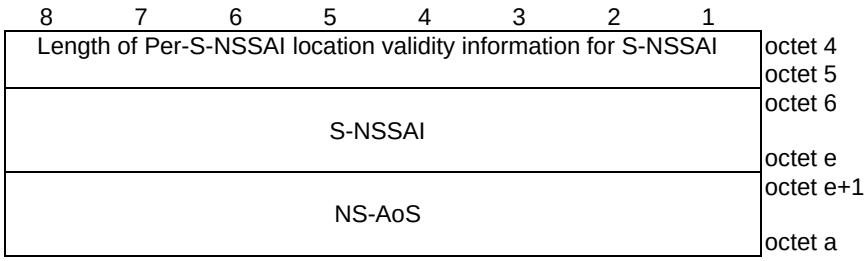


Figure 9.11.3.100.2: Per-S-NSSAI location validity information for S-NSSAI

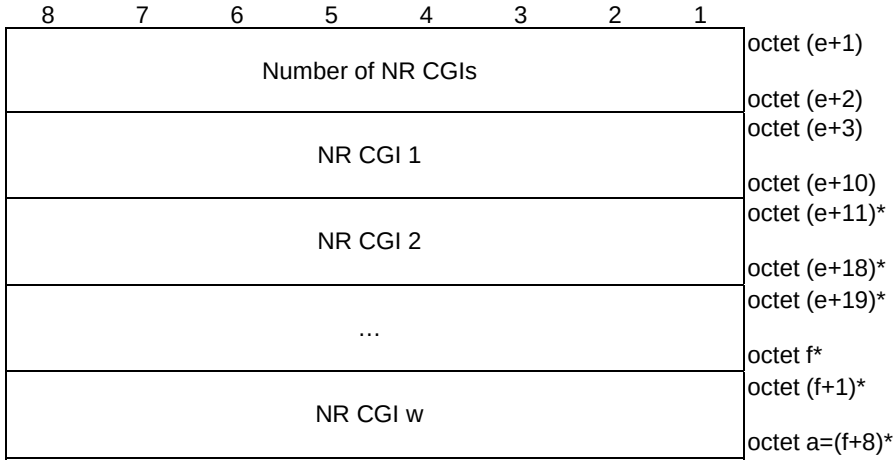


Figure 9.11.3.100.3: NS-AoS

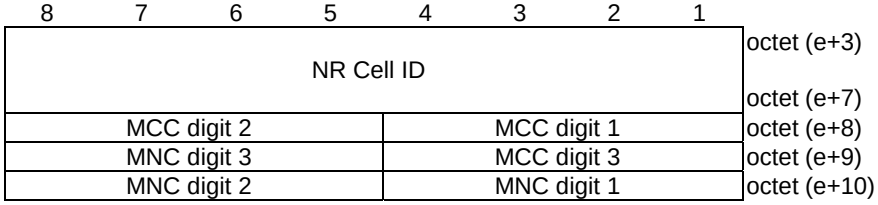


Figure 9.11.3.100.4: NR CGI

Table 9.11.3.100.1: S-NSSAI location validity information information element

S-NSSAI (octet 6 to e) S-NSSAI value is coded as the length and value part of S-NSSAI information element as specified in subclause 9.11.2.8 starting with the second octet. NS-AoS (octet e+1 to octet a) NS-AoS filed consists of the Number of NR cell IDs field and at least two NR CGIs. Number of NR CGIs (octet e+1 to octet e+2) The field indicates the number of NR CGIs included in octets e+3 to octet a. (NOTE). NR CGI (octet e+3 to e+10) The NR CGI globally identifies an NR cell. It contains the NR Cell ID and the PLMN ID of that cell. NR Cell ID (octet e+3 to e+7) The NR Cell ID consists of 36 bits identifying an NR Cell ID as specified in subclause 9.3.1.7 of 3GPP TS 38.413 [31], in hexadecimal representation. Bit 8 of octet e+3 is the most significant bit and bit 5 of octet e+7 is the least significant bit. Bits 1 to 4 of octet e+7 are spare and shall be coded as zero. MCC, Mobile country code (octet e+8 and bits 1 to 4 octet e+9) The MCC field is coded as in ITU-T Recommendation E.212 [42], annex A. MNC, Mobile network code (bits 5 to 8 of octet e+9 and octet e+10) The coding of this field is the responsibility of each administration but BCD coding shall be used. The MNC shall consist of 2 or 3 digits. If a network operator decides to use only two digits in the MNC, bits 5 to 8 of octet e+9 shall be coded as "1111". The MCC and MNC digits are coded as octets 6 to 8 of the Temporary mobile group identity IE in figure 10.5.154 of 3GPP TS 24.008 [12]. NOTE: In this version the specification, the maximum number of NR cell IDs is 300.

9.11.3.101 S-NSSAI time validity information

The purpose of the S-NSSAI time validity information information element is to provide S-NSSAI time validity information of one or more S-NSSAIs to the UE.

The S-NSSAI time validity information information element is coded as shown in figures 9.11.3.101.1 and 9.11.3.101.2 and table 9.11.3.101.1.

The S-NSSAI time validity information information element can contain per-S-NSSAI time validity information for maximum 16 S-NSSAIs.

The S-NSSAI time validity information information is a type 4 information element with a minimum length of 23 octets and a maximum length of 257 octets.

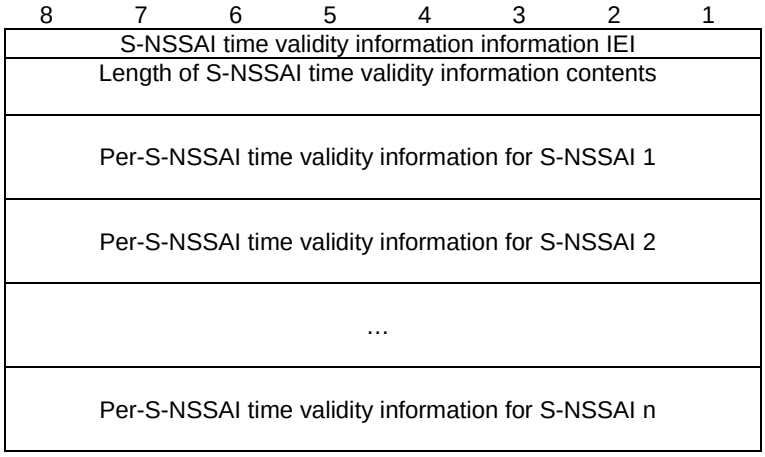


Figure 9.11.3.101.1: S-NSSAI time validity information information element

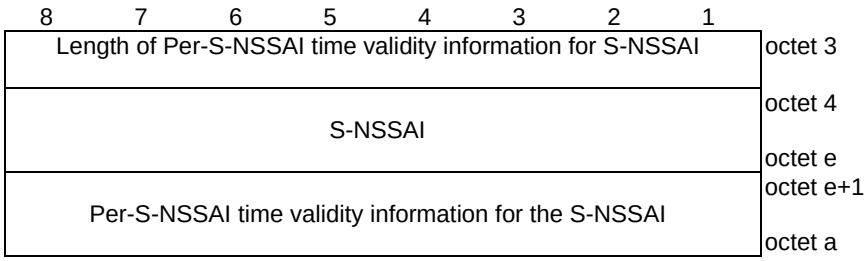


Figure 9.11.3.101.2: Per-S-NSSAI time validity information for S-NSSAI 1

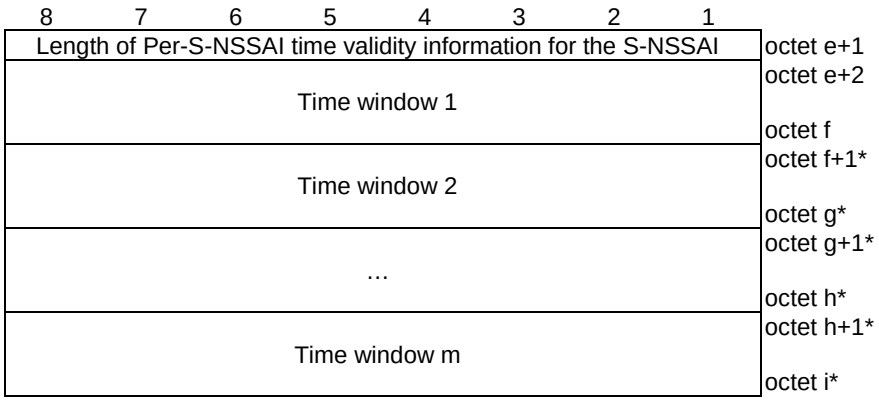


Figure 9.11.3.101.3: Per-S-NSSAI time validity information for the S-NSSAI

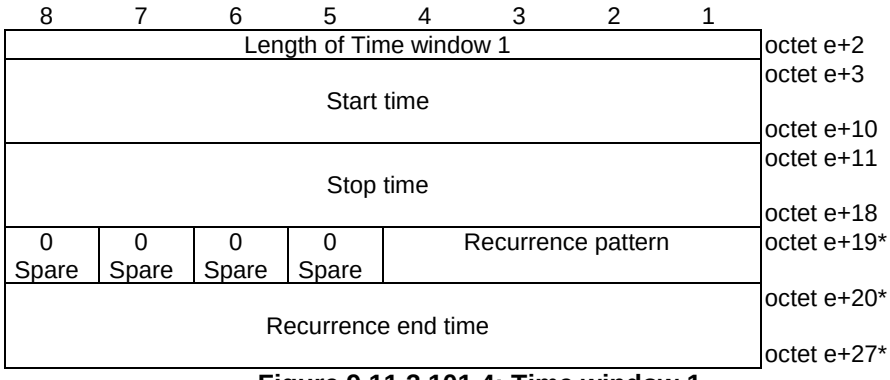


Figure 9.11.3.101.4: Time window 1

Table 9.11.3.101.1: S-NSSAI time validity information information element

S-NSSAI (octet 6 to octet e)
S-NSSAI value is coded as the length and value part of S-NSSAI information element as specified in subclause 9.11.2.8 starting with the second octet.

Start time (octet e+3 to octet e+10)
The field indicates the time when the network slice identified by the S-NSSAI becomes available (for the first time if octet e+20 is included) and is represented by the number of seconds since 00:00:00 on 1 January 1970 UTC and is encoded as the 64-bit NTP timestamp format defined in IETF RFC 5905 [36A], where binary encoding of the integer part is in the first 32 bits and binary encoding of the fraction part in the last 32 bits.

Stop time (octet e+11 to octet e+18)
The field indicates the time when the network slice identified by the S-NSSAI becomes unavailable (for the first time if octet e+20 is included) and is represented by the number of seconds since 00:00:00 on 1 January 1970 UTC and is encoded as the 64-bit NTP timestamp format defined in IETF RFC 5905 [36A], where binary encoding of the integer part is in the first 32 bits and binary encoding of the fraction part in the last 32 bits.

Recurrence pattern (bit 1 to bit 4 of octet e+19)
Bits

4	**3**	**2**	**1**	
0	0	0	0	Everyday
0	0	0	1	Every weekday
0	0	1	0	Every week
0	0	1	1	Every 2 weeks
0	1	0	0	Every month (absolute)
0	1	0	1	Every month (relative)
0	1	1	0	Every quarter (absolute)
0	1	1	1	Every quarter (relative)
1	0	0	0	Every 6 months (absolute)
1	0	0	1	Every 6 months (relative)

All other values are reserved.
The recurrence pattern indicates how often the time window is repeated. For example, if the time window starts at 13:00 on Wednesday January 1st 2020 and stops at 13:30 on Wednesday January 1st 2020 and the recurrent pattern is set to:

- "Everyday", the time window repeats everyday from 13:00 to 13:30;
- "Every week", the time window repeats every Wednesday from 13:00 to 13:30;
- "Every month (absolute)", the time window repeats every 1st day of the month from 13:00 to 13:30; and
- "Every month (relative)", the time window repeats every month on the first Wednesday from 13:00 to 13:30.

Recurrence end time (octet e+20 to octet e+27)
The field indicates the time when the repetition of the time window ends. If the field is not included and octet e+19 is included in the IE, the time window is repeated indefinitely. The field is represented by the number of seconds since 00:00:00 on 1 January 1970 UTC and is encoded as the 64-bit NTP timestamp format defined in IETF RFC 5905 [36A], where binary encoding of the integer part is in the first 32 bits and binary encoding of the fraction part in the last 32 bits.

9.11.3.102 Non-3GPP path switching information

The purpose of the Non-3GPP path switching information information element is to request from the network to keep using the user plane resources of the old non-3GPP access during path switching to the new non-3GPP access.

The Non-3GPP path switching information information element is coded as shown in figure 9.11.3.102.1 and table 9.11.3.102.1.

The Non-3GPP path switching information is a type 4 information element with a length of 3 octets.

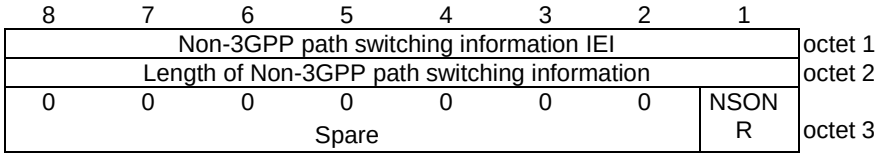


Figure 9.11.3.102.1: Non-3GPP path switching information information element

Table 9.11.3.102.1: Non-3GPP path switching information information element

Non-3GPP path switching while using old non-3GPP resources (NSONR) (octet 3, bit 1) Bit **1** 0 non-3GPP path switching while using old non-3GPP resources not requested 1 non-3GPP path switching while using old non-3GPP resources requested Bits 8 to 2 of octet 3 are spare and shall be coded as zero.

9.11.3.103 Partial NSSAI

The purpose of the Partial NSSAI information element is to deliver one or more S-NSSAIs in a set of tracking areas of a registration area from the network to the UE.

The Partial NSSAI information element is coded as shown in figure 9.11.3.103.1, and table 9.11.3.103.1.

The Partial NSSAI information element is a type 6 information element, with a minimum length of 3 octets and a maximum length of 808 octets.

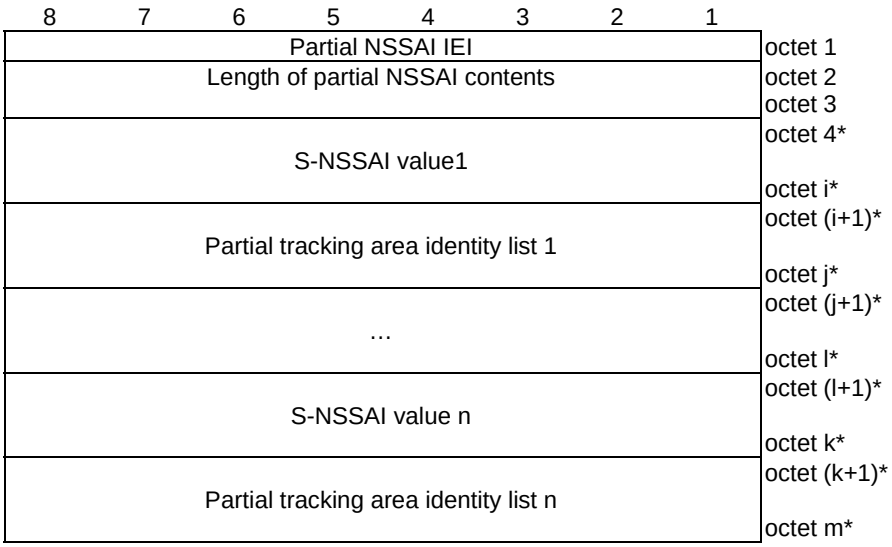


Figure 9.11.3.103.1: Partial NSSAI information element

Table 9.11.3.103.1: Partial NSSAI information element

S-NSSAI value (octet 4 to i) (NOTE 1) S-NSSAI value is coded as the length and value part of S-NSSAI information element as specified in subclause 9.11.2.8 starting with the second octet. Partial tracking area identity list (octet i+1 to j) The partial tracking area identity list field is coded as the length and value part of the 5GS tracking area identity list IE defined in subclause 9.11.3.9 starting with the second octet (NOTE 2).
NOTE 1: The maximum number of S-NSSAIs included in this information element is 7. NOTE 2: A registration area contains maximum 16 different tracking areas, therefore the partial tracking area identity list can contain at the most 15 tracking area identities. NOTE 3: The AMF shall set the Length of partial NSSAI contents to 0 if there are no S-NSSAIs to deliver in a set of tracking areas of a registration area and, the UE shall delete any existing stored partially allowed NSSAI for the current registration area or partially rejected NSSAI for the current registration area.

9.11.3.104 AUN3 indication

The purpose of the AUN3 indication information element is to indicate to the network that the registration request by the 5G-RG is on behalf of an AUN3 device.

The AUN3 indication information element is coded as shown in figure 9.11.3.104.1 and table 9.11.3.104.1.

The AUN3 indication is a type 4 information element with a length of 3 octets.

8	7	6	5	4	3	2	1	
AUN3 indication IEI								octet 1
Length of AUN3 indication								octet 2
0	0	0	0	0	0	0	AUN3 REG	octet 3
Spare								

Figure 9.11.3.104.1: AUN3 indication information element

Table 9.11.3.104.1: AUN3 indication information element

AUN3 device indication bit (AUN3REG) (octet 3, bit 1) Bit **1** 0 AUN3 device registration is not requested 1 AUN3 device registration is requested Bits 8 to 2 of octet 3 are spare and shall be coded as zero.

9.11.3.105 Feature authorization indication

The purpose of the Feature authorization indication information element is to indicate whether the UE that is authorized to operate certain feature.

The Feature authorization indication is a type 4 information element with a minimum length of 3 octets and maximum length of 257 octets.

The Feature authorization indication information element is coded as shown in Figure 9.11.3.105.1 and Table 9.11.3.105.1.

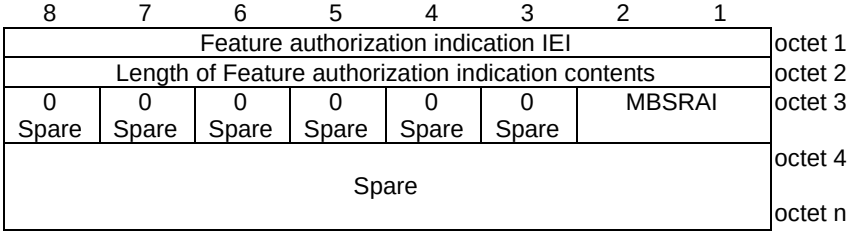


Figure 9.11.3.105.1: Feature authorization indication information element

Table 9.11.3.105.1: Feature authorization indication information element

MBSR authorization indication (MBSRAI) (octet 3, bit 1 to bit 2) This field indicates whether UE is authorized or not to operate as an MBSR node Bits **2 1** 0 0 no information 0 1 not authorized to operate as MBSR but allowed to operate as a UE 1 0 authorized to operate as MBSR 1 1 spare Bits 3 to 8 of octet 3 are spare and shall be coded as zero.

9.11.3.106 Payload container information

The purpose of the Payload container information information element is to provide information related to a payload container.

The Payload container information is a type 1 information element.

The Payload container information information element is coded as shown in figure 9.11.3.106.1 and table 9.11.3.106.1.

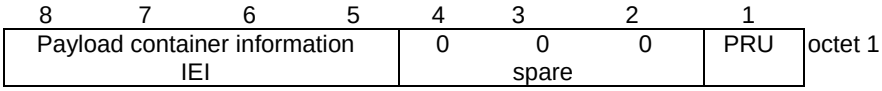


Figure 9.11.3.106.1: Payload container information information element

Table 9.11.3.106.1: Payload container information information element

PRU related content (PRU) (octet 1, bit 1) Bit **1** 0 Payload container not related to PRU 1 Payload container related to PRU Bits 2 to 4 are spare and shall be coded as zero.

9.11.3.107 AUN3 device security key

The purpose of the AUN3 device security key information element is to provide the security keys to the 5G-RG that is acting on behalf of an AUN3 device.

The AUN3 device security key information element is coded as shown in figure 9.11.3.107.1 and table 9.11.3.107.1.

The AUN3 device security key is a type 4 information element with a minimum length of 36 octets.

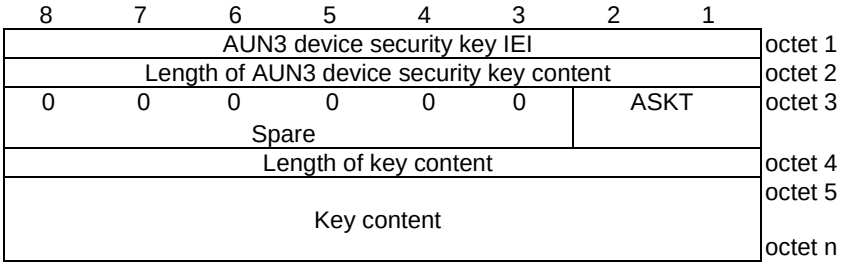


Figure 9.11.3.107.1: AUN3 device security key information element

Table 9.11.3.107.1: AUN3 device security key information element

AUN3 device security key type (ASKT) (bits 1 and 2 of octet 3) The ASKT indicates which AUN3 device security key is included in the IE. Bits **2 1** 0 0 Master session key is included 0 1 K_{WAGF} key is included All other values are unused and shall be interpreted as "Master session key is included", if received by the UE. Key content (octets 5 to n) If ASKT is set to "Master session key included", the Key content contains the value of the Master session key as defined in 3GPP TS 33.501 [24]. If ASKT is set to "K_{WAGF} key included", the Key content contains the value of the K_{WAGF} key as defined in 3GPP TS 33.501 [24].

9.11.3.108 On-demand NSSAI

The purpose of the On-demand NSSAI information element is to provide a list of one or more on-demand S-NSSAIs and the associated slice deregistration inactivity timer value per the on-demand S-NSSAI to the UE.

The On-demand NSSAI information element is coded as shown in figure 9.11.3.108.1, figure 9.11.3.108.2, and table 9.11.3.108.1.

The On-demand NSSAI is a type 4 information element with a minimum length of 5 octets and a maximum length of 210 octets.

