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

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

**Source: Siemens, Volkswagen**

**Title: KI#1, Solution to support SNPN access using 3rd party credentials via external Credential Provider – Note on Potential Key Hierarchy Impact**

**Document for: Discussion / Approval**

**Agenda Item:**

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

*Abstract of the contribution:* *KI#1 Solution #8 - Adding text on potential impacts on the key hierarchy when reusing existing AAA servers as external Credential Provider.*

# Discussion

An external Credential Provider CdP may be used in a 5G SNPN, supporting EAP-based primary network authentication (KI#1, see also TS22.804 section 8.2.5.4). In some vertical deployments (e.g., industrial factory networks), the CdP may be a AAA server (RADIUS, DIAMETER) that is already used for WLAN access authentication or IEEE 802.1X authentication. Such a CdP AAA server would implement an EAP authenticator role providing a MSK key as result of the authentication. Support for this scenario seems attractive, as an already deployed security infrastructure can be re-used by an industrial SNPN 5G network deployment. This contribution adds some explanatory text for this scenario and the potential impact on the EAP/5G key hierarchy as hint to future work at SA WG3.

# Proposal

This pCR proposes to add additional text to the solution #8 of TR 23.700-07.

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

## 6.8 Solution #8: SNPN access using 3rd party credentials via external Credential Provider

### 6.8.1 Introduction

This solution addresses key issue 1 "Enhancements to Support SNPN along with credentials owned by an entity separate from the SNPN".

The solution enables UEs to access an SNPN which makes use of a credential management system managed by a credential provider external to the SNPN 5GS.

### 6.8.2 Functional Description

#### 6.8.2.1 Definitions

The following definitions apply to this solution:

**SNPN:** An SNPN which enables access for UEs using credentials owned by an entity separate from the SNPN.

**Credentials Provider (CdP):** An entity, separate from the SNPN that supports that its credentials are used to access an SNPN.

**CdP-ID:** Identifies the CdP that issued the credentials that a UE is using to access an SNPN.

NOTE: Appropriate terminology regarding Credential Provider can be decided in normative phase.

#### 6.8.2.2 Architecture

Figure 6.8.2.2-1 depicts the architecture for the solution, i.e. the SNPN includes a complete 5GS SNPN network and the CdP provides credential management type of functionality.



Figure 6.8.2.2-1: Access to SNPN services using credentials from Credential Provider (CdP) for authentication in the SNPN

Editor's note: Impacts to security architecture and key derivation resulting from the above architecture need to be evaluated by SA WG3.

#### 6.8.2.3 High level principles of the solution

This solution enables UEs to access an SNPN which makes use of a credential management system managed by a credential provider external to the SNPN. The credential management functionality provided by the CdP includes handling of identifiers and corresponding security material used to identify the devices used within the SNPN and to mutually authenticate these devices and the SNPN 5GS. The credential provider will typically correspond with an already existing credential management system owned by the vertical owner of the SNPN 5GS.

The UE is provisioned with non-AKA credentials managed by the CdP, which include an identifier and related security information and the CdP Identifier. The UE initiates registration in the SNPN using a SUPI containing a network-specific identifier, provided by the CdP and provisioned in the UE.

The AMF initiates primary authentication, registration and subscription management procedures for the UE towards the AUSF and UDM of the SNPN based on existing procedures defined in TS 33.501 [7]. It is assumed that there are AUSF and UDM instances within the SNPN supporting the SUPIs of the CdPs (e.g. SUPI ranges or CdP ID) the SNPN has agreements with.

For the primary authentication procedure, the UDM allows the UE to run primary authentication with non-AKA credentials owned by a certain CdP. The UDM indicates to the AUSF to proceed with primary authentication involving the corresponding CdP. The CdP can be a AAA server providing a MSK key resulting from an EAP authentication run.

One possibility is for the SNPN to delegate the authentication server role to the CdP (i.e. the CdP supports AAA functionality). In this case, the AUSF could act as an EAP authenticator, e.g., for a tunnelled EAP method, and interacts with the CdP to execute the primary authentication procedure using the CdP credentials. The AUSF uses a AAA-P/IWF to interact with the CdP. The AAA-P/IWF undertakes any AAA protocol interworking between SBI services used by the AUSF and the AAA protocol supported by the CdP. This allows the AUSF to remain a full SBA entity within the 5GC architecture.

