**3GPP TSG-SA3 Meeting #103-e *S3-211573***

**e-meeting, 17 - 28 May 2021** Revision of S3-20xxxx

**Source: Intel**

**Title: Updates to solution 14: Removal of Editor's notes: Certificate Handling**

**Document for: Approval**

**Agenda Item: 5.12**

# 1 Decision/action requested

***It is proposed to approve updates to solution 14 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] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile"

[4] IETF RFC 8659: “DNS Certification Authority Authorization (CAA) Resource Record”

[5] IETF RFC 8894: "Simple Certificate Enrolment Protocol"

[6] IETF RFC 7030: "Enrollment over Secure Transport"

[7] IETF RFC 4210: "Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)"

# 3 Rationale

This pCR proposes a resolution of Editor's notes on solution #14 as follows and provide Evaluation:

Editor's Note: Details on how the server certificates are issued to the O-SNPNs and how the server certificates are authenticated by the UE is FFS.

In the solution proposed below, UE is provisioned with a set of root-of-trust certificate information that UE will use to authenticate the O-SNPN as part of UE onboarding. If the AUSF has a certificate issued by a root-of-trust authority, it includes a single certificate. Otherwise, the AUSF includes a chain of certificates that leads to the root-of-trust authority. The following figure shows a generic view of how the O-SNPN can obtain such a certificate with intermediate Certificate Authority (CA), with which the O-SNPN and the device manufacturer have a business agreement. This is a generic architecture for certificate issuance that is widely used today, and, in that sense, the Editor's note is not needed. We propose to delete it. We also provide further explanations on how O-SNPN can use the following TLS extensions and procedure to obtain certificates and authentication mechanism



**Figure 1: Certificate Lifecycle**

O-SNPN prepares a Certificate Signing Request (CSR) and submits it to the CA of their choice (trusted by business agreement) [3]. A CSR carries the list of hosts that should appear in the certificate, along with a public key and proof of possession of the corresponding private key (via a digital signature). CA then validates subscriber's identity (O-SNPN) using different procedures as per business agreement such as following:

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 or 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 aforementioned procedures 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 will provide 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.

Many protocols already exist, which use the above certificate lifecycle process and DV, OV, and EV certificates. Protocols are well documents in this [5], [6], [7].

**Observation 1: 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 as per [3].

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 will allow 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 also can be used together for intermediate certificates to avoid arbitrary public certificates for fraudulent O-SNPN.

**Observation 2: 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.**

Authentication in TLS is generally done via a unified set of protocol messages. Certificate authentication involves two messages: first, an appropriate certificate is sent in the Certificate message, followed by CertificateVerify to prove private key possession. Handshake integrity is verified via the Finished message, which both sides send when the handshake is complete. CertificateVerify message is used to prove possession of the private key corresponding to the certificate sent earlier in the handshake. This message is sent immediately after the certificate and must be followed by the Finished message. The Finished message is the last message sent in every handshake. To verify the handshake integrity, the client and server both send cryptographic signatures of the exchanged data. The handshake proceeds only if the signatures can be verified. Any other result would imply a modification of the network traffic by a third party.

**Observation 3: To verify the handshake integrity, server sends cryptographic signatures of the exchanged data. The handshake proceeds only if the signatures can be verified. Any other result would imply a modification of the network traffic by a third party.**

UE and O-SNPN follow the TLS authentication as per RFC and as per above.

**Proposal 1: Based on the aforementioned explanation it is proposed to delete the Editor’s note on how certificates are issued to the O-SNPN with a note added**.

# 4 Detailed proposal

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

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 33.501: "Security architecture and procedures for 5G System"

[3] 3GPP TR 23.700-07: "Study on enhanced support of non-public networks (Release 17)"

[4] 3GPP TS 23.501: "System Architecture for the 5G System"

[5] IETF RFC 5281: "Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)"

[6] 3GPP TS 23.502: "Procedures for the 5G System (5GS)"

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

…

[x] <doctype> <#>[ ([up to and including]{yyyy[-mm]|V<a[.b[.c]]>}[onwards])]: "<Title>".

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*Next Changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

6.14 Solution #14: Initial access for UE Onboarding for an SNPN from Onboarding SNPN using primary and secondary authentication

6.14.1 Introduction

This solution addresses key issue 4," Securing initial access for UE onboarding between UE and SNPN," for devices without UICC and figure 6.Y.1-1 shows a general use-case for this key issue. The actual provisioning mechanisms are outside the scope of this solution. In this solution, UE authenticates network using one-way authentication as part of authentication procedure and performs mutual authentication with DCS using any EAP method as part of secondary authentication.

