**3GPP TSG-SA3 Meeting #101e *S3-203171***

**e-meeting, 9 – 20 November 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** |  | **rev** |  | **Current version:** | **16.4.0** |  |
|  | | | | | | | | |
| *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 |  | Radio Access Network |  | Core Network | **x** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Authentication method selection for N5CW | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | 5WWC | | | | |  | ***Date:*** | | | 2020-10-30 |
|  |  | | | |  | |  | | |  |
| ***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 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-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | Lack of 5G NAS support over WLAN, the authentication of N5CW over WLAN is based on EAP-AKA', i.e. 5G AKA cannot be used over WLAN.  In case the N5GC device sends a SUCI when performing registration to 5GC over WLAN, the realm part of the SUCI contains '5gc-nn'. This information can be enough for the UDM to determine that EAP based method shall be selected for the authentication request.  However, in case the N5GC devices sends a 5G-GUTI, the AMF could use the SUPI stored locally and send it in the authentication request. Note the SUPI may not contain '5gc-nn' in realm e.g. in case it was an IMSI that was retrieved in the previous authentication procedure over 3GPP access.  Therefore, the UDM is lack of enough information to select EAP-AKA' in this case. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | In case the AMF triggers an authentication procedure using SUPI for a N5CW device e.g. when a valid 5G-GUTI is received in the registration request, the AMF populates an indication in the authentication request that the request is from a N5CW device.  Editorial fixes of Figure 7A.2.4-1. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Authentication procedures for N5CW will fail, in case 5G-GUTI is used in registration request. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 7A.2.4 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  |  | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  |  | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  |  | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | |  | | | | | | | | |

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

### 7A.2.4 Authentication for devices that do not support 5GC NAS over WLAN access

A N5CW device is capable to register to 5GC with 3GPP credentials and to establish 5GC connectivity via a trusted WLAN access network. The reference architecture is captured in clause 4.2.8.5.2 of TS 23.501[2]. The 3GPP credentials are stored as defined in clause 6.1.1.1. The Trusted WLAN Interworking Function (TWIF) provides interworking functionality that enables connectivity with 5GC and implements the NAS protocol stack and exchanges NAS messages with the AMF on behalf of the N5CW device. A single EAP-AKA’ authentication procedure is executed for connecting the N5CW device both to the trusted WLAN access network and to the 5G core network.

Figure 7A.2.4-1: Authentication Procedure for N5CW

0. The N5CW device selects a PLMN and a trusted WLAN that supports "5G connectivity-without-NAS" to this PLMN by using the procedure specified in TS 23.501 [2] clause 6.3.12a, "Access Network selection for devices that do not support 5GC NAS over WLAN".

Steps 1-10: Initial registration to 5GC.

1. The N5CW device associates with the trusted WLAN network and the EAP-AKA’ authentication procedure is initiated.

2. The N5CW device shall provide its Network Access Identity (NAI) The Trusted WLAN Access Point (TWAP) selects a Trusted WLAN Interworking Function (TWIF), e.g. based on the received realm, and sends an AAA request to the selected TWIF.

If the N5CW device registers to 5GC over 3GPP access for the first time when the above procedure is initiated, then the NAI shall include the SUCI. The SUCI shall be constructed as specified in clause 6.12.2.

If the N5CW device has registered to 5GC over 3GPP access when the above procedure is initiated, then the NAI includes the 5G-GUTI assigned to the N5CW device over 3GPP access. This enables the TWIF in step 4a below to select the same AMF as the one serving the N5CW device over 3GPP access.

3. The TWIF shall create a 5GC Registration Request message on behalf of the N5CW device. The TWIF shall use default values to populate the parameters in the Registration Request message, which are the same for all N5CW device that do not support 5G NAS. The Registration type indicates "Initial Registration".

4. The TWIF shall select an AMF (e.g. by using the 5G-GUTI in the NAI, if provided by the N5CW device) and shall send an N2 message to the AMF including the Registration Request, the User Location, an AN Type and an Authentication Method. The Authentication Method indicates EAP-AKA'.

5. In case the AMF triggers an authentication procedure, it sends a request to AUSF by sending Nausf\_UEAuthentication\_Authenticate Request message. The Nausf\_UEAuthentication\_Authenticate Request message contains SUCI or SUPI (in case of a valid 5G-GUTI is received by the AMF) and the Authentication Method. The request message contains also an indication that the request is from a N5CW device.

6. The AUSF shall send Nudm\_UEAuthentication\_Get Request to the UDM including SUCI or SUPI and the N5CW indication and the Authentication Method.

7. Upon reception of the Nudm\_UEAuthentication\_Get Request, the UDM shall invoke SIDF if a SUCI is received. SIDF shall de-conceal SUCI to gain SUPI before UDM can process the request.

8. The EAP-AKA’ procedure will be trigged to perform mutual authentication between the N5CW device and the home network as specified in clause 6.1.3.1.

EAP-AKA' takes place between the N5CW device and AUSF. Over the N2 interface, the EAP messages are encapsulated within NAS Authentication messages. The EAP-AKA’ messages exchanged between the N5CW Device and the TWIF shall be encapsulated into the layer-2 packets, e.g. into IEEE 802.3/802.1x packets, into IEEE 802.11/802.1x packets, into PPP packets, etc.

9. The NAS security context is not be required in this scenario. The AMF shall derive an KTWIF key from the received KAMF key as specified in Annex A.9. NAS security between AMF and TWIF is established similar to unauthenticated emergency calls, i.e. with NULL encryption and NULL integrity protection.

10a. The AMF shall send NAS Security Mode Command to the TWIF. The NAS Security Mode Command shall contain the EAP-Success message and the NULL security algorithms.

10b. The TWIF shall not forward the EAP-Success to the N5CW directly, instead, it shall store the EAP-Success message and wait for KTWIF.

10c. The TWIF shall send the NAS Security Mode Complete message to the AMF.

11. The AMF sends an N2 Initial Context Setup Request and provides the KTWIF key to TWIF.

12. The TWIF shall derive a TNAP key, KTNAP, from the KTWIF key as specified in Appendix A.X and send the TNAP key and the EAP-Success message to the Trusted WLAN Access Point, which forwards the EAP-Success to the N5CW device. The TNAP key corresponds to the PMK (Pairwise Master Key) which is used to secure the WLAN air-interface communication according to IEEE 802.11 [80]. A layer-2 or layer-3 connection is established between the Trusted WLAN Access Point and the TWIF for transporting all user-plane traffic of the N5CW device to TWIF. This connection is later bound to an N3 connection that is created for this N5CW device.

13. The TWIF shall send N2 Initial Context Setup Response message to the AMF.

14. The following steps are captured in clause 4.12b.2 of TS 23.502[8].

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