**3GPP TSG-SA3 Meeting #99e *S3-201410***

**e-meeting, 11-15 May 2020**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | **DRAFT** | **rev** | **-** | **Current version:** | **16.2.0** |  |
|  |
| *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:***  | Correction of SUPI in IKE\_AUTH exchange |
|  |  |
| ***Source to WG:*** | Huawei |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | 5WWC |  | ***Date:*** | 28.04.2020 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-16 |
|  | *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-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)* |
|  |  |
| ***Reason for change:*** | Alignment with S2-2003134: the TNGF never receives the SUPI and will not be able to identify the UE, if the UE includes SUPI in the IKE\_AUTH exchange. |
|  |  |
| ***Summary of change:*** | The registration via trusted non-3GPP access is corrected, so that the UE includes the 5G-GUTI or SUCI in the IKE\_AUTH exchange corresponding to the UE identity provided in the AN parameters first. |
|  |  |
| ***Consequences if not approved:*** | 5G registration procedure via trusted non-3GPP access fails if the UE sends the SUPI in the IKE\_AUTH exchange or in case the UE provides a different identity in the AN parameters and the IKE\_AUTH exchange. |
|  |  |
| ***Clauses affected:*** | 7A.2.1, 7B.3, 9.10 |
|  |  |
|  | **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 change \*\*\*\*\*\*\*

### 7A.2.1 Authentication for trusted non-3GPP access

This clause specifies how a UE is authenticated to 5G network via a trusted non-3GPP access network.

This is based on the specified procedure in TS 23.502 [8] clause 4.12a.2.2 "Registration procedure for trusted non-3GPP access". The authentication procedure is similar to the authentication procedure for trusted non-3GPP access defined in clause 7.2.1 with few differences, which are mentioned below:



Figure 7A.2.1-1: Registration \ Authentication and PDU Session establishment for trusted non-3GPP access

0. The UE selects a PLMN and a TNAN for connecting to this PLMN by using the Trusted Non-3GPP Access Network selection procedure specified in TS 23.501 [2] clause 6.3.12. During this procedure, the UE discovers the PLMNs with which the TNAN supports trusted connectivity (e.g. "5G connectivity").

1. A layer-2 connection is established between the UE and the TNAP. In case of IEEE 802.11 [80], this step corresponds to an 802.11 [80] Association. In case of PPP, this step corresponds to a PPP LCP negotiation. In other types of non-3GPP access (e.g. Ethernet), this step may not be required.

2-3. An EAP authentication procedure is initiated. EAP messages shall be encapsulated into layer-2 packets, e.g. into IEEE 802.3/802.1x packets, into IEEE 802.11/802.1x packets, into PPP packets, etc. The UE provides a NAI that triggers the TNAP to send an AAA request to a TNGF. Between the TNAP and TNGF the EAP packets are encapsulated into AAA messages.

4-10. An EAP-5G procedure is executed as specified in clause 7.2.1with the following modifications:

- The EAP-5G packets shall not be encapsulated into IKEv2 packets. The UE shall also include a UE Id in the AN parameters, e.g. a 5G-GUTI if available from a prior registration to the same PLMN.

- A KTNGF as specified in clause Annex A.9 (equivalentto KN3IWF) is created in the UE and in the AMF after the successful authentication. The KTNGF is transferred from the AMF to TNGF in step 10a (within the N2 Initial Context Setup Request).

- The TNAP is a trusted entity. The TNGF shall generate the KTNAP as specified in Annex A.22 and transfers it from TNGF to TNAP in step 10b (within an AAA message).

- After receiving the TNGF key from AMF in step 10a, the TNGF shall send to UE an EAP-Request/5G-Notification packet containing the "TNGF Contact Info", which includes the IP address of TNGF. After receiving an EAP-Response/5G-Notification packet from the UE, the TNGF shall send message 10b containing the EAP-Success packet.

11. The common TNAP key is used by the UE and TNAP to derive security keys according to the applied non-3GPP technology and to establish a security association to protect all subsequent traffic. In case of IEEE 802.11 [80], the KTNAP is the Pairwise Master Key (PMK) and a 4-way handshake is executed (see IEEE 802.11 [80]) which establishes a security context between the WLAN AP and the UE that is used to protect unicast and multicast traffic over the air. All messages between UE and TNAP are encrypted and integrity protected from this step onwards.

NOTE 1: whether step 11 is performed out of the scope of this document. The current procedure assumes the encryption protection over Layer-2 between UE and TNAP is to be enabled.

12. The UE receives IP configuration from the TNAN, e.g. with DHCP.

13. The UE shall initiate an IKE\_INIT exchange with the TNGF. The UE has received the IP address of TNGF during the EAP-5G signalling in step 9b, subsequently, the UE shall initiate an IKE\_AUTH exchange andshall include the same UE Id (i.e. SUCI or 5G-GUTI) as in the UE Id provided in step 5. The common KTIPSe is used for mutual authentication. The key KTIPSec is derived as specified in Annex A.22.NULL encryption is negotiated as specified in RFC 2410 [81]. After step 13c, an IPsec SA is established between the UE and TNGF (i.e. a NWt connection) and it is used to transfer all subsequent NAS messages. This IPsec SA does not apply encryption but only apply integrity protection.