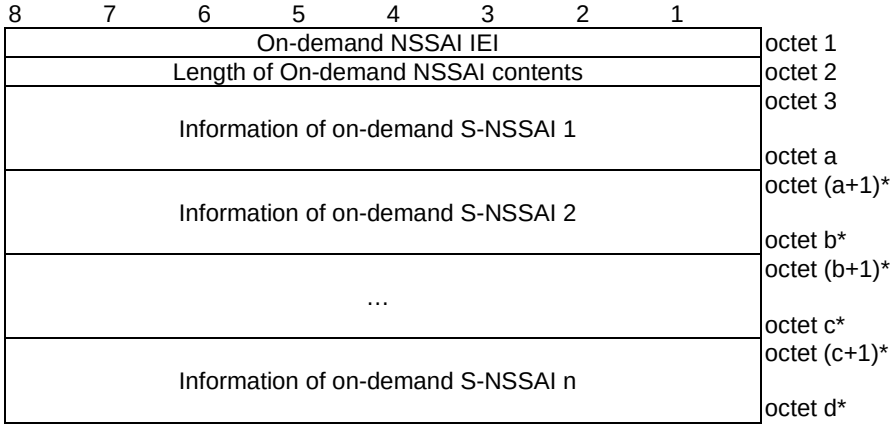


Figure 9.11.3.108.1: On-demand NSSAI information element

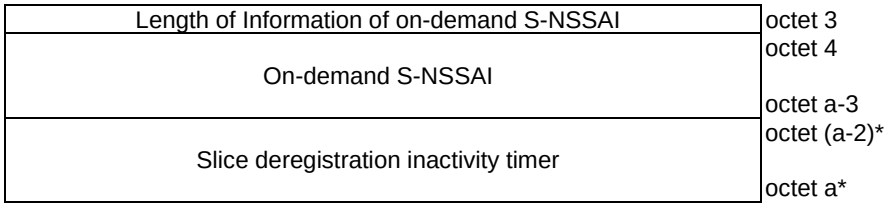


Figure 9.11.3.108.2: Information of on-demand S-NSSAI

Table 9.11.3.108.1: On-demand NSSAI information element

Value part of the On-demand NSSAI information element (octet 3 to d) The value part of the On-demand NSSAI information element consists of one or more Information of on-demand S-NSSAIs. Each Information of on-demand S-NSSAI consists of one on-demand S-NSSAI and optionally the slice deregistration inactivity timer of the on-demand S-NSSAI. The number of information of on-demand S-NSSAIs shall not exceed 16. On-demand S-NSSAI (octet 4 to a-3) On-demand S-NSSAI is coded as the length and value part of S-NSSAI information element as specified in subclause 9.11.2.8 starting with the second octet. Slice deregistration inactivity timer (octet (a-2)* to a*) Slice deregistration inactivity timer is coded as the value part of Time duration information element as specified in subclause 9.9.3.68 of 3GPP TS 24.301 [15] starting with the third octet.

9.11.3.109 Extended 5GMM cause

The purpose of the Extended 5GMM cause information element is to indicate additional information associated with a 5GMM cause.

The Extended 5GMM cause information element is coded as shown in figure 9.11.3.109.1 and table 9.11.3.109.1.

The Extended 5GMM cause is a type 4 information element with a length of 3 octets.

8	7	6	5	4	3	2	1	
Extended 5GMM cause IEI								octet 1
Length of Extended 5GMM cause contents								octet 2
0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	Sat-NR	octet 3

Figure 9.11.3.109.1: Extended 5GMM cause information element

Table 9.11.3.109.1: Extended 5GMM cause information element

Sat-NR value (octet 3, bit 1) Bit **1** 0 Satellite NG-RAN allowed in PLMN 1 Satellite NG-RAN not allowed in PLMN Bit 2 to 8 of octet 3 are spare and shall be coded as zero.

9.11.4 5GS session management (5GSM) information elements

9.11.4.1 5GSM capability

The purpose of the 5GSM capability information element is to indicate UE capability related to the PDU session management.

The 5GSM capability information element is coded as shown in figure 9.11.4.1.1 and table 9.11.4.1.1.

The 5GSM capability is a type 4 information element with a minimum length of 3 octets and a maximum length of 15 octets.

8	7	6	5	4	3	2	1	
5GSM capability IEI								octet 1
Length of 5GSM capability contents								octet 2
TPMIC	ATSSS-ST				EPT-S1	MH6-PDU	RqoS	octet 3
0 Spare	MPQUIC-UDP	MPTCP	ATSSS-LL		0 Spare	SDNAEPC	APMQF	octet 4
0	0	0	0	0	0	0	0	octet 5* -15*
Spare								

Figure 9.11.4.1.1: 5GSM capability information element

Table 9.11.4.1.1: 5GSM capability information element

5GSM capability value
RqoS (octet 3, bit 1)
This bit indicates the 5GSM capability to support reflective QoS.
0 Reflective QoS not supported
1 Reflective QoS supported

Multi-homed IPv6 PDU session (MH6-PDU) (octet 3, bit 2)
This bit indicates the 5GSM capability for Multi-homed IPv6 PDU session.
0 Multi-homed IPv6 PDU session not supported
1 Multi-homed IPv6 PDU session supported

Ethernet PDN type in S1 mode (EPT-S1) (octet 3, bit 3)
This bit indicates UE's 5GSM capability for Ethernet PDN type in S1 mode.
0 Ethernet PDN type in S1 mode not supported
1 Ethernet PDN type in S1 mode supported

Supported ATSSS steering functionalities and steering modes (ATSSS-ST) (octet 3, bits 4 to 7) (NOTE 1)
These bits indicate the 5GSM capability of ATSSS steering functionalities and steering modes
0 0 0 0 ATSSS not supported (NOTE 2)
0 0 0 1 ATSSS Low-Layer functionality with any steering mode allowed for ATSSS-LL supported
0 0 1 0 MPTCP functionality with any steering mode and ATSSS-LL functionality with only active-standby steering mode supported
0 0 1 1 MPTCP functionality with any steering mode and ATSSS-LL functionality with any steering mode allowed for ATSSS-LL supported
All other values are reserved.

Transfer of port management information containers (TPMIC) (octet 3, bit 8)
This bit indicates the 5GSM capability to support transfer of port management information containers
0 Transfer of port management information containers not supported
1 Transfer of port management information containers supported

Access performance measurements per QoS flow rule (APMQF) (octet 4, bit1)
This bit indicates the 5GSM capability to support access performance measurements using the QoS flow of the non default QoS rule, that is used by the service data flow (SDF) traffic.
0 Access performance measurements per QoS flow not supported.
1 Access performance measurements per QoS flow supported.

Secondary DN authentication and authorization over EPC (SDNAEPC) (octet 4, bit 2)
This bit indicates the 5GSM capability to support secondary DN authentication and authorization over EPC
0 Secondary DN authentication and authorization over EPC not supported
1 Secondary DN authentication and authorization over EPC supported

ATSSS-LL functionality support (ATSSS-LL) (octet 4 bits 4 and 5)
This capability indicates the support for ATSSS-LL functionality.
Bit
5 4
0 0 ATSSS-LL functionality not supported (NOTE 2)
0 1 ATSSS-LL functionality with only active-standby steering mode supported
1 0 ATSSS-LL functionality with any steering mode allowed for ATSSS-LL supported
1 1 spare

Supporting MPTCP functionality with any steering mode (MPTCP) (octet 4, bit 6)
This bit indicates whether the MPTCP functionality with any steering mode is supported (NOTE 3).
0 MPTCP functionality with any steering mode not supported (NOTE 2)
1 MPTCP functionality with any steering mode supported

Supporting MPQUIC functionality with any steering mode (MPQUIC-UDP) (octet 4, bit 7)
This bit indicates whether the MPQUIC functionality with any steering mode is supported (NOTE 3).

0	MPQUIC functionality with any steering mode not supported (NOTE 2)
1	MPQUIC functionality with any steering mode supported
All other bits in octet 4 to 15 are spare and shall be coded as zero, if the respective octet is included in the information element.	
NOTE 1: The UE shall populate these bits in the same way as a UE of a previous release..	
NOTE 2: For MA PDU session, at least one of the following fields: ATSSS-ST, ATSSS-LL, MPTCP, and MPQUIC-UDP shall be set to a non-zero value.	
NOTE 3: If ATSSS-LL is set to 00 then this bit shall be set to 0.	

9.11.4.2 5GSM cause

The purpose of the 5GSM cause information element is to indicate the reason why a 5GSM request is rejected.

The 5GSM cause information element is coded as shown in figure 9.11.4.2.1 and table 9.11.4.2.1.

The 5GSM cause is a type 3 information element with a length of 2 octets.

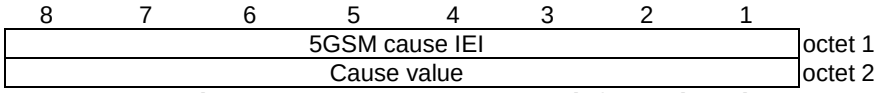


Figure 9.11.4.2.1: 5GSM cause information element

Table 9.11.4.2.1: 5GSM cause information element

Cause value (octet 2) Bits								
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	
0	0	0	0	1	0	0	0	Operator determined barring
0	0	0	1	1	0	1	0	Insufficient resources
0	0	0	1	1	0	1	1	Missing or unknown DNN
0	0	0	1	1	1	0	0	Unknown PDU session type
0	0	0	1	1	1	0	1	User authentication or authorization failed
0	0	0	1	1	1	1	1	Request rejected, unspecified
0	0	1	0	0	0	0	0	Service option not supported
0	0	1	0	0	0	0	1	Requested service option not subscribed
0	0	1	0	0	0	1	1	PTI already in use
0	0	1	0	0	1	0	0	Regular deactivation
0	0	1	0	0	1	0	1	5GS QoS not accepted
0	0	1	0	0	1	1	0	Network failure
0	0	1	0	0	1	1	1	Reactivation requested
0	0	1	0	1	0	0	1	Semantic error in the TFT operation
0	0	1	0	1	0	1	0	Syntactical error in the TFT operation
0	0	1	0	1	0	1	1	Invalid PDU session identity
0	0	1	0	1	1	0	0	Semantic errors in packet filter(s)
0	0	1	0	1	1	0	1	Syntactical error in packet filter(s)
0	0	1	0	1	1	1	0	Out of LADN service area
0	0	1	0	1	1	1	1	PTI mismatch
0	0	1	1	0	0	1	0	PDU session type IPv4 only allowed
0	0	1	1	0	0	1	1	PDU session type IPv6 only allowed
0	0	1	1	0	1	1	0	PDU session does not exist
0	0	1	1	1	0	0	1	PDU session type IPv4v6 only allowed
0	0	1	1	1	0	1	0	PDU session type Unstructured only allowed
0	0	1	1	1	0	1	1	Unsupported 5QI value
0	0	1	1	1	1	0	1	PDU session type Ethernet only allowed
0	1	0	0	0	0	1	1	Insufficient resources for specific slice and DNN
0	1	0	0	0	1	0	0	Not supported SSC mode
0	1	0	0	0	1	0	1	Insufficient resources for specific slice
0	1	0	0	0	1	1	0	Missing or unknown DNN in a slice
0	1	0	1	0	0	0	1	Invalid PTI value
0	1	0	1	0	0	1	0	Maximum data rate per UE for user-plane integrity protection is too low
0	1	0	1	0	0	1	1	Semantic error in the QoS operation
0	1	0	1	0	1	0	0	Syntactical error in the QoS operation
0	1	0	1	0	1	0	1	Invalid mapped EPS bearer identity
0	1	0	1	0	1	1	0	UAS services not allowed
0	1	0	1	1	1	1	1	Semantically incorrect message
0	1	1	0	0	0	0	0	Invalid mandatory information
0	1	1	0	0	0	0	1	Message type non-existent or not implemented
0	1	1	0	0	0	1	0	Message type not compatible with the protocol state
0	1	1	0	0	0	1	1	Information element non-existent or not implemented
0	1	1	0	0	1	0	0	Conditional IE error
0	1	1	0	0	1	0	1	Message not compatible with the protocol state
0	1	1	0	1	1	1	1	Protocol error, unspecified

Any other value received by the UE shall be treated as 0001 1111, " Request rejected, unspecified ". Any other value received by the network shall be treated as 0110 1111, "protocol error, unspecified".

9.11.4.3 Always-on PDU session indication

The purpose of the Always-on PDU session indication information element is to indicate whether a PDU session is established as an always-on PDU session.

The Always-on PDU session indication information element is coded as shown in figure 9.11.4.3.1 and table 9.11.4.3.1.

The Always-on PDU session indication is a type 1 information element.

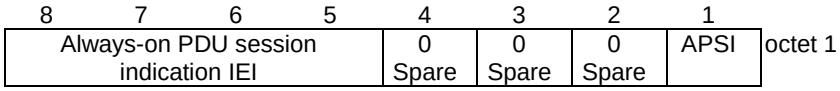


Figure 9.11.4.3.1: Always-on PDU session indication

Table 9.11.4.3.1: Always-on PDU session indication

Always-on PDU session indication (APSI) (octet 1) Bit **1** 0 Always-on PDU session not allowed 1 Always-on PDU session required Bits 2, 3 and 4 are spare and shall be coded as zero,

9.11.4.4 Always-on PDU session requested

The purpose of the Always-on PDU session requested information element is to indicate whether a PDU session is requested to be established as an always-on PDU session.

The Always-on PDU session requested information element is coded as shown in figure 9.11.4.4.1 and table 9.11.4.4.1.

The Always-on PDU session requested is a type 1 information element.

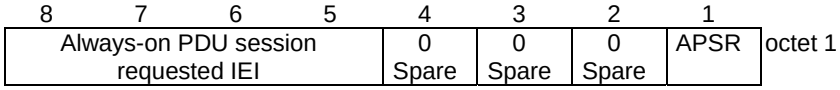


Figure 9.11.4.4.1: Always-on PDU session requested

Table 9.11.4.4.1: Always-on PDU session requested

Always-on PDU session requested (APSR) (octet 1) Bit **1** 0 Always-on PDU session not requested 1 Always-on PDU session requested Bits 2, 3 and 4 are spare and shall be coded as zero,

9.11.4.5 Allowed SSC mode

The purpose of the Allowed SSC mode information element is to indicate the SSC modes allowed to be used by the UE for the PDU session.

The Allowed SSC mode information element is coded as shown in figure 9.11.4.5.1 and table 9.11.4.5.1.

The Allowed SSC mode is a type 1 information element.

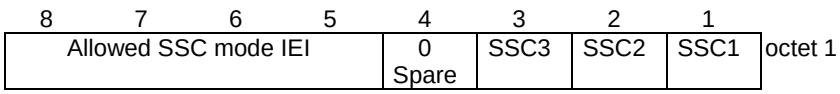


Figure 9.11.4.5.1: Allowed SSC mode information element

Table 9.11.4.5.1: Allowed SSC mode information element

SSC1 (octet 1, bit 1) Bit 1 0 SSC mode 1 not allowed 1 SSC mode 1 allowed SSC2 (octet 1, bit 2) Bit 2 0 SSC mode 2 not allowed 1 SSC mode 2 allowed SSC3 (octet 1, bit 3) Bit 3 0 SSC mode 3 not allowed 1 SSC mode 3 allowed Bit 4 is spare and shall be encoded as zero.

9.11.4.6 Extended protocol configuration options

See subclause 10.5.6.3A in 3GPP TS 24.008 [12].

9.11.4.7 Integrity protection maximum data rate

The purpose of the integrity protection maximum data rate information element is for the UE to indicate to the network the maximum data rate per UE for user-plane integrity protection for uplink and the maximum data rate per UE for user-plane integrity protection for downlink that are supported by the UE.

The integrity protection maximum data rate is coded as shown in figure 9.11.4.7.1 and table 9.11.4.7.2.

The integrity protection maximum data rate is a type 3 information element with a length of 3 octets.

8	7	6	5	4	3	2	1	
Integrity protection maximum data rate IEI								octet 1
Maximum data rate per UE for user-plane integrity protection for uplink								octet 2
Maximum data rate per UE for user-plane integrity protection for downlink								octet 3

Figure 9.11.4.7.1: Integrity protection maximum data rate information element

Table 9.11.4.7.2: Integrity protection maximum data rate information element

Maximum data rate per UE for user-plane integrity protection for uplink (octet 2)								
Bits								
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	
0	0	0	0	0	0	0	0	64 kbps (NOTE 3)
0	0	0	0	0	0	0	1	NULL (NOTE 1)
1	1	1	1	1	1	1	1	Full data rate (NOTE 2)
All other values are spare and shall not be used by a UE compliant to the present version of this specification. If received they shall be interpreted as "64 kbps".								
Maximum data rate per UE for user-plane integrity protection for downlink (octet 3)								
Bits								
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	
0	0	0	0	0	0	0	0	64 kbps (NOTE 3)
0	0	0	0	0	0	0	1	NULL (NOTE 1)
1	1	1	1	1	1	1	1	Full data rate (NOTE 2)
All other values are spare and shall not be used by a UE compliant to the present version of this specification. If received they shall be interpreted as "64 kbps".								
NOTE 1: This value shall be used when N3 data transfer is not supported by the UE or when the UE does not support standalone NR connected to 5GCN.								
NOTE 2: If the UE supports N3 data transfer and supports standalone NR connected to 5GCN (this includes UEs supporting NR-NR dual connectivity, NR-E-UTRA dual connectivity with MN terminated bearers or both of them as described in 3GPP TS 37.340 [51]), then the UE shall use this value.								
NOTE 3: The network can receive this value from a UE compliant to an earlier version of this specification.								

9.11.4.8 Mapped EPS bearer contexts

The purpose of the mapped EPS bearer contexts information element is to indicate a set of EPS bearer contexts for a PDU session, as described in subclause 6.1.4.1.

The mapped EPS bearer contexts information element is a type 6 information element with a minimum length of 7 octet and a maximum length of 65538 octets.

The mapped EPS bearer contexts information element is coded as shown in figure 9.11.4.8.1, figure 9.11.4.8.2, figure 9.11.4.8.3 and table 9.11.4.8.1.

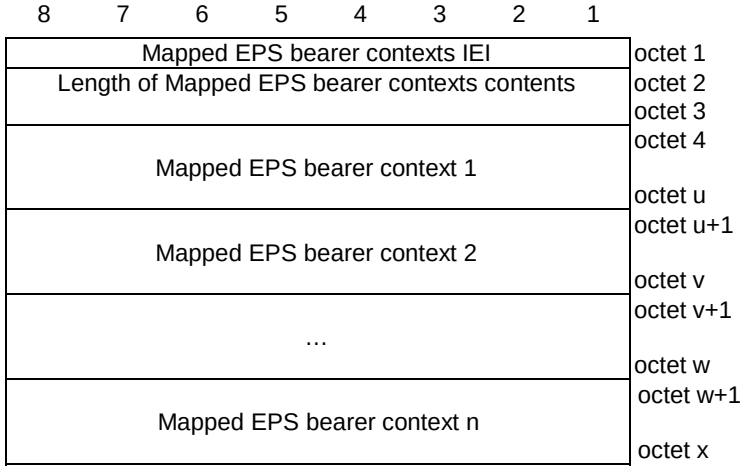


Figure 9.11.4.8.1: Mapped EPS bearer contexts

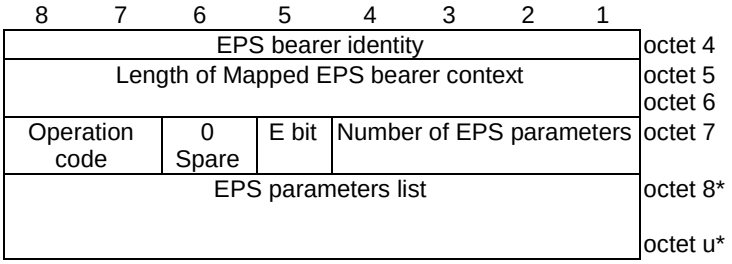


Figure 9.11.4.8.2: Mapped EPS bearer context

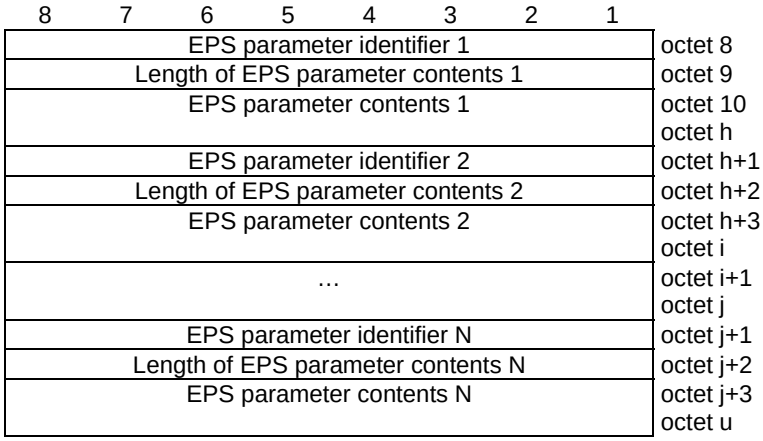


Figure 9.11.4.8.3: EPS parameters list

Table 9.11.4.8.1: Mapped EPS bearer contexts information element

EPS bearer identity (octet 4)

Bits 5 to 8 contain the EPS bearer identity, and are coded as specified in subclause 9.3.2 of 3GPP TS 24.301 [15]. Bits 1 to 4 are spare and shall be coded as zero.

Operation code (bits 8 to 7 of octet 7)
Bits
8 7
0 0 Reserved
0 1 Create new EPS bearer
1 0 Delete existing EPS bearer
1 1 Modify existing EPS bearer

Bit 6 of octet 7 is spare and shall be coded as zero.

E bit (bit 5 of octet 7)
For the "create new EPS bearer" operation, the E bit is encoded as follows:
Bit
5
0 parameters list is not included (NOTE)
1 parameters list is included

For the "modify existing EPS bearer" operation, the E bit is encoded as follows:
Bit
5
0 extension of previously provided parameters list
1 replacement of all previously provided parameters list

If the E bit is set to "parameters list is included", the number of EPS parameters field has non-zero value. If the E bit is set to "extension of previously provided parameters list" or "replacement of previously provided parameters list", the number of parameters field has non-zero value. If the E bit is set to "extension of previously provided parameters" and one of the parameters in the new parameters list already exists in the previously provided parameters, the parameter shall be set to the new value. If the E bit is set to "replacement of all previously provided parameters list" and a parameter in the previously provided parameters is not provided in the new parameters list, the parameter shall be deleted.

For the "create new EPS bearer" operation and "delete existing EPS bearer" operation, bit 5 of octet 7 is ignored.

Number of EPS parameters (bits 4 to 1 of octet 7)
The number of EPS parameters contains the binary coding for the number of EPS parameters in the EPS parameters list field. The number of EPS parameters field is encoded in bits 4 through 1 of octet 7 where bit 4 is the most significant and bit 1 is the least significant bit.

EPS parameters list (octets 8 to u)
The EPS parameters list contains a variable number of EPS parameters.

Each EPS parameter included in the EPS parameters list is of variable length and consists of:
- an EPS parameter identifier (1 octet);
- the length of the EPS parameter contents (1 octet); and
- the EPS parameter contents itself (variable amount of octets).

The EPS parameter identifier field is used to identify each EPS parameter included in the EPS parameters list and it contains the hexadecimal coding of the EPS parameter identifier. Bit 8 of the EPS parameter identifier field contains the most significant bit and bit 1 contains the least significant bit. In this version of the protocol, the following EPS parameter identifiers are specified:
- 01H (Mapped EPS QoS parameters);
- 02H (Mapped extended EPS QoS parameters); and
- 03H (Traffic flow template).
- 04H (APN-AMBR).
- 05H (extended APN-AMBR).

