**SA WG2 Meeting #140E e-meeting S2-200xxxx**

**Elbonia, August 19 – September 1, 2020**

**Source: Siemens, Volkswagen**

**Title: KI#4, Extension to SOL#35 to support external credential provider for onboarding authentication**

**Document for: Discussion/Approval**

**Agenda Item:**

**Work Item / Release: FS\_eNPN / Rel-17**

*Abstract of the contribution: KI#4 Solution #35 - Adding text on support onboarding/provisioning with an existing AAA server used as external Credential Provider*

# Discussion

An external Credential Provider CdP may be used in a 5G SNPN, supporting EAP-based primary network authentication (see also KI#1, and TS22.804 section 8.2.5.4). In some vertical deployments, both the external CdP and the corresponding external provisioning server PS may be part of an existing security infrastructure (e.g., a brownfield factory network).

The external CdP may be used also for onboarding network access authentication. External provisioning servers PS may support different protocols for onboarding (transparent to the 5G network). Support for this scenario seems attractive, as an already deployed security infrastructure can be re-used as CdP and PS by an industrial SNPN 5G network deployment. This contribution adds some explanatory text for this scenario as hint to future work at SA WG3.

# Proposal

This pCR proposes to add the following solution to TR 23.700-07.

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

## 6.35 Solution #35: Solution for On Boarding for SNPN Compatible with SO's Existing Provisioning Server

### 6.35.1 Introduction

This solution addresses key issue 4 "UE Onboarding and remote Provisioning".

Comparing to solution #5 "UE Onboarding and provisioning for an SNPN", the main difference are:

Currently, the solution assumes that device vendor may not maintain a DCS, or the on-boarding network has no agreement with DCS, so the solution does not involve DCS to perform authentication. Instead, the solution assumes that SO holds both UDM and PS because they are both related to subscription management. Since the SO has ownership of on-boarding UE, the solution assumes that the SO could get the UE's default UE credential (e.g. out of band method, for example, by scanning QR code on the on-boarding UE, reading from USB flash from device vendor, etc.), and configures it in its UDM or an external Credential Provider CdP. The UDM/CdP may reuse a primary authentication based default UE credential to authorize the UE for on-boarding. Editor's note: Whether and how to support the DCS in this solution is FFS.

- In solution 5, both credential and configuration information (e.g. PDU session parameters, such as NSSAI, DNN, and other required parameters to access the SNPN) are sent over user plane. However, in this solution, only credential is sent over user plane while the configuration information is sent over control plane. The motivation is to be compatible to existing Provision Server of Subscription Owner (SO).



Figure 6.35.1-1: UE Onboarding in SNPN

The solution requires two parts, one is O-SNPN, which is connected with SO's network, and is "bridge" for on-boarding. Another is SO, which is owner for the on-boarding UE, and provide authentication, provisioning service for the UE. SO's network is consisted of newly established 3GPP part and legacy part. The 3GPP part includes 5GC NEs, such as UDM, AUSF, etc. while the legacy part includes SO's existing NEs, such as provisioning server, external Credential Provider CdP (authentication server), application server, terminals.

NOTE1: SO may also own the O-SNPN.

The solution separates provisioning data into two parts, one is *3GPP configuration subscription data*, which is used for 3GPP network selection and configuration, and another is *N3GPP credential data*, which reuses SO's existing N3GPP credential.

The following assumptions and general procedure are given as below:

- The UE can retrieve or is preprovisioned with *on-boarding information* of SO's network for initial registration for on-boarding. The *on-boarding information* may include PLMN ID, NID, routing ID of SO's network.

- The UE is provisioned with *unique ID* and *default* UE *credential* by device vendor or another stakeholder (e.g., SO) for on-boarding authentication. After on-boarding authentication, the SO could identify whether on-boarding procedure is allowed for UE or not. The *unique ID* may be derived from PEI, and the *default* UE *credential* may be certificate, key, etc. The UE may reuse primary authentication for on-boarding authentication.

Editor's note: The exact definition and details of these default UE credential and on-boarding authentication are FFS and will be determined by SA WG3.

- After on-boarding authentication is successfully performed, the UE is *TO BE* provisioned with *3GPP* *configuration data which is used* to select and access SO's SNPN. The *3GPP configuration data* may includeDNN, NSSAI to access O-SNPN; PLMN ID and NID list for SNPN selection; a newly assigned SUPI for UE identification in SO's SNPN etc.

- After on-boarding authentication is successfully performed, the UE is *TO BE* provisioned with *N3GPP credential data* for authentication of an SNPN. The *N3GPP credential data* may reuse SO's N3GPP credential, e.g. certificate.

- The SO's UDM is provisioned with on-boarding UE's *unique ID*, *default* UE *credential* and desired *3GPP configuration subscription data.* The SO can use the provisioning method which is out of band, for example, the SO may retrieve *unique ID* and *default* UE *credential* by scanning QR code on the UE, or by reading from USB flash from device vendor, the SO may determine desired *3GPP configuration subscription data* based on the UE's specific service requirement, and the SO may configure them on the UDM using O&M.

- The SO's PS could reuse existing Provisioning Server to provide *N3GPP credential data* to the UE, e.g. certificate authority (CA) for certificate issue. The N3GPP credential can replace the default UE credential, and be used for next registration. The onboarding protocol used by PS is transparent to the 5G network.

