**3GPP TSG-SA3 Meeting #107-eS3-221022**

**e-meeting, 16 - 20 May 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** | **1** | **Current version:** |  |  |
|  | | | | | | | | |
| *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:*** | Update to clause I.2.2.2.2 for Onboarding clarifications | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Lenovo | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eNPN | | | | |  | ***Date:*** | | | 2022-05-05 |
|  |  | | | |  | |  | | |  |
| ***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 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-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | According to TS 33.501 Clause I.9.2.3 Primary authentication using DCS, cites the procedure in clause I.2.2.2.2 related to Credentials holder using AAA server for primary authentication. But the actual procedure in clause I.2.2.2.2 does not clarify or describe any sentence (not even a single step) on Onboarding SUPI and Onboarding SUCI usage for the primary authentication which are the actual identifiers used for UE onboarding related primaty authentication according to TS 24.501. Further steps 6-7 cannot be related at all to the UE onboarding related authentication initiation, as UE onboarding related authentication initiation will involve Onboarding SUCI and not a SUPI at all. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | The procedure in I.2.2.2.2 is updated to cover onboarding authentication related steps. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Specification will remain incorrect and incomplete. Because it will be incorrect to refer I.2.2.2.2 to support ‘Primary authentication using DCS for onboarding scenario’ without providing any sort of clarification on how UE Onboarding related authentication works. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | I.2.2.2.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\*\*\* Start of change 1 \*\*\*

#### I.2.2.2.2 Procedure



Figure: I.2.2.2.2-1: Primary authentication with external domain

0. The UE shall be configured with credentials from the Credentials holder e.g., SUPI containing a network-specific identifier and credentials for the key-generating EAP-method used. As part of configuration of the credentials, the UE shall also be configured with an indication that the UE shall use MSK for the derivation of KAUSF after the success of the primary authentication. The exact procedures used to configure the UE are not specified in the present document.

It is further assumed that there exists a trust relation between the SNPN and the Credentials holder AAA Server. These entities need to be mutually authenticated, and the information transferred on the interface need to be confidentiality, integrity and replay protected.

In the case of UE onboarding, the default configuration server (i.e., DCS hosting AAA server) is involved, where the UE shall derive the Onboarding SUPI based on the default credentials as specified in TS 24.501 [35] and TS 23.501 [2]. The UE onboarding specific adaptations are described in each step below where applicable.

1. The UE shall select the SNPN and initiate UE registration in the SNPN.

For construction of the SUCI, existing methods in clause 6.12 can be used. If the home network public key of the SNPN is not provisioned in the UE, the UE shall create a SUCI using null scheme with anonymised SUPI as described in Annex B.

Editor's Note: It is FFS if only SUCI using null scheme with anonymised SUPI should be supported for this use case.

In the case of UE onboarding, the UE shall contruct Onboarding SUCI with ‘null-scheme’ if the public key needed to generate a SUCI is not configured as part of the default UE credentials; or ‘null-scheme’ usage is configured as part of the default UE drecentials as specified in TS 24.501 [35] clause 5.3.2. Further when the UE constructs the Onboarding SUCI with ‘null-scheme’, the username part of the network specific identifier shall be set as described in clause I.9.2.3.

2. The AMF within the SNPN shall initiate a primary authentication for the UE using a Nausf\_UEAuthentication\_Authenticate service operation with the AUSF. The AMF shall discover and select an AUSF based on criterions specified in TS 23.501 [2] clause 5.30.2.9.2.

In the case of UE onboarding, the AMF selects AUSF in the ON-SNPN as specified in TS 23.501 [2] clause 5.30.2.10.2.2.

3. The AUSF shall initiate a Nudm\_UEAuthentication\_Get service operation. The AUSF shall discover and select a UDM based on criterions specified in TS 23.501 [2] clause 5.30.2.9.

NOTE 1: SUPI will be used instead of SUCI in the case of a re-authentication.

In the case of UE onboarding, steps 3 – 5 shall be akipped.

4. In case the UDM receives a SUCI, the UDM shall resolve the SUCI to the SUPI before checking the authentication method applicable for the SUPI. The UDM decides to run primary authentication with an external entity based on subscription data or by looking at the realm part of the SUPI in NAI format.

In case the UDM receives an anonymous SUCI that does not contain the realm part, the UDM shall abort the procedure. If contains, the UDM authorizes the UE based on realm part of SUCI and send the anonymous SUPI and the indicator to the AUSF as described in step5.