If the EPS parameters list contains an EPS parameter identifier that is not supported by the receiving entity the corresponding EPS parameter shall be discarded. The length of EPS parameter contents field contains the binary coded representation of the length of the EPS parameter contents field. The first bit in transmission order is the most significant bit. When the parameter identifier indicates mapped EPS QoS parameters, the length and parameter contents field are coded as specified in subclause 9.9.4.3 of 3GPP TS 24.301 [15]. When the parameter identifier indicates mapped extended EPS QoS parameters, the length and parameter contents field are coded as specified in subclause 9.9.4.30 of 3GPP TS 24.301 [15]. When the parameter identifier indicates traffic flow template, the length and parameter contents field are coded from octet 2 as shown figure 10.5.144 and table 10.5.162 of 3GPP TS 24.008 [12]. When the parameter identifier indicates APN-AMBR, the length and parameter contents field are coded as specified in subclause 9.9.4.2 of 3GPP TS 24.301 [15]. When the parameter identifier indicates Extended APN-AMBR, the length and parameter contents field are coded as specified in subclause 9.9.4.29 of 3GPP TS 24.301 [15].
NOTE: This value shall not be used In this version of the specification.

9.11.4.9 Maximum number of supported packet filters

The purpose of the Maximum number of supported packet filters information element is for the UE to indicate to the network the maximum number of packet filters, associated with signaled QoS rules, that can be supported by the UE for the PDU session that is being established, when the PDU session type "IPv4", "IPv6", "IPv4v6" or "Ethernet".

The Maximum number of supported packet filters is coded as shown in figure 9.11.4.9.1 and table 9.11.4.9.1.

The Maximum number of supported packet filters is a type 3 information element with a length of 3 octets.

8	7	6	5	4	3	2	1	
Maximum number of supported packet filters IEI								octet 1
Maximum number of supported packet filters								octet 2
Maximum number of supported packet filters (continued)			0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	octet 3

Figure 9.11.4.9.1: Maximum number of supported packet filters information element

Table 9.11.4.9.1: Maximum number of supported packet filters information element

Maximum number of supported packet filters (octet 2 to 3) In the Maximum number of supported packet filters field bit 8 of the first octet is the most significant bit and bit 6 of second octet is the least significant bit. Bit 5 to bit 1 of the second octet are spare bits and shall be coded as zero. The number of supported packet filters shall be in the range of 17 to 1024.

9.11.4.10 PDU address

The purpose of the PDU address information element is to assign to the UE:

- an IPv4 address associated with a PDU session;
- an interface identifier for the IPv6 link local address associated with the PDU session; or
- an IPv4 address and an interface identifier for the IPv6 link local address, associated with the PDU session.

This purpose of the PDU address information element is also to enable the W-AGF acting on behalf of the FN-RG to provide an interface identifier for the IPv6 link local address associated with the PDU session suggested to be allocated to the FN-RG, and to enable the SMF to provide SMF's IPv6 link local address to the W-AGF acting on behalf of the FN-RG.

The PDU address information element is coded as shown in figure 9.11.4.10.1 and table 9.11.4.10.1.

The PDU address is a type 4 information element with minimum length of 7 octets and a maximum length of 31 octets.

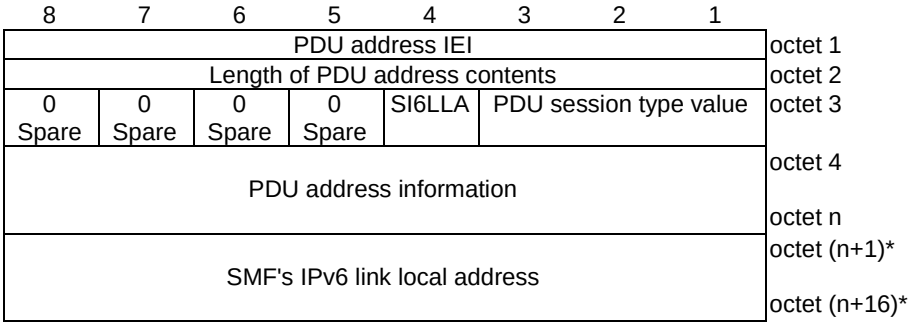


Figure 9.11.4.10.1: PDU address information element

Table 9.11.4.10.1: PDU address information element

PDU session type value (octet 3, bits 1 to 3)
Bits

3	**2**	**1**	
0	0	1	IPv4
0	1	0	IPv6
0	1	1	IPv4v6

All other values are reserved.

SI6LLA (SMF's IPv6 link local address) bit (octet 3, bit 4) (see NOTE)
Bit

4	
0	SMF's IPv6 link local address field is absent
1	SMF's IPv6 link local address field is present

Bits 5 to 8 of octet 3 are spare and shall be coded as zero.

PDU address information (octet 4 to n)

If the PDU session type value indicates IPv4, the PDU address information in octet 4 to octet 7 contains an IPv4 address.

If the PDU session type value indicates IPv6, the PDU address information in octet 4 to octet 11 contains an interface identifier for the IPv6 link local address.

If the PDU session type value indicates IPv4v6, the PDU address information in octet 4 to octet 11 contains an interface identifier for the IPv6 link local address and in octet 12 to octet 15 contains an IPv4 address.

SMF's IPv6 link local address (octet n+1 to n+16)

SMF's IPv6 link local address field contains SMF's IPv6 link local address.

NOTE: In the UE to network direction, the SI6LLA bit shall be set to "SMF's IPv6 link local address field is absent".

9.11.4.11 PDU session type

The purpose of the PDU session type information element is to indicate type of the PDU session.

The PDU session type information element is coded as shown in figure 9.11.4.11.1 and table 9.11.4.11.1.

The PDU session type is a type 1 information element.

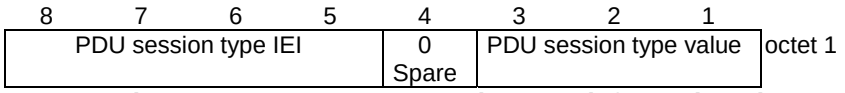


Figure 9.11.4.11.1: PDU session type information element

Table 9.11.4.11.1: PDU session type information element

PDU session type value (octet 1, bit 1 to bit 3)			
Bits			
3	**2**	**1**	
0	0	1	IPv4
0	1	0	IPv6
0	1	1	IPv4v6
1	0	0	Unstructured
1	0	1	Ethernet
1	1	1	reserved
All other values are unused and shall be interpreted as "IPv4v6", if received by the UE or the network.			

9.11.4.12 QoS flow descriptions

The purpose of the QoS flow descriptions information element is to indicate a set of QoS flow descriptions to be used by the UE, where each QoS flow description is a set of parameters as described in subclause 6.2.5.1.1.4.

The QoS flow descriptions information element is a type 6 information element with a minimum length of 6 octets. The maximum length for the information element is 65538 octets.

The QoS flow descriptions information element is coded as shown in figure 9.11.4.12.1, figure 9.11.4.12.2, figure 9.11.4.12.3, figure 9.11.4.12.4, and table 9.11.4.12.1.

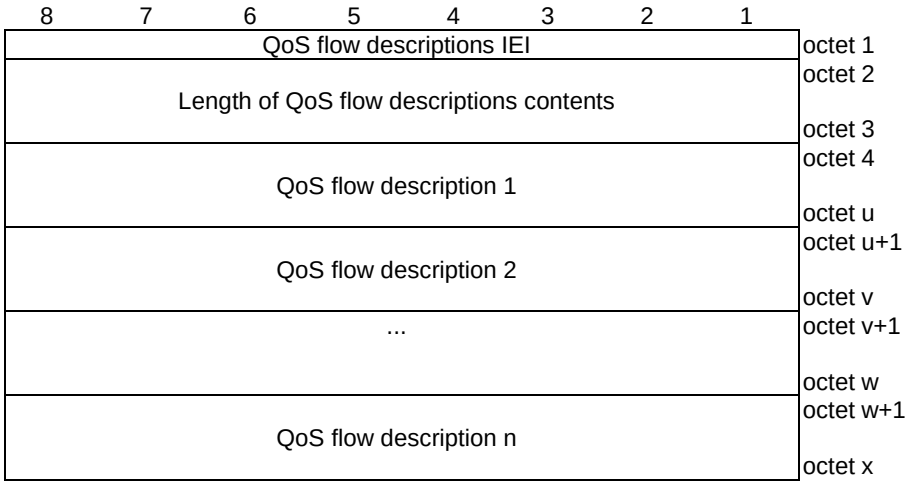


Figure 9.11.4.12.1: QoS flow descriptions information element

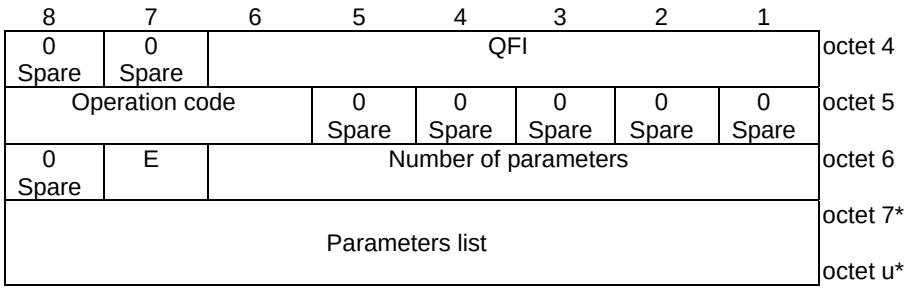


Figure 9.11.4.12.2: QoS flow description

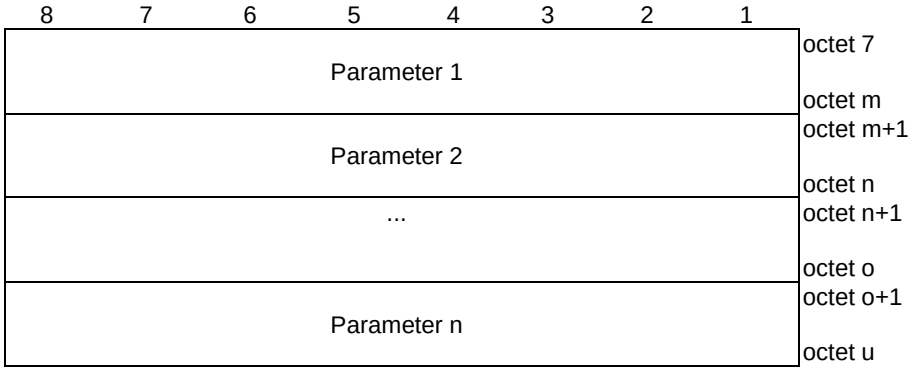


Figure 9.11.4.12.3: Parameters list

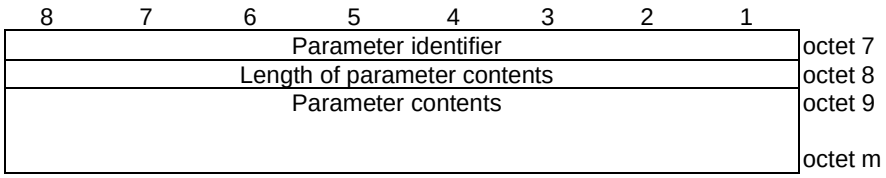


Figure 9.11.4.12.4: Parameter

Table 9.11.4.12.1: QoS flow descriptions information element

QoS flow identifier (QFI) (bits 6 to 1 of octet 4)
QFI field contains the QoS flow identifier.
Bits
6 5 4 3 2 1
0 0 0 0 0 0no QoS flow identifier assigned
0 0 0 0 0 1QFI 1
to
1 1 1 1 1 1QFI 63
The network shall not set the QFI value to 0.

Operation code (bits 8 to 6 of octet 5)
Bits
8 7 6
0 0 1 Create new QoS flow description
0 1 0 Delete existing QoS flow description
0 1 1 Modify existing QoS flow description
All other values are reserved.

E bit (bit 7 of octet 6)
For the "create new QoS flow description" operation, the E bit is encoded as follows:
Bit
7
0 reserved
1 parameters list is included

For the "Delete existing QoS flow description" operation, the E bit is encoded as follows:
Bit
7
0 parameters list is not included
1 reserved

For the "modify existing QoS flow description" operation, the E bit is encoded as follows:
Bit
7
0 extension of previously provided parameters
1 replacement of all previously provided parameters

If the E bit is set to "parameters list is not included", the number of parameters field has zero value. If the E bit is set to "parameters list is included", the number of parameters field has non-zero value. If the E bit is set to "extension of previously provided parameters" or "replacement of all previously provided parameters", the number of parameters field has non-zero value. If the E bit is set to "extension of previously provided parameters" and one of the parameters in the new parameters list already exists in the previously provided parameters, the parameter shall be set to the new value. If the E bit is set to "replacement of all previously provided parameters list" and a parameter in the previously provided parameters is not provided in the new parameters list, the parameter shall be deleted.

Number of parameters (bits 6 to 1 of octet 6)
The number of parameters field contains the binary coding for the number of parameters in the parameters list field. The number of parameters field is encoded in bits 6 through 1 of octet 6 where bit 6 is the most significant and bit 1 is the least significant bit.

Parameters list (octets 7 to u)
The parameters list contains a variable number of parameters.

Each parameter included in the parameters list is of variable length and consists of:
- a parameter identifier (1 octet);
- the length of the parameter contents (1 octet); and
- the parameter contents itself (variable amount of octets).

The parameter identifier field is used to identify each parameter included in the parameters list and it contains the hexadecimal coding of the parameter identifier. Bit 8 of the parameter identifier field contains the most significant bit and bit 1 contains the least significant bit. In this version of the protocol, the following parameter identifiers are specified:
- 01H (5QI);
- 02H (GFBR uplink);
- 03H (GFBR downlink);
- 04H (MFBR uplink);
- 05H (MFBR downlink);
- 06H (Averaging window); and
- 07H (EPS bearer identity).

If the parameters list contains a parameter identifier that is not supported by the receiving entity the corresponding parameter shall be discarded.
The length of parameter contents field contains the binary coded representation of the length of the parameter contents field. The first bit in transmission order is the most significant bit.

When the parameter identifier indicates 5QI, the parameter contents field contains the binary representation of 5G QoS identifier (5QI) that is one octet in length.

5QI:
Bits

8 7 6 5 4 3 2 1	
0 0 0 0 0 0 0 0	Reserved
0 0 0 0 0 0 0 1	5QI 1
0 0 0 0 0 0 1 0	5QI 2
0 0 0 0 0 0 1 1	5QI 3
0 0 0 0 0 1 0 0	5QI 4
0 0 0 0 0 1 0 1	5QI 5
0 0 0 0 0 1 1 0	5QI 6
0 0 0 0 0 1 1 1	5QI 7
0 0 0 0 1 0 0 0	5QI 8
0 0 0 0 1 0 0 1	5QI 9
0 0 0 0 1 0 1 0	5QI 10
0 0 0 0 1 0 1 1	
to	Spare
0 1 0 0 0 0 0 0	
0 1 0 0 0 0 0 1	5QI 65
0 1 0 0 0 0 1 0	5QI 66
0 1 0 0 0 0 1 1	5QI 67
0 1 0 0 0 1 0 0	Spare
0 1 0 0 0 1 0 1	5QI 69
0 1 0 0 0 1 1 0	5QI 70
0 1 0 0 0 1 1 1	5QI 71
0 1 0 0 1 0 0 0	5QI 72
0 1 0 0 1 0 0 1	5QI 73
0 1 0 0 1 0 1 0	5QI 74
0 1 0 0 1 0 1 1	5QI 75
0 1 0 0 1 1 0 0	5QI 76
0 1 0 0 1 1 0 1	
to	Spare
0 1 0 0 1 1 1 0	
0 1 0 0 1 1 1 1	5QI 79
0 1 0 1 0 0 0 0	5QI 80
0 1 0 1 0 0 0 1	Spare
0 1 0 1 0 0 1 0	5QI 82
0 1 0 1 0 0 1 1	5QI 83
0 1 0 1 0 1 0 0	5QI 84
0 1 0 1 0 1 0 1	5QI 85
0 1 0 1 0 1 1 0	5QI 86
0 1 0 1 0 1 1 1	5QI 87
0 1 0 1 1 0 0 0	5QI 88
0 1 0 1 1 0 0 1	5QI 89
0 1 0 1 1 0 1 0	5QI 90
0 1 0 1 1 0 1 1	
to	Spare
0 1 1 1 1 1 1 1	
1 0 0 0 0 0 0 0	
to	Operator-specific 5QIs
1 1 1 1 1 1 1 0	
1 1 1 1 1 1 1 1	Reserved

The network shall consider all other values not explicitly defined in this version of the protocol as unsupported.

If the UE receives a 5QI value (excluding the reserved 5QI values) that it does not understand, the UE shall choose a 5QI value from the set of 5QI values defined in this version of the protocol (see 3GPP TS 23.501 [8]) and associated with:

- GBR QoS flows, if the QoS flow includes a GFBR uplink parameter, a GFBR downlink parameter, a MFBR uplink parameter and a MFBR downlink parameter; and
- non-GBR QoS flows, if the QoS flow does not include any one of a GFBR uplink parameter, a GFBR downlink parameter, a MFBR uplink parameter or a MFBR downlink parameter.

The UE shall use this chosen 5QI value for internal operations only. The UE shall use the received 5QI value in subsequent NAS signalling procedures.

When the parameter identifier indicates "GFBR uplink", the parameter contents field contains one octet indicating the unit of the guaranteed flow bit rate for uplink followed by two octets containing the value of the guaranteed flow bit rate for uplink.

Unit of the guaranteed flow bit rate for uplink (octet 1)
Bits
8 7 6 5 4 3 2 1
0 0 0 0 0 0 0 0 value is not used (see NOTE 2)
0 0 0 0 0 0 0 1 value is incremented in multiples of 1 Kbps
0 0 0 0 0 0 1 0 value is incremented in multiples of 4 Kbps
0 0 0 0 0 0 1 1 value is incremented in multiples of 16 Kbps
0 0 0 0 0 1 0 0 value is incremented in multiples of 64 Kbps
0 0 0 0 0 1 0 1 value is incremented in multiples of 256 Kbps
0 0 0 0 0 1 1 0 value is incremented in multiples of 1 Mbps
0 0 0 0 0 1 1 1 value is incremented in multiples of 4 Mbps
0 0 0 0 1 0 0 0 value is incremented in multiples of 16 Mbps
0 0 0 0 1 0 0 1 value is incremented in multiples of 64 Mbps
0 0 0 0 1 0 1 0 value is incremented in multiples of 256 Mbps
0 0 0 0 1 0 1 1 value is incremented in multiples of 1 Gbps
0 0 0 0 1 1 0 0 value is incremented in multiples of 4 Gbps
0 0 0 0 1 1 0 1 value is incremented in multiples of 16 Gbps
0 0 0 0 1 1 1 0 value is incremented in multiples of 64 Gbps
0 0 0 0 1 1 1 1 value is incremented in multiples of 256 Gbps
0 0 0 1 0 0 0 0 value is incremented in multiples of 1 Tbps
0 0 0 1 0 0 0 1 value is incremented in multiples of 4 Tbps
0 0 0 1 0 0 1 0 value is incremented in multiples of 16 Tbps
0 0 0 1 0 0 1 1 value is incremented in multiples of 64 Tbps
0 0 0 1 0 1 0 0 value is incremented in multiples of 256 Tbps
0 0 0 1 0 1 0 1 value is incremented in multiples of 1 Pbps
0 0 0 1 0 1 1 0 value is incremented in multiples of 4 Pbps
0 0 0 1 0 1 1 1 value is incremented in multiples of 16 Pbps
0 0 0 1 1 0 0 0 value is incremented in multiples of 64 Pbps
0 0 0 1 1 0 0 1 value is incremented in multiples of 256 Pbps
Other values shall be interpreted as multiples of 256 Pbps in this version of the protocol.

Value of the guaranteed flow bit rate for uplink (octets 2 and 3)
Octets 2 and 3 represent the binary coded value of the guaranteed flow bit rate for uplink in units defined by the unit of the guaranteed flow bit rate for uplink.

When the UE indicates subscribed GFBR for uplink, the "GFBR uplink" parameter is not included in the "Parameters list".

When the parameter identifier indicates "GFBR downlink", the parameter contents field contains one octet indicating the unit of the guaranteed flow bit rate for downlink followed by two octets containing the value of the guaranteed flow bit rate for downlink.

Unit of the guaranteed flow bit rate for downlink (octet 1)
The coding is identical to that of the unit of the guaranteed flow bit rate for uplink.

Value of the guaranteed flow bit rate for downlink (octets 2 and 3)
Octets 2 and 3 represent the binary coded value of the guaranteed flow bit rate for downlink in units defined by the unit of the guaranteed flow bit rate for downlink.

When the UE indicates subscribed GFBR for downlink, the "GFBR downlink" parameter is not included in the "Parameters list".

When the parameter identifier indicates "MFBR uplink", the parameter contents field contains the one octet indicating the unit of the maximum flow bit rate for uplink followed by two octets containing the value of maximum flow bit rate for uplink.

Unit of the maximum flow bit rate for uplink (octet 1)
The coding is identical to that of the unit of the guaranteed flow bit rate for uplink.

Value of the maximum flow bit rate for uplink (octets 2 and 3)
Octets 2 and 3 represent the binary coded value of the maximum flow bit rate for uplink in units defined by the unit of the maximum flow bit rate for uplink.

When the UE indicates subscribed MFBR for uplink, the "MFBR uplink" parameter is not included in the "Parameters list".

When the parameter identifier indicates "MFBR downlink", the parameter contents field contains one octet indicating the unit of the maximum flow bit rate for downlink followed by two octets containing the value of the maximum flow bit rate for downlink.

Unit of the maximum flow bit rate for downlink (octet 1)
The coding is identical to that of the unit of the guaranteed flow bit rate for uplink.

Value of the maximum flow bit rate for downlink (octets 2 and 3)
Octets 2 and 3 represent the binary coded value of the maximum flow bit rate for downlink in units defined by the unit of the maximum flow bit rate for downlink.

When the UE indicates subscribed MFBR for downlink, the "MFBR downlink" parameter is not included in the "Parameters list".

In this version of the protocol, for messages specified in the present document, the sending entity shall not request 0 kbps for both the maximum flow bit rate for downlink and the maximum flow bit rate for uplink at the same time. Any entity receiving a request for 0 kbps in both the maximum flow bit rate for downlink and the maximum flow bit rate for uplink shall consider that as a syntactical error (see clause 7).

When the parameter identifier indicates "averaging window", the parameter contents field contains the binary representation of the averaging window for both uplink and downlink in milliseconds and the parameter contents field is two octets in length.

