**3GPP TSG-WG SA2 Meeting #148E  *S2-2108916r03***

**E-meeting, November 15th – 22nd, 2021 (*revision of S2-2108095*)**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **23.501** | **CR** | **3256** | **rev** | **4** | **Current version:** | **17.2.0** |  |
|  |
| *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 |  | Radio Access Network |  | Core Network | **x** |

|  |
| --- |
|  |
| ***Title:***  | UE onboarding architecture |
|  |  |
| ***Source to WG:*** | [Ericsson, Nokia, Nokia Shanghai Bell, Qualcomm, Lenovo, Motorola Mobility, Huawei],Intel |
| ***Source to TSG:*** | SA2 |
|  |  |
| ***Work item code:*** | eNPN |  | ***Date:*** | 2021-11-08 |
|  |  |  |  |  |
| ***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 architecture for UE onboarding, and especially the DCS, has not yet been concluded. The architecture includes AUSF and then a DCS which potentially can either include a AAA server or a AUSF.SA3 agreed the following:*For initial access for UE onboarding, the following authentication methods are concluded to be specified in normative work:**- Primary authentication between UE and AUSF in the O-SNPN. No interaction with DCS during primary authentication. As currently specified in TS 33.501 [2].**- Primary authentication with mutual authentication between UE and DCS. AUSF is involved. DCS can be AAA server, in that case NSSAAF is involved. DCS can also be external entity using AUSF/UDM*.*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\**Changes in r04:The changes in r04 is based on the ongoing discussion in SA3#105e meeting on a compromise proposal S3-213969 for conclusion on KI#4 (Securing initial access for UE onboarding netween UE and SNPN) which is based on the working agreement (S3-213611) agreed in SA3#104e meeting.  |
|  |  |
| ***Summary of change:*** | Editor's note removed and the ON-SNPN architecture with DCS updated.Updated NSSAAF description. |
| ***--*** |  |
| ***Consequences if not approved:*** | Architecture for DCS is not completely described |
|  |  |
| ***Clauses affected:*** | 5.30.2.10.2.2, 6.2.23 |
|  |  |
|  | **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 changes \* \* \* \*

5.30.2.10.2.2 Architecture

Figure 5.30.2.10.2.2-1 and 5.30.2.10.2.2-2 depict the architecture for Onboarding of UEs in an ON-SNPN.



Figure 5.30.2.10.2.2-1: Architecture for UE Onboarding in ON-SNPN in case DCS includes an AUSF and a UDM



Figure 5.30.2.10.2.2-2: Architecture for UE Onboarding in ON-SNPN in case DCS includes a AAA server used for primary authentication



Figure 5.30.2.10.2.2-3: Architecture for UE Onboarding in ON-SNPN in case DCS includes a AAA server used only for secondary authentication

NOTE 1: AUSF in the ON-SNPN interfaces with the DCS owned by an entity that is internal or external to the ON-SNPN.

NOTE 2: The functionality with respect to exchange information between PVS and SO-SNPN to provision SNPN credentials and other data from the SO-SNPN in the UE is out of 3GPP scope.

NOTE 3: The dotted lines in Figure 5.30.2.10.2.2-1 indicate that domains (e.g. DCS domain, PVS domain, and SO-SNPN) may not be separated depending on the deployment scenario.

NOTE 4: See TS 33.501 [29] for the functionality beyond AUSF, and other interfaces required for security.

When the DCS is involved during mutual primary authentication during the Onboarding procedure (as in Figure 5.30.10.2.2-1 and Figure 5.30.10.2.2-2), the following apply:

- When the DCS includes an AUSF and a UDM functionality, then the AMF selects AUSF and UDM in the DCS domain. The ON-SNPN and DCS domain are connected via N32 and SEPP which are not shown in the Figure 5.30.2.10.2.2-1.

- When the DCS includes a AAA server functionality, then the AMF selects AUSF in the ON-SNPN. Based on local configuration the AUSF skips the UDM selection and directly performs primary authentication towards DCS with AAA server functionality. The AUSF uses an NSSAAF (and the NSSAAF may use a AAA-P which is not shown in the figure 5.30.2.10.2.2-2) to relay EAP messages towards the DCS including a AAA Server. NOTE 5: If a given DCS supports both AUSF/UDM functionality as depicted in Figure 5.30.2.10.2.2-1 and AAA server functionality as depicted in Figure 5.30.2.10.2.2-2, the DCS needs to use separate Home Network Identifier for DCS with AUSF/UDM and for DCS with AAA server functionality to ensure correct selection of NFs.

When the DCS is not involved during primary authentication (as in Figure 5.30.10.2.2-3), upon establishment of the restricted PDU Session the ON-SNPN may trigger secondary authentication procedure with the DCS using default credentials as described in clause 11.1 of TS 33.501 [29]. Editor’s note: The architecture option in Figure 5.30.10.2.2-3 intends to reflect SA3 agreements (S2-2109020) and will be further checked based on work progress in SA3.

NOTE 6: The DCS and PVS can be owned by an administrative entity that can be different from either the ON-SNPN or SO-SNPN. The ownership of DCS and PVS is outside the scope of 3GPP.

\* \* \* \* Next change \* \* \* \*

### 6.2.23 NSSAAF

The Network Slice-specific and SNPN Authentication and Authorization Function (NSSAAF) supports the following functionality:

- Support for Network Slice-Specific Authentication and Authorization as specified in TS 23.502 [3] with a AAA Server (AAA-S). If the AAA-S belongs to a third party, the NSSAAF may contact the AAA-S via a AAA proxy (AAA-P).

- Support for access to SNPN using credentials from Credentials Holder using AAA server (AAA-S) as specified in clause 5.30.2.9.2 or using credentials from Default Credentials Server using AAA server (AAA-S) as specified in clause 5.30.2.10.2. If the Credentials Holder or Default Credentials Server belongs to a third party, the NSSAAF may contact the AAA server via a AAA proxy (AAA-P).

NOTE: When the NSSAAF is deployed in a PLMN, it supports Network Slice-Specific Authentication and Authorization, while when the NSSAAF is deployed in a SNPN may support Network Slice-Specific Authentication and Authorization and/or access to SNPN using credentials from Credentials Holder

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