**3GPP TSG-CT WG1 Meeting #135-eC1-22xxxx**

**E-Meeting, 6th – 12th April 2022 *was* C1-222841**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **24.501** | **CR** | **4219** | **rev** | **1** | **Current version:** | **17.6.1** |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME | **X** | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Authentication and key agreement for 5G ProSe UE-to-network relay |
|  |  |
| ***Source to WG:*** | ZTE, InterDigital |
| ***Source to TSG:*** | C1 |
|  |  |
| ***Work item code:*** | 5G\_ProSe |  | ***Date:*** | 2022-04-08 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***Release:*** | Rel-17 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | Security procedure for 5G ProSe Communication via 5G ProSe UE-to-Network Relay over control plane is specified in TS 33.503.The corresponding NAS impacts need to be specified in this specification. |
|  |  |
| ***Summary of change:*** | Remove the description on relay key request in primary authentication procedure since relay key procedure does not rely on existing primary authentication according to TS 33.503.Specify the authentication and key agreement procedure for 5G ProSe UE-to-network relay.Define the related new 5GMM messages for authentication and key agreement procedure for 5G ProSe UE-to-network relay. |
|  |  |
| ***Consequences if not approved:*** | Security procedure for 5G ProSe UE-to-network relay over control plane is not supported. |
|  |  |
| ***Clauses affected:*** | 5.4.1.3.1, 5.5.x (new), 8.2.a (new), 8.2.b (new), 8.2.c (new), 8.2.d (new), 8.2.e (new), 9.7, 9.11.3.aa (new), 9.11.3.bb (new), 9.11.3.cc (new) |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **X** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **X** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **X** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

**\*\*\*\*\*\*\***

\* \* \* First Change \* \* \* \*

##### 5.4.1.3.1 General

The purpose of the 5G AKA based primary authentication and key agreement procedure is to provide mutual authentication between the UE and the network and to agree on the keys KAUSF, KSEAF and KAMF (see 3GPP TS 33.501 [24]). The cases when the 5G AKA based primary authentication and key agreement procedure is used are defined in 3GPP TS 33.501 [24].

The network initiates the 5G AKA based primary authentication and key agreement procedure by sending an AUTHENTICATION REQUEST message to the UE without the EAP message IE. The network shall include the ngKSI and the ABBA in AUTHENTICATION REQUEST message.

The 5G AKA based primary authentication and key agreement procedure is always initiated and controlled by the network. However, the UE can reject the 5G authentication challenge sent by the network.

The UE shall proceed with a 5G authentication challenge only if a USIM is present.

A partial native 5G NAS security context is established in the UE and the network when a 5G authentication is successfully performed. During a successful 5G AKA based primary authentication and key agreement procedure, the CK and IK are computed by the USIM. CK and IK are then used by the ME as key material to compute new keys KAUSF, KSEAF and KAMF. KAMF is stored in the 5G NAS security contexts (see 3GPP TS 33.501 [24]) of both the network and in the volatile memory of the ME while registered to the network, and is the root for the 5GS integrity protection and ciphering key hierarchy.

NOTE 1: Generation of the new KAUSF and the new KSEAF does not result into deletion of the valid KAUSF and the valid KSEAF, if any.

The 5G AKA based primary authentication and key agreement procedure is initiated by an AUTHENTICATION REQUEST message without the EAP message IE.

Upon successful completion of the 5G AKA based primary authentication, the AMF shall initiate a security mode control procedure (see subclause 5.4.2) to take the new partial native 5G NAS security context into use.

NOTE 2: The AMF shall immediately initiate a security mode control procedure (see subclause 5.4.2) after 5G AKA primary authentication is successful to avoid KAUSF key mismatch between the UE and the network.

\* \* \* Next Change \* \* \* \*

### 5.5.x Authentication and key agreement procedure for 5G ProSe UE-to-network relay

#### 5.5.x.1 General

The purpose of the authentication and key agreement procedure for 5G ProSe UE-to-network relay is to perform the authentication for 5G ProSe UE-to-network relay initiated by the 5G ProSe UE-to-network remote UE and to agree on the KAUSF\_P and KNR\_ProSe as specified in 3GPP TS 33.503 [56].