The anonymous SUPI shall be a NAI format as described in clause B.2.1.2.2.

5. The UDM shall provide the AUSF with the UE real SUPI or anonymous SUPI and shall indicate to the AUSF to run primary authentication with an external Credentials holder.

When a Credentials Holder using AAA Server is used for primary authentication, the AUSF uses the MSK to derive KAUSF. It is strongly recommended that the same credentials that are used for authentication between UE and the 5G SNPN are not used for the authentication between the UE and a non-5G network, assuming that 5G SNPN and non-5G network are in different security domains.

NOTE 2: MSKs obtained from the non-5G network could be used to impersonate the 5G SNPN towards the UE.

6. Based on the indication from the UDM, the AUSF shall select an NSSAAF as defined in TS 23.501 [2] and initiate a Nnssaaf\_AIWF\_Authenticate service operation towards that NSSAAF as defined in clause 14.4.2.

In the case of UE onboarding, based on local configuration (e.g., using the realm of the Onboarding SUCI), the AUSF skips the UDM selection and directly performs primary authentication towards the DCS with AAA Server functionality as specified in TS 23.501 [2] clause 5.30.2.10.2. The AUSF uses an NSSAAF (and the NSSAAF may use a AAA-P) to relay EAP messages towards the DCS including a AAA Server. The AUSF shall send the Onboarding SUCI to the NSSAAF.

7. The NSSAAF shall select AAA Server based on the domain name corresponding to the realm part of the SUPI. The NSSAAF shall perform related protocol conversion and relay EAP messages to the AAA Server.

In the case of UE onboarding, the NSSAAF shall select the DCS with AAA Server based on the domain name corresponding to the realm part of the Onboarding SUCI which is received from the AUSF.

NOTE 3: The interface and protocol between NSSAAF and AAA is out of scope of the present document and existing AAA protocols such as RADIUS or Diameter can be used.

8. The UE and AAA Server shall perform mutual authentication. The AAA Server shall act as the EAP Server for the purpose of primary authentication. The EAP Identity received by the AAA Server in the EAP-Response/Identity message in step 7 may contain anonymised SUPI. In such cases, AAA Server uses the EAP-method specific EAP Identity request/response messages to obtain the UE identifier as part of the EAP authentication between the UE and the AAA Server.

In the case of UE onboarding, the UE and the AAA Server shall perform mutual authentication based on the Onboarding SUCI and the UE default credentials (if it can be identified with the digital identifier indicated as part of the username in the received Onboarding SUCI). If the username part of the Onboarding SUCI contains a digital identifier, then the digital identifier shall be used to identify the UE default credentials. Otherwise, if the username part of the Onboarding SUCI contains static string ‘anonymous’ or if username part is not available, any authentication method can be selected by the DCS based on the received Onboarding SUCI (e.g., based on realm part). The choice of primary authentication method used between the UE and the DCS is left to the decision of the DCS.

9. After successful authentication, the MSK and the SUPI (i.e., the UE identifier that is used for the successful EAP authentication) shall be provided from the AAA Server to the NSSAAF.

In the case of UE onboarding, after successful authentication, the MSK and the Onboarding SUPI (i.e., the UE identifier that is used for the successful EAP authentication) shall be provided from the DCS with AAA Server to the NSSAAF.

10. The NSSAAF returns the MSK and the SUPI to the AUSF using the Nnssaaf\_AIWF\_Authenticate service operation response message. The SUPI received from the AAA shall be used when deriving 5G keys (e.g., KAMF) that requires SUPI as an input for the key derivation.

In the case of UE onboarding, the NSSAAF returns the MSK and the Onboarding SUPI to the AUSF. The the Onboarding SUPI received from the AAA Server shall be used when deriving 5G keys (e.g., KAMF) that requires Onboarding SUPI as an input for the key derivation.

11. The AUSF shall use the most significant 256 bits of MSK as the KAUSF. The AUSF shall also derive KSEAF from the KAUSF as defined in Annex A.6.

12. The AUSF shall send the successful indication together with the SUPI of the UE to the AMF together with the resulting KSEAF.

In the case of UE onboarding, the AUSF shall send the successful indication together with the Onboarding SUPI of the UE to the AMF together with the resulting KSEAF.

13. The AMF shall send the EAP success in a NAS message.

14. The UE shall derive the KAUSF from MSK as described in step 11 according to the pre-configured indication as described in step 0.

\*\*\* End of change 1 \*\*\*