**3GPP TSG-SA3 Meeting #110Ad-Hoc-e draft\_S3-231772-r1**

**Electronic meeting, Online, 17 - 21 April 2023**

|  |
| --- |
| *CR-Form-v12.1* |
| **DRAFT CHANGE REQUEST** |
|  |
|  | **3** | **CR** |  | **rev** | **-** | **Current version:** | **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:***  | Support for Prose Secondary Authentication  |
|  |  |
| ***Source to WG:*** | Interdigital, LG Electronics, Samsung, ChinaTelecom, Huawei, HiSilicon |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** |  PROSESA |  | ***Date:*** | 2022-04-06 |
|  |  |  |  |  |
| ***Category:*** | B |  | ***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-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | 1. At TSG-SA Meeting #96, SA Plenary decided to specify the Control Plane based security procedures in Rel-17 without the Prose Secondary Authentication support.
2. Also, SA Plenary agreed that SA2 and SA3 should work on ProSe Secondary Authentication in Rel-18 (SP-220716).

Add support for ProSe Secondary Authentication in the continued work as per decision point#2. |
|  |  |
| ***Summary of change:*** | Add ProSe Secondary Authentication related content sourced from TS 33.503 17.0.1.Add Secondary Authentication Procedure for Remote UE with N3IWF. |
|  |  |
| ***Consequences if not approved:*** | Incomplete CP security procedure to support secondary authentication |
|  |  |
| ***Clauses affected:*** | 6.3.3.3, 6.3.3.4, 7.3.2, 7.5 |
|  |  |
|  | **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:*** | SA3#108e: [S3-222262](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_108e/Docs/S3-222262.zip)SA3#110: [S3-231620](https://www.3gpp.org/ftp/TSG_SA/WG3_Security/TSGS3_108e/Docs/S3-222262.zip)SA3#110Ad-Hoc-e: S3-231775, S3-232104 |

\*\*\*\*\*\*\*\*\*\*\*\* START OF CHANGES

##### 6.3.3.3.x 5G ProSe Remote UE Secondary Authentication via a 5G ProSe Layer-3 UE-to-Network Relay without N3IWF

6.3.3.3.x.1 General

This clause specifies the 5G Prose Remote UE specific secondary authentication between a 5G ProSe Remote UE, which is different from the secondary authentication defined in TS 33.501 [3], via a 5G ProSe Layer-3 UE-to-Network Relay without N3IWF and an external Data Network (DN) based on network-controlled authorization (i.e. using 5G ProSe Remote UE specific authentication) as described in clause 6.3.3.3.2. This procedure is optional to support.

The SMF of the 5G ProSe UE-to-Network Relay triggers the secondary authentication of the 5G ProSe Remote UE based on the subscription information and the local configuration of the SMF when it receives a NAS message (e.g. Remote UE Report) from the 5G ProSe UE-to-Network Relay.

The EAP framework specified in IETF RFC 3748 [12] shall be used for authentication between the 5G ProSe Remote UE and a DN-AAA server in the external data network.

Following clause describes the procedures for initial secondary authentication of the 5G ProSe Remote UE with the external DN-AAA server.

6.3.3.3.x.2 PDU Session secondary authentication of 5G ProSe Remote UE via 5G ProSe Layer-3 UE-to-Network Relay

The PDU session secondary authentication of 5G ProSe Remote UE via 5G ProSe Layer-3 UE-to-Network Relay follows the steps described in figure 6.3.3.3.x.2-1.



Figure 6.3.3.3.x.2-1: Procedure for PDU session secondary authentication of 5G ProSe Remote UE
via 5G ProSe Layer-3 UE-to-Network Relay

1. The 5G ProSe Remote UE 5G ProSe CP based PC5 security establishment with 5G ProSe UE-to-Network Relay as described in 6.3.3.3.2. In addition, the following procedure may happen in this step as described in clause 6.5.1.1 in TS 23.304 [2].

 If there is no PDU session satisfying the requirements of the PC5 connection with the 5G ProSe Remote UE, e.g. S-NSSAI, DNN, QoS, UP security activation status, the 5G ProSe Layer-3 UE-to-Network Relay initiates a new PDU session establishment or modification procedure for relaying.