The procedure as shown in figure 5.5.x.1.1 is initiated by the UE when the UE receives the ProSe direct link establishment request from the 5G ProSe UE-to-network remote UE for establishing secure PC5 unicast link as specified in 3GPP TS 24.554 [19E].

If the network decides to process the relay key request message, the EAP based authentication and key agreement procedure is initiated and controlled by the network. The exchanges of EAP messages between the 5G ProSe UE-to-network remote UE and the network are relayed by the UE.



Figure 5.5.x.1.1: Authentication and key agreement procedure for 5G ProSe UE-to-network relay

#### 5.5.x.2 ProSe relay transaction identity (PRTI)

Editor's note: Handling of PRTI is FFS.

#### 5.5.x.3 UE-initiated authentication and key agreement procedure initiation

Upon receiving a ProSe direct link establishment request from the 5G ProSe UE-to-network remote UE for establishing secure PC5 unicast link as specified in 3GPP TS 24.554 [19E], the UE shall:

a) allocate a PRTI value as specified in clause 5.5.x.2;

b) create a RELAY KEY REQUEST message;

c) set the PRTI IE of the RELAY KEY REQUEST message to the allocated EPTI value;

d) set the relay key request parameters IE with SUCI, Relay Service Code, nonce\_1, etc, received from the of the 5G ProSe UE-to-network remote UE;

e) send the RELAY KEY REQUEST message; and

f) start a timer T35xx upon sending the RELAY KEY REQUEST message.

Editor's note: The definition of the timer T35xx is FFS.

#### 5.5.x.4 UE-initiated authentication and key agreement procedure accepted by the network

Upon receiving the RELAY KEY REQUEST message, the AMF processes the message and interacts with the AUSF as specified in 3GPP TS 33.503 [56]. If EAP-AKA' authentication for the 5G ProSe UE-to-network relay is initiated by the network, the AMF shall:

a) create a RELAY AUTHENTICATION REQUEST message;

b) set the PRTI IE of the RELAY AUTHENTICATION REQUEST message to the PRTI value of the received RELAY AUTHENTICATION REQUEST message;

c) set the EAP message IE to EAP request message received from the AUSF; and

d) send the RELAY AUTHENTICATION REQUEST message to the UE.

Upon receiving the RELAY AUTHENTICATION REQUEST message, the UE stops the timer T35xx and forwards the EAP message to the 5G ProSe UE-to-network remote UE as specified in 3GPP TS 24.554 [19E].

Upon receiving the EAP response message from the 5G ProSe UE-to-network remote UE as specified in 3GPP TS 24.554 [19E], the UE shall:

a) create a RELAY AUTHENTICATION RESPONSE message;

b) set the PRTI IE of the RELAY AUTHENTICATION RESPONSE message to the PRTI value of the received RELAY AUTHENTICATION REQUEST message;

c) set the EAP message IE to EAP request message received from the 5G ProSe UE-to-network remote UE; and

d) start a timer T35xx upon sending the RELAY AUTHENTICATION RESPONSE message to the AMF.

After receiving the RELAY AUTHENTICATION RESPONSE message, the AMF may send a new RELAY AUTHENTICATION REQUEST message carrying EAP request message according to further handling of EAP-AKA' authentication from the AUSF as specified in 3GPP TS 33.503 [56]. The UE repeats the handling of RELAY AUTHENTICATION REQUEST as described above.

Upon receiving the message from the AUSF that the authentication is successful, the AMF shall:

a) create a RELAY KEY ACCEPT message;

b) set the PRTI IE of the RELAY KEY ACCEPT message to the PRTI value of the last received RELAY AUTHENTICATION RESPONSE message;

c) include the EAP message IE and set with EAP-success message received from the AUSF; and

d) include the relay key response parameters IE and set with Key KNR\_ProSe, nonce\_2, etc, received from AUSF;

Upon receiving the RELAY KEY ACCEPT message, the UE forwards the EAP-success message and nonce\_2 to the 5G ProSe UE-to-network remote UE as specified in 3GPP TS 24.554 [19E], and considers the authentication is completed successfully.