NOTE: Details of the authentication procedure and the key hierarchy are for FFS in SA WG3

For the registration and subscription management procedures, it is assumed that the SNPN has provisioned in the UDM/UDR individual subscriptions for the UEs that use non-AKA credentials from the CdP. Alternatively, the SNPN may use common subscription profiles for these UEs.

Editor's note: It is FFS whether the SNPN needs to provide the UE subscription data at UDM/UDR. If this is required, it is FFS the content in UE subscription data that indexed by SUPI/SUCI generated based on CdP-UE ID. It is FFS how to correlate the UE subscription data in SNPN and UE credentials in CdP.

### 6.8.3 Procedures

This clause shows the interactions to enable UEs to access an SNPN which makes use of a credential management system managed by a Credential Provider external to the SNPN proposed in this solution.



Figure 6.8.3-1: UE registration in SNPN using CdP as authentication server

0. The UE is configured with non-AKA credentials from the CdP e.g. SUPI containing a network-specific identifier, CdP ID and security information, and optionally a list of SNPNs that the CdP has an agreement/SLA with.

It is also assumed that there are AUSF and UDM instances within the SNPN that support the SUPIs of the CdPs (e.g. SUPI ranges or CdP ID) the SNPN has agreements with. The AMF selects these AUSF/UDM instances based on information locally configured in the AMF or provided by the SNPN NRF.

1. The UE selects the SNPN and initiates UE registration in the SNPN. The UE creates a SUCI based on the SUPI provided by the CdP and provisioned in the UE.

NOTE 1: It is assumed that the SUPI provisioned by the CdP is on NAI format and includes also the CdP ID in the domain part of the NAI, e.g. UEID@CdPID. Whether the SUPI within the SUCI is encrypted is FFS in SA WG3.

2. The AMF within the SNPN initiates primary authentication for the UE using a Nausf\_UEAuthentication\_Authenticate service operation with the AUSF as currently specified in TS 33.501 [7]. The AMF selects an AUSF based on the SUCI presented by the UE as specified in TS 23.501 [4].

3. The AUSF checks with UDM within the SNPN for the authentication method to be executed for the UE using a Nudm\_UEAuthentication\_Get service operation as currently specified in TS 33.501 [7]. The AUSF selects a UDM also using the SUCI provided by the AMF as specified in TS 23.501 [4]. The UDM resolves the SUCI to the SUPI before checking the authentication method applicable for the UE.

4. The UDM provides the AUSF with the UE SUPI and the applicable authentication method for the UE. In this case, the UDM indicates to the AUSF to run primary authentication with non-AKA credentials owned by a certain CdP. The UDM provides the AUSF also with the address of the CdP if required.

NOTE 2: The SNPN may support credentials managed by different CdPs.

5. Based on the indication from the UDM, the AUSF interacts with the CdP to execute the primary authentication procedure. The AUSF uses a AAA-P/IWF to interact with the CdP. The AAA-P/IWF undertakes any AAA protocol interworking between SBI services used by the AUSF and the AAA protocol supported by the CdP.

NOTE 3: In this case, the AUSF is not exposing primary authentication services externally to the SNPN 5GS but rather the AUSF is consuming primary authentication service from an authentication server external to the SNPN based on SNPN configuration.

Editor's note: It is FFS whether CdP is a 5GC NF since the CdP can use the SUPI in step 5.

6. The UE executes the applicable authentication method with the CdP.

7. After successful authentication, the AMF is provided with the successful indication together with the SUPI of the UE and the resulting security key.

NOTE 4: Details of the authentication procedure are for FFS in SA WG3. This includes potential impacts on key hierarchy, the possibility to use a tunnelled EAP method to allow using, as CdP, a AAA server exporting a MSK key, and how UE is aware of key hierarchy to be used.

8. After successful authentication, the AMF continues with the registration procedure for the UE in the SNPN. The AMF selects a UDM based on the UE's SUPI to perform AMF registration and subscription management procedures with UDM. The SNPN may have provisioned individual subscriptions for the UEs that use non-AKA credentials from the CdP in the UDM/UDR. Alternatively, the SNPN may use common subscription profiles for these UEs.

NOTE 5: The details of how subscriptions for UEs that use credentials from the CdP are provisioned/managed within the UDM/UDR are Out of Scope of this solution.

9. The AMF completes the registration procedure in the SNPN. The security keys result from the primary authentication procedure using CdP non-AKA credentials are used for subsequent security procedures within the SNPN (i.e. Security Mode Command).

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