**3GPP TSG-CT WG1 Meeting #136-eC1-22xxxx**

**E-Meeting, 12th – 20th May 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **24.501** | **CR** | **4365** | **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:*** | Secondary authentication via L3 relay | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | OPPO, ZTE, Interdigital | | | | | | | | | |
| ***Source to TSG:*** | C1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5G\_ProSe | | | | |  | ***Date:*** | | | 2022-4-15 |
|  |  | | | |  | |  | | |  |
| ***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 can be 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:*** | | In clause 6.3.3.3.4 of TS 33.503, the PDU session authentication and authorization procedure for the L3 remote UE is defined.  The exsiting PDU SESSION AUTHENTICATION COMMAND message and PDU SESSION AUTHENTICATION COMPLETE message are updated to include the remote user ID and exchange the EAP messages for L3 remote UE between the L3 relay UE and SMF. Since in the remote UE report procedure, the remote user ID has not been defined, still in this CR, the definition of Remote user ID IE is left to FFS.  Diferrent from the exisitng PDU session authentication, instead of PDU SESSION AUTHENTICATION RESULT/REJECT message, the REMOTE UE REPORT RESPONSE message is used to inform the result to the L3 relay UE and send the EAP-success/failure to L3 remote UE.  The stage 3 implementation is needed. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Add PDU session authentication for remote UE. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Missing stage 2 requirements. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 6.3.1.1, 6.3.1.2.1, 6.3.1.2.2, 6.6.2.3, 8.3.4.1, 8.3.4.a(new), 8.3.5.1, 8.3.5.b(new), 8.3.20.1, 8.3.20.c(new), 8.3.20.d(new), 8.3.20.e(new) and 9.11.4.f(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:*** | | Revision compared to C1-223022: Editorial changes and change the Remote UE handling information list IE to type 6 IE. Remote UE handling information list IE is used in the SM messages. | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

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

#### 6.3.1.1 General

The purpose of the PDU session authentication and authorization procedure is to enable the DN:

a) to authenticate the upper layers of the UE, when establishing the PDU session;

b) to authorize the upper layers of the UE, when establishing the PDU session;

c) both of the above;

d) to re-authenticate the upper layers of the UE after establishment of the PDU session; or

e) to authenticate the upper layers of the 5G ProSe layer-3 remote UE, upon receipt of the REMOTE UE REPORT message.

The PDU session authentication and authorization procedure can be performed only during or after the UE-requested PDU session procedure establishing a non-emergency PDU session. The PDU session authentication and authorization procedure shall not be performed during or after the UE-requested PDU session establishment procedure establishing an emergency PDU session.

The upper layers store the association between a DNN and corresponding credentials, if any, for the PDU session authentication and authorization.

The network authenticates the UE using the Extensible Authentication Protocol (EAP) as specified in IETF RFC 3748 [34].

EAP has defined four types of EAP messages:

a) an EAP-request message;

b) an EAP-response message;

c) an EAP-success message; and

d) an EAP-failure message.

The EAP-request message is transported from the network to the UE using the PDU SESSION AUTHENTICATION COMMAND message of the PDU EAP message reliable transport procedure.

The EAP-response message to the EAP-request message is transported from the UE to the network using the PDU SESSION AUTHENTICATION COMPLETE message of the PDU EAP message reliable transport procedure.

If the PDU session authentication and authorization procedure is performed during the UE-requested PDU session establishment procedure:

a) and the DN authentication of the UE completes successfully, the EAP-success message is transported from the network to the UE as part of the UE-requested PDU session establishment procedure in the PDU SESSION ESTABLISHMENT ACCEPT message.

b) and the DN authentication of the UE completes unsuccessfully, the EAP-failure message is transported from the network to the UE as part of the UE-requested PDU session establishment procedure in the PDU SESSION ESTABLISHMENT REJECT message.

If the PDU session authentication and authorization procedure is performed after the UE-requested PDU session establishment procedure:

a) and the DN authentication of the UE completes successfully, the EAP-success message is transported from the network to the UE using the PDU SESSION AUTHENTICATION RESULT message of the PDU EAP result message transport procedure.

b) and the DN authentication of the UE completes unsuccessfully, the EAP-failure message is transported from the network to the UE using the PDU SESSION RELEASE COMMAND message of the network-requested PDU session release procedure.

There can be several rounds of exchange of an EAP-request message and a related EAP-response message for the DN to complete the authentication and authorization of the request for a PDU session (see example in figure 6.3.1.1).