14. After the NWtp connection is successfully established, the TNGF responds to AMF with an N2 Initial Context Setup Response message.

15. Finally, the NAS Registration Accept message is sent by the AMF and is forwarded to UE via the established NWt connection.

16-18. The UE initiates a PDU session establishment. This is carried out exactly as specified in TS 23.502 [8] clause 4.12a.5. The TNGF may establish one or more IPSec child SA’s per PDU session.

19. User plane data for the established PDU session is transported between the UE and TNGF inside the established IPSec child SA.

\*\*\*\*\*\*\* End of change \*\*\*\*\*\*\*

\*\*\*\*\*\*\* change 2\*\*\*\*\*\*\*

## 7B.3 Authentication for FN-RG

The FN-RG connects to 5GC via W-5GAN, which has the W-AGF function that provides connectivity to the 5GC via N2 and N3 reference points. Since the FN-RG is a non-wireless entity defined by BBF or CableLabs, it doesn’t support N1. The W-AGF provides N1 connectivity on behalf of the FN-RG. The authentication method is executed between the FN-RG and AUSF as shown in Figure 7B.c.

The W-AGF may authenticate the FN-RG; this is controlled by local policies.

It is assumed that there is a trust relationship between the wireline operator that manages the W-5GAN and the PLMN operator managing the 5GC. The AMF trusts the W-5GAN based on mutual authentication executed when security is established on the interface between the two using NDS/IP or DTLS.



Figure7B.c FN-RG authentication procedure

1. A layer-2 (L2) connection is established between the FN-RG and the FAGF function in the W-AGF.

2. The FN-RG is authenticated by the W-AGF. Authentication method used for FN-RG is defined by BBF or CableLabs and out of scope of 3GPP.

3-4. The W-AGF shall perform initial registration on behalf of the FN-RG. The W-AGF shall generate a Registration Request message and send it to the AMF over N2. The Registration Request message contains the SUCI of the FN-RG. The N2 message contains an indication that the W-AGF has authenticated the FN-RG.

5. The AMF shall select an AUSF based on the received SUCI. The AMF shall send a Nausf\_UEAuthentication\_Authenticate Request message to the AUSF. It contains the SUCI of the FN-RG. It also contains the authenticated indication generated by the W-AGF.

6. The AUSF shall send a Nudm\_UEAuthentication\_Get Request to the UDM. It contains the SUCI of the FN-RG and the authenticated indication.

7. The UDM shall invoke the SIDF and maps the SUCI to the SUPI.

8. The UDM decides, based on the subscription profile of the SUPI and the authenticated indication that authentication has been completed by the W-5GAN, that authentication by the home network is not required for the FN-RG.

9. The UDM shall send a Nudm\_UEAuthentication\_Get Response to the AUSF. It contains the SUPI of the FN-RG and an indication that authentication by the home network is not required.

10. After checking the indication set by the UDM, The AUSF shall not perform authentication and shall send a Nausf\_UEAuthentication\_Authenticate Response to the AMF. It contains the SUPI of the FN-RG and the indication that authentication by the home network is not required set by the UDM.

This response from AUSF indicates that authentication is not required, and no KSEAF is included.

11. After checking the indication to make sure that the authentication by the home network is not required, the AMF shall estabilish the NAS security between AMF and W-AGF with NULL encryption and NULL integrity protection.

12. The AMF shall send Registration Accept message to the W-AGF. This message contains 5G-GUTI and other parameters.

13. The W-AGF shall send a Registration Complete message back to the AMF. The W-AGF shall store the 5G-GUTI for use in later NAS procedures.

\*\*\*\*\*\*\*End of change 2\*\*\*\*\*\*\*

\*\*\*\*\*\*\* change 3\*\*\*\*\*\*\*

## 9.10 Security mechanisms for the interface between W-5GAN and 5GC

The W-AGF function in Wireline 5G Access network (W-5GAN) terminates the following interfaces:

- N2 interface between the W-5GAN and the AMF

- N3 interface between the W-5GAN and the UPF

The security of the N2 interface between the W-5GAN and the AMF is as defined in clause 9.2 of the present document.

The security of the N3 interface between the W-5GAN and the UPF is as defined in clause 9.3 of the present document.

NOTE: Clauses 9.2 and 9.3 require that the N2 and N3 interfaces are integrity, confidentiality, and replay protected. The same protection can be achieved by placing the AGF in the same trust domain as the AMF and the SMF.

\*\*\*\*\*\*\* End of change 3\*\*\*\*\*\*\*