When the parameter identifier indicates EPS bearer identity, the length of EPS bearer identity is one octet, bits 5 to 8 of the parameter contents contain the EPS bearer identity as specified in subclause 9.3.2 of 3GPP TS 24.301 [15] and bits 1 to 4 of the parameter contents are spare and shall be coded as zero. The UE shall not include the EPS bearer identity parameter in any mobile originated 5GSM messages (see NOTE 1).

NOTE 1: The total number of EPS bearer identities included in all QoS flow descriptions of a UE cannot exceed fifteen.
NOTE 2: In this release of the specifications if received it shall be interpreted as value is incremented in multiples of 1 Kbps. In earlier releases of specifications, the interpretation of this value is up to implementation.

9.11.4.13 QoS rules

The purpose of the QoS rules information element is to indicate a set of QoS rules to be used by the UE, where each QoS rule is a set of parameters as described in subclause 6.2.5.1.1.2:

a) for classification and marking of uplink user traffic; and

b) for identification of a QoS flow which the network is to use for a particular downlink user traffic.

NOTE: The UE needs to be aware of a QoS flow which the network is to use for a particular downlink user traffic e.g. to determine whether a resource is available for downlink media of a media stream of an SDP media description provided by the UE in an IMS session.

The QoS rules may contain a set of packet filters consisting of zero or more packet filters for UL direction, zero or more packet filters for DL direction, zero or more packet filters for both UL and DL directions or any combinations of these. The set of packet filters determine the traffic mapping to QoS flows.

The QoS rules information element is a type 6 information element with a minimum length of 7 octets. The maximum length for the information element is 65538 octets.

The QoS rules information element is coded as shown in figure 9.11.4.13.1, figure 9.11.4.13.2, figure 9.11.4.13.3, figure 9.11.4.13.4 and table 9.11.4.13.1.

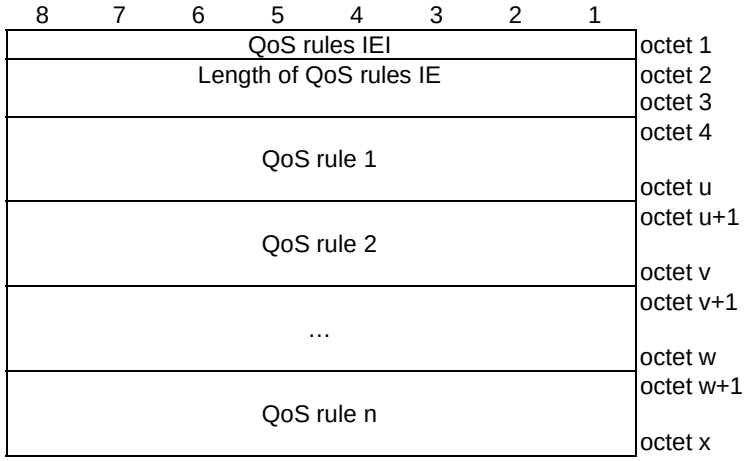


Figure 9.11.4.13.1: QoS rules information element

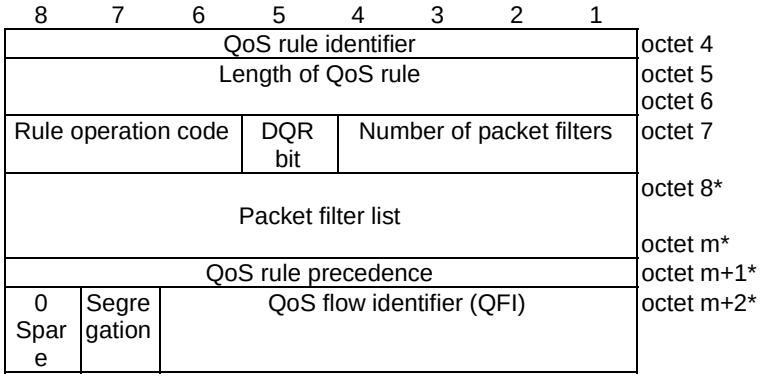


Figure 9.11.4.13.2: QoS rule (u=m+2)

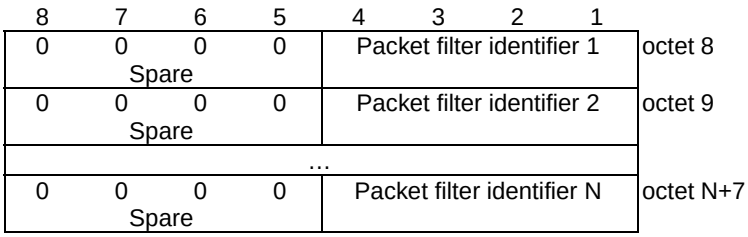


Figure 9.11.4.13.3: Packet filter list when the rule operation is "modify existing QoS rule and delete packet filters" (m=N+7)

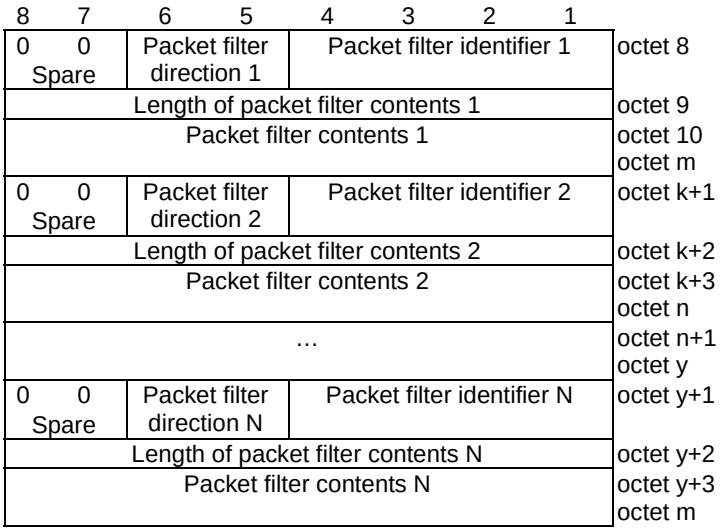


Figure 9.11.4.13.4: Packet filter list when the rule operation is "create new QoS rule", or "modify existing QoS rule and add packet filters" or "modify existing QoS rule and replace all packet filters"

Table 9.11.4.13.1: QoS rules information element

QoS rule identifier (octet 4)
The QoS rule identifier field is used to identify the QoS rule.
Bits
8 7 6 5 4 3 2 1
0 0 0 0 0 0 0 0 no QoS rule identifier assigned
0 0 0 0 0 0 0 1 QRI 1
to
1 1 1 1 1 1 1 1 QRI 255
The network shall not set the QRI value to 0.

QoS rule precedence (octet m+1)
The QoS rule precedence field is used to specify the precedence of the QoS rule among all QoS rules (both the signalled QoS rules as described in subclause 6.2.5.1.1.2 and the derived QoS rules as described in subclause 6.2.5.1.1.3) associated with the PDU session of the QoS flow. This field includes the binary coded value of the QoS rule precedence in the range from 0 to 255 (decimal). The higher the value of the QoS rule precedence field, the lower the precedence of that QoS rule is. For the "delete existing QoS rule" operation, the QoS rule precedence value field shall not be included. For the "create new QoS rule" operation, the QoS rule precedence value field shall be included.
The value 80 (decimal) is reserved.

Segregation bit (bit 7 of octet m+2) (see NOTE 1)
In the UE to network direction the segregation bit indicates whether the UE is requesting the network to bind service data flows described by the QoS rule to a dedicated QoS Flow and it is encoded as follows. In the network to UE direction this bit is spare.
Bit
7
0 Segregation not requested
1 Segregation requested

QoS flow identifier (QFI) (bits 6 to 1 of octet m+2) (see NOTE 1)
The QoS flow identifier (QFI) field contains the QoS flow identifier.
Bits
6 5 4 3 2 1
0 0 0 0 0 0no QoS flow identifier assigned
0 0 0 0 0 1QFI 1
to
1 1 1 1 1 1QFI 63
The network shall not set the QFI value to 0.
For the "delete existing QoS rule" operation, the QoS flow identifier value field shall not be included. For the "create new QoS rule" operation, the QoS flow identifier value field shall be included.

DQR bit (bit 5 of octet 7)
The DQR bit indicates whether the QoS rule is the default QoS rule and it is encoded as follows:
Bit
5
0 the QoS rule is not the default QoS rule.
1 the QoS rule is the default QoS rule.

Rule operation code (bits 8 to 6 of octet 7)
Bits
8 7 6
0 0 0 Reserved
0 0 1 Create new QoS rule
0 1 0 Delete existing QoS rule
0 1 1 Modify existing QoS rule and add packet filters
1 0 0 Modify existing QoS rule and replace all packet filters
1 0 1 Modify existing QoS rule and delete packet filters
1 1 0 Modify existing QoS rule without modifying packet filters
1 1 1 Reserved

Number of packet filters (bits 4 to 1 of octet 7)

The number of packet filters contains the binary coding for the number of packet filters in the packet filter list. The number of packet filters field is encoded in bits 4 through 1 of octet 7 where bit 4 is the most significant and bit 1 is the least significant bit. For the "delete existing QoS rule" operation and for the "modify existing QoS rule without modifying packet filters" operation, the number of packet filters shall be coded as 0. For the "create new QoS rule" operation and the "modify existing QoS rule and replace all packet filters" operation, the number of packet filters shall be greater than or equal to 0 and less than or equal to 15. For all other operations, the number of packet filters shall be greater than 0 and less than or equal to 15.

Packet filter list (octets 8 to m)
The packet filter list contains a variable number of packet filters.

For the "delete existing QoS rule" operation, the length of QoS rule field is set to one.

For the "delete existing QoS rule" operation and the "modify existing QoS rule without modifying packet filters" operation, the packet filter list shall be empty.

For the "modify existing QoS rule and delete packet filters" operation, the packet filter list shall contain a variable number of packet filter identifiers. This number shall be derived from the coding of the number of packet filters field in octet 7.

For the "create new QoS rule" operation and for the "modify existing QoS rule and replace all packet filters" operation, the packet filter list shall contain 0 or a variable number of packet filters. This number shall be derived from the coding of the number of packet filters field in octet 7.

For the "modify existing QoS rule and add packet filters" operation, the packet filter list shall contain a variable number of packet filters. This number shall be derived from the coding of the number of packet filters field in octet 7.

Each packet filter is of variable length and consists of
a packet filter direction (2 bits);
- a packet filter identifier (4 bits);
- the length of the packet filter contents (1 octet); and
- the packet filter contents itself (variable amount of octets).

The packet filter direction field is used to indicate for what traffic direction the filter applies.
Bits
6 5
0 0 reserved
0 1 downlink only (see NOTE 2)
1 0 uplink only
1 1 bidirectional

The packet filter identifier field is used to identify each packet filter in a QoS rule. The least significant 4 bits are used. When the UE requests to "create new QoS rule", "modify existing QoS rule and replace all packet filters" or "modify existing QoS rule and add packet filters", the packet filter identifier values shall be set to 0.

The length of the packet filter contents field contains the binary coded representation of the length of the packet filter contents field of a packet filter. The first bit in transmission order is the most significant bit.

The packet filter contents field is of variable size and contains a variable number (at least one) of packet filter components. Each packet filter component shall be encoded as a sequence of a one octet packet filter component type identifier and a fixed length packet filter component value field. The packet filter component type identifier shall be transmitted first.

In each packet filter, there shall not be more than one occurrence of each packet filter component type. Among the "IPv4 remote address type" and "IPv6 remote address/prefix length type" packet filter components, only one shall be present in one packet filter. Among the "IPv4 local address type" and "IPv6 local address/prefix length type" packet filter components, only one shall be present in one packet filter.

Among the "single local port type" and "local port range type" packet filter components, only one shall be present in one packet filter. Among the "single remote port type" and "remote port range type" packet filter components, only one shall be present in one packet filter. Among the "destination MAC address type" and "destination MAC address range type" packet filter components, only one shall be present in one packet filter. Among the "source MAC address type" and "source MAC address range type" packet filter components, only one shall be present in one packet filter. If the "match-all type" packet filter component is present in the packet filter, no other packet filter component shall be present in the packet filter and the length of the packet filter contents field shall be set to one. If the "Ethertype type" packet filter component is present in the packet filter and the "Ethertype type" packet filter component value is neither "0800H" (for IPv4) nor "86DDH" (for IPv6), no IP packet filter component shall be present in the packet filter.

The term "IP packet filter component" refers to "IPv4 remote address type", "IPv4 local address type", "IPv6 remote address/prefix length type", "IPv6 local address/prefix length type", "Protocol identifier/Next header type", "Single local port type", "Local port range type", "Single remote port type", "Remote port range type", "Security parameter index type", "Type of service/Traffic class type" and "Flow label type".

The term local refers to the UE and the term remote refers to an external network entity.

Packet filter component type identifier

Bits	
8 7 6 5 4 3 2 1	
0 0 0 0 0 0 0 1	Match-all type (see NOTE 2)
0 0 0 1 0 0 0 0	IPv4 remote address type
0 0 0 1 0 0 0 1	IPv4 local address type
0 0 1 0 0 0 0 1	IPv6 remote address/prefix length type
0 0 1 0 0 0 1 1	IPv6 local address/prefix length type
0 0 1 1 0 0 0 0	Protocol identifier/Next header type
0 1 0 0 0 0 0 0	Single local port type
0 1 0 0 0 0 0 1	Local port range type
0 1 0 1 0 0 0 0	Single remote port type
0 1 0 1 0 0 0 1	Remote port range type
0 1 1 0 0 0 0 0	Security parameter index type
0 1 1 1 0 0 0 0	Type of service/Traffic class type
1 0 0 0 0 0 0 0	Flow label type
1 0 0 0 0 0 0 1	Destination MAC address type
1 0 0 0 0 0 1 0	Source MAC address type
1 0 0 0 0 0 1 1	802.1Q C-TAG VID type
1 0 0 0 0 1 0 0	802.1Q S-TAG VID type
1 0 0 0 0 1 0 1	802.1Q C-TAG PCP/DEI type
1 0 0 0 0 1 1 0	802.1Q S-TAG PCP/DEI type
1 0 0 0 0 1 1 1	Ethertype type
1 0 0 0 1 0 0 0	Destination MAC address range type
1 0 0 0 1 0 0 1	Source MAC address range type

All other values are reserved.

The description and valid combinations of packet filter component type identifiers in a packet filter are defined in 3GPP TS 23.501 [8].

For "match-all type", the packet filter component shall not include the packet filter component value field.

For "IPv4 remote address type", the packet filter component value field shall be encoded as a sequence of a four octet IPv4 address field and a four octet IPv4 address mask field. The IPv4 address field shall be transmitted first.

For "IPv4 local address type", the packet filter component value field shall be encoded as defined for "IPv4 remote address type".

For "IPv6 remote address/prefix length type", the packet filter component value field shall be encoded as a sequence of a sixteen octet IPv6 address field and one octet prefix length field. The IPv6 address field shall be transmitted first.

For "IPv6 local address/prefix length type", the packet filter component value field shall be encoded as defined for "IPv6 remote address /prefix length".

For "protocol identifier/Next header type", the packet filter component value field shall be encoded as one octet which specifies the IPv4 protocol identifier or Ipv6 next header.

For "single local port type" and "single remote port type", the packet filter component value field shall be encoded as two octets which specify a port number.

For "local port range type" and "remote port range type", the packet filter component value field shall be encoded as a sequence of a two octet port range low limit field and a two octet port range high limit field. The port range low limit field shall be transmitted first.

For "security parameter index", the packet filter component value field shall be encoded as four octets which specify the IPSec security parameter index.

For "type of service/traffic class type", the packet filter component value field shall be encoded as a sequence of a one octet type-of-service/traffic class field and a one octet type-of-service/traffic class mask field. The type-of-service/traffic class field shall be transmitted first.

For "flow label type", the packet filter component value field shall be encoded as three octets which specify the IPv6 flow label. The bits 8 through 5 of the first octet shall be spare whereas the remaining 20 bits shall contain the IPv6 flow label.

For "destination MAC address type" and "source MAC address type", the packet filter component value field shall be encoded as 6 octets which specify a MAC address. When the packet filter direction field indicates "bidirectional", the destination MAC address is the remote MAC address and the source MAC address is the local MAC address.

For "802.1Q C-TAG VID type", the packet filter component value field shall be encoded as two octets which specify the VID of the customer-VLAN tag (C-TAG). The bits 8 through 5 of the first octet shall be spare whereas the remaining 12 bits shall contain the VID. If there are more than one C-TAG in the Ethernet frame header, the outermost C-TAG is evaluated.

For "802.1Q S-TAG VID type", the packet filter component value field shall be encoded as two octets which specify the VID of the service-VLAN tag (S-TAG). The bits 8 through 5 of the first octet shall be spare whereas the remaining 12 bits shall contain the VID. If there are more than one S-TAG in the Ethernet frame header, the outermost S-TAG is evaluated.

For "802.1Q C-TAG PCP/DEI type", the packet filter component value field shall be encoded as one octet which specifies the 802.1Q C-TAG PCP and DEI. The bits 8 through 5 of the octet shall be spare, the bits 4 through 2 contain the PCP and bit 1 contains the DEI. If there are more than one C-TAG in the Ethernet frame header, the outermost C-TAG is evaluated.

For "802.1Q S-TAG PCP/DEI type", the packet filter component value field shall be encoded as one octet which specifies the 802.1Q S-TAG PCP. The bits 8 through 5 of the octet shall be spare, the bits 4 through 2 contain the PCP and bit 1 contains the DEI. If there are more than one S-TAG in the Ethernet frame header, the outermost S-TAG is evaluated.

For "ethertype type", the packet filter component value field shall be encoded as two octets which specify an ethertype.

For "destination MAC address range type", the packet filter component value field shall be encoded as a sequence of a 6 octet destination MAC address range low limit field and a 6 octet destination MAC address range high limit field. The destination MAC address range low limit field shall be transmitted first. When the packet filter direction field indicates "bidirectional", the destination MAC address range is the remote MAC address range.

For "source MAC address range type", the packet filter component value field shall be encoded as a sequence of a 6 octet source MAC address range low limit field and a 6 octet source MAC address range high limit field. The source MAC address range low limit field shall be transmitted first. When the packet filter direction field indicates "bidirectional", the source MAC address is the local MAC address range.
NOTE 1: Octet m+2 shall not be included without octet m+1. NOTE 2: The "Match-all type" packet filter component type identifier shall not be used with packet filter direction "downlink only".

9.11.4.14 Session-AMBR

The purpose of the Session-AMBR information element is to indicate the initial subscribed PDU session aggregate maximum bit rate when the UE establishes a PDU session or to indicate the new subscribed PDU session aggregate maximum bit rate if it is changed by the network.

The Session-AMBR information element is coded as shown in figure 9.11.4.14.1 and table 9.11.4.14.1.

The Session-AMBR is a type 4 information element with a length of 8 octets.

8	7	6	5	4	3	2	1	
Session-AMBR IEI								octet 1
Length of Session-AMBR contents								octet 2
Unit for Session-AMBR for downlink								octet 3
Session-AMBR for downlink								octet 4-5
Unit for Session-AMBR for uplink								octet 6
Session-AMBR for uplink								octet 7-8

Figure 9.11.4.14.1: Session-AMBR information element

Table 9.11.4.14.1: Session-AMBR information element

Unit for Session-AMBR for downlink (octet 3) 0 0 0 0 0 0 0 0 value is not used (see NOTE) 0 0 0 0 0 0 0 1 value is incremented in multiples of 1 Kbps 0 0 0 0 0 0 1 0 value is incremented in multiples of 4 Kbps 0 0 0 0 0 0 1 1 value is incremented in multiples of 16 Kbps 0 0 0 0 0 1 0 0 value is incremented in multiples of 64 Kbps 0 0 0 0 0 1 0 1 value is incremented in multiples of 256 kbps 0 0 0 0 0 1 1 0 value is incremented in multiples of 1 Mbps 0 0 0 0 0 1 1 1 value is incremented in multiples of 4 Mbps 0 0 0 0 1 0 0 0 value is incremented in multiples of 16 Mbps 0 0 0 0 1 0 0 1 value is incremented in multiples of 64 Mbps 0 0 0 0 1 0 1 0 value is incremented in multiples of 256 Mbps 0 0 0 0 1 0 1 1 value is incremented in multiples of 1 Gbps 0 0 0 0 1 1 0 0 value is incremented in multiples of 4 Gbps 0 0 0 0 1 1 0 1 value is incremented in multiples of 16 Gbps 0 0 0 0 1 1 1 0 value is incremented in multiples of 64 Gbps 0 0 0 0 1 1 1 1 value is incremented in multiples of 256 Gbps 0 0 0 1 0 0 0 0 value is incremented in multiples of 1 Tbps 0 0 0 1 0 0 0 1 value is incremented in multiples of 4 Tbps 0 0 0 1 0 0 1 0 value is incremented in multiples of 16 Tbps 0 0 0 1 0 0 1 1 value is incremented in multiples of 64 Tbps 0 0 0 1 0 1 0 0 value is incremented in multiples of 256 Tbps 0 0 0 1 0 1 0 1 value is incremented in multiples of 1 Pbps 0 0 0 1 0 1 1 0 value is incremented in multiples of 4 Pbps 0 0 0 1 0 1 1 1 value is incremented in multiples of 16 Pbps 0 0 0 1 1 0 0 0 value is incremented in multiples of 64 Pbps 0 0 0 1 1 0 0 1 value is incremented in multiples of 256 Pbps Other values shall be interpreted as multiples of 256 Pbps in this version of the protocol. Session-AMBR for downlink (octets 4 and 5) Octets 4 and 5 represent the binary coded value of PDU session aggregated maximum bit rate for downlink in units defined by octet 3. Unit for Session-AMBR for uplink (octet 6) The coding is identical to the unit coding defined for Session-AMBR for downlink (octet 3) Session-AMBR for uplink (octets 7 and 8) Octets 7 and 8 represent the binary coded value of PDU session aggregated maximum bit rate for uplink in units defined by octet 6.
NOTE: In this release of the specifications if received it shall be interpreted as value is incremented in multiples of 1 Kbps. In earlier releases of specifications, the interpretation of this value is up to implementation.

9.11.4.15 SM PDU DN request container

The purpose of the SM PDU DN request container information element is to carry a DN-specific identity of the UE in the network access identifier (NAI) format.

The SM PDU DN request container information element is coded as shown in figure 9.11.4.15.1 and table 9.11.4.15.1.

The SM PDU DN request container is a type 4 information element with minimal length of 3 octets and maximum length of 255 octets.