The SMF shall set the authenticator retransmission timer specified in IETF RFC 3748 [34] subclause 4.3 to infinite value.

NOTE: The PDU session authentication and authorization procedure provides a reliable transport of EAP messages and therefore retransmissions at the EAP layer of the SMF do not occur.

Figure 6.3.1.1: PDU session authentication and authorization procedure

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

##### 6.3.1.2.1 PDU EAP message reliable transport procedure initiation

In order to initiate the PDU EAP message reliable transport procedure, the SMF shall create a PDU SESSION AUTHENTICATION COMMAND message.

The SMF shall set the PTI IE of the PDU SESSION AUTHENTICATION COMMAND message to "No procedure transaction identity assigned".

The SMF shall set the EAP message IE of the PDU SESSION AUTHENTICATION COMMAND message to the EAP-request message provided by the DN or generated locally.

The SMF shall set the Remote user ID IE of the PDU SESSION AUTHENTICATION COMMAND message to the remote user identify if received in the Remote UE context connected IE in the REMOTE UE REPORT message.

The SMF shall send the PDU SESSION AUTHENTICATION COMMAND message, and the SMF shall start timer T3590 (see example in figure 6.3.1.1).

Upon receipt of the PDU SESSION AUTHENTICATION COMMAND message, if the UE provided a DNN during the PDU session establishment, the UE shall stop timer T3396, if it is running for the DNN provided by the UE. If the UE did not provide a DNN during the PDU session establishment, the UE shall stop the timer T3396 associated with no DNN if it is running.

Upon receipt of the PDU SESSION AUTHENTICATION COMMAND message, if the UE provided an S-NSSAI and a DNN during the PDU session establishment, the UE shall stop timer T3584, if it is running for the [S-NSSAI of the PDU session, DNN] combination. If the UE provided a DNN but did not provide an S-NSSAI during the PDU session establishment, the UE shall stop timer T3584, if it is running for the same [no S-NSSAI, DNN] combination provided by the UE. If the UE provided an S-NSSAI but did not provide a DNN during the PDU session establishment, the UE shall stop timer T3584, if it is running for the same [S-NSSAI, no DNN] combination provided by the UE. If the UE provided neither a DNN nor an S-NSSAI during the PDU session establishment, the UE shall stop timer T3584, if it is running for the same [no S-NSSAI, no DNN] combination provided by the UE. The timer T3584 to be stopped includes the timer T3584 applied for all the PLMNs, if running, and the timer T3584 applied for the registered PLMN, if running.

Upon receipt of the PDU SESSION AUTHENTICATION COMMAND message, if the UE provided an S-NSSAI during the PDU session establishment, the UE shall stop timer T3585, if it is running for the S-NSSAI of the PDU session. If the UE did not provide an S-NSSAI during the PDU session establishment, the UE shall stop the timer T3585 associated with no S-NSSAI if it is running. The timer T3585 to be stopped includes the timer T3585 applied for all the PLMNs, if running, and the timer T3585 applied for the registered PLMN, if running.

NOTE 1: Upon receipt of the PDU SESSION AUTHENTICATION COMMAND message for a PDU session, if the UE provided a DNN (or no DNN) and an S-NSSAI (or no S-NSSAI) when the PDU session is established, timer T3396 associated with the DNN (or no DNN, if no DNN was provided by the UE) is running, and timer T3584 associated with the DNN (or no DNN, if no DNN was provided by the UE) and the S-NSSAI (or no S-NSSAI, if no S-NSSAI was provided by the UE) is running, then the UE stops both the timer T3396 and the timer T3584.

NOTE 2: Upon receipt of the PDU SESSION AUTHENTICATION COMMAND message for a PDU session, if the UE provided a DNN (or no DNN) and an S-NSSAI (or no S-NSSAI) when the PDU session is established, timer T3585 associated with the S-NSSAI (or no S-NSSAI, if no S-NSSAI was provided by the UE) is running, and timer T3584 associated with the DNN (or no DNN, if no DNN was provided by the UE) and the S-NSSAI (or no S-NSSAI, if no S-NSSAI was provided by the UE) is running, then the UE stops both the timer T3585 and the timer T3584.

