**SA WG2 Meeting #143E S2-20xxxxx**

**24 February-09 March 2021, Elbonia (revision of S2-20xxxx)**

**Source: Ericsson (Rapporteur)**

**Title: KI#4 conclusion from FS\_eNPN moderated email discussion**

**Document for: Approval**

**Agenda Item: 8.2.1**

**Work Item / Release: FS\_eNPN / Rel-17**

*Abstract of the contribution: This contribution proposes changes to KI#4 conclusion inline with the moderated email discussions for the FS\_eNPN open issues for KI#4.*

# 1. Introduction

The FS\_eNPN moderated email discussion is captured in S2-21xxxxx.

# 2. Discussion

## 2.1 Questions and answers for KI#4

The questions and answers related to KI#2 are listed in S2-21xxxx.

## 2.2 Proposed way forward for KI#4

The following includes the propsoed way forward as listed in S2-21xxxxx.

## KI#4-Q1: CP provisioning

Majority stated yes, but a number with a dependency on SA3.

It is proposed to wait for SA3, and if SA3 states it is feasible to include also CP based provisioning for SNPNs.

## KI#4-Q2: Selection of CP or UP

The issue depends on whether CP provisioning is to be supported for SNPNs (see question KI#4-Q1), and if supported then same/similar outcome as for PNI-NPN can be used.

It is proposed to wait for SA3, and if SA3 states it is feasible to include also CP based provisioning for SNPNs, then agree on the same outcome for selection of CP vs UP as for PNI-NPN. EN is removed.

# 3. Conclusion

The proposed way forward for "KI#4-Q1: CP provisioning" proposed to wait for SA3.

The proposed way forward for "KI#4-Q2: Selection of CP or UP" proposed to use same logic as when selection UP or Cp for PNI-NPN.

# 4. Proposal

It is proposed to make the following changes to TR 23.700-07.

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

## 8.4 Key Issue #4: UE onboarding and remote provisioning

### 8.4.1 Conclusions for SNPN case

**UE onboarding for SNPN (Component 1 of KI#4)**

- It should be possible to support a registration procedure that enables support for UE onboarding using Default UE credentials and with an O-SNPN as the Onboarding Network (ON).

Editor's note: In order to support UE onboarding using Default UE credentials and O-SNPN as the Onboarding Network (ON) the distribution of security functions when primary authentication is used should be decided by SA WG3, e.g. whether and how to support the primary authentication based on default credential in case DCS is deployed or not.

- It should be possible that one SNPN can take the role of both Onboarding Network (ON) and SO (Subscription Owner), and it should be possible that the ON and SO are different SNPNs i.e. O-SNPN and SO-SNPN.

Editor's note: DCS is potentially introduced to authenticate a UE with default UE credentials or provide means to another entity to do it. There are two potential mechanisms for DCS to authenticate the UE. 1) DCS interacts with O-SNPN and Network Function in SO-SNPN (Subscription Owner SNPN) is not involved in the authentication procedure. As a result, the SO-SNPN is not directly involved with the authentication procedure but gets informed of its result and then performs remote provisioning. 2) DCS interacts with SO-SNPN and Network Function in SO-SNPN (Subscription Owner SNPN) is involved in the authentication procedure. As a result, the SO-SNPN is directly involved and aware of the result of authentication procedure and performs remote provisioning. SA WG3 needs to evaluate the two above mechanisms from security perspective and provide feedback.

Editor's note: It is up to SA3, whether DCS can interact with PS after the primary authentication for provisioning.

Editor's note: The decision on whether primary authentication is required during initial access to the O-SNPN is dependent on SA WG3 feedback; until this feedback is received, it is assumed that such authentication is required.

- A network authentication mechanism that prevents the UE from performing the UE onboarding procedure with a rogue network needs to be supported.

NOTE 1: How to perform authentication between UE and the network is discussed in SA3.

- During the onboarding registration procedure, the UE registers with its Onboarding SUCI which is based on the Onboarding SUPI. Onboarding SUPI is encoded as a network specific identifier taking the format of a NAI (i.e. user@realm). The SNPN, which interacts with DCS, may determine the corresponding DCS identity or address/domain, based on the input from the UE or when primary authentication is used based on information (e.g. DCS address) locally provisioned at SNPN, using mechanisms similar to those for AUSF and UDM discovery and selection described in TS 23.501 [4].