#### 5.5.x.5 UE-initiated authentication and key agreement procedure not accepted by the network

If the UE-initiated authentication and key agreement procedure is not accepted by the network, the AMF shall:

a) create a RELAY KEY REJECT message;

b) set the PRTI IE of the RELAY KEY REJECT message to the PRTI value of the received RELAY KEY REQUEST message if the network decides to reject the RELAY KEY REQUEST message; or

 set the PRTI IE of the RELAY KEY REJECT message to the PRTI value of the received RELAY AUTHENTICATION RESPONSE message and include the EAP message IE set with EAP-failure message if the AMF receives an EAP-failure message from the AUSF; and

c) send the RELAY KEY REJECT message to the UE.

#### 5.5.x.6 Abnormal cases in the UE

Editor's note: The abnormal cases in the UE are FFS.

#### 5.5.x.7 Abnormal cases on the network side

Editor's note: The abnormal cases on the network side are FFS.

\* \* \* Next Change \* \* \* \*

### 8.2.a Relay key request

#### 8.2.a.1 Message definition

The RELAY KEY REQUEST message is sent by the UE to the AMF for initiation of PC5 keys establishment with the 5G ProSe UE-to-network remote UE as specified in 3GPP TS 33.503 [56]. See table 8.2.a.1.

Message type: RELAY KEY REQUEST

Significance: dual

Direction: UE to network

Table 8.2.a.1: RELAY KEY REQUEST message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator9.2 | M | V | 1 |
|  | Security header type | Security header type9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet9.5 | M | V | 1/2 |
|  | Relay key request message identity | Message type9.7 | M | V | 1 |
|  | PRTI | ProSe relay transaction identity9.11.3.aa | M | V | 1 |
|  | Relay key request parameters | Relay key request parameters9.11.3.bb | M | LV | TBD |

\* \* \* Next Change \* \* \* \*

### 8.2.b Relay key accept

#### 8.2.b.1 Message definition

The RELAY KEY ACCEPT message is sent by the AMF to the UE as specified in 3GPP TS 33.503 [56]. See table 8.2.b.1.

Message type: RELAY KEY ACCEPT

Significance: dual

Direction: network to UE

Table 8.2.b.1: RELAY KEY ACCEPT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator9.2 | M | V | 1 |
|  | Security header type | Security header type9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet9.5 | M | V | 1/2 |
|  | Relay key accept message identity | Message type9.7 | M | V | 1 |
|  | PRTI | ProSe relay transaction identity9.11.3.aa | M | V | 1 |
|  | EAP message | EAP message9.11.2.2 | M | LV-E | 6-1502 |
|  | Relay key response parameters | Relay key response parameters9.11.3.cc | M | TLV-E | TBD |

\* \* \* Next Change \* \* \* \*

### 8.2.c Relay key reject

#### 8.2.c.1 Message definition

The RELAY KEY REJECT message is sent by the AMF to the UE to indicate the rejection of the relay key request. See table 8.2.c.1.

Message type: RELAY KEY REJECT

Significance: dual

Direction: network to UE

Table 8.2.c.1: RELAY KEY REJECT message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator9.2 | M | V | 1 |
|  | Security header type | Security header type9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet9.5 | M | V | 1/2 |
|  | Relay key reject message identity | Message type9.7 | M | V | 1 |
|  | PRTI | ProSe relay transaction identity9.11.3.aa | M | V | 1 |
| xx | EAP message | EAP message9.11.2.2 | O | LV-E | 6-1502 |

#### 8.2.c.2 EAP message

EAP message IE is included if the RELAY KEY REJECT message is used to convey EAP-failure message.

\* \* \* End of Changes \* \* \* \*

### 8.2.d Relay authentication request

#### 8.2.d.1 Message definition

The RELAY AUTHENTICATION REQUEST message is sent by the network to the UE to initiate authentication of the 5G ProSe UE-to-network remote UE as specified in 3GPP TS 33.503 [56]. See table 8.2.c.1.