Upon successful security establishment, the 5G ProSe Layer-3 UE-to-Network Relay stores the 5GPRUK ID as described in clause 6.3.3.3.2 and sends a DCA (Direct Communication Accept) message to the Remote UE. The DCA may include an indication that a PDU Session with secondary authentication is pending if the L3 UE-to-Network Relay determines the DN that is associated with the relay service code requires secondary authentication for the 5G ProSe Remote UE based on the fact that the L3 UE-to-Network Relay performed secondary authentication with the same DN either in step 1 or step 4, and there is no stored authentication information associated with the Remote UE. Based on the indication in the DCA message, the 5G ProSe Remote UE may refrain from sending any data traffic over the PC5 link until successful completion of subsequent PDU Session secondary authentication.

2. For IP PDU Session Type and IP traffic over the PC5 reference point, the IPv6 prefix or IPv4 address is allocated for the 5G ProSe Remote UE as defined in clause 5.5.1.3 in TS 23.304 [2]. In addition, the 5G ProSe Layer-3 UE-to-Network Relay may configure a traffic filter (e.g. as a default filter for IP or non-IP traffic) for the PC5 link to prevent any data traffic until successful completion of subsequent PDU Session secondary authentication.

3. The 5G ProSe Layer-3 UE-to-Network Relay sends a Remote UE Report message to the SMF for the PDU session associated with the 5G ProSe Layer-3 UE-to-Network Relay, as described in clause 6.3.3.3.2, step 18.

Editor's Notes: How to support multiple Remote User IDs in Remote UE Report is FFS.

NOTE 1: In the case of Home Routed roaming, the SMF in the call flow is the H-SMF (and the V-SMF is not shown for simplicity). SMF selection by AMF is performed as per TS 23.502 [13], clause 4.3.2.2.3 (e.g. using PLMN ID of the SUPI, S-NSSAI, etc.).

4. The SMF resolves the 5G ProSe Remote UE's SUPI of the 5G ProSe Remote UE using the Remote User ID, as described in clause 6.3.3.3.2, step 19.

5. The SMF retrieves Remote UE's SM subscription data from the UDM by triggering Nudm\_SDM\_Get service operation. The SMF may include DNN, S-NSSAI of the PDU Session for relaying in addition to the Remote UE's SUPI as input parameters. The SMF determines based on the subscription data of the 5G ProSe Remote UE (i.e. Secondary authentication indication as per TS 23.502 [13], Table 5.2.3.3.1). The SMF may also check whether the 5G ProSe Remote UE has been authenticated by the same DN as indicated in the subscription data and, if secondary authentication is required, the SMF triggers a PDU Session secondary authentication of 5G ProSe Remote UE via 5G ProSe Layer-3 UE-to-Network Relay by sending PDU Session Authentication Command message to the 5G ProSe Layer-3 UE-to-Network Relay including the 5GPRUK ID of the Remote UE and an EAP-Request/Identity.

Editor's Notes: how SMF is notified with the 5G ProSe remote UE's subscription update is FFS.

Note 2: The information on a successful authentication between a 5G ProSe Remote UE and an SMF may be saved in SMF and/or UDM.

6. Based on the 5GPRUK ID, the 5G ProSe Layer-3 UE-to-Network Relay forwards the EAP-Request/Identity to the 5G ProSe Remote UE via PC5 signalling(6a). The 5G ProSe Remote UE returns the EAP-Response/Identity to the 5G ProSe Layer-3 UE-to-Network Relay via PC5 signalling(6b).

7. The 5G ProSe Layer-3 UE-to-Network Relay sends PDU Session Authentication Complete message to the SMF including the 5GPRUK ID of the Remote UE and an EAP-Response/Identity received from the 5G ProSe Remote UE.

8. The SMF sends an EAP-Response/Identity to the DN-AAA.

9. The DN AAA server and the 5G ProSe Remote UE should exchange EAP messages, as required by the EAP method. The SMF and 5G ProSe Layer-3 UE-to-Network Relay shall include the 5GPRUK ID in the NAS messages transporting the EAP messages.

