**3GPP TSG-SA3 Meeting #107-e *S3-221020***

**e-meeting, 16 - 20 May 2022**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** | **1** | **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 |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Resolving Editor’s Note related to UE onboarding | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Lenovo | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eNPN | | | | |  | ***Date:*** | | | 2022-05-05 |
|  |  | | | |  | |  | | |  |
| ***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:*** | | Securing initial access for UE onboarding in SNPNs topic has two Editor’s Notes on the identifier to be sent by the UE for onboarding registration. Further Primary authentication using DCS clearly states that, ‘The choice of primary authentication method used between the UE and the DCS is left to the decision of the DCS.’, so adopting any restricted type of identifier (as listed in C4-221172 such as skipping username or static keyword) for onboarding cannot work for scenarios if the legacy AAA or DCS selects method such as EAP-AKA for authentication. Further it also does not allow the DCS to select any default credentials related to the UE to initiate any specific authentication method. More related observations are presented in the discussion paper S3-221017. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Resolved the ENs related to identifcation along with clarifications. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Adopting only restricted identifier privacy modes such as skipping username or static keyword for onboarding cannot work for all scenarios if the legacy AAA or DCS selects method such as EAP-AKA for authentication. Further it does not allow the DCS to select any default credentials related to the UE at the network side to initiate any specific authentication method if the implementation involves DCS which support different method of authentication for different set of UEs. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | I.9.1, 1.9.2.1, I.9.2.3 and I.9.2.4.1 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 Change 1\*\*\*\*\*

## 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 network specific identifier (i.e., in NAI format) 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 network specific identifier used to identify the UE and default credentials may contain a privacy protected digital identifier as username (e.g., a set of strings assigned by the default credentials server to identify the default credentials of a UE) and the realm pointing to the default credentials server.

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 UE may use the digital identifier based NAI as the Onboarding SUCI (if the UE is required to use ‘null-scheme’ as specified in TS 24.501 [35] clause 5.3.2 and if the digital identifier is configured as part of the default credentials).

### 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.

Credentials required to authenticate the UE using default UE credentials, are provisioned at the AUSF or AUSF/UDM of the ON-SNPN. The provisioning of this information is out of scope of this document.

### 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 UE is required to use ‘null-scheme’ for onboarding as specified in TS 24.501 [35] clause 5.3.2, the UE uses any one of the following methods to construct and send Onboarding SUCI based on the configured default credentials which can be upto implementation.

* The UE may skip the username part of NAI,
* The UE may use static string such as ‘anonymous’ for the username part of NAI, (or)
* The UE may use the digital identifier as the username part of NAI.

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 U can be used.

### I.9.2.4 Secondary authentication

#### I.9.2.4.1 Secondary authentication using DCS

After successful primary authentication as described in I.9.2.2 (i.e., primary authentication without using DCS), 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.

#### I.9.2.4.2 Secondary authentication using DN-AAA

After successful primary authentication as described in I.9.2.2 or I.9.2.3, upon the establishment of the Onboarding PDU Session, the ON-SNPN may trigger secondary authentication procedure with a DN-AAA server as described in clause 11.1.

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