**3GPP TSG-SA3 Meeting #107-e *S3-220685***

**e-meeting, 16-20 May 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **1357** | **rev** | **-** | **Current version:** | **15.15.0** |  |
|  | | | | | | | | |
| *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:*** | Clarifications to secondary authentication PDU Session Container | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Intel | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5GS\_Ph1-SEC | | | | |  | ***Date:*** | | | 2022-05-09 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | F |  | | | | | ***Release:*** | | | Rel-15 |
|  | *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:*** | | 1)  TS 23.502 clause 4.3.2.3 also clarifies that the SMF can use the DN-specific identity provided by the UE inside the EAP message in the PDU Session Authentication Complete message. In steps 9,10, It is erroneously assumed that EAP messages are encapsulated in the SM PDU DN Request container.  2) In TS 24.501, the SM PDU DN Request Container is only supported in the PDU session establishment request message specified in 24.501 clauses 8.3.1. Thus, the UE can only send a secondary authentication identity in step 4. The current text seems to imply that the SM PDU DN Request Container is forwarded on the N4 interface, which is incorrect. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | 1)In Step 9, the SM PDU DN Request container is replaced with a PDU Session Authentication message.  2) In step 10, the SM PDU DN Request container is replaced with PDU Session Authentication Complete message  3) In 11, 12, 13, References to the SM PDU DN Request container are removed.. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Secondary authentication method is erroenous and out of sync with other working groups. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 11.1.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\*\*\* BEGIN CHANGES \*\*\*

11 Security procedures between UE and external data networks via the 5G Network

11.1 EAP based secondary authentication by an external DN-AAA server

11.1.1 General

This sub-clause specifies support for optional to use secondary authentication between the UE and an external data network (DN).

The EAP framework specified in RFC 3748 [27] shall be used for authentication between the UE and a DN-AAA server in the external data network. The SMF shall perform the role of the EAP Authenticator. In the non-roaming scenario, the SMF shall perform the role of EAP Authenticator. And In the local break out scenario, the V-SMF of visited nework shall perform the role of EAP Authenticator. In the Home Routed deployment scenario, the H-SMF shall perform the role of the EAP Authenticator and the V-SMF shall transport the EAP messages exchanged between the UE and H-SMF. It shall rely on the external DN-AAA server to authenticate and authorize the UE's request for the establishment of PDU sessions.

Between the UE and the SMF, EAP messages shall be sent in the SM NAS message. This message is received at the AMF over N1 and delivered to the SMF over N11 using either the Nsmf\_PDUSession\_CreateSMContext service operation or the Nsmf\_PDUSession\_Update SM Context service operation, as specified in TS23.502 [8]. The SMF that takes the role of the EAP authenticator communicates with the external DN-AAA over N4 and N6 via the UPF.

The SMF invokes the Namf\_Communication\_N1N2MessageTransfer service operation to transfer the N1 NAS message containing the EAP message, towards the UE via the AMF.

Following clauses describe the procedures for initial Authentication and Re-Authentication with the external DN-AAA server.

11.1.2 Authentication

****

**Figure 11.1.2-1: Initial EAP Authentication with an external AAA server**

This procedure concerns both roaming and non-roaming scenarios. In the non-roaming case, the V-SMF is not involved. In the HR roaming case, the V-SMF shall proxy the signalling between the AMF in the VPLMN and the H-SMF in the HPLMN. In the LBO roaming case, only one SMF in VPLMN is involved.

The following procedure is based on sub-clauses 4.2.2.2.2, 4.3.2.2.1 and 4.3.2.3 in TS 23.502 [8].

NOTE 1: Steps 1-6 are borrowed from clause 4.2.2.2.2 and 4.3.2.2.1 TS 23.502 [8] and are for information only. Steps 7 to 15are related to authentication and are normative text.

1-3. The NG-UE registers with the network performing primary authentication with the AUSF/ARPF based on its network access credentials and establishes a NAS security context with the AMF.

4. The UE initiates establishment of a new PDU Session by sending a NAS message containing a PDU Session Establishment Request within the N1 SM container, slice information (identified by S-NSSAI) , PDU session ID and the PDN it would like to connect to (identified by DNN).

The PDU Session Establishment Request may contain SM PDU DN Request Container IE containing information for the PDU session authorization by the external DN.