10. The DN-AAA sends EAP-Success or EAP-Failure to the SMF.

11. Upon successful PDU Session secondary authentication via the Relay procedure, the SMF stores the 5G ProSe Remote UE information in the 5G ProSe Layer-3 UE-to-Network Relay's SM context including 5G ProSe Remote UE identity (e.g. GPSI, SUPI), individual authentication information received from DN‑AAA.

12. The SMF sends Remote UE Report Ack message to the 5G ProSe Layer-3 UE-to-Network Relay indicating the result of the PDU Session secondary authentication, including the 5GPRUK ID of the remote UE and an EAP success or failure message. In the case of successful secondary authentication, the message may include QoS authorization info for the 5G ProSe Layer-3 UE-to-Network Relay to enforce. In case the secondary authentication is failed, the NAS message may indicate that 5G ProSe Layer-3 UE-to-Network Relay should release the PC5 link with the 5G ProSe Remote UE.

13. In the case of successful secondary authentication for the 5G ProSe Remote UE, the 5G ProSe Layer-3 UE-to-Network Relay stores any received authentication info associated with the 5G ProSe Remote UE. In case the secondary authentication is failed, the 5G ProSe UE-to-Network Relay releases the PC5 link with the 5G ProSe Remote UE and may keep the PDU session as the default PDU session or release it if there is no more 5G ProSe Remote UE using the same PDU session.

6.3.3.3.x.3 Re-Authentication of Remote UE via L3 UE-to-Network Relay without N3IWF

The Re-Authentication of Remote UE via L3 UE-to-Network Relay follows the steps described in Figure 6.3.3.3.x.3-1. The call flow is based on the call flow in TS 33.501 [3], Figure 11.1.3-1 with the main difference that the EAP messages for Re-authentication are exchanged between the Remote UE and DN-AAA using PC5 transport provided via the PC5 link with the UE-to-Network Relay.



Figure 6.3.3.3.x.3-1: EAP Re-Authentication of Remote UE via L3 UE-to-Network Relay
with an external AAA server

1-2. Secondary Authentication for the 5G ProSe Remote UE via the 5G ProSe Layer-3 UE-to-Network Relay has been established according to the procedures specified in clause 6.3.3.3.x, PDU Session secondary authentication of the 5G ProSe Remote UE via the 5G ProSe Layer-3 UE-to-Network Relay.

 Secondary Re-authentication may either be initiated by the SMF of the 5G ProSe Layer-3 UE-to-Network Relay or the external DN-AAA server. If Re-authentication is initiated by the SMF of the 5G ProSe Layer-3 UE-to-Network Relay, the procedure proceeds with step 3 (skipping steps 3a and 3b). If Re‑authentication is initiated by the external DN/AAA server, the procedure proceeds with the alternative steps 3a and 3b.

3. The SMF of the 5G ProSe Layer-3 UE-to-Network Relay decides to initiate Secondary Re-Authentication for the 5G ProSe Remote UE.

3a. The DN AAA server decides to initiate Secondary Re-Authentication for the 5G ProSe Remote UE.

3b. The DN AAA shall send a Secondary Re-Authentication request to the UPF of the 5G ProSe Layer-3 UE-to-Network Relay, and the UPF of the 5G ProSe Layer-3 UE-to-Network Relay forwards it to the SMF of the 5G ProSe Layer-3 UE-to-Network Relay. The Secondary Re-authentication request contains the GPSI, and the IP/MAC address of the UE allocated to the PDU Session and the MAC address if the PDU session is of Ethernet PDU type for the 5G ProSe Remote UE. The SMF of the 5G ProSe Layer-3 UE-to-Network Relay retrieves the corresponding 5GPRUK ID of the 5G ProSe Remote UE from the 5G ProSe Layer-3 UE-to-Network Relay's SM context using the GPSI. The GPSI of the 5G ProSe Remote UE is obtained by SMF from UDM using Nudm\_SDM\_Get service operation during the PDU Session secondary authentication procedure (see clause 6.3.3.3.x.2, step 9).

4. The SMF of the 5G ProSe Layer-3 UE-to-Network Relay may send an EAP Request/Identity message to the 5G ProSe Layer-3 UE-to-Network Relay including 5GPRUK ID of the 5G ProSe Remote UE. In case the procedure is initiated by the DN AAA, the SMF retrieves the 5GPRUK ID of the 5G ProSe Remote UE that is mapped with the received GPSI.

