**3GPP TSG-SA3 Meeting #105e *S3-214079-r1***

**e-meeting, 8 - 19 November 2021**

**Source:** **Nokia****, Nokia Shanghai Bell**

**Title: Adding methods for authentication during onboarding**

**Document for: Approval**

**Agenda Item: 4.17**

# 1 Decision/action requested

***The contribution proposes adding methods for authentication during onboarding***

# 2 References

 [1] S3-213610 – “Living document for eNPN: draftCR to TS 33.501 capturing Security aspects of eNPN”

# 3 Rationale

In SA3#104-adhoc a working agreement related to UE authentication has been defined and introduced into the conclusions of Ki#4 of TR 33.857.

According to these conclusions two different mechanism for authentications of onboarding UEs shall be part of the normative standard, i.e., primary authentication of UE without DCS involvement reusing existing mechanism in TS 23.501 or primary authentication using a DCS which is acting as a credential holder towards the onboarding network.

This CR proposes to add a new clause to Annex I, which concentrates all normative changes within TS 33.501 related to UE onboarding. The proposed clause contains a General subclause describing the onboarding concept to the extent relevant for TS 33.501 and two subclauses for each of the concluded authentication methods.

Furthermore, since primary authentication of onboarding UEs without DCS involvement includes the handling of various Root CA Certificates, it is proposed to extend the Nudm\_UEAuthentication method to take this into account.

# 4 Detailed proposal

SA3 is kindly requested to approve the below changes to eNPN draft CR in [1]

\*\*\* BEGIN CHANGES \*\*\*

I.Y Support for UE Onboarding

I.Y.1 General

A SNPN may grant access for onboarding to UEs, although the UE is not in possession of a subscriber profile issued by the SNPN. In this way an onboarding UE can get connectivity to a provisioning server and retrieve a regular subscriber profile. The SNPN providing access to an onboarding UE is referred to as onboarding SNPN.

Although an onboarding UE does not have a subscriber profile issued by the onboarding SNPN, primary authentication between the onboarding UE and network is executed.

For this purpose, the UE is pre-provisioned with a default subscriber profile (referred to as default credentials), which is not specific to an onboarding SNPN, but issued and provisioned on the UE prior to onboarding.

Two different variants for primary authentication during onboarding are supported:

- Authentication and authorization of the onboarding UE is executed by the onboarding SNPN

- Authentication and authorization of the onboarding UE is executed by an entity, which is external to the onboarding SNPN and which is referred to as Default Credential Server.

I.Y.2 Primary Authentication by Onboarding Network

An onboarding network can authenticate and authorize an onboarding UE utilising primary authentication, which is based on a key deriving EAP method, e.g. EAP-TLS as outlined in Annex B. Where default Credentials consists of a private key, a corresponding X.509 certificate and identifier.

Depending on the origin of the onboarding UE, the UE's default certificate may be issued within different PKIs, the AUSF needs the CA root certificate during the onboarding process. Furthermore, the onboarding network authorises access to the onboarding network for provisioning.

For retrieving the CA root certificate and UE authorization the AUSF utilizes the Nudm\_UEAuthentication\_get service as described in Figure I.Y.2-1.



**Figure I.Y.2-1: Using Authorization request during primary authentication to retrieve CA certificate.**

1. UE and onboarding networks start primary authentication, i.e., steps 1 to 2 of Figure B.2.1.1-1 are executed.

Note: If the null scheme is used for SUCI concealment and deconcealment. the scheme input is left empty, i.e., the SUCI does not contain the default identity of the UE as defined for TLS privacy as described in B.2.1.2.2. This implies that authorization first can be executed we the real identity is know as described in B.2.1.2.2

2. After the AUSF has derived the O-SUPI from the default certificate presented by the onboarding UE; the AUSF sends the authorization request including the O-SUPI to the UDM of the onboarding network.

3. The UDM checks, based on the realm of the received O-SUPI, if a CA Root Cert is available, which can be used for verification of the client certificate. Furthermore, depending on the operator configuration, the UDM checks if the O-SUPI can be authorised for onboarding.

Note: Configuration of the CA Root Certificate and configuration of authorisation methods for onboarding UEs is outside the scope of this specification.

4. In case of a positive authorization decision, the UDM returns the CA Root Certificate to the AUSF,

5. The AUSF verifies the validity of the UE's default client certificate using the CA Root Certificate.

6. The primary authentication continues.i.e. steps 6 -20 of Figure B.2.1.1.-1is executed.

I.Y.3 Primary Authentication using Default Credential Server

Editor's Note: This clause will describe how a Default Credential Server can be utilized during UE onboarding.

\*\*\* NEXT CHANGE \*\*\*

14.2.2 Nudm\_UEAuthentication\_Get service operation

**Service operation name:** Nudm\_UEAuthentication\_Get

**Description:** Requester NF gets the authentication data from UDM. For AKA based authentication, this operation can be also used to recover from synchronization failure situations. If SUCI is included, this service operation returns the SUPI.

**Inputs, Required:** SUPI or SUCI, serving network name.

**Inputs, Optional:** Synchronization Failure indication and related information (i.e. RAND/AUTS).

**Outputs, Required:** Authentication method and corresponding authentication data for a certain UE as identified by SUPI or SUCI input.

Editor's note: How the UDM indicates to the AUSF to run primary authentication with an external Credentials holder is FFS.

**Outputs, Optional:** SUPI if SUCI was used as input. AKMA Indication, if the subscriber has an AKMA subscription (see TS 33.535 [91]), CA Root certificate.

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