**3GPP TSG-SA3 Meeting #104 AdHoc-e *draft\_S3-213452-r2***

**e-meeting, 27 - 30 September 2021** Revision of S3-20xxxx

**Source: Intel**

**Title: Proposal for conclusion for Key Issue 4**

**Document for: Approval**

**Agenda Item: 5.4**

# 1 Decision/action requested

***It is proposed to approve the conclusion to key issue 4 in TR 33.857***

# 2 References

[1] 3GPP TS 33.501: "Security architecture and procedures for 5G System."

[2] IETF RFC 5216: "The EAP-TLS Authentication Protocol".

[3] S3-211573: "Updates to solution 14: Removal of Editor's notes: Certificate Handling."

# 3 Rationale

# This pCR proposes the conclusion of KI #4, Securing initial access for UE onboarding. There are multiple solutions proposed to address KI-#4 for securing the initial access for UE onboarding that can be categorized as follows:

1. with primary authentication performed between the UE and the DCS in the role of AAA authentication server via the NSSAAF.
2. with primary authentication performed between the UE and the AUSF in the OSNPN. In this configuration, the UE uses a digital certificate to authenticate with the OSNPN, but there is no interaction with the DCS during the primary authentication procedure. The PKI is out of scope.
3. With primary authentication performed between the UE and the AUSF in the OSNPN, followed by a secondary authentication with the DCS in the role of AAA server. In this configuration, the AUSF is configured not to request the UE's client certificate during primary authentication (e.g., because the OSNPN has no NSSAAF supporting interworking with legacy protocols).

SA2 is currently working on the following architecture and has concluded some of the aspects related to the architecture, as shown in the following diagram.



**Figure 1: Initial Access for onboarding using NSSAAF based Primary Authentication only**

NSSAAF (acts as an intermediate function) is enhanced to support an AAA interface to a 3rd party credential holder in the Device Manufacturer's domain.

For Option in figure 1, in general, the O-SNPN interacts with the DCS to perform primary authentication. Based on the UE identifier received from the O-SNPN. The authentication method can be either AKA-based (5G AKA or EAP-AKA'); the selected EAP method shall be a key-generating EAP method that provides mutual authentication. There is a need to specify an interface between the O-SNPN and the DCS for these solutions to perform primary authentication. SA2 has agreed to enhance NSSAF's functionality to support 5GS aware AAA server functionality, as shown in figure 1.

**Observation 1: An SNPN that takes the role of O-SNPN may not necessarily have a deployed NSSAA function.**

 Another option proposed in SA2, as shown in figure 2, requires DCS owners to support a service-based interface as defined by 3GPP. In this Option, When the DCS includes an AUSF and a UDM, the AMF uses N12 towards AUSF and N8 towards UDM using N32 and SEPP.



**Figure 2: Initial Access for onboarding using Primary Authentication over N32**

**Observation 2: Mandating device manufacturers supporting a 3GPP-defined new interface and mimicking the role of AUSF or UDM with N32 support puts the burden on device manufacturers.**

For option 2, primary authentication is performed using UE's self-signed certificate and network certificates. However, whether O-SNPN has an NSSAA function(upgraded with legacy AAA interface) is the real issue. The basic assumption in this key issue is that UE already has default credentials, aka device manufacture's credentials, aka DCS credentials issued by DCS authority. If UE already has DCS credentials, UE can still use these during primary authentication with DCS provided O-SNPN has deployed the NSSAA function. Furthermore, it is unclear how UE decides to send a self-signed certificate or any other certificate for primary authentication.

**Observation 3: For option2, i.e., mutual authentication with UE's self-signed certificate, the real issue is whether O-SNPN has an NSSAA function (upgraded with legacy AAA interface). If UE already has DCS credentials, UE can still use these during primary authentication with DCS provided O-SNPN has deployed the NSSAA function**

For option 3, During the Registration procedure, UE authenticates the network with one-way primary authentication of O-SNPN using an appropriate EAP method, e.g., EAP-TLS. The mutual authentication required between DCS and UE is provided as part of the secondary authentication shown in figure 2

 

**Figure 3: Initial Access for onboarding using both Primary and Secondary Authentication**

The one-way primary authentication, whereby only the UE authenticates the network, is sufficient for generating key material used to derivate the NAS and AS keys for signaling protection to prevent MITM attacks. From the perspective of key derivation (for both NAS and RRC keys), it is irrelevant whether one-way or two-way authentication was used during primary authentication. Therefore, all key hierarchy and derivation remain the same as defined in 33.501.

The mutual authentication between UE and O-SNPN is performed via secondary authentication relying on the DCS credentials. The UE is allowed to set up a PDU session for U-plane provisioning but with limited connectivity. The AUSF, SMF, and UPF can be isolated on a distinct network slice dedicated to UE onboarding to mitigate further security issues. If the UE receives slice information (i.e., S\_NSSAI) from AMF during Registration, it uses it as part of PDU Session establishment.

Option 3 based solutions avoid putting a burden on the DCS to support a service-based interface for onboarding, e.g., when the DCS is owned by a device vendor supporting a traditional AAA interface based on Diameter or RADIUS protocol

**Observation 3: Irrespective of one-way or mutual primary authentication, in both cases, the key material for AS and NAS security is generated**

During previous meetings, comments were raised for one-way authentication related to any third party acquiring an O-SNPN certificate. We believe this issue exists in both one-way and two-way authentications. Furthermore, this issue of fraudulent certificates is almost non-existent, as explained below.