When the UEs are deployed without a provisioned subscription, it provides a solution on how UE subscription/credentials are afterward provisioned to the UEs. The solution enables UEs to get network connectivity to an O-SNPN ("onboarding SNPN") so that it can be provisioned with necessary subscription credentials and configuration for the SO-SNPN that will own the UE's subscription ("SNPN owning the subscription"). The solution removes the complexity of O-SNPN by avoiding the need for any new Control plane interfaces, the connectivity between the O-SNPN and DCS relying on the existing interface for secondary authentication. ****

**Figure 6.14.1-1: UE onboarding in non-public network**

6.14.2 Solution details

6.14.2.0 General

Following pre-conditions are assumed:

- The UE is provisioned with some default UE credentials and a unique UE identifier at the manufacturing time. The unique UE identifier is assumed to be unique within the DCS. It takes the form of a Network Access Identifier (NAI), which is composed of the user part and the realm part, which may identify the domain name of the DCS. UE is provisioned with set of roots of trust certificate information that UE will use to authenticate O-SNPN during the authentication.

- The UE is not provisioned with *subscription credentials* that grant access to a SO-SNPN.

- The Onboarding SNPN (O-SNPN) that is used by the UE in the onboarding process is not necessarily the same as the SO-SNPN (Subscription Owner SNPN) for which subscription credentials will be provisioned in the UE.

- The O-SNPN operator has access to a Default Credential Server (DCS), which is used to verify that UE is subject to onboarding based on the UE identifier and the associated default UE credentials. The DCS is used for UE authentication/authorization in the O-SNPN during the establishment of a PDU Session for onboarding purposes. The DCS owner is out of this document's scope and can be inside or outside of the O-SNPN, e.g., DCS can be owned by the device manufacturer, by an SNPN other than the O-SNPN, or by a 3rd party.

In some deployments, the DCS and the Provisioning Server can be the same entity. In deployments where the DCS and the Provisioning Server are different entities, it is expected that they communicate with each other for the purpose of UE authentication based on the default UE credentials via an interface that is outside of this solution's scope.

NOTE 1: Provisioning is out of scope of this solution

The SO-SNPN owning the subscription (SO-SNPN) interacts with the Provisioning Server during the UE onboarding procedure and provides the corresponding UE's subscription credentials and UE's configuration data to be provisioned to the UE. The actual provisioning mechanisms are outside the scope of this solution

Editor's Note: The need for three different authentications and the threats mitigated by each is FFS

****

**Figure 6.14.2-1 UE Onboarding for Remote Provisioning Procedure**

0. UE pre-configuration: The UE is provisioned with default UE credentials that allow for successful UE authentication and a unique UE identifier. A configuration may also include information for selecting SNPN needed to access the provisioning server.

1. Initial access to the Onboarding SNPN:

a. Selection of SNPN: UE selects the O-SNPN based on the indication in SIB broadcasted by O-SNPN (e.g., "Support for onboarding" indicator). In this step, if the UE wants to initiate the UE onboarding, the UE either automatically discovers and selects the O-SNPN network based on the broadcasted information or presents a list of available ONs to the user for manual selection. The UE registers to O-SNPN for onboarding by including an indication in the Registration Request, indicating that the registration is for UE onboarding.   
Editor's Note: The security implications of securing Uu interface with only network auth (i.e., no authentication of the UE) is FFS

b. Registration Procedure: During the registration procedure, the UE provides the UE-specific information, e.g corresponding identity (encoded in SUPI format) to the network. The user may also provide the UE with additional information, such as an application identifier and/or Service Provider Identifier. An authentication using non-AKA (e.g. EAP-TLS) based method is performed. The SUPI is of the type of NAI in the form of username@realm. The "username" shall be either "anonymous" or UE identity can be omitted if the subscriber identifier privacy is required by SNPN. The UE performs the one-way authentication of O-SNPN based on O-SNPN's certificate.

2. Configuration PDU session: UE obtains limited connectivity to the Provisioning Server. In the Configuration PDU Session Establishment Request, the UE includes DCS identity and optionally includes PS identity, SO-SNPN identity, or both. When the UE provides SO-SNPN identity, the SMF in the O-SNPN may decide to override the PS identity provided by the UE and send the new PS identity to the UE in the PDU Session Establishment Accept as PCO parameter. The PS identity received in the PDU Session Establishment Accept overrides any configured PS identity in the device. It is assumed that one and only one Configuration PDU session can be established, and connectivity of this PDU session is limited (cf. RLOS), so that the UE can only access a Provisioning Server.

3. The PDU session establishment authentication/authorization is performed as described in TS 23.502 [6] clause 4.3.2.3 and in TS 33.501[2] clause 11.1.2. Secondary authentication is triggered with the DCS by the SMF during PDU Session establishment. The SMF selects the DCS either based on the DCS identity sent from the UE to the SMF or based on the realm part of the UE identity. It is required that the secondary authentication performed between the UE and the DCS is an EAP authentication that supports mutual authentication

Editor's Note: If the O-SNPN can perform mutual EAP authentication with DCS as part of secondary authentication, it needs to be clarified why such a EAP authentication cannot be performed as part of primary authentication in step 1.

