**3GPP TSG-SA3 Meeting #106-e *draft\_S3-220171-r1***

**e-meeting, 14 - 25 February 2022**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **TS 33.501** | **CR** | **1277** | **rev** | **-** | **Current version:** | **17.4.0** |  |
|  |
| *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 |  |

|  |
| --- |
|  |
| ***Title:***  | Delete Editor’s Notes |
|  |  |
| ***Source to WG:*** | Huawei, HiSilicon |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | TEI17 |  | ***Date:*** | 2022-02-14 |
|  |  |  |  |  |
| ***Category:*** | F |  | ***Release:*** | Rel-17 |
|  | *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:*** | The third Editor’s Note is changed to a NOTE.The reason is :The roaming scenario is not considered in the scope of the SID/WID of 5G NSWO, so the studied did not include this part. The Editor’s Note is captured only because the LS replied from SA2 mentioned the case. So did the co-existence with EPS NSWO case. However, it is impossible to address the Editor’s Note in the last R-17 SA3 meeting. So we propose to turn the Editor’s Note to a Note to mark the solution does not address the romaing issue and the co-existence with EPS NSWO. |
|  |  |
| ***Summary of change:*** | Turn a Editor’s Note to a Note. |
|  |  |
| ***Consequences if not approved:*** | The work contains unaddrssed issues. |
|  |  |
| ***Clauses affected:*** | Annex S.3 |
|  |  |
|  | **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:*** |  |

\*\*\*\* Start of Change\*\*\*\*

# S.3 Authentication procedure

An HPLMN that supports 5G NWSO and wants the UE to use 5G NSWO shall configure the UE to use 5G NSWO. This configuration shall be either on the USIM or ME, with configuration on the USIM taking precedence over the ME.

A UE that supports 5G NSWO and is configured to use 5G NSWO shall always use 5G NSWO (i.e., it shall not use EPS NSWO defined in TS 23.402[97]).

NOTE: Such a configuration ensures that the UE supporting 5G NSWO cannot be downgraded to use EPS NSWO.



1.When the UE decides to perform NSWO, the UE establishes a WLAN connection between the UE and the WLAN Access Network (AN), using procedures specified in IEEE 802.11[80].

2.The WLAN AN sends an EAP Identity/Request to the UE.

3.The UE sends an EAP Response/Identity message. The UE shall use the SUCI in NAI format (i.e., username@realm format) as its identity irrespective of whether SUPI Type configured on the USIM is IMSI or NAI. If the SUPI Type configured on the USIM is IMSI, the UE shall construct the SUCI in NAI format with username containing the encrypted MSIN and the realm part containing the MCC/MNC.

Editor’s Note: username@realm format needs to be specified for SUCI in NAI format in clause 28.7.3 of TS 23.003.

4.The EAP Response/Identity message shall be routed over the SWa interface towards the NSWO NF based on the realm part of the SUCI.

NOTE 1: NSWO NF acts as SBI/AAA proxy between the AUSF and the WLAN Access Network.

5.The NSWO NF shall send the message Nausf\_UEAuthentication\_Authenticate Request with SUCI, Serving Network name and NSWO indicator towards the AUSF. NSWO\_indicator is used to indicate to the AUSF that the authentication request is for Non-seamless WLAN offload purposes. The NSWO NF shall set the Serving Network name to "5G:NSWO".

6.The AUSF (acting as the EAP authentication server) shall send a Nudm\_UEAuthentication\_Get Request to the UDM including SUCI and the NSWO indicator.

Editor’s Note: Either existing service operations used for primary authentication (Nausf\_UEAuthentication\_Authenticate and Nudm\_UEAuthentication\_Get) can be reused for NSWO or new service operations for NSWO execution independent from primary authentication service (e.g., Nausf\_UEAuthentication\_NSWOAuthenticate and Nudm\_UEAuthentication\_GetNSWO) could be defined. The reuse of existing service operations is assumed here but this is FFS and needs to be updated once this issue is resolved.

7.Upon reception of the Nudm\_UEAuthentication\_Get Request, the UDM shall invoke SIDF. SIDF shall de-conceal SUCI to gain SUPI before UDM can process the request. Based on the NSWO indicator, the UDM/ARPF shall select the EAP-AKA´ authentication method. UDM shall generate and include the EAP-AKA’ authentication vector (RAND, AUTN, XRES, CK´ and IK´) and may include SUPI to AUSF in a Nudm\_UEAuthentication\_Get Response message.

8.The AUSF shall store XRES for future verification. The AUSF shall send the EAP-Request/AKA'-Challenge message to the NSWO NF in a Nausf\_UEAuthentication\_Authenticate Response message.

9.The NSWO NF shall send the EAP-Request/AKA'-Challenge message to the WLAN AN over the SWa interface.

10.The WLAN AN forwards the EAP-Request/AKA'-Challenge message to the UE.

11.At receipt of the RAND and AUTN in the EAP-Request/AKA'-Challenge message, the ME shall construct the SN name by setting it to “5G:NSWO”, and the USIM in the UE shall verify the freshness of the AV' by checking whether AUTN can be accepted as described in TS 33.102 [40]. If so, the USIM computes a response RES. The USIM shall return RES, CK, IK to the ME. The ME shall derive CK' and IK' according to Annex A.3. If the verification of the AUTN fails on the USIM, then the USIM and ME shall proceed as described in sub-clause 6.1.3.3. The UE may derive MSK from CK’ and IK’ as per Annex F and as described in RFC 5448[12]. When the UE is performing NSWO authentication, the KAUSF shall not be generated by the UE.

12.The UE shall send the EAP-Response/AKA'-Challenge message to the WLAN AN.

13.The WLAN AN forwards the EAP-Response/AKA'-Challenge message over the SWa interface to the NSWO NF.

14.The NSWO NF shall send the Nausf\_UEAuthentication\_Authenticate Request with EAP-Response/AKA'-Challenge message to AUSF.

15.The AUSF shall verify if the received response RES matches the stored and expected response XRES. If the AUSF has successfully verified, it continues as follows to step 16, otherwise it returns an error to the NSWO NF. The AUSF shall derive the required MSK key from CK’ and IK’ as per Annex F and as described in RFC 5448[12], based on the NSWO indicator received in step 5. The AUSF shall not generate the KAUSF.

16. The AUSF shall send Nausf\_UEAuthentication\_Authenticate Response message with EAP-Success and MSK key to NSWO NF. The AUSF may optionally provide the SUPI to NSWO NF.The AUSF/UDM shall not perform the linking increased home control to subsequent procedures (as stated in present document clause 6.1.4).

17.The NSWO NF shall send the EAP-success and MSK to WLAN AN over the SWa interface. The EAP-Success message is forwarded from WLAN AN to the UE.

18.Upon receiving the EAP-Success message, the UE derives the MSK as specified in step 11, if it has not derived the MSK earlier. The UE uses MSK to perform 4-way handshake to establish a secure connection with the WLAN AN.

NOTE:Roaming scenario and the co-existence with EPS is not specificed in this specification.

\*\*\*\* End of Change\*\*\*\*