Editor's note: SA WG3 should provide feedback on whether the UEs permanent identifier (SUPI or SUCI) may be used for finding the DCS identity or address/domain that can authenticate the UE, as well their security properties.

- The DCS can be an entity external to the 5GC of O-SNPN.

- The NG-RAN of the Onboarding network includes an indication for Onboarding enabled in the SIB (per O-SNPN, considering that the NG-RAN can be shared) so that the UE can discover and select an appropriate O-SNPN. The UE may or may not be pre-configured with O-SNPN network selection information (e.g. O-SNPN network identifiers).

NOTE 2: Whether the indication for Onboarding is sufficient or more SIB information is needed can be further discussed in the normative phase.

- Upon registration to an SNPN for Onboarding, the UE provides an indication at RRC level that the RRC connectionis for onboarding. This information will be specified only for SNPN and allows NG-RAN to select an appropriate AMF that supports onboarding procedures.

NOTE 3: RAN WGs can work with SA2 to decide whether handling of RAN-level congestion is feasible.

- Upon registration to an SNPN for Onboarding, the UE provides an indication at NAS level that the registration request is for onboarding to allow AMF to, e.g., select an appropriate SMF and perform other onboarding-related configuration. When UE performs initial Registration for onboarding, the UE does not request to be registered over a network slice and as such the UE does not include Requested NSSAI in either RRC or NAS; it is up to the network to decide which network slice is used for the onboarding and provisioning procedures.

- Using PLMN credentials for UE onboarding and PLMN as Onboarding Network (ON) is already possible.

- Onboarding network should support functionality to restrict usage to only on-boarding service.

- When Onboarding network is O-SNPN, the information required to restrict the usage to only onboarding service is locally configured in the AMF and SMF, and the AMF and SMF restrict the usage when the UE indicates that the registration is for Onboarding (e.g., onboarding registration type) or NG-RAN indicates that the access is for Onboarding.

- When Onboarding network is a PLMN, the functionality to restrict usage is activated for the UE by AMF based on received operator subscription from the UDM. How the subscription profile is defined, e.g. using DNN, S-NSSAI or other information dedicated for onboarding, is up to operator's decision.

- The UE shall initiate de-registration from the on-boarding network after finishing the remote provisioning or the on-boarding network shall initiate the de-registration after successful completion of onboarding or based on timer configured for on-boarding service.

**Remote provisioning for SNPN credentials (Component 2 of KI#4)**

- Usage of a PLMN as Onboarding Network for a UE equipped with a USIM shall be possible. The SO-SNPN credentials can be transmitted to UE via UP connectivity. The UE shall be configured with Default credentials in USIM to register with a PLMN where the UE can register with the Default credentials in order to communicate with the provisioning server;

- The UE may support the Control Plane remote provisioning or the User Plane remote provisioning.

- It is assumed that the UDM (or AAA) of SO-SNPN is provisioned with UE credentials/subscription data when remote provisioning is successfully performed. Existing mechanism for provisioning subscription in UDM/UDR can be reused.

- When User Plane is used for provisioning of SO-SNPN credentials:

- The User plane remote provisioning protocol used and how the UE downloads the SO-SNPN credential from the Provisioning Server (PS) after PDU session establishment in the O-SNPN is out of scope of SA WG2;

- For the provisioning of IMSI accompanied by AKA credentials, GSMA RSP is used, Provisioning Server (PS) can provision the credential to UE over User Plane (UP) connectivity;

- For the provisioning of Non-AKA credentials, the credentials can be provided to UE over UP connectivity;

- A restricted PDU session is supported to be dedicated for the remote provisioning. Upon successful establishment of restricted access PDU session, if the UE still does not have a PS address via any of the methods listed below, the device uses a well-known FQDN to perform PS discovery.

- When Onboarding network is O-SNPN, the information required to restrict the usage is locally configured in the SMF, and the SMF restricts the usage for the UE registered for onboarding.

- When Onboarding network is a PLMN, the functionality to restrict usage is activated for the UE by SMF based on received existing subscription profile from the UDM and on existing policies from PCF, or local configuration.