Message type: RELAY AUTHENTICATION REQUEST

Significance: dual

Direction: Network to UE

Table 8.2.c.1: RELAY AUTHENTICATION REQUEST message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator9.2 | M | V | 1 |
|  | Security header type | Security header type9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet9.5 | M | V | 1/2 |
|  | Relay authentication request message identity | Message type9.7 | M | V | 1 |
|  | PRTI | ProSe relay transaction identity9.11.3.aa | M | V | 1 |
|  | EAP message | EAP message9.11.2.2 | M | LV-E | 6-1502 |

\* \* \* Next Change \* \* \* \*

### 8.2.e Relay authentication response

#### 8.2.e.1 Message definition

The RELAY AUTHENTICATION RESPONSE message is sent by the UE to the network to forward the authentication response from the 5G ProSe UE-to-network remote UE as specified in 3GPP TS 33.503 [56]. See table 8.2.e.1.

Message type: RELAY AUTHENTICATION RESPONSE

Significance: dual

Direction: UE to network

Table 8.2.e.1: RELAY AUTHENTICATION RESPONSE message content

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IEI | Information Element | Type/Reference | Presence | Format | Length |
|  | Extended protocol discriminator | Extended protocol discriminator9.2 | M | V | 1 |
|  | Security header type | Security header type9.3 | M | V | 1/2 |
|  | Spare half octet | Spare half octet9.5 | M | V | 1/2 |
|  | Relay authentication response message identity | Message type9.7 | M | V | 1 |
|  | PRTI | ProSe relay transaction identity9.11.3.aa | M | V | 1 |
|  | EAP message | EAP message9.11.2.2 | M | LV-E | 6-1502 |

\* \* \* Next Change \* \* \* \*

## 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 |
|  |  |  |  |  |  |  |  |  |  |

\* \* \* Next Change \* \* \* \*

#### 9.11.3.aa ProSe relay transaction identity

The purpose of the ProSe relay transaction identity is to uniquely identify an authentication and key agreement procedure for 5G ProSe UE-to-network relay. The PRTI allows distinguishing up to 254 different bi-directional messages.

Bits 1 to 8 of the forth octet of messages for authentication and key agreement procedure for 5G ProSe UE-to-network relay as specified in subclause 5.5.x contain the ProSe relay transaction identity.

The ProSe relay transaction identity information element is coded as shown in table 9.11.3.aa.1.

Table 9.11.3.aa.1: ProSe relay transaction identity

|  |
| --- |
|  |
| 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.bb 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 as specified in 3GPP TS 33.503 [56].

The relay key request parameters information element is coded as shown in figure 9.11.3.bb.1 and table 9.11.3.bb.1.

The relay key request parameters is a type 6 information element.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Relay key request parameters IEI | octet 1 |
| Length of Relay key request parameters | octet 2octet 3 |
| Relay service code | octet 4octet 6 |
| Nonce\_1 | octet 7octet 22 |
| Remote UE identity | octet 23octet n |

Figure 9.11.3.bb.1: Relay key request parameters information element

Editor's note: Whether other parameters are included is FFS and will be determined by SA3.

Table 9.11.3.bb.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].Remote UE identity (octet 23 to n)Remote UE identity indicates the 5G ProSe UE-to-network remote UE identity which 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). |

\* \* \* Next Change \* \* \* \*

#### 9.11.3.cc 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 as specified in 3GPP TS 33.503 [56].

The relay key response parameters information element is coded as shown in figure 9.11.3.cc.1 and table 9.11.3.cc.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 2octet 3 |
| Key KNR\_ProSe | octet 4octet 35 |
| Nonce\_2 | octet 36octet 51 |

Figure 9.11.3.cc.1: Relay key response parameters information element

Editor's note: Whether other parameters are included is FFS and will be determined by SA3.

Table 9.11.3.cc.1: Relay key response parameters information element

|  |
| --- |
| Key KNR\_ProSe (octet 4 to 35)Key KNR\_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 7 to 22)Nonce\_2 is the 128-bit nonce value as defined in 3GPP TS 24.554 [19E]. |

\* \* \* End of Changes \* \* \* \*