**3GPP TSG-SA3 Meeting #104-e Ad-hoc** ***S3-213474-r1***

**e-meeting, 27 – 30 September 2021**

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

**Title:** **Proposal for a solution to KI#4.**

**Document for: Approval**

**Agenda Item:** **5.4**

# 1 Decision/action requested

***The contribution proposes a new solution to KI4***

# 2 References

[1] 3GPP TR 33.857:” Study on enhanced security support for Non-Public Networks”

[2] 3GPP TR 23.700-07:” Study on enhanced support of non-public networks”

# 3 Rationale

This CR is a resubmission of S3-212769 which aims to provide clarity of the configuration proposed as one of the conclusions discussed for KI4. It incorporates comments from SA3-104e. As commented in last meeting, it has similarities with configurations already standardized in TS 33.501 but aim to provide visibility of the proposed conclusion.

This CR provides a solution to KI#4 which enables the possibility to execute mutual authenticate between an onboarding UE and the onboarding network during registration without involvement of the default credential server. Subsequently industry specific protocol for provisioning of credentials can be used.

# 4 Detailed proposal

It is proposed that SA3 agree the below pCR for inclusion in the TR [1].

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

## 6.Y Solution #Y: Secure mutually authenticated onboarding without DCS

### 6.Y.1 Introduction

This solution addresses key issue#4 Securing initial access for UE onboarding between UE and SNPN. The scope of the solution is limited to cases, in which the subsequent onboarding shall be executed using a restricted PDU session.

The aim of the solution is the reduce the complexity of deploying the 3GPP technology into already well-defined ecosystems which includes provisioning schemes. That could be OPC UA or another industry specific provisioning protocol or framework. The actual provisioning protocol is out of scope for this solution.

In this solution each UE is equipped with a private key and a UE default certificate issued by a CA run e.g. by the device manufacturer.. During UE onboarding the O-SNPN can execute primary authentication and verify the UE default certificate without involvement of a DCS. The CA certificate for the verification of UE default certificate as well as the identity of the onboarding UE is configured at the O-SNPN prior to onboarding.

The final provisioning of the SO-SNPN credentials including mutual authentication between UE and Provisioning Server (PS) is preformed over an industry defined protocol or framework.

### 6.Y.2 Solution details

Figure 6.Y.2-1 shows a generalisation of the solution.



**Figure y19.Y.2-1: initial access and provisioning.**

Prior to onboarding the UE is provisioned with default credentials, e.g. during manufacturing, and the UDM is provisioned with onboarding records containing information to verify the UE default credentials.

1. The UE sends a Registration Request including a SUCI to the network.

2. AMF / SEAF forwards request to AUSF.

3. Based on the received SUCI the AUSF concludes that the UE wants to execute authenticated access and selects a corresponding EAP-TLS method configured.

4. UE and AUSF execute EAP based authentication using the selected EAP-TLS method. This is following the procedure in TS 33.501 [2]. The PKI of the UE default and server certificates are out of scope.

5. Before the last step of the EAP procedure the AUSF calculates KAUSF and KSEAF as defined in TS 33.501 [2], i.e., The MSK resulting from the executed EAP session is used as input for the derivation of KAUSF.

6. The AUSF returns response message including EAP Success message, KSEAF and SUPI.

7. AMF / SEAF finalizes the EAP session towards the UE.

8. SEAF calculates the KAMF as specified in 3GPP TS 33.501 [2].

9. UE calculates all 5G keys according to the definitions in TS 33.501 [2].

10. UE and AMF establish security context as defined in TS 33.501 [2].

11. The UE and PS establishes a secure connection utilising an industry specific protocol. The same protocol is utilised to provisioning the device specific credentials to the device.

The actual provisioning of the subscriber profile is executed subsequently and outside the scope of this solution.

6.Y.3 System impact

No system impact identified.

6.Y.4 Evaluation

This solution provides the options to authenticate a device without interaction with a DCS by using already standardised methods in TS 33.501 [2] in the context of SNPN. . It enables the UE and O-SNPN to mutually authenticate and hereby establish a security context, which might be further utilised for provisioning. This can be achieved without involvement of the DCS; i.e., without the need for integration between the O-SNPN and DCS. The default credentials needs to be provisioned to the UE prior to onboarding. w

The solution enables an SNPN provider to utilise an industry specific protocol for provisioning of credentials but still enable mutual authentication to create the security context of the transport layer.

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