**3GPP TSG-SA3 Meeting #108-e *S3-221918***

**e-meeting, 22 - 26 August 2022**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** | **1443** | **rev** |  | **Current version:** |  |  |
|  |
| *For* [***HELP***](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:***  |  Alignment of NAS transport protocol for 5G-RG over Wireline |
|  |  |
| ***Source to WG:*** | Ericsson |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | 5WWC |  | ***Date:*** | 2022-08-15 |
|  |  |  |  |  |
| ***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-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | A Rel-16 CR (CR 2066, based on S2-2204943) with Rel-17 mirror (CR 2063, based on S2-2204944) has been agreed in SA2 for 23.316 aligning the procedures for 5G-RG with the BBF protocols. |
|  |  |
| ***Summary of change:*** | Replace the use of EAP-5G with the generic protocol W-CP for NAS transport. |
|  |  |
| ***Consequences if not approved:*** | Misalignment with other specifications  |
|  |  |
| ***Clauses affected:*** | 7B.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:*** |  |

\*\*\*\*\* First change \*\*\*\*\*

## 7B.2 Authentication for 5G-RG

The 5G-RG can be connected to 5GC via W-5GAN, NG RAN or via both accesses. The registration procedure for the 5G-RG connecting to 5GC via NG-RAN is specified in TS 23.316 [79] clause 4.11. The registration procedure for the 5G-RG connecting to 5GC via W-5GAN is specified in TS 23.316 [79] clause 7.2.1.

The Untrusted non-3GPP access procedure defined in clause 7.2.1 is used as the basis for registration of the 5G-RG. The 5G-RG shall support both 5G-AKA and EAP-AKA’ and it shall be authenticated by the 3GPP home network. The 5G-RG is equivalent to a normal UE.

As 5G-RG is a UE from 5GC point of view, the authentication framework defined in clause 6.1.3 shall be used to authenticate the 5G-RG.

In case of 5G-RG connects to 5GC via 5G-RAN, comparing to clause 6.1, the difference is:

- UE is replaced by 5G-RG.

In case of 5G-RG connects to 5GC via W-5GAN, the W-CP protocol stack shall be used between the 5G-RG and the W-5GANfor encapsulating NAS message. The authentication method is executed between the 5G-RG and AUSF as shown below.



Figure 7B.2-1 5G-RG authentication procedure

1. 5G-RG establishes a W-CP connection with a W-5GAN. The detail of connection is out of the scope of 3GPP.

2. (void)

3. The 5G-RG shall send a message using W-CP protocol stack that contains a Registration message containing UE security capabilities and the SUCI. If there is an available security context, the 5G-RG shall integrity protect the Registration Request message and shall send the 5G-GUTI instead of SUCI. If the 5G-RG has registered to the same AMF through NG RAN, and if this is the first time that the 5G-RG connects to the 5GC throughW-5GAN, the value of corresponding UL NAS COUNT used for integrity protection is 0; else it can use the existing non-3GPP specific UL NAS COUNT for integrity protection.

NOTE: Since the 5G-RG will not use non-3GPP access, and to avoid to create new category of security context, so the non-3GPP specific security context is used to refer to the security context that 5G-RG is used through wireline access.

4. The W-AGF shall select an AMF as specified in TS 23.316[79]. The W-AGF shall then forward the Registration Request received from the UE to the selected AMF within an N2 initial UE message

5. If the AMF receives a 5G-GUTI and the Registration is integrity protected, it may use the security context to verify the integrity protection as describe in clause 6.4.6. If the 5G-RG has registered to the same AMF through NG RAN, and if this is the first time that the AMF receives UE’s NAS signalling through wireline access, the value of corresponding UL NAS COUNT used for integrity verification is 0; else it can use the existing non-3GPP specific UL NAS COUNT for integrity verification. If integrity is verified successfully, it indicates that 5G-RG is authenticated by AMF. If integrity is verified successfully and no newer security context has been activated over the NG RAN, then step 8 to step 11 may be skipped. If integrity is verified successfully and a newer security context has been activated over the NG RAN then authentication may be skipped but the AMF shall activate the newer context with a NAS SMC procedure as described in step 8 and onwards. Otherwise, the AMF shall authenticate the 5G-RG.

If the AMF decides to authenticate the 5G-RG, it shall use one of the methods from clause 6.1.3. In this case, the AMF shall send a key request to the AUSF. The AUSF may initiate an authentication procedure as specified in clause 6.1.3. Between AMF and UE (5G-RG), the authentication packets are encapsulated within NAS authentication messages and the NAS authentication messages are carried in N2 signalling between the AMF and W-AGF, and then are encapsulated using W-CP protocol stack message between the W-AGF and the UE (5G-RG).

In the final authentication message from the home network, the AUSF shall send the anchor key KSEAF derived from KAUSF to the SEAF. The SEAF shall derive the KAMF from KSEAF and send it to the AMF which is used by the AMF to derive NAS security keys. If EAP-AKA' is used for authentication as described in clause 6.1.3.1, then the AUSF shall include the EAP-Success. The 5G-RG also derives the anchor key KSEAF and from that key it derives the KAMF followed by NAS security keys. The NAS COUNTs associated with NAS connection identifier "0x02" are set at the 5G-RG and AMF.

6. The AMF shall send a Security Mode Command (SMC) to the UE (5G-RG) in order to activate NAS security associated with NAS connection identifier "0x02". This message is first sent to W-AGF (within an N2 message). If EAP-AKA' is used for authentication, the AMF shall encapsulate the EAP-Success received from AUSF within the SMC message.

7. The W-AGF shall forward the NAS SMC to 5G-RG .

8. The W-AGF shall forward the NAS packet containing NAS SMC Complete to the AMF over the N2 interface.

9. The AMF upon reception of the NAS SMC Complete from the UE (5G-RG) or upon success of integrity protection verification, initiates the NGAP procedure to set up the AN context. AMF shall compute the W-AGF key, KWAGF that is an equivalent to key KN3IWF, using the uplink NAS COUNT associated with NAS connection identifier "0x02" as defined in Annex A.9.

10. Upon receiving NAS Security Mode Complete, the AMF shall send an N2 Initial Context Setup Request message to the W-AGF. The message contains the KWAGF.

NOTE: Whether the key KWAGF is used by the 5G-RG and W-AGF is out of the scope of 3GPP.

11. (void)

12. Upon receiving the NAS Registration Accept message from the AMF, the W-AGF shall forward it to the 5G-RG over the established W-CP. All further NAS messages between the UE and the W-AGF shall be sent over the established W-CP.

\*\*\*\*\* End of changes \*\*\*