**3GPP TSG-SA3 Meeting #116 *draft\_S3-242368\_r1***

**Jeju, South Korea, 20th - 24th May 2024**

|  |
| --- |
| *CR-Form-v12.2* |
| **CHANGE REQUEST** |
|  |
|  | **33.402** | **CR** | **0150** | **rev** | **-** | **Current version:** | **18.0.0** |  |
|  |
| *For* ***[HE](http://www.3gpp.org/3G_Specs/CRs.htm%22%20%5Cl%20%22_blank)******[LP](http://www.3gpp.org/3G_Specs/CRs.htm%22%20%5Cl%20%22_blank)*** *on using this form: comprehensive instructions can be found at <http://www.3gpp.org/Change-Requests>.* |
|  |

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

|  |
| --- |
|  |
| ***Title:***  | Clarification on the condition for provisioning of the ePDG identity to the UE |
|  |  |
| ***Source to WG:*** | ZTE Corporation, Nokia |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | TEI18 |  | ***Date:*** | 2024-05-06 |
|  |  |  |  |  |
| ***Category:*** | F |  | ***Release:*** | Rel-18 |
|  | *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-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19)* |
|  |  |
| ***Reason for change:*** | In clause 8.2.2 of TS 33.402, it is unclear whether the ePDG identity shall be provide by ePDG to UE in the IKE\_AUTH response message in first IKE\_AUTH exchange if the UE has requested with a CERTREQ payload in step 2. This need to be clarified. |
|  |  |
| ***Summary of change:*** | Provide clarifications to clause 8.2.2. |
|  |  |
| ***Consequences if not approved:*** | The content of IKE\_AUTH response message is unclear. |
|  |  |
| ***Clauses affected:*** | 8.2.2 |
|  |  |
|  | **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:*** |  |

\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*

### 8.2.2 Tunnel full authentication and authorization

The tunnel end point in the network is the ePDG. As part of the tunnel establishment attempt the use of a certain APN is requested. When a new attempt for tunnel establishment is performed by the UE the UE shall use IKEv2 as specified in RFC 5996 [30]. The authentication of the UE in its role as IKEv2 initiator terminates in the 3GPP AAA Server. The UE shall send EAP messages over IKEv2 to the ePDG. The ePDG shall extract the EAP messages received from the UE over IKEv2, and send them to the 3GPP AAA Server. The UE shall use the Configuration Payload of IKEv2 to obtain the Remote IP address.

The EAP-AKA message parameters and procedures regarding authentication are omitted. Only decisions and processes relevant to the use of EAP-AKA within IKEv2 are explained.

The message flow for the full authentication is depicted in the Figure 8.2.2-1.



Figure 8.2.2-1: Tunnel full authentication and authorization

As the UE and ePDG generate nonces as input to derive the encryption and authentication keys in IKEv2, replay protection is provided. For this reason, there is no need for the 3GPP AAA Server to request the user identity again using the EAP-AKA specific methods (as specified in RFC 4187 [7]), because the 3GPP AAA Server is certain that no intermediate node has modified or changed the user identity.

1. The UE and the ePDG exchange the first pair of messages, known as IKE\_SA\_INIT, in which the ePDG and UE negotiate cryptographic algorithms, exchange nonces and perform a Diffie\_Hellman exchange.

2. The UE sends the user identity (in the IDi payload) and the APN information (in the IDr payload) in this first message of the IKE\_AUTH phase, and begins negotiation of child security associations. The UE omits the AUTH parameter in order to indicate to the ePDG that it wants to use EAP over IKEv2. The user identity shall be compliant with Network Access Identifier (NAI) format specified in TS 23.003 [8], containing the IMSI or the pseudonym, as defined for EAP-AKA in RFC 4187 [7]). The UE shall send the configuration payload (CFG\_REQUEST) within the IKE\_AUTH request message to obtain an IPv4 and/or IPV6 home IP Address and/or a Home Agent Address. If the UE is provisioned with the ePDG root certificate, it shall include the CERTREQ payload within the IKE\_AUTH request message to request ePDG’s certificate.