8	7	6	5	4	3	2	1	
SM PDU DN request container information IEI								octet 1
SM PDU DN request container information length								octet 2
DN-specific identity								octets 3*-n*

Figure 9.11.4.15.1: SM PDU DN request container information element

Table 9.11.4.15.1: SM PDU DN request container information element

DN-specific identity (octet 3 to octet n) A DN-specific identity of the UE in the network access identifier (NAI) format according to IETF RFC 7542 [37], encoded as UTF-8 string.

9.11.4.16 SSC mode

The purpose of the SSC mode information element is to indicate SSC mode.

The SSC mode information element is coded as shown in figure 9.11.4.16.1 and table 9.11.4.16.1.

The SSC mode is a type 1 information element.

8	7	6	5	4	3	2	1	
SSC mode IEI				0 Spare	SSC mode value			octet 1

Figure 9.11.4.16.1: SSC mode information element

Table 9.11.4.16.1: SSC mode information element

SSC mode value (octet 1, bit 1 to bit 4)			
Bits			
3	**2**	**1**	
0	0	1	SSC mode 1
0	1	0	SSC mode 2
0	1	1	SSC mode 3
1	0	0	unused; shall be interpreted as "SSC mode 1", if received by the network
1	0	1	unused; shall be interpreted as "SSC mode 2", if received by the network
1	1	0	unused; shall be interpreted as "SSC mode 3", if received by the network
All other values are reserved.			

9.11.4.17 Re-attempt indicator

The purpose of the Re-attempt indicator information element is to indicate a condition under which the UE is allowed in the current PLMN or its equivalent PLMN(s) or the current SNPN or its equivalent SNPNs for the same DNN, to re-attempt a session management procedure (see 3GPP TS 24.301 [15]) corresponding to the 5GS session management procedure which was rejected by the network.

The Re-attempt indicator information element is coded as shown in figure 9.11.4.17.1 and table 9.11.4.17.1.

The Re-attempt indicator is a type 4 information element with a length of 3 octets.

8	7	6	5	4	3	2	1	
Re-attempt indicator IEI								octet 1
Length of Re-attempt indicator contents								octet 2
0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	EPLM NC	RATC	octet 3

Figure 9.11.4.17.1: Re-attempt indicator

Table 9.11.4.17.1: Re-attempt indicator

RATC (octet 3, bit 1) Bit **1** 0 UE is allowed to re-attempt the procedure in S1 mode 1 UE is not allowed to re-attempt the procedure in S1 mode EPLMNC (octet 3, bit 2) Bit **2** 0 UE is allowed to re-attempt the procedure in an equivalent PLMN or equivalent SNPN 1 UE is not allowed to re-attempt the procedure in an equivalent PLMN or equivalent SNPN Bits 3 to 8 of octet 3 are spare and shall be encoded as zero.

9.11.4.18 5GSM network feature support

The purpose of the 5GSM network feature support information element is to indicate whether certain session management related features are supported by the network.

The 5GSM network feature support information element is coded as shown in figure 9.11.4.18.1 and table 9.11.4.18.1.

The 5GSM network feature support is a type 4 information element with a minimum length of 3 octets and a maximum length of 15 octets.

8	7	6	5	4	3	2	1	
5GSM network feature support IEI								octet 1
Length of 5GSM network feature support contents								octet 2
0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	NAPS	EPT-S1	octet 3
0	0	0	0	0	0	0	0	octet 4* -15*
Spare								

Figure 9.11.4.18.1: 5GSM network feature support information element

Table 9.11.4.18.1: 5GSM network feature support information element

5GSM network feature support contents Ethernet PDN type in S1 mode (IEPT-S1) (octet 3, bit 1) This bit indicates network's capability for Ethernet PDN type in S1 mode. 0 Ethernet PDN type in S1 mode not supported 1 Ethernet PDN type in S1 mode supported Non-3GPP access path switching (NAPS) (octet 3, bit 2) This bit indicates whether non-3GPP access path switching is supported. Bit **2** 0 non-3GPP access path switching not supported 1 non-3GPP access path switching supported All other bits in octet 3 to 15 are spare and shall be coded as zero, if the respective octet is included in the information element.

9.11.4.19 Void

9.11.4.20 Serving PLMN rate control

See subclause 9.9.4.28 in 3GPP TS 24.301 [15].

9.11.4.21 5GSM congestion re-attempt indicator

The purpose of the 5GSM congestion re-attempt indicator information element is to indicate whether the back-off timer is applied in the registered PLMN or all PLMNs or in the registered SNPN or all equivalent SNPNs, and additionally to indicate whether the back-off timer is applied in the current access type or both 3GPP access type and non-3GPP access type.

The 5GSM congestion re-attempt indicator information element is coded as shown in figure 9.11.4.21.1 and table 9.11.4.21.1.

The 5GSM congestion re-attempt indicator is a type 4 information element with a length of 3 octets.

8	7	6	5	4	3	2	1	
5GSM congestion re-attempt indicator IEI								octet 1
Length of 5GSM congestion re-attempt indicator contents								octet 2
0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	0 Spare	CATBO	ABO	octet 3

Figure 9.11.4.21.1: 5GSM congestion re-attempt indicator

Table 9.11.4.21.1: 5GSM congestion re-attempt indicator

ABO (All PLMNs Back-off timer) (octet 3, bit 1) Bit **1** 0 The back-off timer is applied in the registered PLMN or registered SNPN. 1 The back-off timer is applied in all PLMNs or all equivalent SNPNs. CATBO (Current Access Type Back-off Timer) (octet 3, bit 2) Bit **2** 0 The back-off timer is applied in both 3GPP access type and non-3GPP access type 1 The back-off timer is applied in the current access type Bits 3 to 8 of octet 3 are spare and shall be encoded as zero.

9.11.4.22 ATSSS container

The purpose of the ATSSS container information element is to transfer parameters associated with ATSSS.

The ATSSS container information element is coded as shown in figure 9.11.4.22.1 and table 9.11.4.22.1.

The ATSSS container is a type 6 information element with a minimum length of 3 octets and a maximum length of 65538 octets.

8	7	6	5	4	3	2	1	
ATSSS container IEI								octet 1
Length of ATSSS container contents								octet 2 octet 3
ATSSS container contents								octet 4* octet x*

Figure 9.11.4.22.1: ATSSS container information element

Table 9.11.4.22.1: ATSSS container information element

ATSSS container contents are defined in 3GPP TS 24.193 [13B].

9.11.4.23 Control plane only indication

The purpose of the control plane only indication information element is to indicate that a PDU session is only for control plane CIoT 5GS optimization.

The control plane only indication information element is coded as shown in figure 9.11.4.23.1.

The control plane only indication is a type 1 information element.

8	7	6	5	4	3	2	1	
Control plane only indication IEI				0 Spare	0 Spare	0 Spare	CPOI value	octet 1

Figure 9.11.4.23.1: Control plane only indication information element

Table 9.11.4.23.1: Control plane only indication information element

Control plane only indication value (CPOI) (octet 1) Bit **1** 0 reserved 1 PDU session can be used for control plane CIoT 5GS optimization only The value 0 is reserved. If received, it shall be interpreted as if the control plane only indication IE was not included in the message. Bits 4 to 2 of octet 1 are spare and shall be all encoded as zero.

9.11.4.24 IP header compression configuration

The purpose of the IP header compression configuration information element is to negotiate ROHC channel setup parameters specified in IETF RFC 5795 [39B] and, optionally, provide additional header compression context setup parameters.

The IP header compression configuration information element is coded as shown in figure 9.11.4.24.1 and table 9.11.4.24.1.

The IP header compression configuration is a type 4 information element with a minimum length of 5 octets and a maximum length of 257 octets.

The optional Additional IP header compression parameters container field conveys the additional header compression context setup parameters as specified in 3GPP TS 23.501 [8] in a generic container. This field corresponds to the profile-specific information in the header of the ROHC IR packet type in IETF RFC 5795 [39B].

8	7	6	5	4	3	2	1	
IP header compression configuration IEI								octet 1
Length of IP header compression configuration contents								octet 2
Spare	P0x0104	P0x0103	P0x0102	P0x0006	P0x0004	P0x0003	P0x0002	octet 3
MAX_CID								octet 4 octet 5
Additional IP header compression context setup parameters type								octet 6*
Additional IP header compression context setup parameters container								octet 7* octet n*

Figure 9.11.4.24.1: IP header compression configuration information element

Table 9.11.4.24.1: IP header compression configuration information element

ROHC Profiles (octet 3)

The ROHC Profiles shall indicate which of the ROHC profiles is supported. When a particular bit is set to 1, this indicates that the corresponding profile is supported. The No Compression profile 0x0000 (see IETF RFC 5795 [39B]) shall always be supported. When all the bits are set to 0, this indicates that only the No Compression profile 0x0000 is supported.

Profile 0x0002 support indicator (see IETF RFC 3095 [33A] and IETF RFC 4815 [38A]) (octet 3 bit 1)

0 RoHC profile 0x0002 (UDP/IP) is not supported
1 RoHC profile 0x0002 (UDP/IP) is supported

Profile 0x0003 support indicator (see IETF RFC 3095 [33A] and IETF RFC 4815 [38A]) (octet 3 bit 2)

0 RoHC profile 0x0003 (ESP/IP) is not supported
1 RoHC profile 0x0003 (ESP/IP) is supported

Profile 0x0004 support indicator (see IETF RFC 3843 [34A] and IETF RFC 4815 [38A]) (octet 3 bit 3)

0 RoHC profile 0x0004 (IP) is not supported
1 RoHC profile 0x0004 (IP) is supported

Profile 0x0006 support indicator (see IETF RFC 6846 [40B]) (octet 3 bit 4)

0 RoHC profile 0x0006 (TCP/IP) is not supported
1 RoHC profile 0x0006 (TCP/IP) is supported

Profile 0x0102 support indicator (see IETF RFC 5225 [39A]) (octet 3 bit 5)

0 RoHC profile 0x0102 (UDP/IP) is not supported
1 RoHC profile 0x0102 (UDP/IP) is supported

Profile 0x0103 support indicator (see IETF RFC 5225 [39A]) (octet 3 bit 6)

0 RoHC profile 0x0103 (ESP/IP) is not supported
1 RoHC profile 0x0103 (ESP/IP) is supported

Profile 0x0104 support indicator (see IETF RFC 5225 [39A]) (octet 3 bit 7)

0 RoHC profile 0x0104 (IP) is not supported
1 RoHC profile 0x0104 (IP) is supported

Bits 8 is spare and shall be set to 0.

MAX_CID (octet 4 and octet 5)

This is the MAX_CID value as specified in 3GPP TS 36.323 [25]. It is encoded in binary coding with a value in the range from 1 to 16383.

Additional IP header compression context parameters type (octet 6).

The Additional IP header compression context parameters type octet indicates the profile associated with the profile-specific information in the Additional IP header compression context parameters container.

Bits
8 7 6 5 4 3 2 1 Type

0 0 0 0 0 0 0 0 0x0000 (No Compression)
0 0 0 0 0 0 0 1 0x0002 (UDP/IP)
0 0 0 0 0 0 1 0 0x0003 (ESP/IP)
0 0 0 0 0 0 1 1 0x0004 (IP)
0 0 0 0 0 1 0 0 0x0006 (TCP/IP)
0 0 0 0 0 1 0 1 0x0102 (UDP/IP)
0 0 0 0 0 1 1 0 0x0103 (ESP/IP)
0 0 0 0 0 1 1 1 0x0104 (IP)
0 0 0 0 1 0 0 0 Other

0 0 0 0 1 0 0 1 to 1 1 1 1 1 1 1 1 Spare Additional IP header compression context parameters container (octets 7 to n). Additional IP header compression context parameters container carries the profile-specific information (see IETF RFC 5795 [39B]). The maximum size is 251 octets. NOTE: If the Additional IP header compression context setup parameters container is included, then the Additional IP header compression context parameters type shall be included in the octet 6.

9.11.4.25 DS-TT Ethernet port MAC address

The purpose of the DS-TT Ethernet port MAC address information element is to signal the MAC address of the DS-TT Ethernet port used for a PDU session of "Ethernet" PDU session type.

The DS-TT Ethernet port MAC address information element is coded as shown in figure 9.11.4.25.1 and table 9.11.4.25.1.

The DS-TT Ethernet port MAC address is a type 4 information element with a length of 8 octets.

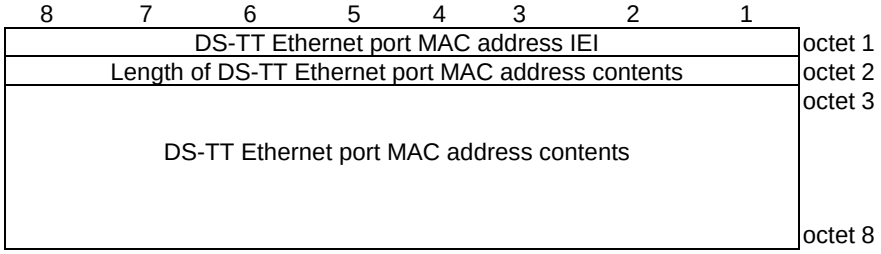


Figure 9.11.4.25.1: DS-TT Ethernet port MAC address information element

Table 9.11.4.25.1: DS-TT Ethernet port MAC address information element

DS-TT Ethernet port MAC address contents (octets 3 to 8) The DS-TT Ethernet port MAC address contents consist of the binary representation of the MAC address of the DS-TT Ethernet port used for the PDU session, starting with the LSB bit of the first octet of the MAC address included in bit 1 of octet 3.

9.11.4.26 UE-DS-TT residence time

The purpose of the UE-DS-TT residence time information element is to signal the time taken within the UE and the DS-TT to forward a packet i.e. between the ingress of the UE and the DS-TT port in the DL direction, or between the DS-TT port and the egress of the UE in the UL direction.

The UE- DS-TT residence time information element is coded as shown in figure 9.11.4.26.1 and table 9.11.4.26.1.

The UE-DS-TT residence time is a type 4 information element with a length of 10 octets.

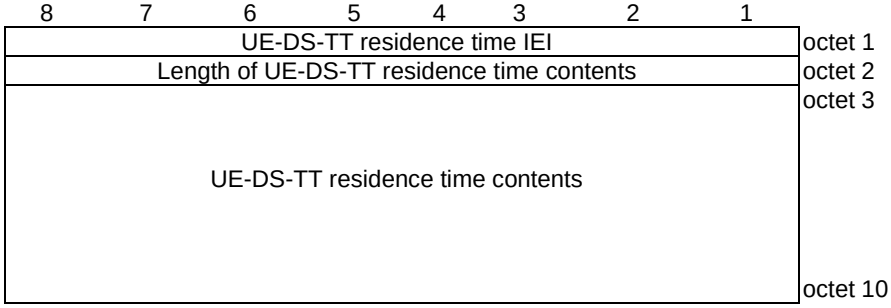


Figure 9.11.4.26.1: UE-DS-TT residence time information element

Table 9.11.4.26.1: UE-DS-TT residence time information element

UE-DS-TT residence time contents (octets 3 to 10) The UE-DS-TT residence time contents contain the UE-DS-TT residence time encoded as specified for the correctionField in IEEE Std 1588-2019 [43B], with the LSB bit of the first octet of the UE-DS-TT residence time included in bit 1 of octet 3. If the UE-DS-TT residence time.is too big to be represented, all bits of octets 3 to 10 shall be coded as "1" except the MSB bit of octet 10.

9.11.4.27 Port management information container

The purpose of the Port management information container information element is to transport a port management service message as specified in clause 8 of 3GPP TS 24.539 [19BA].

The Port management information container information element is coded as shown in figure 9.11.4.27.1 and table 9.11.4.27.1.

The Port management information container is a type 6 information element with a minimum length of 4 octets and a maximum length of 65538 octets.

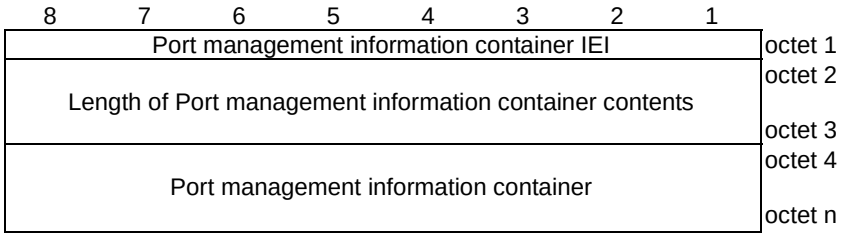


Figure 9.11.4.27.1: Port management information container information element

Table 9.11.4.27.1: Port management information container information element

Port management information container (octet 4 to n) A port management service message as specified in clause 8 of 3GPP TS 24.539 [19BA].

9.11.4.28 Ethernet header compression configuration

The purpose of the Ethernet header compression configuration information element is to negotiate the use of EHC and the length of the CID field in the EHC packet (see 3GPP TS 38.323 [29]).

The Ethernet header compression configuration information element is coded as shown in figure 9.11.4.28.1 and table 9.11.4.28.1.

The Ethernet header compression configuration is a type 4 information element with the length of 3 octets.

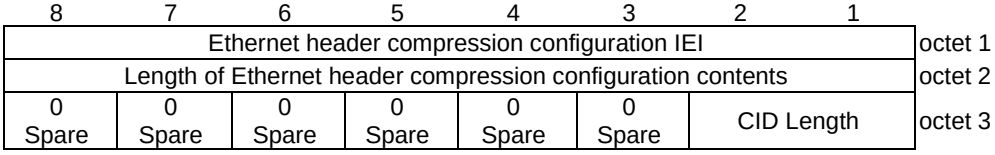


Figure 9.11.4.28.1: Ethernet header compression configuration information element

Table 9.11.4.28.1: Ethernet header compression configuration information element

Length of CID field value (CID Length) (octet 3 bits 1 and 2)		
Bit		
2	**1**	
0	0	Ethernet header compression not used
0	1	7 bits
1	0	15 bits
All other values shall be interpreted as "7 bits".		
Bits 3 to 8 of octet 3 are spare and shall be coded as zero.		

9.11.4.29 Remote UE context list

The purpose of the Remote UE context list information element is to provide identity and optionally IP address of a 5G ProSe remote UE connected to, or disconnected from, a UE acting as a 5G ProSe layer-3 UE-to-network relay.

The Remote UE context list information element is coded as shown in figure 9.11.4.29.1, figure 9.11.4.29.2, table 9.11.4.29.1 and table 9.11.4.29.2.

The Remote UE context list is a type 6 information element with a minimum length of 16 octets and a maximum length of 65538 octets.

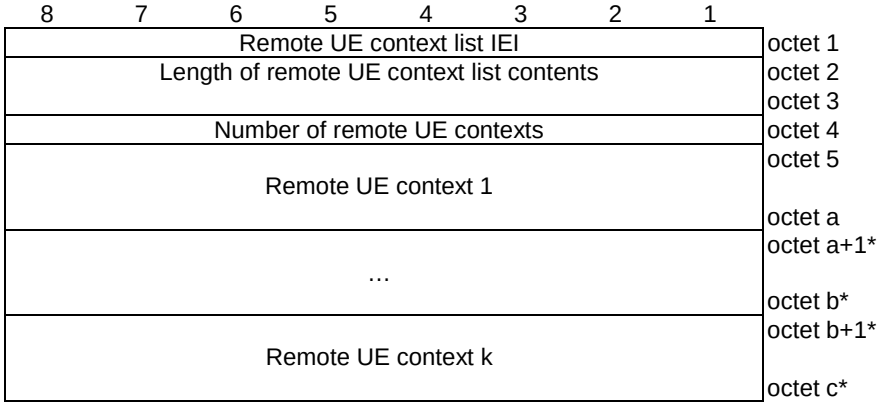


Figure 9.11.4.29.1: Remote UE context list

Table 9.11.4.29.1: Remote UE context list

Remote UE context (octet 5 etc) The contents of remote UE context are applicable for one individual UE and are coded as shown in figure 9.11.4.29.2 and table 9.11.4.29.2.

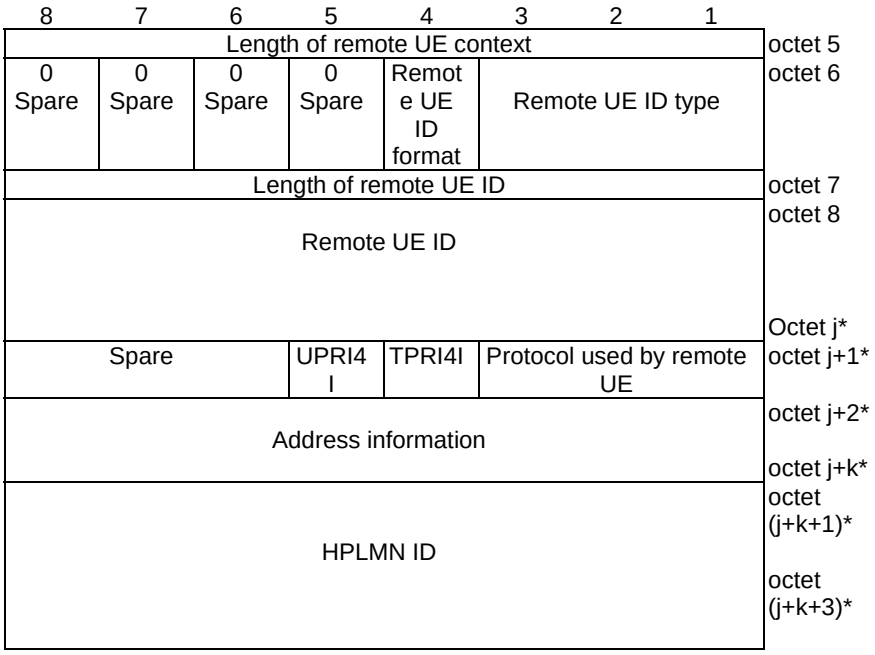


Figure 9.11.4.29.2: Remote UE context

Table 9.11.4.29.2: Remote UE context

Remote UE ID type (bits 1 to 3 of octet 6)
Bits

3	2	1	
0	0	1	UP-PRUK ID
0	1	0	CP-PRUK ID
0	1	1	IMEI
1	0	0	IMEISV

All other values are reserved.

Remote UE ID format (bit 4 of octet 6) (NOTE)
Bit

4	
0	Network access identifier (NAI)
1	64-bit string

Bits 5 to 8 of octet 6 are spare and shall be coded as zero.

Remote UE ID (octet 8 to octet j)
The UP-PRUK ID as specified in 3GPP TS 33.503 [56], the CP-PRUK ID as specified in 3GPP TS 33.503 [56], the IMEI or the IMEISV of the 5G ProSe Remote UE. If the remote UE ID type field indicates "UP-PRUK ID" or "CP-PRUK ID", and the remote UE ID format field indicates "NAI", the remote UE ID field contains the UP-PRUK ID or the CP-PRUK ID in the NAI format as defined in 3GPP TS 23.003 [4], encoded as UTF-8 string. If the remote UE ID type field indicates "UP-PRUK ID", and the remote UE ID format field indicates "64-bit string", the remote UE ID field contains the UP-PRUK ID as a 64-bit string, encoded using binary encoding. If the remote UE ID type field indicates "IMEI" or "IMEISV", the remote UE ID field contains the IMEI or the IMEISV encoded as 5GS mobile identity information element for type of identity "IMEI" or "IMEISV" as specified in subclause 9.11.3.4, starting with the fourth octet.

