**3GPP TSG-SA3 Meeting #106-e *draft\_S3-220335-r5***

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **1326** | **rev** | 1 | **Current version:** | **17.4.1** |  |
|  | | | | | | | | |
| *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:*** | Clarification and corrections to UE Onboarding in SNPNs | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Qualcomm Incorporated, Nokia, Nokia Shanghai Bell, Intel, Ericsson | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eNPN | | | | |  | ***Date:*** | | | 2022-01-28 |
|  |  | | | |  | |  | | |  |
| ***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:*** | | The editor’s note in I.9.2.1 stating that additional requirements are FFS is no longer needed as there are already two other editor’s notes in this section to address the issues related to default credential identifer and there are no other open issues that will result in a new editors note.  Scenarios in which I.9.2.2 can be used is not described.  EAP-TTLS refers to Annex X rather than Annex U.  The existing text related to secondary authentication using DCS in I.9.2.4 contains wrong clause reference and misleading or redundant requirements. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | The first editor’s note in I.9.2.1 is deleted.  Addition of a NOTE in I.9.2.2 to clarify the usage scenario.  EAP-TTLS reference to the wrong Annex is corrected.  Removal of redundant or misleading requirements text and the credentials used for secondary authentication is further clarified by adding a NOTE. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Ambiguity regarding credentials used and incorrect references remains | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 2, I.9.2.1, I.9.2.2, I.9.2.3, I.9.2.4 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | | Merger of S3-220335, S3-220155? and S3-220256 | | | | | | | | |

**\*\*\*\* START OF CHANGES \*\*\*\***

**\*\*\*\* NEXT CHANGES \*\*\*\***

# 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 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.

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.

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".

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.

### 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 and data used to authenticate the UE using default credentials, , dependent on the authentication method, and optionally UE authorization information, are provisioned to the 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.

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 using DN-AAA

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. More generally, 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 CHANGES \*\*\*\***