**3GPP TSG-SA3 Meeting #103-e** ***S3-211732-r2***

**e-meeting, 17 - 28 May 2021**

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

**Title:** **Evaluation and system impact for solution 19**

**Document for: Approval**

**Agenda Item:** **5.12**

# 1 Decision/action requested

***The contribution proposes to add evaluation and system impact to solution 19***

# 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] GSMA SGP.21 eSIM Architecture Specification, <https://www.gsma.com/esim/esim-specification>

[4] Bootstrapping Remote Secure Key Infrastructures (BRSKI), https://datatracker.ietf.org/doc/draft-ietf-anima-bootstrapping-keyinfra/

# 3 Rationale

This pCR provides update to the System Impact and Evaluation sections of Solution 19.

# 4 Detailed proposal

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

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

## 6.19 Solution #19: Secure onboarding without client authentication

### 6.19.1 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.

In this solution one-way authentication including 5G key hierarchy is executed. The main difference to other solutions is that the network does not authenticate the UE, e.g., no peer authentication is applied during EAP-TLS authentication, The main difference of the modified variant with respect to EAP-TLS is that it does include server authentication only, but no client authentication.

That is, no default credentials or default credential server needs to be involved. Default credentials will be used only during the actual provisioning step, which is outside the scope of this solution.

### 6.19.2 Solution details

Figure 6.19.2-1 shows a generalisation of the solution.



**Figure 6.19.2-1: initial access and sharing of identity.**

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 unauthenticated access and selects a corresponding EAP-TLS method configured without client authentication. The selection of the EAP method might be carried out by the AUSF, or the AUSF might invoke the UDM for this (not shown in Figure 6.19.2-1)

4. UE and AUSF execute EAP based authentication using the selected EAP-TLS method. This is following the procedure in TS 33.501 [2] described for EAP-TLS except that the selected EAP-TLS method without client authentication.

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 EMSK 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. The SUPI is set to a predefined constant value, which indicates to the SEAF that the UE has not been authenticated.

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

8. SEAF calculates the KAMF as specified in 3GPP TS 33.501 [2] with the difference that not a real SUPI, but a reserved string is used as input to the key derivation function. The calculation of the remaining 5G keys is according to 3GPP TS 33.501 [2].

9. UE calculates all 5G keys according to the definitions in TS 33.501 [2], with the difference that not a real SUPI but the same reserved string also used by the SEAF is used as input to the key derivation function.

After the one-way authentication has been executed, the UE can request a restricted PDU Session as studied in TR 23.007-7 [3] and currently standardized in TS 23.501 [4]. The actual provisioning of the Subscriber profile is executed subsequently and outside the scope of this solution.

Editors note: The security implications of skipping client authentication is FFS.

Editors note: The impact on the authentication procedure if the UDM is not involved in the choice of authentication method is ffs.

Editors note: It is ffs how the root certificate used to verify the O-SNPN server cerifificate is pre-provisioned in the UE.

Editors note: Interoperability between different authentication method and identification of potential bidding down attacks is FFS.

Editors note: The construction of SUCI based on information provisioned to the UE is FFS.

### 6.19.3 System impact

The solution has impact on the following system components:

UE: Support of EAP-TLS without client authentication

### AUSF: Support of EAP-TLS without client authentication6.19.4 Evaluation

This solution provides an approach for how an onboarding UE can attach to an onboarding network without usage of a default credentials server. It relies on one-way authentication, i.e. the UE authenticates the network, but the network does not authenticate the UE.

Unauthenticated UE could connect to the onboarding network for purposes other than provisioning but can be prevented by restricting onboarding connectivity to trusted provisioning servers as one solution among others In this solution, UE is not authenticated. This means an adversary can register any number of UEs and exhaust the resources in the onboarding network. Furthermore, such registered malicious UEs can be used to send any amount of control plane messages to the NFs in the onboarding network, the implications of which has not been fully studied

The solution could be used for initial access for provisioning protocols like the consumer variant of GSMA RSP [3]. GSMA RSP is self-contained and doesn’t have any security requirements for the transport layer. Omitting client authentication will minimise the need for adaptation, when the protocol is self-contained from a security perspective.

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