**3GPP TSG-SA3 Meeting #106-e *draft\_S3-220188-r3***

**e-meeting, 14 – 25 February 2022** revision of S3-22xxxx

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | **1282** | **rev** | **-** | **Current version:** | **17.4.0** |  |
|  |
| *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 |  |

|  |
| --- |
|  |
| ***Title:***  | Clarification on MSK and anonymous SUPI usage |
|  |  |
| ***Source to WG:*** | Huawei, HiSilicon |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | eNPN |  | ***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:*** | There is an EN “*It is FFS if only SUCI using null scheme with anonymised SUPI should be supported for this use case.*”According to step 1 in I.2.2.2.2, “*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*”.And according to B.2.1.2.2, “*if the operator determines to provide subscription identifier privacy for the UE in TLS layer, …, the "null-scheme" could be used in NAS layer while still preserving subscription identifier privacy, by omitting the username part from NAI as described in RFC 4282 clause 2.3 [y].*”. It is unclear how does the UE know the operator determines that.Since the credential is from CH with AAA server, the SNPN should let AAA server to determine whether to provide subscription identifier by using anonymised SUCI as depicted in step 8 in I.2.2.2.2. Besides, as agreed in CR#3847 (C1-220790) for TS 24.501 in C1-133-bis-e meeting,“*If:**a) the UE uses the "null-scheme" as specified in 3GPP TS 33.501 [24] to generate a SUCI;**b) the UE operates in SNPN access operation mode and:**1) the UE is not registering or registered for onboarding services in SNPN, and the AAA server of CH acts as EAP server of the EAP based primary authentication and key agreement procedure; or**2) the UE is registering or registered for onboarding services in SNPN and the AAA server of DCS acts as EAP server of the EAP based primary authentication and key agreement procedure;**Editor's note: (WI:eNPN, CR#3847) it is FFS how the UE knows whether the AAA server of CH or DCS acts as EAP server of the EAP based primary authentication and key agreement procedure.**….**then the UE shall use anonymous SUCI as specified in 3GPP TS 23.003 [4].*”According to CT1, the UE constructs anonymous SUCI if the UE operates in SNPN access operation mode and the credential is from a CH with AAA.Similarly, 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.Besides, as depicted in clause 5.4.1.2.3 in TS 24.501, “*Upon receiving an EAP-success message, the ME shall:**a) delete the valid KAUSF and the valid KSEAF, if any;**b) if the ME has not generated a new KAUSF and a new KSEAF and has not created a partial native 5G NAS security context when handling the EAP-request message which resulted into generation of EMSK or MSK as described above:**1) if the UE operates in SNPN access operation mode and credentials in the selected entry of the "list of configuration data" are from a CH with the AAA server then generate a new KAUSF from the MSK otherwise generate a new KAUSF from the EMSK;*”According to CT1, the UE uses MSK for Kausf derivation if the UE operates in SNPN access operation mode and the credential is from a CH with AAA.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, the UE could just use one pre-configured indication for anonymised SUPI and MSK derivation, not separate.However, according to step 0 in I.2.2.2.2 that “*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.*”, it may raise confuse that two separate indication is needed. One for anonymised SUPI construction and another one for MSK for Kausf derivation.Thus, it is proposed to clarify the indication to avoid ambiguation that anonymised SUPI construction needs another indication and delete the remaining EN. |
|  |  |
| ***Summary of change:*** | Make clarification on the pre-configured indication.UE uses the pre-configured indication to construct anonymised SUPI. |
|  |  |
| ***Consequences if not approved:*** | It is not clear how does the UE use anonymised SUPI. |
|  |  |
| ***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 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 the credential is from a CH with AAA server, and UE shall use 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 this 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 home network public key of the SNPN is not provisioned in the UE and SUPI privacy needs to be preserved, then, the UE shall create a SUCI using null scheme with anonymised SUPI as described in Annex B.

NOTE 1: The UE may skip the username part of NAI SUPI while sending SUCI to be analogous to using anonymous identifier as described in Annex B.

Editor’s Note: How does the UE know SUPI privacy needs to be preserved is to be aligned with CT1.

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 select an AUSF based on the HNI of the SUCI (*i.e. realm for NSI SUPI type*) presented by the UE as specified in TS 23.501 [2].

Editor’s Note: It is FFS how does the AMF selects AUSF in step 2 using realm part of SUPI which is also used for NSSAAF to select AAA server in step 7, since the AUSF and AAA server is located in different domain.

3. The AUSF shall initiate a Nudm\_UEAuthentication\_Get service operation. The AUSF shall select a UDM also using the SUCI/SUPI provided by the AMF as specified in TS 23.501 [2].

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 anonymousSUCI shall be a NAI format as described in clause B.2.1.2.2.

Editor's Note: It is FFS why the existing UDM service with mandatory IE 'Authentication method' need to be invoked for an authentication based on credentials held by an external entity.

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 3GPP TS 23.501 [2] and initiate a Nnssaaf\_AIWF\_Authenticate service operation towards that NSSAAF as defined in clause 14.4.x.

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.

Editor's Note: It is FFS if the SUPI needs to be sent to the external entity (AAA).

Editor's Note: The details of the interface and protocol between AUSF and AAA are FFS.

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.

Editor's Note: The details of the interface and protocol between AUSF and AAA are FFS.

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.

Editor's note: It is FFS if and how clause 1.2.2.3 aligns with TS 23.501 5.30.2.9.2 Credentials Holder using AAA Server for primary authentication and authorization.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*