Protocol used by remote UE (octet j+1, bits 1 to 3)
Bits

3	2	1	
0	0	0	No IP info
0	0	1	IPv4
0	1	0	IPv6
1	0	0	Unstructured
1	0	1	Ethernet

All other values are reserved.

TCP port range for IPv4 indicator (TPRI4I) (octet j+1, bits 4)
Bit

4	
0	TCP port range for IPv4 absent
1	TCP port range for IPv4 present

UDP port range for IPv4 indicator (UPRI4I) (octet j+1, bits 5)
Bit

5	
0	UDP port range for IPv4 absent
1	UDP port range for IPv4 present

Bits 4 to 8 of octet j+1 are spare and shall be coded as zero.

The length of remote UE ID field contains the binary coded representation of the length of the remote UE ID field. The first bit in transmission order is the most significant bit.

If the Protocol used by remote UE indicates IPv4 and:
- TPRI4I bit indicates "TCP port range for IPv4 absent" and UPRI4I bit indicates "UDP port range for IPv4 absent", the Address information in octet j+2 to octet j+5 contains the IPv4 address.
- TPRI4I bit indicates "TCP port range for IPv4 present" and UPRI4I bit indicates "UDP port range for IPv4 absent", the Address information in octet j+2 to octet j+9 contains the IPv4 address followed by the TCP port range field.
- TPRI4I bit indicates "TCP port range for IPv4 absent" and UPRI4I bit indicates "UDP port range for IPv4 present", the Address information in octet j+2 to octet j+9 contains the IPv4 address followed by the UDP port range field.
- TPRI4I bit indicates "TCP port range for IPv4 present" and UPRI4I bit indicates "UDP port range for IPv4 present", the Address information in octet j+2 to octet j+13 contains the IPv4 address followed by the UDP port range field followed by the TCP port range field.
See NOTE.
The UDP port range field consists of the lowest UDP port number field followed by the highest UDP port number field, of the UDP port range assigned to the remote UE in the NAT function of 5G ProSe layer-3 UE-to-network relay.
The TCP port range field consists of the lowest TCP port number field followed by highest TCP port number field, of the TCP port range assigned to the remote UE in the NAT function of 5G ProSe layer-3 UE-to-network relay.
Each port number field is two octets long and bit 8 of first octet of the port number field represents the most significant bit of the port number and bit 1 of second octet of the port number field the least significant bit.

If the Protocol used by remote UE indicates IPv6, the Address information in octet j+2 to octet j+9 contains the /64 IPv6 prefix of a remote UE. Bit 8 of octet j+2 represents the most significant bit of the /64 IPv6 prefix and bit 1 of octet j+9 the least significant bit.

If the Protocol used by remote UE indicates Ethernet, the Address information in octet j+2 to octet j+7 contains the remote UE MAC address. Bit 8 of octet j+2 represents the most significant bit of the MAC address and bit 1 of octet j+7 the least significant bit.

If the Protocol used by remote UE indicates Unstructured, the Address information octets are not included.

If the Protocol used by remote UE indicates No IP info, the Address information octets are not included

If the Remote UE ID type field indicates "PRUK ID" and the Remote UE ID format field indicates "64-bit string", then the HPLMN ID field is present otherwise the HPLMN ID field is absent. The HPLMN ID field indicates HPLMN ID of the 5G ProSe remote UE and is coded as value part of the PLMN ID information element as specified in 3GPP TS 24.554 [19E] subclause 11.3.33 starting with the second octet.

NOTE: In the present release of the specification, providing information for IP protocols other than UDP or TCP is not specified

9.11.4.30 Requested MBS container

The purpose of the Requested MBS container information element is for UE to request to join or leave one or more multicast MBS sessions.

The Requested MBS container information element is coded as shown in figure 9.11.4.30.1, figure 9.11.4.30.2, figure 9.11.4.30.3, figure 9.11.4.30.4 and table 9.11.4.30.1.

The Requested MBS container is a type 6 information element with a minimum length of 8 octets and a maximum length of 65538 octets.

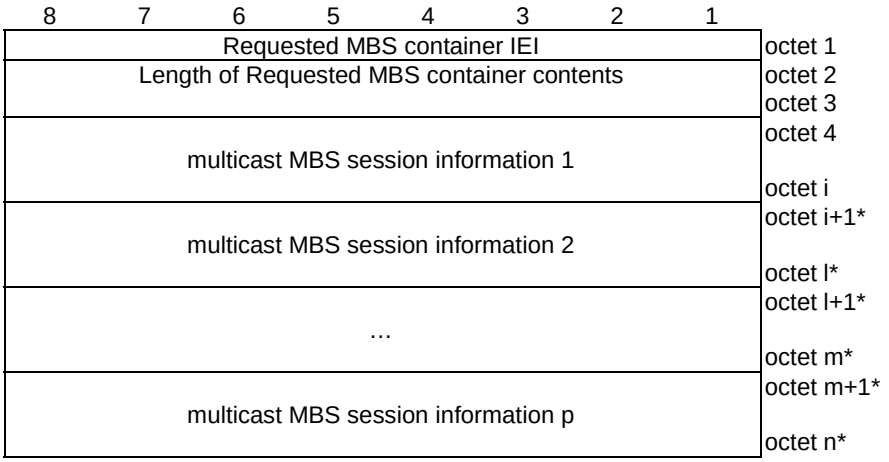


Figure 9.11.4.30.1: Requested MBS container information element

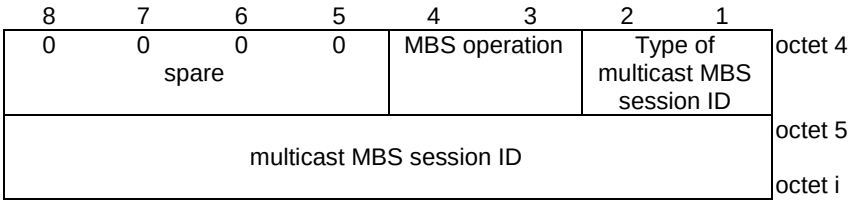


Figure 9.11.4.30.2: multicast MBS session information

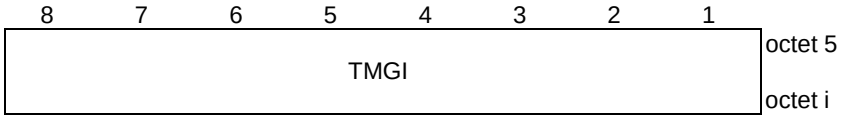


Figure 9.11.4.30.3: multicast MBS session ID for Type of multicast MBS session ID = "Temporary Mobile Group Identity (TMGI)"

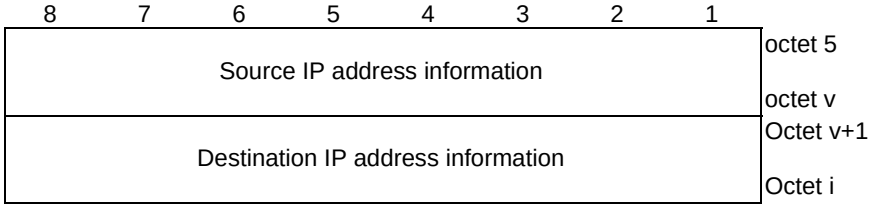


Figure 9.11.4.30.4: multicast MBS session ID for Type of multicast MBS session ID = "Source specific IP multicast address for IPv4" or "Source specific IP multicast address for IPv6"

Table 9.11.4.30.1: Requested MBS container information element

Type of multicast MBS session ID (bits 1 to 2 of octet 4)
Bits
2 1
0 1 Temporary Mobile Group Identity (TMGI)
1 0 Source specific IP multicast address for IPv4
1 1 Source specific IP multicast address for IPv6
All other values are reserved.

MBS operation (bits 3 to 4 of octet 4)
Bits
4 3
0 1 Join multicast MBS session
1 0 Leave multicast MBS session
All other values are reserved.

Bits 5 to 8 of octet 4 are spare and shall be coded as zero.

If Type of multicast MBS session ID is set to "Temporary Mobile Group Identity (TMGI)", the multicast MBS session ID contains the TMGI (octet 5 to i) and is coded as described in subclause 10.5.6.13 in 3GPP TS 24.008 [12] starting from octet 2. The structure of the TMGI is defined in 3GPP TS 23.003 [4].

If Type of multicast MBS session ID is set to "Source specific IP multicast address for IPv4" or " Source specific IP multicast address for IPv6", the multicast MBS session ID contains the Source IP address information and the Destination IP address information.

Source IP address information (octet 5 to v)
This field contains the IP unicast address used as source address in IP packets for identifying the source of the multicast service.

If the type of multicast MBS session ID indicates "Source specific IP multicast address for IPv4", the Source IP address information in octet 5 to octet 8 contains an IPv4 address. If the type of multicast MBS session ID indicates "Source specific IP multicast address for IPv6", the Source IP address information in octet 5 to octet 20 contains an IPv6 address.

Destination IP address information (octet v+1 to i)
This field contains the IP multicast address used as destination address in related IP packets for identifying a multicast service associated with the source.

If the type of multicast MBS session ID indicates "Source specific IP multicast address for IPv4", the Destination IP address information in octet v+1 to octet v+4 contains an IPv4 address. If the type of multicast MBS session ID indicates "Source specific IP multicast address for IPv6", the Source IP address information in octet v+1 to octet v+16 contains an IPv6 address.

9.11.4.31 Received MBS container

The purpose of the Received MBS container information element is to indicate to the UE the information of the multicast MBS sessions that the network accepts or rejects the UE to join, the information of the multicast MBS sessions that the UE is removed from, or the information of the updated MBS service area.

The Received MBS container information element is coded as shown in figure 9.11.4.31.1, figure 9.11.4.31.2, figure 9.11.4.31.3, figure 9.11.4.31.4, figure 9.11.4.31.5, figure 9.11.4.31.6, figure 9.11.4.31.7, figure 9.11.4.31.8, figure 9.11.4.31.9, figure 9.11.4.31.10, figure 9.11.4.31.11 and table 9.11.4.31.1.

The Received MBS container is a type 6 information element with a minimum length of 9 octets and a maximum length of 65538 octets.

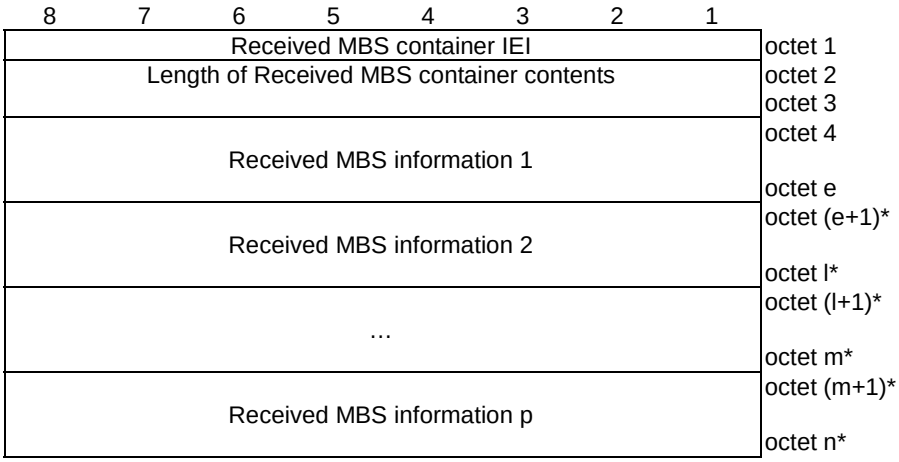


Figure 9.11.4.31.1: Received MBS container information element

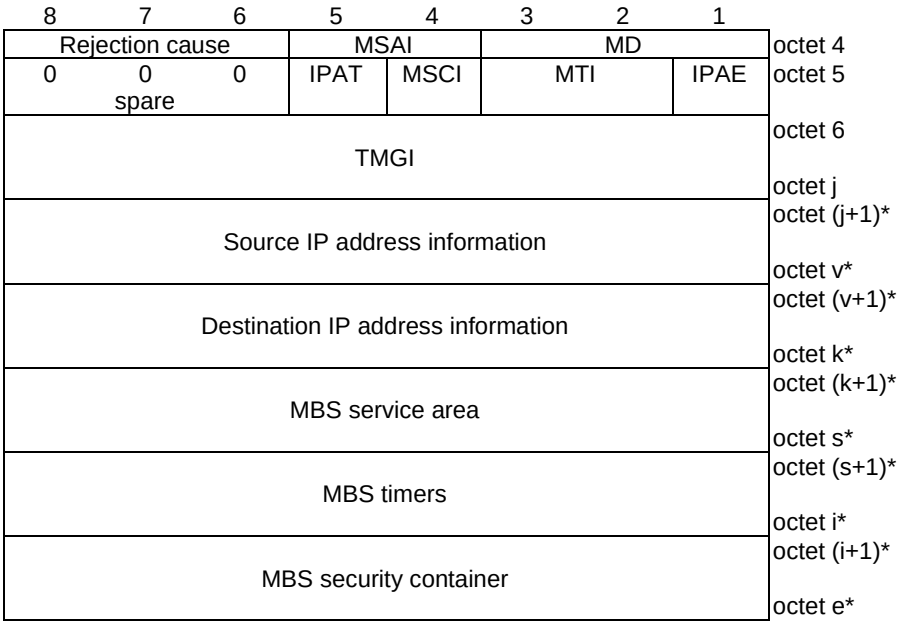


Figure 9.11.4.31.2: Received MBS information

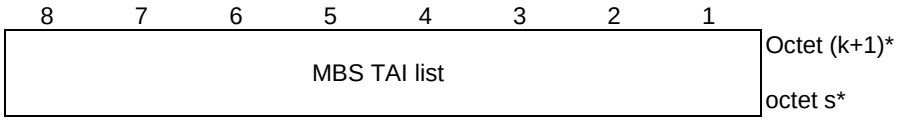


Figure 9.11.4.31.3: MBS service area for MBS service area indication = "MBS service area included as MBS TAI list"

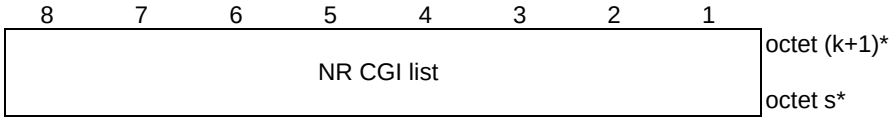


Figure 9.11.4.31.4: MBS service area for MBS service area indication = "MBS service area included as NR CGI list"

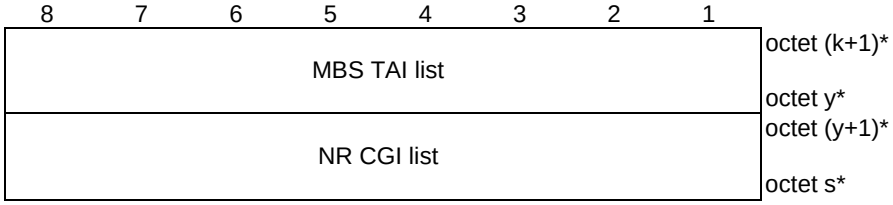


Figure 9.11.4.31.5: MBS service area for MBS service area indication = "MBS service area included as MBS TAI list and NR CGI list"

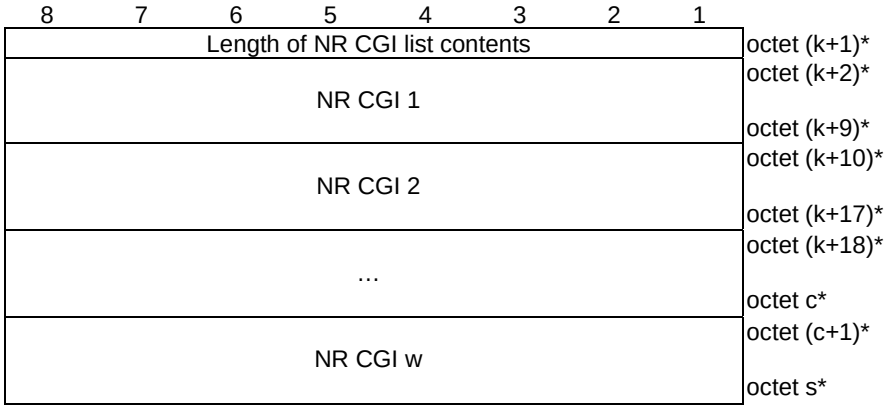


Figure 9.11.4.31.6: NR CGI list

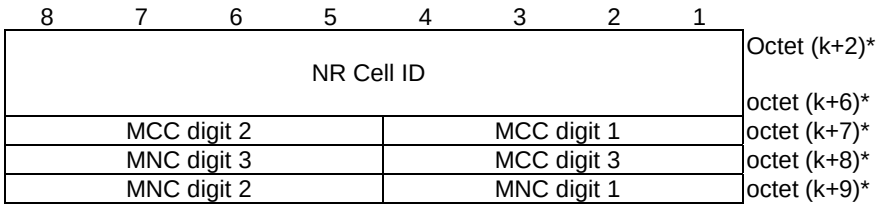


Figure 9.11.4.31.7: NR CGI

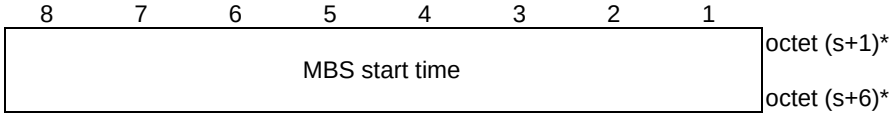


Figure 9.11.4.31.8: MBS timers for MBS timer indication = "MBS start time"

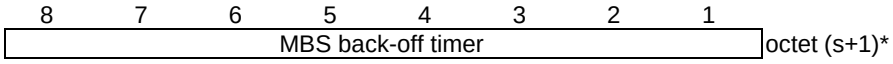


Figure 9.11.4.31.9: MBS timers for MBS timer indication = "MBS back-off timer"

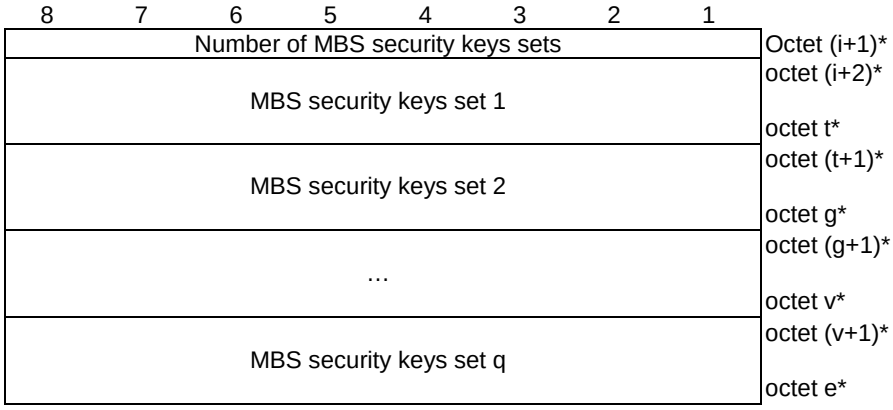


Figure 9.11.4.31.10: MBS security container

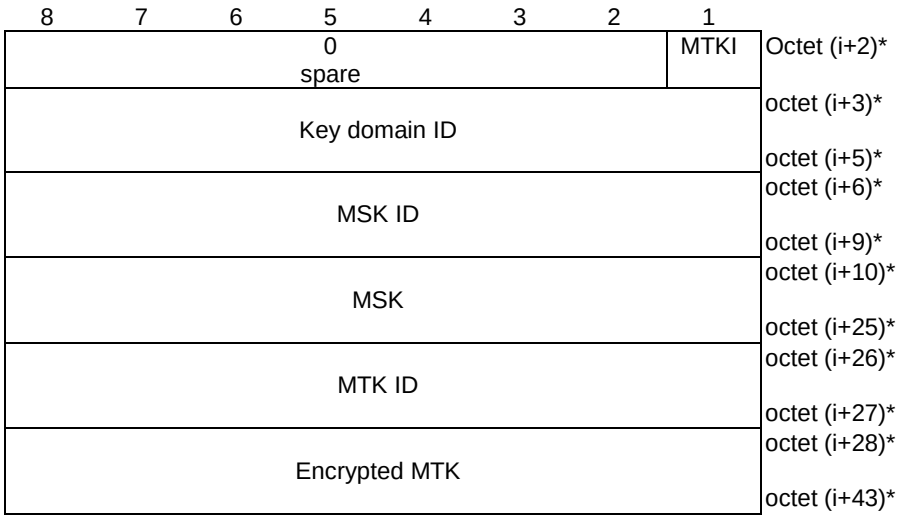


Figure 9.11.4.31.11: MBS security keys set

Table 9.11.4.31.1: Received MBS container information element

MBS decision (MD) (bits 1 to 3 of octet 4)
The MD indicates the network decision of the join requested by the UE, the network requests to remove the UE from the multicast MBS session or the network request to update the MBS service area or the security information of multicast MBS session.
Bits

3	**2**	**1**	
0	0	1	MBS service area update
0	1	0	MBS join is accepted
0	1	1	MBS join is rejected
1	0	0	Remove UE from multicast MBS session
1	0	1	MBS security information update

All other values are unused in this version of the specification and interpreted as 000 if received.

If MD is set to "MBS join is rejected" or “Remove UE from multicast MBS session”, bits 6 to 8 of octet 4 shall contain the Rejection cause which indicates the reason of rejecting the MBS join request or the reason of removing the UE from multicast MBS session, respectively, otherwise bits 6 to 8 of octet 4 are spare and shall be coded as zero.

MBS service area indication (MSAI) (bits 4 and 5 of octet 4)
The MSAI indicates whether and how the MBS service area is included in the IE.
Bits

5	**4**	
0	0	MBS service area not included
0	1	MBS service area included as MBS TAI list
1	0	MBS service area included as NR CGI list
1	1	MBS service area included as MBS TAI list and NR CGI list

Rejection cause (bits 6 to 8 of octet 4)
The Rejection cause indicates the reason of rejecting the join request or the reason of removing the UE from the MBS session.
Bits

8	**7**	**6**	
0	0	0	No additional information provided
0	0	1	Insufficient resources
0	1	0	User is not authorized to use MBS service
0	1	1	multicast MBS session has not started or will not start soon
1	0	0	User is outside of local MBS service area
1	0	1	Session context not found
1	1	0	multicast MBS session is released

All other values are unused in this version of the specification and interpreted as 000 if received.