Organization validated (OV) certificates require identity and authenticity verification. Domain validation (DV) certificates are issued based on proof of control over a domain name. With this approach, a confirmation email to one of the approved email addresses, a phone or snail mail, or any other verified manual process is used to verify the domain ownership. If the administrator approves, then the certificate is issued. If confirmation using the procedures mentioned above is not possible, then any other means of communication and practical demonstration of control are allowed. Extended Validation (EV) certificates also require identity and authenticity verification but with very strict requirements. Validation procedures are extensively documented, leaving much less room for inconsistencies. After successful validation, the CA issues the certificate. In addition to the certificate itself, the CA provides all of the intermediary certificates required to chain to their root of trust.

EV Certificates cannot be obtained by individuals or rogue entities, or non-incorporated entities. When fraudulent certificate requests are submitted, CAs tend to maintain a list of domain names and refuse to issue certificates for them without manual confirmation. EV certificates can be used to provide certificates to O-SNPN by subordinate CA's or CA's.

**Observation 4: EV certificates can be used to provide certificates to ON by subordinate CA's or CA's. When fraudulent certificate requests are submitted, CAs tend to maintain a list of domain names and refuse to issue certificates for them.**

To further ascertain the security of one-way authentication, O-SNPN with a business relationship with Intermediate CA and Registration Authority can use the following certificate extensions.

Name constraints [3]: The Name Constraints extension can be used to constrain the identities for which a CA can issue certificates. Identity namespaces can be explicitly excluded or permitted. This allows an O-SNPN to obtain a subordinate CA that can issue certificates only for the O-SNPN-owned domain names. This CA can't issue certificates to random namespaces.

Signed Certificate Timestamps (SCT)[3]: UEs can enforce an SCT policy to verify signatures and consider the certificate trusted.

Extended Key usage and named constraint can be used together for intermediate certificates to avoid arbitrary public certificates for fraudulent O-SNPN.

**Observation 5: SCT, Extended Key usage, and named constraint can also be used together for intermediate certificates to avoid arbitrary public certificates for fraudulent O-SNPN and provide a reliable authentication/verification mechanism of server certificates' one-way authentication**.

Alternative conclusions proposed that Key issue 4's conclusion should be based on key issue 1. We want to point out that both use cases are different with different architecture in mind. In Key issue 4, the AAA server or DCS is from the device manufacturers, while in key issue 1, the AAA server is, e.g., an enterprise server. Enterprise server maintains the subscription profile of 5G private network, and UDM stores the subscription. An SNPN that takes the role of O-SNPN may not necessarily have a deployed NSSAA function (e.g., if it does not support enterprise use case scenarios). It is erroneous to assume that the NSSAA function is available in a network deployment because it is supported in the specification.

**Observation 6: Key issue 1 and key issue 4 both have different use-cases and architecture scenarios. Key issue 4 conclusions should not be based on only Key issue 1***.*

# 4 Proposal

Based on the previous analysis, we propose the following 4 options to cater all the deployment scenarios the following:

Security for initial access for UE onboarding between UE and OSNPN can be based on the following configurations

1. with primary authentication performed between the UE and the DCS in the role of AAA authentication server via the NSSAAF.
2. with primary authentication performed between the UE and the AUSF in the OSNPN. In this configuration, the UE uses a digital certificate issued by the device manufacturer to authenticate with the OSNPN, but there is no interaction with the DCS during the primary authentication procedure.
3. with primary authentication performed between the UE and the AUSF in the OSNPN, followed by a secondary authentication with the DCS in the role of AAA server. In this configuration, the AUSF is configured not to request the UE's client certificate during primary authentication (e.g., because the OSNPN has no NSSAAF supporting interworking with legacy protocols).

# 5 Detailed proposal

**\* \* \* \* Start of Changes \* \* \***

7.X Conclusions on KI #4: Securing initial access for UE onboarding between UE and SNPN

Security for initial access for UE onboarding between UE and OSNPN can be based on the following configurations

1. with primary authentication performed between the UE and the DCS in the role of AAA authentication server via the NSSAAF.

2. with primary authentication performed between the UE and the AUSF in the OSNPN. In this configuration, the UE uses a digital certificate to authenticate with the OSNPN, but there is no interaction with the DCS during the primary authentication procedure. The PKI of the default credentials is out of scope.

3. with primary authentication performed between the UE and the AUSF in the OSNPN, followed by a secondary authentication with the DCS in the role of AAA server. In this configuration, the AUSF is configured not to request the UE's client certificate during primary authentication (e.g., because the OSNPN has no NSSAAF supporting interworking with legacy protocols).

4. with primary authentication performed between the UE and the AUSF in the OSNPN. In this configuration, the UE uses a digital certificate issued by the device manufacturer to authenticate with the OSNPN, and there is interaction with the DCS to retrieve the necessary information for the primary authentication procedure.

If the UE already has a subscription (e.g., if it is equipped with an eSIM), the UE can use this subscription to obtain user plane connectivity with a Provisioning Server.

For 5GS aware DCS case, the UE Identity protection can be based on the concealment mechanism dependent on the SIDF offered by the UDM as in the 5GS. For non-5GS aware DCS case, the UE Identity protection can be based on a protection mechanism supported by the DCS (i.e., AAA functions).

Editor's Note: Further Privacy aspects of the Default UE Credentials are FFS.

Editor’s Note: Further conclusion(s) are FFS.