**3GPP TSG-SA3 Meeting #107e *draft\_S3-221049-r2***

 ***Merger of S3-221008, S3-221009, S3-221111, S3-221112, and S3-221049.***

e-meeting, 16 – 20 May 2022

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  |  | **CR** | **CR1406** | **rev** | **2** | **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:***  |  Resolving the Editor’s Notes for UE onboarding in SNPNs |
|  |  |
| ***Source to WG:*** | Xiaomi, Ericsson, Nokia, CableLabs, Intel, Qualcomm, Philipps |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | eNPN |  | ***Date:*** | 2022-05-09 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** |  |
|  | *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:*** | Reason for change #1:In current version of TS 33.501, there is an Editor’s Note in clause I.9.2.1 "*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*" that needs to be resolved.First, in step #8 of clause I.2.2.2.2, it is stated that "*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*". Second, according to clause 2.1.4 of **RFC 5216 (EAP-TLS)**, it is stated that "*EAP-TLS peer and server implementations MAY support privacy. Disclosure of the username is avoided by utilizing a* ***privacy Network Access Identifier (NAI) [RFC4282]*** *in the EAP-Response/Identity, and* ***transmitting the peer certificate within a TLS session providing confidentiality***".Third, according to clause 7.3 of RFC 5281(**EAP-TTLS**), it is stated that "***The identity of the user is provided during phase 2, where it is protected by the TLS tunnel***". Based on the above observations, the DCS/AAA server and UE can first establish a secure TLS tunnel when the DCS/AAA server receives the anonymized SUPI. After that, the DCS/AAA server can request the real identity (e.g. SUPI) from the UE in a secure TLS tunnel. Then the DCS/AAA server can uniquely identify the UE based on the SUPI and retrieve the default credential to authenticate the UE. Therefore, the anonymous SUCI or skipping default credentials identifier has no impact on the scope of ‘UE being verified as 'uniquely identifiable and verifiably secure". Which SUCI privacy method is applied on top is not relevant, since at the end of a succesful authentication procedure the onboarding network will have authenticated and identified the SUPI derived from the default UE credentials, not the SUCI.Please note that an anonymized SUCI doesn’t imply that the ON or DCS never learns the identity, it’s just transferred after the onboarding network or DCS has been authenticated.Reason for change #2:TS 33.501 section I.5 and 6.12 describes how to handle and use the “secure verifiable identifier” as a SUPI/SUCI. Please note that the format of the SUPI is in NAI format which makes it flexible and adaptable to any identifier value.In current version of TS 33.501, there is another Editor’s Note in clause I.9.2.1 "It is FFS, how the default credential identifier i.e., verifiably secure identifier is used as SUPI during the authentication procedure related to Onboarding" that needs to be resolved.In TS 23.501, it is stated in clause 5.30.2.10.2.4 that “*The SUPI shall uniquely identify the UE and shall be derived from the Default UE credentials*”, and it is also stated in clause 5.30.2.10.2.6 that "***The SUPI used for onboarding may contain an IMSI or a network-specific identifier****. The ON-SNPN may determine the corresponding DCS identity or address/domain, based on the SUCI (i.e. based on the Home Network Identifier of the SUCI)*".Furthermore, according to the analysis for change #1, **the DCS/AAA server is able to obtain the real SUPI for identifying the UE and retrieve its default credential based on the SUPI**. Retrieving UE’s default credential by the DCS/AAA server using the SUPI could be based on e.g. a mapping table between the SUPI of the UE and its default credential, regardless how the SUPI is constructed.Therefore, there is no need to study how default credential identifier can be used as the SUPI used for onboarding. |
|  |  |
| ***Summary of change:*** | "Editor's Note: 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" are analysed as follows" is removed."Editor’s Note: It is FFS, how the default credential identifier i.e., verifiably secure identifier is used as SUPI during the authentication procedure related to Onboarding" is removed. |
|  |  |
| ***Consequences if not approved:*** | Editor's Notes remain unresolved. |
|  |  |
| ***Clauses affected:*** | Annex 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 the Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### I.9.2.1 Requirements

The primary authentication shall be performed before initial access for UE onboarding is allowed. The UE shall use Default UE credentials for the primary authentication. Credentials or means used to authenticate the UE based on Default UE credentials may be stored within the ON-SNPN or in a Default Credentials Server (DCS) that is external to the ON-SNPN.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of the Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*