SA WG2 Meeting #139E (e-meeting) S2-2004205r12

Elbonia, 1-12 June 2020 (was S2-200xxxx)

**Source: Qualcomm Incorporated, Orange, Ericsson, Deutsche Telekom**

**Title: Compartmentalise key issue #4**

**Document for: Discussion/Approval**

**Agenda Item: 8.2**

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

*Abstract of the contribution: Key issue #4 has two distinct components that need to be made clear in order to assess solutions and split work responsibilities with other groups inside and outside 3GPP.*

# Discussion

Key issue #4 (UE Onboarding and remote provisioning) has two distinct components that is better to be made clear in order to allow easier solution evaluation but also work split between SA2 and primarily SA3.

In Rel-16 prior to connecting to a Standalone Non-Public Network, UE is required to have a subscription to the network, consisting of:

* SNPN-ID
* Subscriber ID (IMSI or NAI)
* Security credential (Certificate, Password or ‘K for USIM)

The problem statement Rel-17 is how the UE can perform initial access to this SNPN (“onboarding”) only by using “default credentials” and then what procedures need to be followed in order to provision subscription to the UE for SNPN that is required to access.

This is a two component problem and these two components are distinct i.e. different solutions can apply to each one of these two components:

Component 1: 5GS procedures for UE establishing restricted access without SNPN subscription, only for accessing the Provisioning Server

Component 2: Procedures for provisioning of subscription, after this access (see Component 1) is established.

# Proposal

It is proposed to clarify the above in the description of the key issue #4 by reshuffling the text to make clear which goals are for component 1 and which are for component 2.

Implement the following changes in TR 23.700-07.

>>>Start 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 22.261: "Service requirements for next generation new services and markets".

[3] 3GPP TS 22.263: " Service requirements for Video, Imaging and Audio for Professional Applications (VIAPA)".

[4] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

[5] 3GPP TS 23.122: "Non-Access-Stratum (NAS) functions related to Mobile Station in idle mode".

 >>>Next Changes<<<

## 3.1 Terms

For the purposes of the present document, the terms given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

**Default credentials**: Information that the UE have before the actual onboarding procedure to make it uniquely identifiable and verifiably secure.

**Default Credential Server (DCS)**: The server that can authenticate a UE with default credentials or provide means to another entity to do it.

**NPN:** Non-Public Network as defined in TS 23.501 [4]. The terminology NPN refers to both SNPN and PNI-NPN in this TR unless otherwise stated.

**Onboarding Network (ON)**: The network providing initial registration and/or access to the UE for UE onboarding.

**Provisioning Server:** The server that will provision the UE.

**Subscription Owner (SO):** The entity that will as result of the onboarding procedure provide the subscription data for the UE.

**UE onboarding:** Provisioning of information, to a UE and within the network, required for the UE to get authorized access and connectivity to an NPN.

**NPN credentials:** Information that the UE uses for authentication to access a NPN. NPN credentials may be 3GPP credentials or non-3GPP credentials.

NOTE: the definition of terms has the scope to provide a common language compared to the definitions in specific solutions. It is up to solutions to use the common terms, when applicable.

>>>Next Changes<<<

## 5.4 Key issue #4: UE Onboarding and remote provisioning

### 5.4.1 Description

The Key Issue is aiming to study the architecture and solutions to support UE onboarding and provisioning for the NPN. This key issue includes some common aspects such as:

- Means for a UE, that is verifiably secure and uniquely identifiable to 5GS, for onboarding and remote provisioning;

- Support of exposure via APIs to support UE onboarding and remote provisioning, if required.

But also specific aspects for component 1 (UE onboarding i.e. to enable 3GPP connectivity):

- How does the UE discover and select the onboarding SNPN before UE NPN credentials and other information to enable UE to get 3GPP connectivity are provisioned.

NOTE X: Provisioning of PLMN credentials is not in scope of this KI. A UE accessing a PLMN is assumed to have provisioned 3GPP credentials.- How and whether the onboarding SNPN authenticates the UE, and establishes a secure 3GPP connectivity, before the UE's NPN credentials and other information to enable SNPN access are provisioned.

- How to establish a secure connectivity between the UE and the network entity for provisioning the NPN credentials and other information to enable SNPN access, i.e how to enable ciphering and integrity protection of the connection and the authentication of UE at the Provisioning Server.

- How does the 5G system provides and updates in the network the subscription of an authorized UE in order to allow the UE to request connectivity to a desired SNPN.

- Architecture including which NFs are involved, and which scenario(s) the solution is addressing, including:

- Which network entity performs UE's subscription provisioning and where is the network entity located.

- If the network entity performing UE subscription provisioning is external to the SNPN, what is the service-based interface exposed by the SNPN towards that network entity for UE onboarding and provisioning.

And for component 2 (remote provisioning of credentials to allow access to NPN services):

- SNPN case: provisioning of NPN credentials () and other information to enable SNPN access.

- PNI-NPN case: provisioning of NPN credentials for access to specific slice(s) and/or PDU sessions offering NPN services, i.e for Network Slice Specific Authentication and Authorization and/or secondary aauthentication for PDU sessions

- Means to remotely provision the required new or updated information to the UE for enabling the UE to access the NPN using 5GS, including e.g.:

- Triggers and procedures used to initiate the provisioning procedure.

- How the network entity provisions the NPN credentials to the UE.

The associated solutions need to consider the following UE characteristics:

- Before the UE onboarding process there should be information in the UE for it to be "uniquely identifiable and verifiably secure".

NOTE 1: This does not mean the UE is required to support the frequency bands the PLMN deploys for public network.

- A TE might not have an interface that can be used to provision the MT.

NOTE 2: This key issue covers devices with and without a UICC.

NOTE 3: Security aspects should be discussed and confirmed by SA WG3.

NOTE x: For the provisioning of IMSI accompanied by AKA credentials it is assumed that protocol for provisioning in USIM outside 3GPP scope is used, e.g. as specified in GSMA RSP.

NOTE y: The separation in two components 1 and 2 is done for readability.

>>>End of changes<<<