**3GPP TSG-SA3 Meeting #108e *S3-222123***

**e-meeting, 22 - 26 August 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **1469** | **rev** | **-** | **Current version:** | **17.6.0** |  |
|  | | | | | | | | |
| *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:*** | clarification on the internal authentication and an external authentication | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eNPN | | | | |  | ***Date:*** | | | 2022-08-18 |
|  |  | | | |  | |  | | |  |
| ***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:*** | | NOTE 1a in I.2.2.2.2 says,” *The UDM needs to be configured with a list of realms and the intended authentication server (external or internal)*”  The reader may curious why the NOTE mention the “internal” considering the whole clause I.2.2.2.2 is specified for external authenticaiton. Thus, the relationship between the use of the external authentication server and internal authentication server is not clear and cannot be found through the whole spec. Therefore, based on what has been specified here and there in TS 33.501, the relationship beteween external authentication server and internal authentication server is clarified, i.e. based on the UDM determination. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Clarify how the UDM deterimes the role(authenticator or authentication server) of primary authentication. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The procedures when using external authentication server and internal authentication server is not clear. | | | | | | | | |
|  | |  | | | | | | | | |
| ***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:*** | |  | | | | | | | | |

\*\*\*\*\*\*\*\*\* Begin 1st change\*\*\*\*\*\*\*\*\*

# I.2 Authentication in standalone non-public networks

## I.2.1 General

One of the major differences of non-public networks is that authentication methods other than AKA based ones may be used in a standalone non-public network (SNPN). When an AKA-based authentication method is used, clause 6.1 shall apply. When an authentication method other than 5G AKA or EAP-AKA' is used, only the non-AKA specific parts of clause 6.1 shall apply. An example of running such an authentication method is given in Annex B with EAP-TLS.

The choice of the supported authentication methods for access to SNPNs follows the principles described in clauses I.2.2 and I.2.3.

The authentication server can be an internal authentication server or an external authentication server. The internal authentication server is the AUSF, and the authentication method can be 5G-AKA or EAP-AKA´ as described in clause 6.1, or can be EAP-TLS as described in Annex B. When external authentication server is the AAA, the primary authentication procedure is described in Annex I.2.2.2.2. When external authentication server is an AUSF, then the primary authentication procedure is described in Annex I.2.4. The UDM decides to run primary authentication withinternal authentication server or external authentication server.\*\*\*\*\*\*\*\*\* End of 1st change\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\* Begin 2nd 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 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.   
  
When the procedures of this clause are used for onboarding purposes, the onboarding specific adaptations includes: the 'credentials' used is 'Default credentials', the 'SUPI' used is 'onboarding SUPI', the 'SUCI' used is 'onboarding SUCI' respectively.

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. Otherwise, if the EAP method supports SUPI privacy, the UE may send an anonymous value SUCI based on configuration.

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. In the case of onboarding, steps 3-5 are omitted. If steps 3-5 are not omitted, 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.

In case the UDM receives an anonymous SUCI, the UDM decides to run primary authentication with an external entity based the realm part of the SUPI in NAI format.

NOTE 1a: The UDM needs to be configured with a list of realms and the intended authentication server

In case the UDM receives an anonymous SUCI that does not contain the realm part, the UDM shall abort the procedure. Otherwise, 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. 5. In case the UDM received a SUCI in previous steps, the UDM shall provide the AUSF with the SUPI or anonymous SUPI and shall indicate to the AUSF to run primary authentication with a AAA Server in 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.

11-13. In case of onboarding or SUCI received in step 2 is not anonymous, steps 11-13 are omitted. Otherwise, the AUSF verifies that the SUPI corresponds to a valid subscription in the SNPN by informing the UDM about the authentication result for the received SUPI using a Nudm\_UEAuthentication\_ResultConfirmation service operation. The UDM stores the authentication state for the SUPI and if there is not a subscription corresponding to the SUPI, the UDM shall return an error.

If the verification of the SUPI is not successful, then the AUSF rejects the UE access to the SNPN.  
  
NOTE 4: If the above failure happens, the error is no failed authentication but lacking subscription in the SNPN.

14. 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.

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

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

17. 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\*\*\*\*\*\*\*\*\*