**3GPP TSG-SA3 Meeting #107-e S3-220863**

**e-meeting, 16 – 20 May 2022 Revision of S3-22xxxx**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **1376** | **rev** | **-** | **Current version:** | **17.5.0** |  |
|  | | | | | | | | |
| *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 | **X** | ME | **X** | Radio Access Network |  | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Address EN for NPN | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, Hisilicon | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eNPN | | | | |  | ***Date:*** | | | 2022-05-16 |
|  |  | | | |  | |  | | |  |
| ***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:*** | | There are 3 ENs, i.e.  “*EN1: It is FFS if only SUCI using null scheme with anonymised SUPI should be supported for this use case.*”  “*EN2: It is FFS how using anonymous SUCI or skipping default credentials identifier to initiate onboarding will meet the scope of ‘UE being verified as "uniquely identifiable and verifiably secure.*”  “*EN3: It is FFS, how the default credential identifier i.e., verifiably secure identifier is used as SUPI during the authentication procedure related to Onboarding.*”  All of the ENs are used to address SUPI privacy issue.  In order to try our best to protect SUPI privacy, it is proposed:  If DCS/AAA is used, the UE shall use anonymous SUCI in registration request, and the UE and the DCS/AAA may use EAP to achieve ID privacy, because the credential is from DCS/AAA, the UDM has no public key to protect the SUPI.  If AUSF/UDM is used, the UE shall reuse SUCI protection scheme in registration request, because the credential is from UDM which may be configured with public key.  In addition, since the credential is from CH with AAA server, the AUSF and UE shall use MSK for Kausf derivation, instead of EMSK according requirement from RFC 3748 stating that “*The EMSK is not shared with the*  *authenticator or any other third party.*” and “*In existing implementations, a AAA server acting as an EAP server transports the MSK to the authenticator*”. It is agreed that UE needs to pre-configure an indication to use MSK for Kausf derivation if DCS/AAA is used.  So, the reason why the UE uses anonymised SUPI and MSK for Kausf derivation is the same reason that the credential is from a CH with AAA/DCS, the UE could just use one pre-configured indication for anonymised SUPI and MSK derivation, not separate.  Thus, it is proposed to provide SUCI privacy, clarify the indication and delete the remaining EN. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | UE uses the pre-configured indication to construct anonymised SUPI.  The pre-configured indication is the same with what is configured for MSK usage. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Unresolved EN. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | I.2.2.2, I.9.2.1 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#### 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 credential is from a CH with AAA server, and the UE shall use anonymised SUCI for initial registration and MSK for the derivation of KAUSF after the success of the primary authentication accordingly. 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.

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 credential is from a CH with AAA server according to the pre-configured indication as described in step 0 and 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.

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.

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.

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.

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.

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.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.

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.

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.

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 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*