**3GPP TSG-SA3 Meeting #101-e *S3-202939***

**e-meeting, 09-20 November 2020** Revision of S3-XXXX

**Source: Intel**

**Title: Solution to UE onboarding for non-public networks**

**Document for: Approval**

**Agenda Item: 5.12**

1 Decision/action requested

***It is proposed to approve the solution in TR 33.857.***

2 References

[1] 3GPP TR 23.700-07: " Study on enhanced support of non-public networks ."

3 Rationale

This contribution provides a solution to key issue 3, “Securing initial access for UE onboarding between UE and SNPN ”. The solution is based on Solution 6.5 in TR 23.700-07[1].

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)"

[XX] 3GPP TS 23.501: " System architecture for the 5G System (5GS)"

…

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

**\*\*\*\*NEXT CHANGES \*\*\***

6.Y Solution #Y: UE Onboarding and provisioning for an SNPN from Onboarding SNPN

6.Y.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. 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. Also, the solution can be used to perform UE onboarding via either 3GPP access (i.e., via an O-SNPN) or via non-3GPP access like Wi-Fi, the connectivity between the UE and the Provisioning Server being established via the Internet. 

Figure 6.Y.1-1: UE onboarding in non-public network

6.Y.2 Solution details

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.

- 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 a PLMN 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.

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 as part of a UE provisioning procedure (i.e. result of KI#2)..

 

**Figure 6.Y.2-1 UE Onboarding for Remote Provisioning Procedure**

1. 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 PLMN or SNPN needed to access the provisioning server.
2. Onboarding SNPN:
	1. 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. During the registration procedure, the UE provides the device-specific information, e.g., its default UE credential and corresponding identity (SUPI) to the network. The user may also provide the UE with additional information, such as an application identifier and/or Service Provider Identifier. In this solution, NAS SMC is performed with null algorithms.

Editor’s Note: It is FFS if there are security issues due to use of null algorithms for security over radio interface.

Editor’s Note: Privacy implications of transferring the identity in plaintext is FFS

1. 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.
2. The PDU session establishment authentication/authorization is performed as described in TS 23.502 [XX] clause 4.3.2.3 and in TS 33.501[2] clause 11.1.2. Secondary authentication is triggered by the SMF during PDU Session establishment with the DCS based on the DCS identity sent from the UE to the SMF.
3. 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 may discover and connect the DCS using 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.

NOTE: 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.

1. The Provisioning Server selects the SO-SNPN owning the subscription- and contacts the future SO-SNPN owning the subscription to provide the subscription credentials for access to the SNPN owning the subscription, and may retrieve other UE configuration parameters. The Provisioning Server selects the SNPN owning the subscription in one of the following ways:
	1. If the UE is pre-configured with the identity of the future SNPN, the UE provides this identity to the Provisioning Server.
	2. The Provisioning Server determines the future SNPN by comparing the UE identity with a configured onboarding list.

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

1. The Provisioning Server provisions the UE's subscription credentials for the SO-SNPN and other configuration information into the UE over the secure connection.
Editor’s Note: The provisioning procedure is based on the outcome of Key issue 2’s security requirements and is FFS.
2. Upon successful provisioning in the previous step, the UE releases the Configuration PDU Session and deregisters from the O-SNPN. The UE will then perform SNPN selection and register to the appropriate SNPN as per received configuration and general SNPN selection procedures.
3. Upon a successful de-registration, the device 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.Y.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

Editor’s Note:Further system impact is FFS based on the changes to the solution.

6.Y.4 Evaluation

Editor’s Note: Each solution should motivate how the potential security requirements of the key issues being addressed are fulfilled.

FFS

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