**3GPP TSG-SA3 Meeting #106-eS3-220435**

**e-meeting, 14 - 25 February 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **1352** | **rev** |  | **Current version:** | **17.4.2** |  |
|  | | | | | | | | |
| *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 | **x** | Core Network | **x** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Update to Clause 1.9 for Onboarding Initial Access | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Lenovo, Motorola Mobility | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eNPN | | | | |  | ***Date:*** | | | 2022-02-07 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | B |  | | | | | ***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:*** | | To support secure initial access for UE onboarding in SNPNs, it is required that, the choice of primary authentication method used between the UE and the DCS is left to the decision of the DCS. In this regard, it is very essential that the DCS is provided means to identify the default information or credentials related to UE requesting onboarding access, to initiate and perform authentication of the onboarding UE to allow the related onboarding access. Whereas, the requirements in the current specifcation does not cover the identification part which may allow skipping username part of NAI or usage of anonymous word in the username part leading to default credentails retrieval issue at the network side and authorized UE identification delay at the network side leading to more malicious authentictaion message exchange processing at the network side. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Resolved the ENs related to default credential identifcation along with clarifications. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Onboarding will allow all malicious UEs to flood the network with onboarding request, where the DCS at the network side will not be able to identify the genuine UEs requesting onaboarding authentication. Because the current onabording procedure may allow skipping username part of NAI or usage of anonymous word in the username part leading to default credentails retrieval issue at the network side and authorized UE identification delay at the network side leading to more malicious authentictaion message exchange processing at the network side. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 1.9.1, 1.9.2.1 and 1.9.2.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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.9 Securing initial access for UE onboarding in SNPNs

## I.9.1 General

Onboarding of UEs for SNPNs is specified in clause 5.30.2.10 of TS 23.501 [2].

Onboarding of UEs for SNPNs allows the UE to access an Onboarding Network (ONN) based on Default UE credentials identified with a NAI for the purpose of provisioning the UE with SNPN credentials and any other necessary information. The Default UE credentials are pre-configured on the UE. The NAI used to identify the default credentials shall contain a privacy protected digital identifier as username (i.e., a set of strings assigned by the default credentials server to identify the default credentials of a UE) and a realm pointing to the default credentials provider.

To provision SNPN credentials in a UE that is configured with Default UE credentials, the UE selects an SNPN as ONN and establishes a secure connection (or initial access) with that SNPN referred to as Onboarding SNPN (ON-SNPN).

The present clause specifies securing of the initial access for UE onboarding.

## I.9.2 Authentication

### 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.

The default credentials related to a UE onboarding shall be identified with a privacy protected digital identifier assigned by the DCS. The UE shall use the digital identifier based NAI as SUPI for the onboarding.

Editor’s Note: additional requirements are FFS.

### I.9.2.2 Primary authentication without using DCS

When the primary authentication is performed between the UE and the ON-SNPN, any one of the existing authentication methods defined in the present document may be used, i.e., 5G AKA, EAP-AKA’ or any other key-generating EAP authentication method (e.g., EAP-TLS).

The choice of primary authentication method used is left to the decision of the ON-SNPN.

### I.9.2.3 Primary authentication using DCS

When the primary authentication is performed between the UE and the DCS, the authentication requirements and procedures defined in clause I.2 for Credential Holder shall apply with the DCS taking the role of the Credentials Holder. When the DCS uses AAA Server for primary authentication, AUSF directly selects the NSSAAF as specified in 23.501 [2]. In this case, the UDM is not involved in the procedure defined in clause I.2.2.2.2, and the step 3 to step 5 shall be skipped. If the Default credentials does not support SUCI concealment service (i.e., if the DCS doesn’t support SIDF), then the SUCI shall be generated using null scheme and optionally digital identifier based SUPI is protected (i.e., for non-repudiation) with a digital signature.

NOTE 1: The default credentials used by the UE to optionally sign the SUPI and its related configuration can be upto the DCS which is outside the scope of 3GPP.

The choice of primary authentication method used between the UE and the DCS is left to the decision of the DCS.

When the primary authentication is performed between the UE and the DCS via the AUSF using EAP-TTLS, Annex X can be used.

### I.9.2.4 Secondary authentication using DCS

When the DCS is not involved during primary authentication, after successful primary authentication as described in I.7.2.2, upon the establishment of the Onboarding PDU Session, the ON-SNPN may trigger secondary authentication procedure with the DCS using Default UE credentials as described in clause 11.1.

The UE shall use Default UE credentials for the primary authentication. The secondary authentication is performed between the UE and the DCS. The secondary authentication may use the same Default UE credentials or a different UE credentials.

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