- When user plane remote provisioning is used, it shall be possible to pre-configure the Provisioning Server (PS) address, SO-SNPN identity on the UE, and it shall also be possible that the O-SNPN provides the PS address to the UE after successful authentication and authorization. The PS address from the O-SNPN shall be integrity protected. The PS address for an SO-SNPN provided by the network is prioritized, if any configured PS address for the SO-SNPN stored in the UE. Provisioning of PS address to the UE can be supported using one of the following methods:

a. SMF may deliver onboarding configuration data as part of extended Protocol Configuration Options (PCO) in PDU Session Establishment Response to UE. This is similar to use of PCO to configure Autoconfiguration server for UE in Wireless and Wireline Convergence (TR 23.716 [28] clause 6.10).

b. Alternatively, onboarding configuration data may be configured in the UE during Registration Procedure.

c. In addition, onboarding configuration data may be configured in the UE using service specific policies subject to UE capabilities similar to what is used for V2X communications as specified in TS 23.287 [29] clause 5.1.1 for ways how parameters may be made available to the UE and TS 23.287 [29] clause 6.2.5 for AF-based service parameter provisioning and TS 24.587 [30] clause 5.2.4 for configuration parameters such as validity timer, server address and geographical area.

- When Control Plane is used for provisioning of SO-SNPN credentials:

- Remote provisioning based on UE Parameters Update Procedure as defined in TS 23.502 [6] can be used for provisioning of credentials and other information to enable access to SO-SNPN. After Registration Complete, while onboarding is still in progress, UPU is imminent, thus, the NAS signalling connection shall not be released. It shall be possible that the SO-SNPN credentials being provisioned are not accessible (e.g. by using an additional credential in the UE) by the onboarding network;

Editor's note: SA WG3 feedback will need to be taken into account for including of the CP based provisioning.

- Control Plane remote provisioning procedure assumes a Provisioning Server that communicates with the 5GC using 3GPP-defined protocols. The Provisioning server has the trusted relationship with the entity owning the subscription data of the UE.

NOTE 4: With control plane provisioning, UE does not make use of PS address.

NOTE 5: SA WG3 may evaluate these mechanisms and provide guidance on appropriateness of use for SNPNs.

Editor's note: SA WG3 to determine whether and how Control Plane based provisioning using UE Parameters Update (UPU) procedure and User Plane provisioning can support devices without UICC i.e. how to secure the provisioned credentials between the PS and an endpoint in ME.

### 8.4.2 Conclusions for PNI-NPN case

**UE Onboarding for PNI-NPN (Component 1 of KI#4)**

- No enhancement for the UE onboarding (component 1 of KI#4) with PLMN credentials used for primary authentication and PLMN network selection are needed for the case of PNI-NPN credentials provisioning.

**Remote provisioning for PNI-NPN credentials (Component 2 of KI#4)**

- At least network initiated remote provisioning of credentials to allow access to PNI-NPN services should be supported in Rel-17;

- Both procedures using Control Plane and using User Plane protocols after establishing PDU session shall be enabled for remote provisioning the PNI-NPN credentials used for NSSAA and/or PDU Session secondary authentication;

The UE may support the Control Plane remote provisioning or the User Plane remote provisioning.

Editor's note: SA WG3 feedback for the suitability of the procedure will need to be taken into account.

Editor's note: whether an extra security layer for protection of credentials between PS and UE is needed should be decided by SA WG3.

- For User Plane remote provisioning:

- The protocol for provisioning of PNI-NPN credentials used for NSSAA and/or PDU Session secondary authentication, i.e. how the UE download the NPN credential from the PS after PDU session establishment in PNI-NPN, is out of scope of SA WG2;

- The PS address and DNN/NSSAI used to access PS may be provided to the UE during or after the Registration procedure;

Editor's note: The vertical may verify the UE before PNI-NPN credential is provisioned to UE, and how this is done should be decided by SA WG3.

- Upon successful remote provisioning of the UE, the UE Subscription Data in the UDM/UDR may be updated to enable the access to the PNI-NPN. The existing procedures are used to update the UE configuration and UE context in the network resulting from the updated UE Subscription Data

Editor's note: for PNI-NPN credentials remote provisioning, whether the 3GPP operator could decide to update the UE Subscription Data (e.g., S-NSSAI, DNN, CAG information) in the UDM/UDR used to access to the PNI-NPN based on the input from the vertical which may be outside 3GPP operator domain should be decided by SA WG3.

- For Control Plane remote provisioning:

- It is assumed that the PS communicates with the 5GC using 3GPP defined protocols.

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