4. The UE discovers the Provisioning Server using the stored PS identity. At this point, the stored PS identity is either the PS identity pre-configured in the UE, or the PS identity entered manually by the user, or the PS identity received by the O-SNPN. If the UE still does not have a stored PS identity, then the UE uses a well-known FQDN to perform PS discovery. The UE provides the provisioning server with the unique UE identifier, optionally the identity of the selected SO-SNPN. The provisioning server discovers the DCS using DCS identity sent from the UE to PS or based on the realm part of the unique UE identity and authenticates the UE and make a secure connection for provisioning with the UE, based on the default UE credentials. Interface between DCS and PS is out of the scope of this solution.  
Editor's Note: The security implications of PS relying on the DCS credentials to authenticate the UE is FFS

NOTE 2: This solution assumes there is trust relationship between DCS and PS. Specifics of the interface between DCS and PS including the aspects of mutual authentication, encryption and integrity protection are out of the scope of this solution.

NOTE 3: When the Onboarding network is the same as SNPN owning the subscription of the UE, the Provisioning Server is owned by the Onboarding Network

5. Upon successful provisioning, the UE releases the Configuration PDU Session and deregisters from the O-SNPN.

6. Upon a successful de-registration, the UE initiates a regular procedure, including a selection of a SO-SNPN, Registration using the provisioned credentials with the SO-SNPN owning the subscription, and PDU Session establishment(s). Depending on the provisioned subscription credentials, the UE may select an SNPN that is the same or different from the SNPN owning the credentials.

6.14.2.1 Using EAP-TLS Authentication Procedures over 5G Networks for initial one-way authentication

Figure 6.14.2.1-1 below shows the EAP-TLS Authentication Procedures over 5G Networks as described in TS 33.501 Annex B.2.1; the difference with respect to the EAP-TLS authentication procedure for one-way authentication is highlighted and described below.

****

**Figure** **6.14.2.1-1: Using EAP-TLS Authentication Procedures over 5G Networks for initial one-way authentication**

Step 1: When the UE sends a registration request with Registration Type as Onboarding, the UE sends an anonymous SUCI described in clause B 2.1.2.2 of TS 33.501 [2].

Step 2: The AMF (SEAF) selects an AUSF and sends the Nausf\_UEAuthentication\_Authenticate Request message to the AUSF, including information to assist the AUSF in selecting the EAP-TLS authentication method for one-way authentication.

NOTE 1: The information to assist the AUSF in selecting EAP-TLS for one-way authentication can be sent as an explicit parameter or can be encoded inside the realm part of the SUCI. Alternatively, the AMF (SEAF) can use a dedicated AUSF for onboarding.

Step 3,4,5: are not required as the AUSF determines the authentication method.

It is required that the secondary authentication performed between the UE and the DCS is an EAP authentication that supports mutual authentication

Step 6,7,8,9: Same procedure as described in TS 33.501[2] Annex B.2.1

Step 10-11: The AUSF replies to the SEAF with EAP-Request/EAP-TLS in the Nausf\_UEAuthentication\_Authenticate Response, which may include a chain of TLS certificates leading to root of trust certificate authority.

Step 12: The UE authenticates the server with the received message from step 8.

.

NOTE 2: The underlying assumption is that the device is configured with a set of root-of-trust certificates at manufacturing time.

NOTE 3: If the AUSF has a certificate issued by a root-of-trust authority, it includes a single certificate in step 10. Otherwise, the AUSF includes a chain of certificates that leads to the root-of-trust authority.

NOTE 4: O-SNPN prepares a Certificate Signing Request (CSR) and submits it to the CA of their choice (trusted by business agreement) [ZZ]. A CSR carries the list of hosts that should appear in the certificate, along with a public key and proof of possession of the corresponding private key (via a digital signature). CA then validates subscriber's identity (O-SNPN) using different procedures as per business agreement.

Extended Validation (EV) certificates[ZZ] can be used to provide certificates to ON by subordinate CA's or CA's. 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 ON by subordinate CA's or CA's.

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 as per [ZZ]. Signed Certificate Timestamps(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.

To verify the TLS handshake integrity, the server sends cryptographic signatures of the exchanged data. The handshake proceeds only if the signatures can be verified. Any other result would imply a modification of the network traffic by a third party.

Step 13-14: If the TLS server authentication is successful, the UE replies with EAP-Response/EAP-TLS in the Authenthentication Response message. The response message does not include the TLS Certificate, and TLS\_certificate\_verify message as the network authentication of the UE is not required.

With one-way authentication where only the UE authenticates the onboarding network, the key material for AS and NAS security is generated following the same procedure as described in TS 33.501[2] Annex B.2.1

6.14.3 System impact

UE:

- During the registration procedure, UE provides information to the SNPN, indicating that the registration is for restricted onboarding service only.

- the UE might have been provisioned with some initial default configuration, including PLMN ID and NID of the SNPN, S-NSSAI, DNN needed to access the provisioning server.

NG-RAN:

- A new indication in SIB to indicate that the SNPN provides access to onboarding service.

5GC:

- SMF to provide Limited connectivity to the provisioning server

- AMF to handle Registration procedure for onboarding

- AUSF to handle one-way authentication

6.14.4 Evaluation

**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*End of Changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***