IP address existence (IPAE) (bit1 of octet 5)
The IPAE indicates whether the Source IP address information and Destination IP address information are included in the IE or not.
Bit

1	
0	Source and destination IP address information not included
1	Source and destination IP address information included

If IPAE is set to "Source and destination IP address information included", Source IP address information and Destination IP address information shall be included in the IE, otherwise Source IP address information and Destination IP address information shall not be included in the IE (NOTE 1).

MBS timer indication (MTI) (bits 2 and 3 of octet 5)
The MTI indicates whether there is MBS timer included in the IE or not.
Bit

3	**2**	
0	0	No MBS timers included
0	1	MBS start time included
1	0	MBS back-off timer included

All other values are unused in this version of the specification and interpreted as 00 if received

MBS security container indication (MSCI) (bit 4 of octet 5)
The MSCI indicates whether the MBS security container is included in the IE or not

Bit
4
0 MBS security container not included
1 MBS security container included

IP address type (IPAT) (bit 5 of octet 5)
The IPAT indicates the type of the source IP address information and destination IP address information. This field is ignored when IPAE is set to "Source and destination IP address information not included".
Bit
5
0 Source IP address information and destination IP address information are IPv4
1 Source IP address information and destination IP address information are IPv6

Bits 6 to 8 of octet 5 are spare and shall be coded as zero.

TMGI (octets 6 to j)
The TMGI is coded as described in subclause 10.5.6.13 in 3GPP TS 24.008 [12] starting from octet 2. The structure of the TMGI is defined in 3GPP TS 23.003 [4].

Source IP address information (octet j+1 to v)
This field contains the IP unicast address used as source address in IP packets for identifying the source of the multicast service. The value of this field is copied from the corresponding source IP address information in the requested MBS container. If the IPAT indicates "Source and destination IP address information are IPv4", the Source IP address information in octet j+1 to octet j+4 contains an IPv4 address. If the IPAT indicates "Source and destination IP address information are IPv6", the Source IP address information in octet j+1 to octet j+16 contains an IPv6 address

Destination IP address information (octet v+1 to k)
This field contains the IP multicast address used as destination address in related IP packets for identifying a multicast service associated with the source. The value of this field is copied from the corresponding destination IP address information in the requested MBS container. If the IPAT indicates "Source and destination IP address information are IPv4", the Destination IP address information in octet v+1 to octet v+4 contains an IPv4 address. If the IPAT indicates "Source and destination IP address information are IPv6", the Destination IP address information in octet v+1 to octet v+16 contains an IPv6 address.

MBS service area (octet k+1 to s)
The MBS service area contains the MBS TAI list, the NR CGI list or both, that identifies the service area(s) for a local MBS service.

MBS TAI list (octet k+1 to s)
The MBS TAI list is coded as octet 2 and above of the 5GS tracking area identity list IE defined in subclause 9.11.3.9.

NR CGI (octet k+2 to k+9)
The NR CGI globally identifies an NR cell. It contains the NR Cell ID and the PLMN ID of that cell.

NR Cell ID (octet k+2 to k+6)
The NR Cell ID consists of 36 bits identifying an NR Cell ID as specified in subclause 9.3.1.7 of 3GPP TS 38.413 [31], in hexadecimal representation. Bit 8 of octet k+2 is the most significant bit and bit 5 of octet k+6 is the least significant bit. Bits 1 to 4 of octet k+6 are spare and shall be coded as zero.

MCC, Mobile country code (octet k+7 and bits 1 to 4 octet k+8)
The MCC field is coded as in ITU-T Recommendation E.212 [42], annex A.

MNC, Mobile network code (bits 5 to 8 of octet k+8 and octet k+9)
The coding of this field is the responsibility of each administration but BCD coding shall be used. The MNC shall consist of 2 or 3 digits. If a network operator decides to use only two digits in the MNC, bits 5 to 8 of octet k+8 shall be coded as "1111".

The MCC and MNC digits are coded as octets 6 to 8 of the Temporary mobile group identity IE in figure 10.5.154 of 3GPP TS 24.008 [12].

MBS start time (octets s+1 to s+6)
The MBS start time is coded as described in subclause 10.5.3.9 in 3GPP TS 24.008 [12] starting from octet 2 till octet 7.

MBS back-off timer (octet s+1)
The MBS back-off timer is coded as octet 3 described in subclause 10.5.7.4a in 3GPP TS 24.008 [12].

MTK indication (MTKI) (bit1 of octet i+2)
The MTKI indicates whether the MTK ID and Encrypted MTK are included in the MBS security keys set or not.
Bit
1
0 MTK ID and Encrypted MTK not included
1 MTK ID and Encrypted MTK included

Bits 2 to 8 of octet i+2 are spare and shall be coded as zero

Key domain ID (octet i+3 to i+5)
The key domain ID is 3 bytes long and is defined in 3GPP TS 33.246 [57] (NOTE 2).

MBS Service Key Identifier (MSK ID) (octets i+6 to i+9)
The MSK ID is 4 bytes long and is defined in 3GPP TS 33.246 [57].

MBS Service Key (MSK) (octets i+10 to i+25)
The MSK is 16 bytes long and is defined in 3GPP TS 33.246 [57].

MBS Traffic Key Identifier (MTK ID) (octets i+26 to i+27)
The MTK ID is 2 bytes long and is defined in 3GPP TS 33.246 [57].

Encrypted MBS Traffic Key (Encrypted MTK) (octets i+28 to i+43)
The Encrypted MTK is 16 bytes long and contains the encrypted version of MTK using MSK as defined in 3GPP TS 33.246 [57].

NOTE 1: The IPAE bit is not expected to be set to "Source and destination IP address information included" when the MBS decision (MD) indicates "Remove UE from multicast MBS session".
NOTE 2: As specified in annex W in 3GPP TS 33.501 [24], the UE should not try to use the MCC and MNC constructing the key domain ID in another context, e.g., the UE should not compare those MCC and MNC to parameters received from lower layers.

9.11.4.32 PDU session pair ID

The purpose of the PDU session pair ID information element is to indicate a PDU session pair ID.

The PDU session pair ID information element is coded as shown in figure 9.11.4.32.1 and table 9.11.4.32.1.

The PDU session pair ID is a type 4 information element with a length of 3 octets.

8	7	6	5	4	3	2	1	
PDU session pair ID IEI								octet 1
Length of PDU session pair ID IE								octet 2
PDU session pair ID								octet 3

Figure 9.11.4.32.1: PDU session pair ID information element

Table 9.11.4.32.1: PDU session pair ID information element

PDU session pair ID (octet 3)								
Bits								
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	
0	0	0	0	0	0	0	0	PDU session pair ID 0
				to				to
0	0	0	0	0	1	1	0	PDU session pair ID 6
All other values are reserved.								

9.11.4.33 RSN

The purpose of the RSN information element is to indicate an RSN.

The RSN information element is coded as shown in figure 9.11.4.33.1 and table 9.11.4.33.1.

The RSN is a type 4 information element with a length of 3 octets.

8	7	6	5	4	3	2	1	
RSN IEI								octet 1
Length of RSN IE								octet 2
RSN								octet 3

Figure 9.11.4.33.1: RSN information element

Table 9.11.4.33.1: RSN information element

RSN (octet 3)								
Bits								
8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	
0	0	0	0	0	0	0	0	v1
0	0	0	0	0	0	0	1	v2
All other values are spare and shall not be used by a UE compliant to the present version of this specification.								

9.11.4.34 ECS address

The purpose of the ECS address information element is to indicate the ECS address (either IPv4 address, IPv6 address, or FQDN) and the associated spatial validity condition.

The ECS address information element is coded as shown in figure 9.11.4.34.1, figure 9.11.4.34.2, figure 9.11.4.34.3, figure 9.11.4.34.4, figure 9.11.4.34.5, figure 9.11.4.34.6, table 9.11.4.34.1, table 9.11.4.34.2, table 9.11.4.34.4 and table 9.11.4.34.5.

The ECS address information element is a type 6 information element with minimum length of 8 octets and a maximum length of 65538 octets.

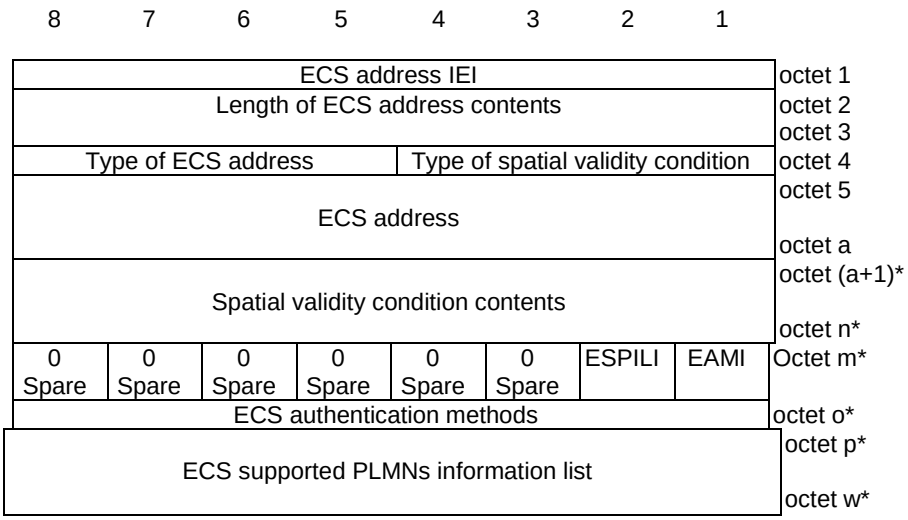


Figure 9.11.4.34.1: ECS address information element

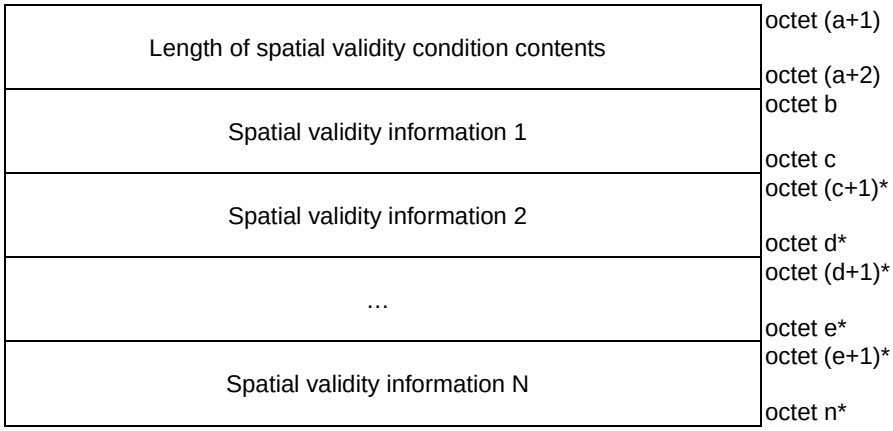


Figure 9.11.4.34.2: Spatial validity condition contents

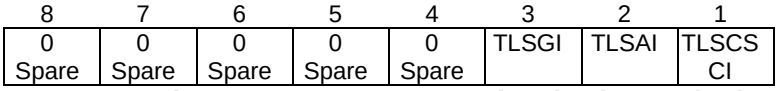


Figure 9.11.4.34.3: ECS authentication methods

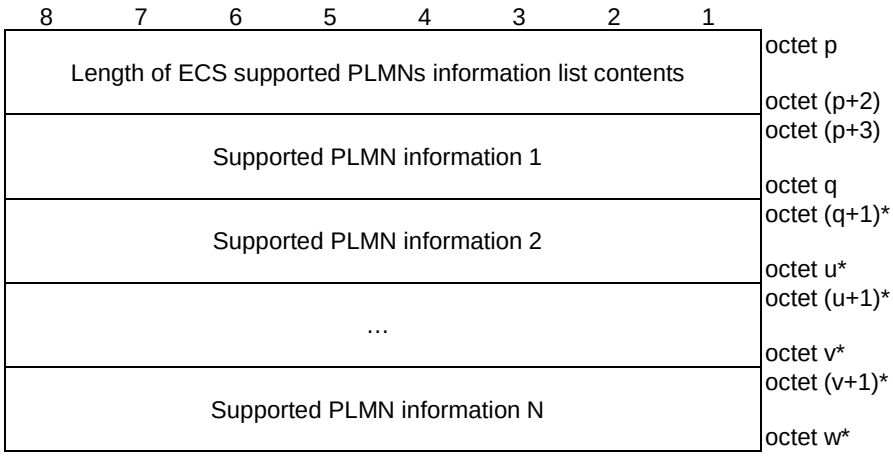


Figure 9.11.4.34.4: ECS supported PLMNs information list contents

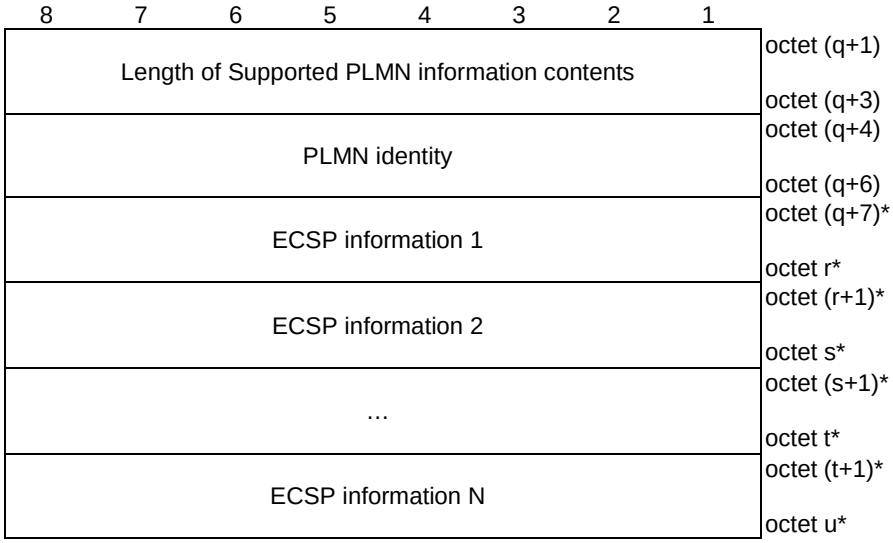


Figure 9.11.4.34.5: Supported PLMN information contents

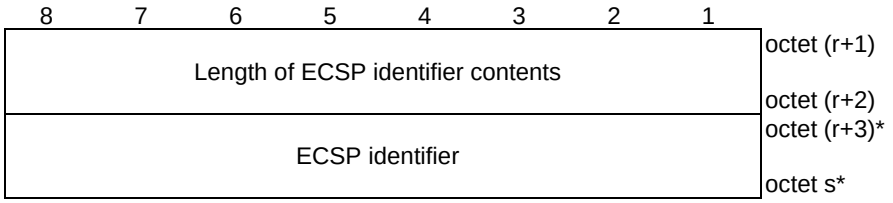


Figure 9.11.4.34.6: ECSP information contents

Table 9.11.4.34.1: ECS address information element

Type of ECS address (octet 4, bit 1 to 4)
Bits

4	3	2	1	
0	0	0	0	IPv4
0	0	0	1	IPv6
0	0	1	0	FQDN
1	1	1	1	Unspecified

All other values are spare. The receiving entity shall ignore an ECS address IE with type of ECS address containing a spare value.

Type of spatial validity condition (octet 4, bit 5 to 8)
Bits

8	7	6	5	
0	0	0	0	No spatial validity condition
0	0	0	1	Geographical service area
0	0	1	0	Tracking area
0	0	1	1	Country-wide

All other values are spare. The receiving entity shall ignore a spatial validity condition with type of spatial validity condition containing an unknown value.

If the type of ECS address indicates IPv4, then the ECS address field contains an IPv4 address in octet 5 to octet 8.

If the type of ECS address indicates IPv6, then the ECS address field contains an IPv6 address in octet 5 to octet 20 and is encoded according to IETF RFC 4291 [66].

If the type of ECS address indicates FQDN, then the ECS address field contains in octet 5 the length of FQDN value and in octet 6 to octet a an FQDN value encoded as defined in subclause 19.4.2 in 3GPP TS 23.003 [4].

If the type of ECS address indicates unspecified, then the remaining fields of ECS address information element shall be passed to the upper layers.

Spatial validity condition contents (octet (a+1)* to n*)

The spatial validity condition contents contain a variable number of spatial validity condition information.

ECS authentication methods indicator (EAMI) (octet m*, bit 1)
Bits

1	
0	ECS authentication methods field is not included
1	ECS authentication methods field is included

If the EAMI bit is set to "ECS authentication methods field is included" then the ECS authentication methods field is included otherwise the ECS authentication methods field is not included. ECS authentication methods is an optional field and is included based on operator requirements.

ECS supported PLMNs information list indication (ESPILI) (octet m*, bit 2)

Bits

2	
0	ECS supported PLMNs information list field is not included
1	ECS supported PLMNs information list field is included

If the ESPILI bit is set to "ECS supported PLMNs information list field is included" then the ECS supported PLMNs information list field is included otherwise the ECS supported PLMNS information list field is not included.

ECS supported PLMNs information list (octet p* to w*)

The ECS supported PLMNs information list contains a variable number of supported PLMN information field. The supported PLMN information field is coded according to figure 9.11.4.34.5.

Table 9.11.4.34.2: Spatial validity condition contents

If the type of spatial validity condition of the ECS address indicates No spatial validity condition, then the spatial validity condition information field is empty. If the type of spatial validity condition of the ECS address indicates geographical service area, then the spatial validity condition information field contains a geographical service area which is specified by geographical descriptions as defined in 3GPP TS 23.032 [4B]. If the type of spatial validity condition of the ECS address indicates tracking area, then the spatial validity condition information field contains a TAI as defined in subclause 9.11.3.8 starting from octet 2. If the type of spatial validity condition of the ECS address indicates country-wide, then the spatial validity condition information field contains an MCC as defined in in ITU-T Recommendation E.212 [42], annex A. The first MCC digit is coded in bit 1 to 4 of the octet b, the second MCC digit is coded in bit 5 to 8 of the octet b, and the third MCC digit is coded in bit 1 to 4 of the octet b+1. Bit 5 to bit 8 of the octet b+1 shall be padded with 1. If only two digits are used for for MCC, octet b+1 shall be padded with 1.

Table 9.11.4.34.3: ECS authentication methods contents

ECS authentication methods (octet o*) TLS client server certificate indicator (TLSCSCI) (octet o*, bit 1) 0 TLS client server certificate not supported 1 TLS client server certificate supported TLS with AKMA indicator (TLSAI) (octet o*, bit 2) 0 TLS with AKMA not supported 1 TLS with AKMA supported TLS with GBA indicator (TLSGI) (octet o*, bit 3) 0 TLS with GBA not supported 1 TLS with GBA supported

Table 9.11.4.34.4: Supported PLMN information contents

PLMN identity: The PLMN identity for which the EDN configuration information can be provided by the ECS. This is encoded as octet 3 to octet 5 in figure 9.11.3.85.1. ECSP information: The identifier of the ECSP(s) associated with the PLMN and whose information is available at the ECS. The ECSP information is coded according to figure 9.11.4.34.z.

Table 9.11.4.34.5: ECSP information contents

ECSP identifier This field contains one ECSP identifier. The ECSP identifier is encoded as a UTF-8 string.

9.11.4.35 Void

9.11.4.36 N3QAI

The purpose of the N3QAI information element is to indicate a set of QoS parameters to be used by the UE for non-3GPP access network resource management behind the UE.

The N3QAI information element is a type 6 information element with a minimum length of 9 octets. The maximum length for the information element is 65538 octets.

The N3QAI information element is coded as shown in figure 9.11.4.36.1, figure 9.11.4.36.2, figure 9.11.4.36.3, figure 9.11.4.36.4, and table 9.11.4.36.1.

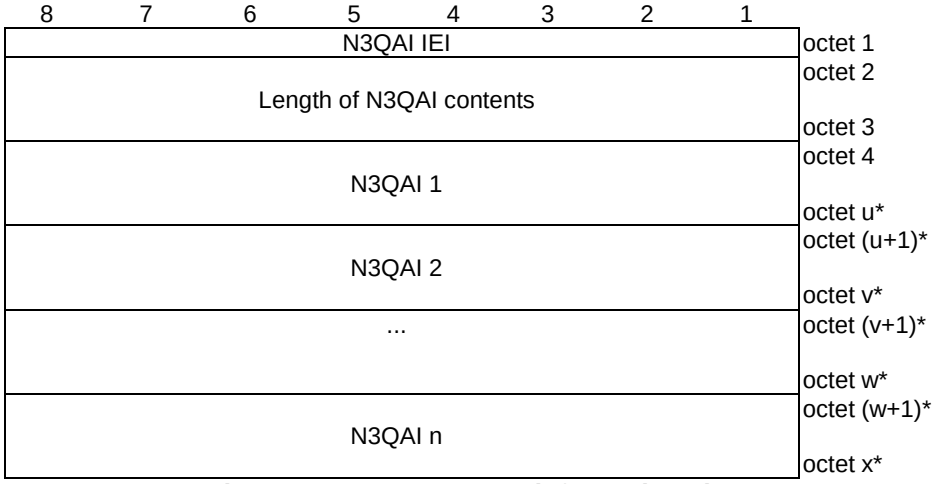


Figure 9.11.4.36.1: N3QAI information element

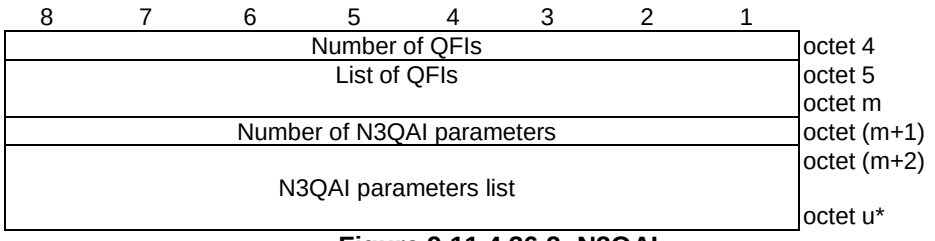


Figure 9.11.4.36.2: N3QAI

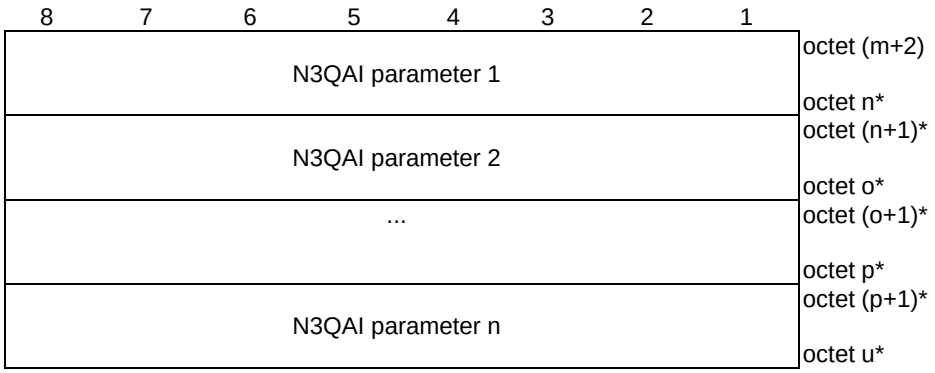


Figure 9.11.4.36.3: N3QAI parameters list

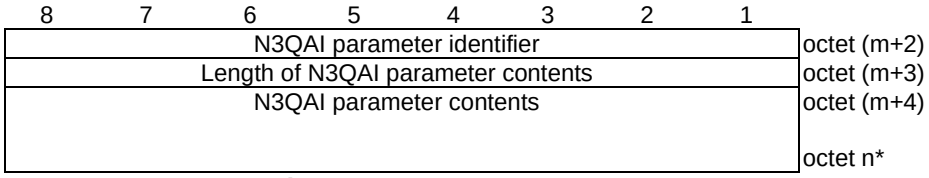


Figure 9.11.4.36.4: N3QAI parameter

Table 9.11.4.36.1: N3QAI information element

Number of QFIs (octet 4)
The number of QFIs field contains the binary coding for the number of QFIs associated with the same N3QAI parameters. This field is encoded in bits 8 through 1 of octet 4 where bit 8 is he most significant and bit 1 is the least significant bit.