3. The ePDG sends the Authentication and Authorization Request message to the 3GPP AAA Server, containing the user identity and APN. The UE shall use the NAI as defined in accordance with clause 19.3 of 3GPP TS 23.003 [8], the 3GPP AAA server shall identify based on the realm part of the NAI that combined authentication and authorization is being performed for tunnel establishment with an ePDG which allows only EAP-AKA (and not an I-WLAN PDG as defined in TS 33.234 [9], which would allow also EAP-SIM). The different Diameter application IDs will help the 3GPP AAA Server distinguish among authentications for trusted access, as specified in clause 6 of the present document (which requires EAP-AKA' authentication), and authentications for tunnel setup in EPS (which allows only EAP-AKA).

4. The 3GPP AAA Server shall fetch the authentication vectors from HSS/HLR (if these parameters are not available in the 3GPP AAA Server). The 3GPP AAA Server shall lookup the IMSI of the authenticated user based on the received user identity (root NAI or pseudonym) and include the EAP-AKA as requested authentication method in the request sent to the HSS. The HSS shall then generate authentication vectors with AMF separation bit = 0 and send them back to the 3GPP AAA server.

5. The 3GPP AAA Server initiates the authentication challenge. The user identity is not requested again.

6. The ePDG shall respond with its identity, a certificate if the UE has requested with a CERTREQ payload in step 2, and send the AUTH parameter to protect the previous message it sent to the UE (in the IKE\_SA\_INIT exchange). The EAP message received from the 3GPP AAA Server (EAP-Request/AKA-Challenge) is included in order to start the EAP procedure over IKEv2.

7. The UE checks the authentication parameters and responds to the authentication challenge. The IKE\_AUTH request message includes the EAP message (EAP-Response/AKA-Challenge) containing UE’s response to the authentication challenge.

8. The ePDG forwards the EAP-Response/AKA-Challenge message to the 3GPP AAA Server.

8.a The AAA checks, if the authentication response is correct.

8.b-e If dynamic IP mobility selection is executed embedded to the authentication and authorization, the selected mobility mode is sent to the user in an AKA-Notification request, over Diameter A&A answer and IKE\_AUTH message. The UE responds to this over IKEv2 and the ePDG forwards the response to the 3GPP AAA Server.

8A. The 3GPP AAA Server shall initiate the Subscriber Profile Retrieval and 3GPP AAA Server registration to the HSS. The 3GPP AAA Server checks in user's subscription if he/she is authorized for non-3GPP access.

9. When all checks are successful, the 3GPP AAA Server sends the final Authentication and Authorization Answer (with a result code indicating success) including the relevant service authorization information, an EAP success and the key material to the ePDG. This key material shall consist of the MSK generated during the authentication process. When the SWm and SWd interfaces between ePDG and 3GPP AAA Server are implemented using Diameter, the MSK shall be encapsulated in the EAP-Master-Session-Key-AVP, as defined in RFC 4072 [10].

10. The MSK shall be used by the ePDG to generate the AUTH parameters in order to authenticate the IKE\_SA\_INIT phase messages, as specified for IKEv2 in RFC 5996 [30]. These two first messages had not been authenticated before as there was no key material available yet. According to RFC 5996 [30], the shared secret generated in an EAP exchange (the MSK), when used over IKEv2, shall be used to generated the AUTH parameters.

11. The EAP Success/Failure message is forwarded to the UE over IKEv2.

12. The UE shall take its own copy of the MSK as input to generate the AUTH parameter to authenticate the first IKE\_SA\_INIT message. The AUTH parameter is sent to the ePDG.

13. The ePDG checks the correctness of the AUTH received from the UE. At this point the UE is authenticated. In case S2b is used, PMIP signalling between ePDG and PDN GW can now start, as specified in TS 23.402 [5]. The ePDG continues with the next step in the procedure described here only after successful completion of the PMIP binding update procedure.

14. The ePDG calculates the AUTH parameter which authenticates the second IKE\_SA\_INIT message. The ePDG shall send the assigned Remote IP address in the configuration payload (CFG\_REPLY).

15 The AUTH parameter is sent to the UE together with the configuration payload, security associations and the rest of the IKEv2 parameters and the IKEv2 negotiation terminates.

\*\*\*\*\*\*\*\*\*\*\*\*\* End of 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*