Upon receipt of a PDU SESSION AUTHENTICATION COMMAND message and a PDU session ID, using the NAS transport procedure as specified in subclause 5.4.5, the UE passes to the upper layers the EAP message received in the EAP message IE of the PDU SESSION AUTHENTICATION COMMAND message. Apart from this action and the stopping of timers T3396, T3584 and T3485 (if running), the authentication and authorization procedure initiated by the DN is transparent to the 5GSM layer of the UE.

Upon receipt of a PDU SESSION AUTHENTICATION COMMAND message including the Remote user ID IE, the UE shall pass to the upper layer as defined in 3GPP TS 24.554 [19E] the EAP message received in the EAP message IE of the PDU SESSION AUTHENTICATION COMMAND message.

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

##### 6.3.1.2.2 PDU EAP message reliable transport procedure accepted by the UE

The UE shall create a PDU SESSION AUTHENTICATION COMPLETE message when:

a) the upper layers provide an EAP-response message responding to the received EAP-request message; or

b) the UE receives an EAP message from the 5G ProSe layer-3 remote UE as defined in 3GPP TS 24.554 [19E].

The UE shall set the EAP message IE of the PDU SESSION AUTHENTICATION COMPLETE message to the EAP-response message.

The UE shall set the Remote user ID IE of the PDU SESSION AUTHENTICATION COMPLETE message to the remote user identity from which the EAP message is received if the EAP message is received from the 5G ProSe layer-3 remote UE.

The UE shall transport the PDU SESSION AUTHENTICATION COMPLETE message and the PDU session ID, using the NAS transport procedure as specified in subclause 5.4.5. Apart from this action, the authentication and authorization procedure initiated by the DN is transparent to the 5GSM layer of the UE.

Upon receipt of a PDU SESSION AUTHENTICATION COMPLETE message, the SMF shall stop timer T3590 and provides the EAP message received in the EAP message IE of the PDU SESSION AUTHENTICATION COMPLETE message to the DN or handles it locally.

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

#### 6.6.2.3 Remote UE report procedure accepted by the network

Upon receipt of the REMOTE UE REPORT message, the SMF shall send a REMOTE UE REPORT RESPONSE message to the UE.

The SMF shall include the PTI from the REMOTE UE REPORT message.

The SMF shall set the EAP message IE to an EAP-success message or an EAP-failure message to be sent to the 5G ProSe layer-3 remote UE if the EAP-success message or the EAP-failure message is received from the DN.

The SMF may include the Remote UE handling information IE if the PDU session authentication and authorization procedure for the 5G ProSe layer-3 remote UE were performed.

The SMF may include the Authorized QoS flow description IE to indicate the QoS flow parameters to the 5G ProSe layer-3 relay UE when the PDU session authentication and authorization procedure for the 5G ProSe layer-3 remote UE is successful.

Editor’s note: Whether and why the Authorized QoS flow description IE is included is FFS.

Upon receipt of the REMOTE UE REPORT RESPONSE message, the UE shall stop timer T3586 and enter the state PROCEDURE TRANSACTION INACTIVE.

Upon receipt of the REMOTE UE REPORT RESPONSE message including the EAP message IE, the UE shall pass the EAP message received in the EAP message IE to the upper layer as defined in 3GPP TS 24.554 [19E].

Upon receipt of the REMOTE UE REPORT RESPONSE message including the Remote UE handling information IE, the UE shall pass the Remote UE handling information IE to the upper layer as defined in 3GPP TS 24.554 [19E].

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

#### 8.3.4.1 Message definition

The PDU SESSION AUTHENTICATION COMMAND message is sent by the SMF to the UE for authentication of the UE establishing the PDU session or of the UE participating in the PDU session. See table 8.3.4.1.1.

Message type: PDU SESSION AUTHENTICATION COMMAND

Significance: dual

Direction: network to UE

Table 8.3.4.1.1: PDU SESSION AUTHENTICATION COMMAND 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 |
|  | PDU SESSION AUTHENTICATION COMMAND message identity | Message type  9.7 | M | V | 1 |
|  | EAP message | EAP message  9.11.2.2 | M | LV-E | 6-1502 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.11.4.6 | O | TLV-E | 4-65538 |
| 7A | Remote UE handling information list | Remote UE handling information list  9.11.4.f | O | TLV-E | 4-65538 |

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

#### 8.3.4.a Remote UE handling information list

The Remote UE handling information list IE is included in the message when the network needs to transmit the EAP message to a 5G ProSe layer-3 remote UE.