The solution uses on-boarding authentication procedure using *unique ID*, *default* UE *credential* and *on-boarding information* for UDM to authenticate the UE for on-boarding. If on-boarding authentication successes, it means the SO holds UE's default UE credential, and the UE can be authorized for on-boarding. The on-boarding authentication may reuse existing primary authentication.

The solution reuses existing user plane protocol for PS to provide *N3GPP credential data* to the UE, e.g. using CMPv2 for credential provisioning or other protocols out of scope of 3GPP. So, the solution could be compatible to SO's existing provisioning server (e.g. CA).

The solution reuses existing UPU or UCU procedure for UDM to provide *3GPP configuration subscription data* to the UE. So, the solution has minimal changes.

### 6.35.2 Functional Description

#### 6.35.2.1 Introduction

The procedure hereby described allows a UE, which is not initially provisioned with network credentials to access an On-boarding SNPN (O-SNPN) and to obtain network credentials and configuration for the SO.

#### 6.35.2.2 Architecture



Figure 6.35.2.2-1: Architecture for UE Onboarding to an SNPN

UDM: UDM is used to perform:

Reusing primary authentication as on-boarding authentication: retrieve UE's unique ID and default UE credential, use unique ID and default UE credential for mutual authentication and security establishment with the UE. An external Credential Provider CdP may be used for onboarding network access authentication.

3GPP configuration subscription data provisioning: retrieve UE's desired 3GPP configuration subscription data, provide 3GPP configuration subscription data to the successfully authenticated UE via existing procedure.

PS: provide N3GPP credential data to the successfully authenticated UE. The PS may reuse existing provisioning server, e.g. CA.

### 6.35.3 Procedures



Figure 6.35.3-1: High-level flow for onboarding of the UE into an SNPN

**Pre-condition:**

a) UE has been provisioned *unique ID* and *default* UE *credential* that allows for successful mutual authentication of the device during the on-boarding authentication (step 6).

b) UDM has been provisioned *unique ID*, *default* UE *credential* and desired *3GPP configuration subscription data* of on-boarding UEs.

Editor's note: How provisioning of the default UE credential is protected and potential leakage of default UE credential is avoid are FFS and will be determined by SA WG3.

**Call-flow:**

1. RAN broadcasts on-boarding information.

2. In order to be consistent with current procedure, UE constructs SUCI according to on-boarding information and unique ID, e.g. its based on PEI, PLMN ID, NID, and routing ID using NAI format.

3. UE registers to the network using the SUCI.

**Success case:**

4. UE and UDM performs on-boarding authentication which may reuse primary authentication based on *default* UE *credential*. The UDM retrieves UE context according to *unique ID* in the SUCI.

5. The UE establishes a configuration PDU session. This PDU Session may be established either to a well-known or pre-configured S-NSSAI or DNN, or the UE receives the URSP including the S-NSSAI or DNN for on-boarding, or the UE receives the S-NSSAI by using the indication that this is registration for UE onboarding provided by the UE in step 6, which is used just for provisioning purposes and has limited connectivity capabilities. Based on this information, the AMF selects a designated SMF which in turn selects a designated PSA that provides a restricted data connection to the Provisioning Server.

NOTE 1: It is assumed that connectivity of this PDU session is limited (cf. RLOS), so that the UE can only access a Provisioning Server, or a restricted onboarding network.

The UE discovers and connects, at application level, to a provisioning server address (that was preconfigured in the UE or received in step 6 from O-SNPN or is derived from the application identifier and/or Service Provider Identifier provided by the user in step 1).

The UE retrieves *N3GPP credential data* from the PS, the UE may reuse existing N3GPP credential management protocol with PS. For example, possibly to reuse CMPv2, EST protocol to ask CA for signing a SO's certificate or other similar protocols.  
Note: In a SNPN, the decision on which credential management protocol to use may be up to the subscription owner, so that different PS realizations can be used. Different credential management protocols may be used by different PS deployments, depending on the preferences of the SO. It is FFS how a credential management protocol is selected if a PS supports multiple credential management protocols.

6. The UDM triggers to provide the *3GPP configuration subscription data* to the UE after successful on-boarding authentication, e.g. using UPU procedure to send PLMN ID, NID, routing ID, newly assigned SUPI, etc. to the UE, and using UCU procedure to send MM and SM policy to the UE. The UDM may delay triggering after receiving successfully provisioning notification from PS.

7. Upon a successful provisioning in the previous step, the UE releases the configuration PDU session and deregisters from the O-SNPN. The UE initiates a regular procedure, including selection of an SNPN, registration using the provisioned credentials with the SNPN owning the subscription, and PDU Session establishment(s). Depending on the provisioned network credentials the UE may select an SNPN that is the same or different from the SNPN owning the credentials.

Failure case:

4. The UE receives reject message, the reason may include UDM cannot find UE's *default* UE *credential*, authentication failed, etc.

5. UE re-selects *on-boarding information* and try again.

### 6.35.4 Impacts on services, entities and interfaces

The solution could be compatible for external authentication procedure (depending on the outcome on Key Issue #1).

The solution could be compatible for SO's existing provisioning server, e.g. certificate authority (CA).

The solution could have the least modification based on current procedure.

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