**3GPP TSG-SA3 Meeting #106-e *draft\_S3-220335-r2***

**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 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:*** | 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 \*\*\*\***

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.501: "System Architecture for the 5G System".

…….

[99] RFC 5281: "Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)".

[100] RFC 6678: "Requirements for a Tunnel-Based Extensible Authentication Protocol (EAP) Method".

[101] General Data Protection Regulation, <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=EN>.

 [102] 3GPP TS 33.246: "Security of Multimedia Broadcast/Multicast Service (MBMS)".

 [103] 3GPP TS 23.247: "Architectural enhancements for 5G multicast-broadcast services".

[104] 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)".

[105] 3GPP TS 23.288: "Architecture enhancements for 5G System(5GS) to support network data analytics services".

[106] 3GPP TS 23.554 Application architecture for MSGin5G Service; Stage 2.

[107] 3GPP TS 22.262 Message service with the 5G System (5GS); Stage 1.

[xxx] IEC 62443: Industrial communication networks - Network and system security.

**\*\*\*\* 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 based on the type of the credentials.

When digital certificates are used as UE default credentials, root certificates are stored in AUSF of ON-SNPN, and the UDM is not used.

When AKA credentials are used as UE’s default credentials, the authentication profile and the corresponding configuration related to default credentials are made available to the AUSF and UDM. How the authentication profile and corresponding configuration related to the default credentials is made available to the AUSF and UDM of the ON-SNPN is out of the scope of this document. In this case, UE uses the Release-16 network selection procedure to select ON-SNPN.

NOTE x: The main usage of the configuration based on AKA credentials described above relates to a closed network, e.g. a network handling operation technology as standardised in IEC 62443 series [xxx].

### 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. 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).

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 DCS

When the DCS is not involved during primary authentication, after successful primary authentication as described in I.9.2.2, 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.

### I.9.2.YY 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.

NOTE y: The DN-AAA server can be the DCS or the PVS.

**\*\*\*\* END OF CHANGES \*\*\*\***