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

#### 8.3.5.1 Message definition

The PDU SESSION AUTHENTICATION COMPLETE message is sent by the UE to the SMF in response to the PDU SESSION AUTHENTICATION COMMAND message and indicates acceptance of the PDU SESSION AUTHENTICATION COMMAND message. See table 8.3.5.1.1.

Message type: PDU SESSION AUTHENTICATION COMPLETE

Significance: dual

Direction: UE to network

Table 8.3.5.1.1: PDU SESSION AUTHENTICATION COMPLETE 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 |
|  | PDU SESSION AUTHENTICATION COMPLETE message identity | Message type  9.7 | M | V | 1 |
|  | EAP message | EAP message  9.11.2.2 | M | LV-E | 6-1502 |
| 7B | Extended protocol configuration options | Extended protocol configuration options  9.11.4.6 | O | TLV-E | 4-65538 |
| 7A | Remote UE handling information list | Remote UE handling information list  9.11.4.f | O | TLV-E | 4-65538 |

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

#### 8.3.5.b Remote UE handling information list

This Remote UE handling information list IE is included in the message when the UE needs to transmit the EAP message to a 5G ProSe layer-3 remote UE.

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

#### 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 |
| 78 | EAP message | EAP message  9.11.2.2 | O | TLV-E | 6-1502 |
| 7A | Remote UE handling information list | Remote UE handling information list  9.11.4.f | O | TLV-E | 4-65538 |
| 79 | Authorized QoS flow descriptions | QoS flow descriptions  9.11.4.12 | O | TLV-E | 6-65538 |

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

#### 8.3.20.c EAP message

This EAP message IE is included when the external DN performs authentication and authorization of the UE using EAP.

#### 8.3.20.d Remote UE handling information list

This Remote UE handling information list IE is included in the message when the network needs to inform the secondary authentication information to the 5G ProSe layer-3 relay UE.

#### 8.3.20.e Authorized QoS flow descriptions

This Authorized QoS flow descriptions IE is included in the message when the network needs to indicate the QoS flow parameters to the 5G ProSe layer-3 relay UE and the PDU session authentication and authorization procedure for the 5G ProSe layer-3 remote UE is successful.

Editor’s note: Whether and why the Authorized QoS flow description IE is included is FFS.

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

#### 9.11.4.f Remote UE handling information

The purpose of the Remote UE handling information list information element is to inform the secondary authentication information to the 5G ProSe layer-3 relay UE.

The Remote UE handling information list information element is coded as shown in figure 9.11.4.f.1 and table 9.11.4.f.1.

The Remote UE handling information list is a type 6 information element with a length of 4 octets.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Remote UE handling information list IEI | | | | | | | | octet 1 |
| Length of remote UE handling information list contents | | | | | | | | octet 2  octet 3 |
| Number of remote UE handling information | | | | | | | | octet 4 |
| Remote UE handling information 1 | | | | | | | | octet o1  octet o2 |
| … | | | | | | | | octet o2+1  octet o3 |
| Remote UE handling information n | | | | | | | | octet o3+1  octet o4 |

Figure 9.11.4.f.1: Remote UE handling information list information element

Table 9.11.4.f.1: Remote UE handling information list information element

|  |
| --- |
| Remote UE handling information : |
|  |
| The contents of remote UE handling information are applicable for one individual UE and are coded as shown in figure 9.11.4.f.2 and table 9.11.4.f.2. |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |  |
| Length of remote UE handling information | | | | | | | | octet 5 |
| Number of user identities | | | | | | | | octet 6 |
| Length of user identity 1 | | | | | | | | octet 7 |
| User identity 1 | | | | | | | | octet 8 |
| octet q |
| … | | | | | | | |  |
| Length of user identity v | | | | | | | | octet m |
| User identity v | | | | | | | | octet m+1 |
| octet j |
| Spare | | | | | | DLRI | AR | octet (j+1)\* |

Figure 9.11.4.f.2: Remote UE handling information

Table 9.11.4.f.2: Remote UE handling information

|  |
| --- |
| User identity (octet 8 to octet q) |
| The user identity field is coded as specified in figure 9.11.4.29.2 and table 9.11.4.29.2. |
|  |
| Authentication result (AR) (bit 1 octet j+1):  0 Secondary authentication is successful |
| 1 Secondary authentication is not successful |
|  |
| 5G ProSe direct link release indication (DLRI) (bit 2 octet j+1):  0 5G ProSe direct link is not released  1 5G ProSe direct link is released |
|  |

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