5. The 5G ProSe Layer-3 UE-to-Network Relay forwards the EAP message to the 5G ProSe Remote UE via PC5 signalling.

6. The 5G ProSe Remote UE may respond with an EAP Response/Identity message to the 5G ProSe Layer-3 UE‑to‑Network Relay via PC5 signalling.

7. The 5G ProSe Layer-3 UE-to-Network Relay forwards the EAP Response/Identity to SMF of the 5G ProSe Layer-3 UE-to-Network Relay.

8. The SMF of the 5G ProSe Layer-3 UE-to-Network Relay forwards the EAP Response/Identity to the UPF of the 5G ProSe Layer-3 UE-to-Network Relay, selected during initial authentication, over N4 interface. Then, the UPF of the 5G ProSe Layer-3 UE-to-Network Relay shall forward the EAP Response/Identity message to the DN AAA Server. This establishes an end-to-end connection between the SMF of the 5G ProSe Layer-3 UE-to-Network Relay and the external DN-AAA server for EAP exchange.

9. The DN AAA server and the 5G ProSe Remote UE shall exchange EAP messages as required by the EAP method.

10. After the completion of the authentication procedure, DN AAA server either sends EAP Success or EAP Failure message to the SMF of the 5G ProSe Layer-3 UE-to-Network Relay. This completes the Re-authentication procedure at the SMF of the 5G ProSe Layer-3 UE-to-Network Relay.

11. If the authentication is successful, EAP-Success and 5GPRUK ID of the 5G ProSe Remote UE shall be sent to the 5G ProSe Layer-3 UE‑to-Network Relay.

12. The 5G ProSe Layer-3 UE-to-Network Relay shall forward the EAP-Success to the corresponding 5G ProSe Remote UE via PC5 signalling.

13. If authentication is not successful, EAP-Failure and 5GPRUK ID of the 5G ProSe Remote UE shall be sent to the 5G ProSe Layer-3 UE‑to-Network Relay.

14. The 5G ProSe Layer-3 UE-to-Network Relay shall forward EAP-Failure to the corresponding 5G ProSe Remote UE via PC5 signalling and shall release the PC5 link with the 5G ProSe Remote UE.

15. The 5G ProSe Layer-3 UE-to-Network Relay shall send a Remote UE Report message indicating the 5G ProSe Remote UE is disconnected to the SMF of the 5G ProSe Layer-3 UE-to-Network Relay.

16. The SMF may release the PDU session that was used for the relay service.

Editor's Notes: It is FFS whether this procedure is needed, depending on the outcome of secondary Authentication and authorization procedure.

6.3.3.3.x.4 Secondary Authentication Revocation of Remote UE via L3 UE-to-Network Relay without N3IWF

At any time, a DN-AAA may revoke the authentication and authorization for a PDU Session associated with 5G ProSe UE-to-Network Relay service and according to the request from the DN-AAA server, the SMF may request the 5G ProSe Layer-3 UE-to-Network Relay to release the PC5 link with the revoked 5G ProSe Remote UE, or release the PDU Session of the 5G ProSe Layer-3 UE-to-Network Relay as specified in clause 4.3.4 of TS 23.502 [10] when it is not used by other 5G ProSe Remote UE(s).

\*\*\*\*\*\*\*\*\*\*\*\* NEXT CHANGES

##### 6.3.3.4.x Secondary Authentication Procedure for Remote UE with N3IWF

A 5G ProSe Remote UE connects to the N3IWF via a 5G ProSe UE-to-Network Relay is specified in 6.5.1.2.1 in TS 23.304 [2]. The secondary authentication for the 5G ProSe Remote UE may happen in step 6 of 6.5.1.2.1 in TS 23.304 [2] during the procedure when PDU session associated with 5G ProSe UE-to-Network Relay service is established or modified. In this case, the secondary authentication may be triggered by the SMF of the 5G ProSe Remote UE, as defined in clause 11 of TS 33.501[3] can be reused.

\*\*\*\*\*\*\*\*\*\*\*\* NEXT CHANGES

\*\*\*\*\*\*\*\*\*\*\*\* NEXT CHANGES

###

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