List of QFIs (octet 5 to octet m)
This field indicates QoS flow(s) associated with the same N3QAI parameters. This field contains QFI values encoded as below:

Bits	
8 7 6 5 4 3 2 1	
0 0 0 0 0 0 0 0	Reserved
0 0 0 0 0 0 0 1	QFI 1
to	
0 0 1 1 1 1 1 1	QFI 63

The other values are spare. If spare value is used, the UE shall ignore the value.

Number of N3QAI parameters (bits 8 to 1 of octet (m+1))
The number of N3QAI parameters field contains the binary coding for the number of N3QAI parameters in the N3QAI parameters list field. The number of N3QAI parameters field is encoded in bits 8 through 1 of octet (m+1) where bit 8 is the most significant and bit 1 is the least significant bit.

N3QAI parameters list (octets (m+2) to q*)
The N3QAI parameters list field contains a variable number of N3QAI parameters.

Each N3QAI parameter included in the N3QAI parameters list is of variable length and consists of:
- a N3QAI parameter identifier (1 octet);
- the length of the N3QAI parameter contents (1 octet); and
- the N3QAI parameter contents itself (variable number of octets).

The N3QAI parameter identifier field is used to identify each parameter included in the N3QAI parameters list and it contains the hexadecimal coding of the parameter identifier. Bit 8 of the parameter identifier field contains the most significant bit and bit 1 contains the least significant bit. In this version of the protocol, the following parameter identifiers are specified:
- 01H (5QI);
- 02H (GFBR uplink);
- 03H (GFBR downlink);
- 04H (MFBR uplink);
- 05H (MFBR downlink);
- 06H (Averaging window);
- 07H (Resource type);
- 08H (Priority level);
- 09H (Packet delay budget);
- 0AH (Packet error rate);
- 0BH (Maximum data burst volume);
- 0CH (Maximum packet loss rate downlink);
- 0DH (Maximum packet loss rate uplink);
- 0EH (ARP); and
- 0FH (Periodicity).

If the N3QAI parameters list contains a N3QAI parameter identifier that is not supported by the receiving entity, the corresponding parameter shall be discarded.
The length of N3QAI parameter contents field contains the binary coded representation of the length of the parameter contents field. The first bit in transmission order is the most significant bit.

For the N3QAI parameter identifiers indicating "5QI", "GFBR uplink", "GFBR downlink", "MFBR uplink", "MFBR downlink", and "Averaging window", the format of the N3QAI parameter contents follows the table 9.11.4.12.1 of subclause 9.11.4.12 of this specification.

For the N3QAI parameter identifiers indicating "Resource type", "Priority level", "Packet delay budget", "Packet error rate", "Maximum data burst volume", "Maximum packet loss rate downlink", and "Maximum packet loss rate uplink", the format of the N3QAI parameter contents follows the table 9.3.1.1-2 of subclause 9.3.1.1 of 3GPP TS 24.502 [18].

When the N3QAI parameter identifier indicates "ARP", the N3QAI parameter contents field contains the binary representation of ARP that is one octet in length. The range of the ARP priority level is 1 to 15 with 1 as the highest priority as specified in subclause 5.7.2.2 of 3GPP TS.23.501 [8].

When the N3QAI parameter identifier indicates "Periodicity", the N3QAI parameter contents field contains the binary representation of the periodicity for the traffic with a unit of microsecond. (NOTE 1)

NOTE 1: The periodicity refers to the time interval between start of two data bursts for supporting consumer real time applications e.g., XR.

9.11.4.37 Non-3GPP delay budget

The purpose of the Non-3GPP delay budget information element is to indicate the non-3GPP delay budget for the non-3GPP network behind the UE to the network.

The Non-3GPP delay budget information element is a type 6 information element with a minimum length of 8 octets. The maximum length for the information element is 65538 octets.

The Non-3GPP delay budget information element is coded as shown in figure 9.11.4.37.1.

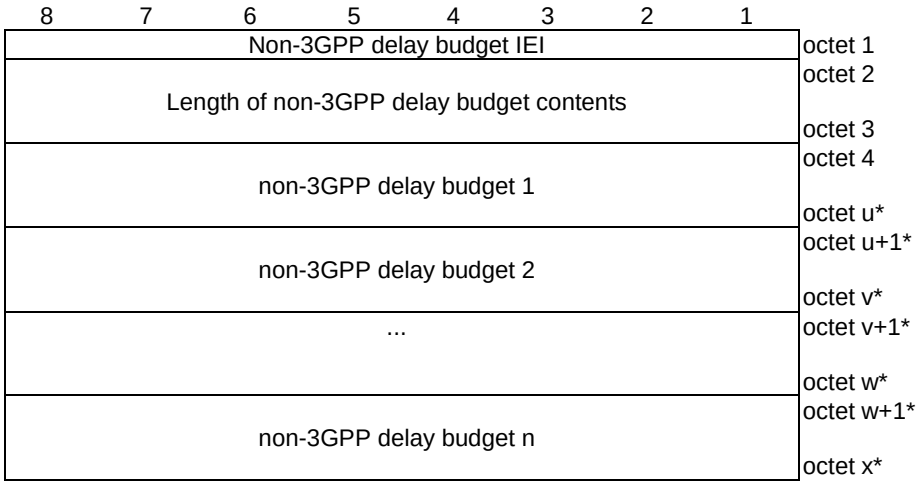


Figure 9.11.4.37.1: Non-3GPP delay budget information element

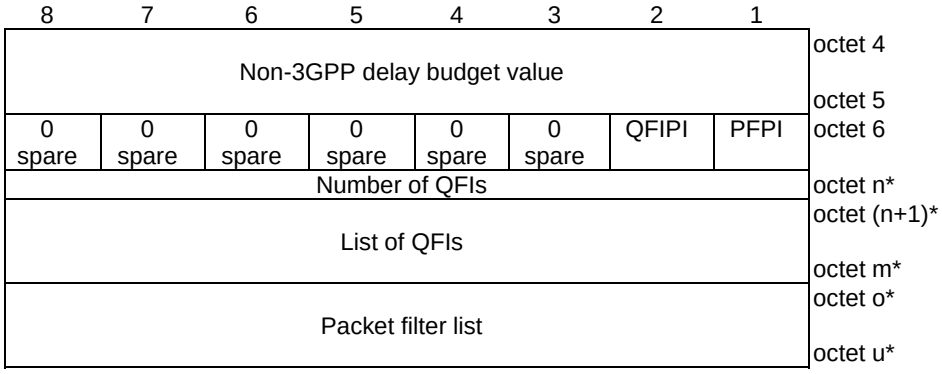


Figure 9.11.4.37.2: Non-3GPP delay budget

Table 9.11.4.37.1: Non-3GPP delay budget information element

The Non-3GPP delay budget value field contains the binary representation of the Non-3gpp delay budget in units of 0.5ms.
Bits
8 7 6 5 4 3 2 1 8 7 6 5 4 3 2 1
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
thru
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

Packet filter presence indicator (PFPI) (bit 1 of octet 6)
Bit
1
0 Packet filter list associated with the Non-3GPP delay budget value is not present
1 Packet filter list associated with the Non-3GPP delay budget value is present

QoS flow identifier presence indicator (QFIPI) (bit 2 of octet 6)
Bit
2
0 QoS flow identifier associated with the Non-3GPP delay budget value is not present
1 QoS flow identifier associated with the Non-3GPP delay budget value is present

Number of QFIs (octet n*)
The number of QFIs field is present if QFIPI is set to 1. If QFIPI is not set to 1, this field shall not be included in the non-3GPP delay budget. The number of QFIs field contains the binary coding for the number of QFIs associated with the same non-3GPP delay budget value. This field is encoded in bits 8 through 1 of octet 4 where bit 8 is he most significant and bit 1 is the least significant bit.

List of QFIs (octet (n+1)* to octet m*)
The list of QFIs field is present if QFIPI is set to 1. If QFIPI is not set to 1, this field shall not be included in the non-3GPP delay budget. This field indicates QoS flow(s) associated with the same non-3GPP delay budget value. This field contains QFI values encoded as below
Bits
8 7 6 5 4 3 2 1
0 0 0 0 0 0 0 0 Reserved
0 0 0 0 0 0 0 1 QFI 1
to
0 0 1 1 1 1 1 1 QFI 63
The other values are spare. If spare value is used, the UE shall ignore the value.

Packet filter list (octet 7 to u)
The packet filter list is present if PFPI is set to 1. If not present, this field shall not be included in the non-3GPP delay budget. The encoding of the packet filter list follows the figure 9.11.4.13.4 and the table 9.11.4.13.1.

9.11.4.38 URSP rule enforcement reports

The purpose of the URSP rule enforcement reports information element is to provide one or more URSP rule enforcement reports to the network. Each URSP rule enforcement report includes all the connection capabilities contained in the traffic descriptor of each URSP rule associated to the PDU session.

The URSP rule enforcement reports information element is coded as shown in figure 9.11.4.38.1, figure 9.11.4.38.2, and table 9.11.4.38.1.

The URSP rule enforcement reports is a type 4 information element with a minimum length of 4 octets.

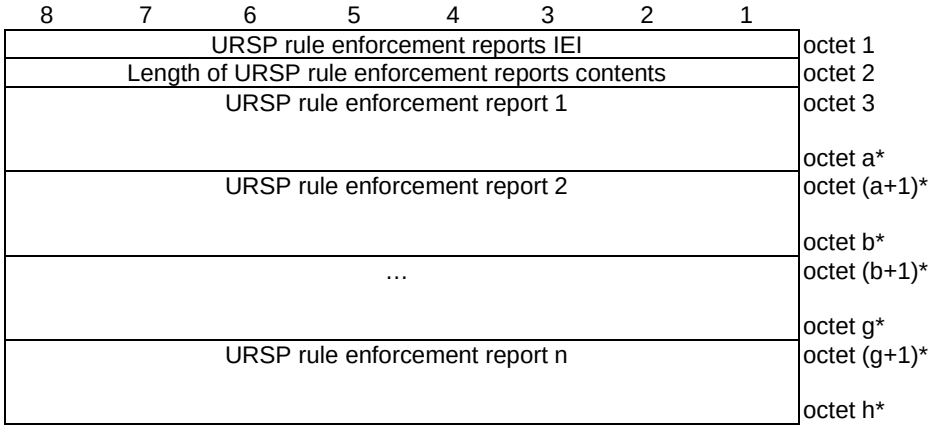


Figure 9.11.4.38.1: URSP rule enforcement reports information element

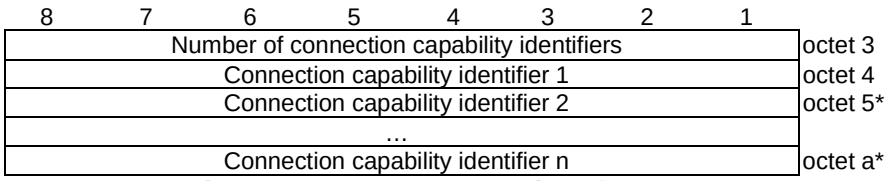


Figure 9.11.4.38.2: URSP rule enforcement report

Table 9.11.4.38.1: URSP rule enforcement reports information element

URSP rule enforcement report (octet 3 to octet a) The URSP rule enforcement report field contains all the connection capabilities contained in the traffic descriptor of one reported URSP rule. Number of connection capability identifiers (octet 3) The number of connection capability identifiers field indicates number of indicated connection capability identifiers in binary representation. The value of this field shall be set to at least one, and the receiving entity shall ignore the URSP rule enforcement reports IE with "Number of connection capability identifiers" field set to zero. Connection capability identifier Connection capability identifier is encoded as defined in 3GPP TS 24.526 [19] table 5.2.1.

9.11.4.39 Protocol description

The purpose of the Protocol description information element is to provide protocol description for UL PDU set handling to the UE.

The Protocol description information element is a type 6 information element with a minimum length of 6 octets.

The Protocol description information element is coded as shown in figure 9.11.4.39.1, figure 9.11.4.39.2, figure 9.11.4.39.3, figure 9.11.4.39.4, and table 9.11.4.39.1.

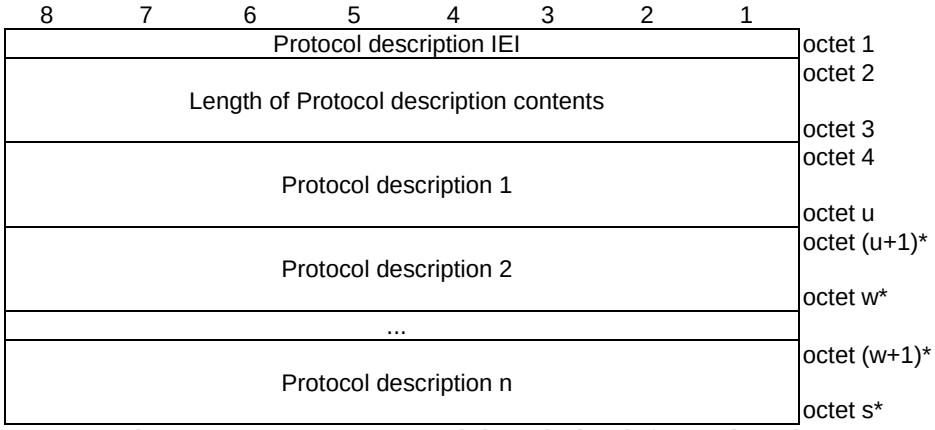


Figure 9.11.4.39.1: Protocol description information element

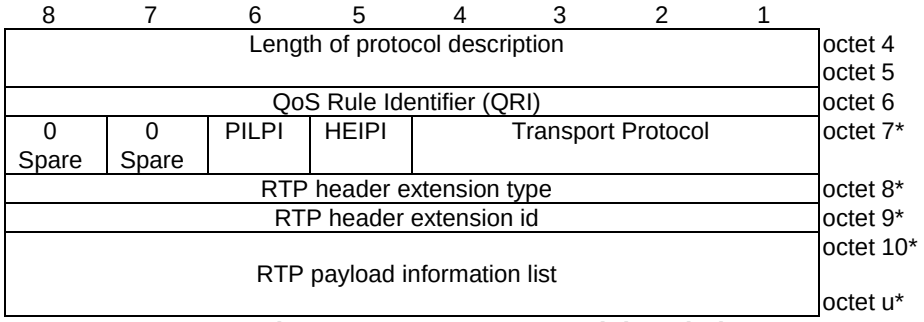


Figure 9.11.4.39.2: Protocol description

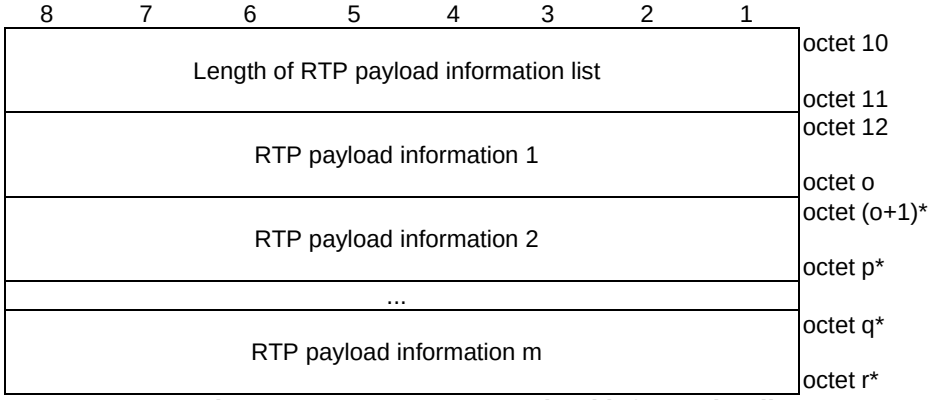


Figure 9.11.4.39.3: RTP payload information list

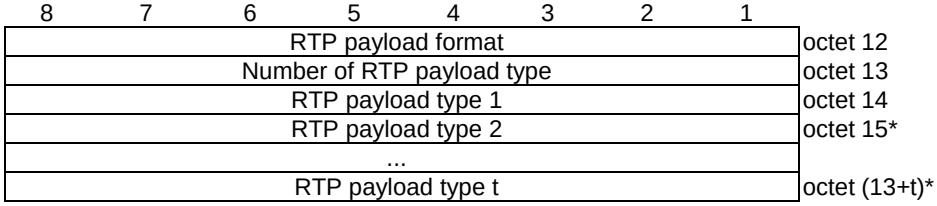


Figure 9.11.4.39.4: RTP payload information

Table 9.11.4.39.1: Protocol description information element

Length of protocol description (octet 4 and octet 5) (see NOTE 1)
The length of protocol description field indicates the length of the protocol description entry.

QoS Rule Identifier (QRI) (octet 6)
The QoS Rule Identifier (QRI) field contains the QoS rule identifier as specified in subclause 9.11.4.13. Each protocol description entry is associated with the QoS rule identified by the QRI field.

Transport Protocol (octet 7, bits 1 to 4)
The Transport Protocol field indicates the transport protocol used by the media flow, e.g., RTP or SRTP as specified in 3GPP TS 26.522 [69].
Bits

4	**3**	**2**	**1**	
0	0	0	1	RTP
0	0	1	0	SRTP

All other values are spare.

If Transport Protocol field indicates a spare value, the corresponding entry for the protocol description shall be ignored.

RTP header extension information presence indicator (HEIPI) (bit 5 of octet 7)
The HEIPI field indicates whether the RTP header extension information (RTP header extension type field and RTP header extension id field) is included in the IE or not.
Bit

5	
0	RTP header extension information not included
1	RTP header extension information included

RTP payload information list presence indicator (PILPI) (bit 6 of octet 7)
The PILPI field indicates whether the RTP payload information list is included in the IE or not.
Bit

6	
0	RTP payload information list not included
1	RTP payload information list included

RTP header extension type (octet 8)
The RTP header extension type field contains the RTP header extension type, i.e the RTP Header Extension for PDU Set Marking as specified in subclause 4.2 of 3GPP TS 26.522 [69].
Bits

8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	
0	0	0	0	0	0	0	1	RTP Header Extension for PDU Set Marking

All other values are spare.

RTP header extension id (octet 9)
If RTP header extension type has a value other than spare values,the RTP header extension id field contains the RTP header extension id which is coded as binary representation of an integer between 1(inclusive) and 255(inclusive) as defined in IETF RFC 8285 [70].

RTP payload information list (octets 10 to u) (see NOTE 2)
The RTP payload information list contains the RTP payload information for the RTP stream, which can be used to derive the PDU set information.

RTP payload format (octet 12)

Bits

8	**7**	**6**	**5**	**4**	**3**	**2**	**1**	
0	0	0	0	0	0	0	1	RTP payload format for H.264/AVC codec as specified in subclause A.2.2 of 3GPP TS 26.522 [69]
0	0	0	0	0	0	1	0	RTP payload format for H.265/HEVC codec as specified in subclause A.2.2 of 3GPP TS 26.522 [69]

All other values are spare.

If the RTP payload format indicates a spare value, the corresponding entry for the RTP payload information shall be ignored. RTP payload type (octet 14) The RTP payload type field indicates the RTP or SRTP payload type, it contains the binary representation of an integer between 0(inclusive) and 127(inclusive). The other values are spare. If spare value is used, the UE shall ignore the value.
NOTE 1: If the value of the length of protocol description field is set to 1, the corresponding entry for the protocol description shall be deleted for the associated QoS rule. If the value of the length of protocol description field is greater than 1, the corresponding entry for the protocol description shall be added or replaced for the associated QoS rule. NOTE 2: In this release of the specification, the RTP payload information list contains only one RTP payload information entry.

9.12 3GPP specific coding information defined within present document

9.12.1 Serving network name (SNN)

The serving network name (SNN) is used:

- in the Network name field of the AT_KDF_INPUT attribute defined in IETF RFC 5448 [40];
- in K_{AUSF} derivation function as specified in 3GPP TS 33.501 [24] annex A; and
- in RES* and XRES* derivation function as specified in 3GPP TS 33.501 [24] annex A.

SNN shall contain a UTF-8 string without terminating null characters.

SNN is of maximum length of 1020 octets.

SNN consists of SNN-service-code and SNN-network-identifier, delimited by a colon.

SNN-network-identifier identifies the serving PLMN or the serving SNPN.

MCC and MNC in the SNN-PLMN-ID are MCC and MNC of the serving PLMN. If the MNC of the serving PLMN has two digits, then a zero is added at the beginning.

MCC and MNC in the SNN-SNPN-ID are MCC and MNC of the serving SNPN. If the MNC of the serving SNPN has two digits, then a zero is added at the beginning.

SNN-NID contains an NID in hexadecimal digits.

ABNF syntax of SNN is specified in table 9.12.1.1

Table 9.12.1.1: ABNF syntax of SNN

```
SNN = SNN-service-code ":" SNN-network-identifier

SNN-service-code = %x35.47 ; "5G"

SNN-network-identifier = SNN-PLMN-ID / SNN-SNPN-ID

SNN-PLMN-ID = SNN-mnc-string SNN-mnc-digits "." SNN-mcc-string SNN-mcc-digits "." SNN-3gppnetwork-
string "." SNN-org-string ; applicable when not operating in SNPN access operation mode.

SNN-SNPN-ID = SNN-mnc-string SNN-mnc-digits "." SNN-mcc-string SNN-mcc-digits "." SNN-3gppnetwork-
string "." SNN-org-string ":" SNN-NID ; applicable when operating in SNPN access operation mode.


SNN-mnc-digits = DIGIT DIGIT DIGIT ; MNC of the PLMN ID
```