5a. The AMF selects a V-SMF and sends either Nsmf\_PDUSession\_CreateSMContext Request or Nsmf\_PDUSession\_UpdateSMContext Request with the N1 SM container as one of its payload. It also forwards SUPI PDU Session ID, the received S-NSSAI, and the DNN.

5b. The V-SMF sends an Nsmf\_PDUSession\_CreateSMContext Responseor Nsmf\_PDUSession\_UpdateSMContext Response correspondingly to the AMF.

In case of a single SMF being involved in the PDU session setup, e.g. non-roaming or local breakout, that single SMF takes the role of both V-SMF and H-SMF. In this case, steps 6 and 17 are skipped.

6. The V-SMF sends an Nsmf\_PDUSession\_Create Request to the H-SMF.

7. The H-SMF obtains subscription data from the UDM for the given SUPI obtained from the AMF in step 5. The SMF checks the subscription data whether the secondary authentication is required and whether the UE request is allowed according to the user subscription and local policies. If not allowed, the H-SMF will reject UE's request via SM-NAS signalling and skip rest of the procedure. If secondary authentication is required, the SMF may also check whether the UE has been authenticated and/or authorized by the same DN, as indicated DNN in step 5, or the same AAA server in a previous PDU session establishment. The SMF may skip steps 8 to 15 if positive.

Note 2: The information on a successful authentication/authorization between a UE and an SMF may be saved in SMF and/or UDM.

8. The H-SMF shall trigger EAP Authentication to obtain authorization from an external DN-AAA server. If there is no existing N4 session, the H-SMF selects a UPF and establishes an N4 Session with it. The H-SMF notifies the DN-AAA server with the GPSI, if available, and the IP address(es) of the UE allocated to the PDU Session if the PDU session is of IP PDU type or the MAC address if the PDU session is of Ethernet PDU type.

9. The H-SMF may send an EAP Request/Identity message to the UE

10. The UE may send an EAP Response/Identity message contained within a NAS message. The DN-specific identity shall comply with Network Access Identifier (NAI) format.

To avoid the additional round-trip in steps 9 and 10, the secondary authentication DN-specific identity may be sent by the UE in step 4. In this case, H-SMF forms an EAP Response/Identity message that contains the identity.

11. If there is no existing N4 session, the H-SMF selects a UPF and establishes an N4 Session with it.

12. The DN specific identity, if provided by the UE, is forwarded to the UPF. The H-SMF identifies the DN AAA server based on the DN specific identity provided by the UE and on local configuration.

The UPF shall forward the DN specific identity within an EAP Response/Identity message to the DN AAA Server.

13. The DN AAA server and the UE shall exchange EAP messages, as required by the EAP method. In addition, it may send additional authorization information as defined in TS 23.501 clause 5.6.6.

14. After the successful completion of the authentication procedure, DN AAA server shall send EAP Success message to the H-SMF.

15. This completes the authentication procedure at the SMF. The SMF may save the DN-specific ID and DNN (or DN's AAA server ID if available) in a list for successful authentication/authorization between UE and an SMF. Alternatively, the SMF may update the list in UDM.

If the authorization is successful, PDU Session Establishment proceeds further starting at step 7a of Figure 4.3.2.2.1-1 in TS 23.502 [8].

16a-16b. The SMF initiates a N4 Session Modification procedure with the selected UPF as in steps 10a and 10b of Fig 4.3.2.2.1-1 in TS 23.502 [8].

17. The H-SMF sends an Nsmf\_PDUSession\_Create Response to the V-SMF. This message shall include EAP Success to be sent to the UE to V-SMF.

18. The V-SMF sends Namf\_Communication\_N1N2MessageTransfer to the AMF as in step 11 of Figure 4.3.2.2.1-1 in TS 23.502 [8]. This message shall include EAP Success to be sent to the UE within the NAS SM PDU Session Establishment Accept message.

19. The AMF forwards NAS SM PDU Session Establishment Accept message along with EAP Success to the UE as described in steps 12 and step 13 of Figure 4.3.2.2.1-1 in TS 23.502 [8].

The UE-requested PDU Session Establishment authentication/authorization by a DN-AAA server proceeds further as described in sub-clause 4.3.2.3 in TS 23.502 [8].

\*\*\* END CHANGES \*\*\*