SA WG2 Meeting #140E (e-meeting) S2-2004823r11

Elbonia, 19 August-1 September 2020 (was S2-200xxxx)

**Source: Qualcomm Incorporated, Ericsson**

**Title: KI#4, Interim Conclusions**

**Document for: Discussion/Approval**

**Agenda Item: 8.2**

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

*Abstract of the contribution: Analyses the similarities and difference identified in the solutions documented in TR 23.700-07 for Key Issue #4 and proposes interim conclusions.*

# Categorisation of solutions of KI#4

Key Issue #4 as it has been modified in SA2#139E contains two distinct components (component 1: UE onboarding and component 2: remote provisioning) and applies to both SNPN and PNI-NPN. There are 17 solutions documented in TR 23.700-07 for Key Issue #4 and can be categorised as follows as applying both these two components for SNPN or only to the remote provisioning component for PNI-NPN. One solution (solution 29) is not categorised since it refers to a separate “standalone” topic i.e. indications provided from onboarding SNPN.

1. **For SNPN**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Solutions | UE Onboarding using Default UE credentials in Onboarding SNPN (O-SNPN) (NOTE) | UE Onboarding using PLMN credentials and PLMN as ON | UE Onboarding with no credentials for primary authentication | Remote Provisioning (CP) | Remote Provisioning (UP) |
| 5 | X |  | X |  | X |
| 6 | X |  |  | X |  |
| 27 | X |  |  | X | X |
| 30 | X |  |  | X |  |
| 31 | X | X |  |  | X |
| 33 |  | X |  |  | X |
| 34 |  | X |  |  | X |
| 35 | X |  |  | X | X |
| 36 | X |  |  |  |  |
| 37 | X |  |  |  |  |
| 39 |  | X |  |  | X |
| 40 | X |  |  |  | X |

For onboarding (component 1), there are three different options that have been proposed:

* UE Onboarding using Default UE credentials (non-3GPP) and O-SNPN as Onboarding Network (ON)
* UE Onboarding using 3GPP PLMN credentials (IMSI, AKA) and PLMN as Onboarding Network (ON)
* UE Onboarding using no primary authentication credentials and O-SNPN as Onboarding Network (ON)

For remote provisioning of SO-SNPN credentials there two categories of solutions:

* Using Control Plane methods for remote provisioning, meaning some modifications in the UE Configuration Update or UE Parameter Update procedure
* Using User Plane protocols after the UE establishes a PDU session as per the UE onboarding procedures listed above

NOTE: The following definitions are assumed as defined in TR 23.700-07:

**Default UE 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 UE 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.

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

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

**Provisioning Server:** The server that provisions the authenticated/authorized UE with the subscription data and optionally other configuration information.

**Subscription Owner (SO):** The entity that stores and as result of the UE Onboarding procedures provide the subscription data and optionally other configuration information via the PS to the UE.

Given the UE onboarding and remote provisioning components are rather distinct up to a point is possible to combine the use of UE onboarding option with either control or user plane remote provisioning as explained in the figure below.

Primary authentication using

Default UE credentials in O-SNPN

Primary authentication using

PLMN credentials in PLMN ON

No primary authentication

User plane protocols

Using control plane

procedure e.g.

UPU, UCU

UE Onboarding (component 1)

Remote Provisioning (component 2)

1. **For PNI-NPN**

|  |  |  |  |
| --- | --- | --- | --- |
| Solutions | Onboarding | Provisioning (CP) | Provisioning (UP) |
| 7 |  |  | X |
| 27 |  |  |  |
| 28 |  | X | X |
| 31 |  |  | X |
| 32 |  | X |  |
| 33 |  |  | X |
| 38 |  | X |  |

For PNI-NPN, there is no UE onboarding concept, since the UE always has access to the PLMN using its UICC-stored/ PLMN credentials and the purpose is to provision credentials used for secondary authentication (NSSAA or secondary PDU session authentication). It is therefore assumed that UE will get initial connectivity following normal PLMN access procedures and then it can be provisioned with NSSAA or secondary PDU session authentication.

For provisioning of NSSAA or secondary PDU session authentication there are also two approaches:

* Using Control Plane methods for remote provisioning, meaning some modifications in the UE Configuration Update or UE Parameter Update procedure
* Using User Plane protocols after the UE establishes a PDU session as per the UE onboarding procedures listed above

Primary authentication using

PLMN credentials

User plane protocols

Using Control

Plane procedure

e.g. UPU, UCU

UE Onboarding (component 1)



N/A

Remote Provisioning (component 2)

# Analysis of solutions and proposed interim conclusions

1. **SNPN**

UE Onboarding (Component 1 of KI#4)

As there are three different options for onboarding for restricted access the following interim conclusions are proposed:

* UE Onboarding with Default UE credentials in Onboarding SNPN (O-SNPN) as Onboarding Network (ON) used for primary authentication shall be possible
* For UE onboarding with default credentials the distribution of security functions between the O-SNPN and SO-SNPN should be decided by SA3
* Decision on whether primary authentication by O-SNPN is always needed or absence of primary authentication by O-SNPN should be allowed for UE onboarding to be decided by SA3
* Using PLMN credentials and using PLMN as Onboarding Nework (ON) for UE onboarding is already possible and does not require any further standardisation work

Provisioning (Component 2 of KI#4)

* Both options of using CP procedures and using user plane protocols after establishing PDU session with restricted access shall be enabled from the architecture to perform remote provisioning for SO-SNPN credentials
* User plane remote provisioning protocol used for provisioning of SO-SNPN credentials shall be left out of scope of SA2. TBD in SA3 whether out of scope of 3GPP as well
* Control plane procedures for remote provisioning of SO-SNPN credentials shall be based on existing UE Parameters Update procedure

1. **PNI-NPN**

Onboarding (Component 1 of KI#4)

* No UE onboarding (component 1 of KI#4) is needed for the case of PNI-NPN credentials provisioning since the primary authentication for initial access is based on PLMN credentials

Provisioning (Component 2 of KI#4)

* Both options of using CP procedures and using user plane protocols after establishing PDU session shall be enabled from the architecture for PNI-NPN credentials used for NSSAA and/or PDU Session secondary authentication
* User plane remote provisioning protocol for provisioning of PNI-NPN credentials used for NSSAA and/or PDU Session secondary authentication shall be left out of scope of SA2. TBD in SA3 whether out of scope of 3GPP as well

# Conclusion

It is proposed to document the following text in TR 23.700-07.

>>>>START CHANGES<<<<







# 8 Conclusions

## 8.X Key Issue #4: UE onboarding and remote provisioning

Editor's note: These are \*INTERIM\* conclusions for Key issue #4

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

**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 SNPN credentials can be transmitted to UE via CP or UP. In case UP is used, as described in Solution #39, the UE shall be configured with Default credentials in USIM to attach to any PLMN where the UE can register with the Default credentials in order to communicate with the provisioning server.In case CP is used, as described in Solution #34, the UE shall be remote provisioned with the SNPN credentials via UPU procedure.

- When control plane is used for UE Onboarding then control plane method is used for provisioning of SO-SNPN credentials. Both options of procedures using Contol Plane and using User Plane protocols after establishing PDU session with restricted access PDU session through O-SNPN shall be enabled from the architecture to perform remote provisioning for SO-SNPN credentials and can be used regardless of which Onboarding procedure is used;

- When user plane is used for UE Onboarding (as in component 1), uUser plane remote provisioning protocol used for provisioning of SO-SNPN credentials .How the UE downloads the NPN credential from the Provisioning Server (PS) after PDU session establishment in the O-SNPN is out of scope of SA2 and uses industry developed mechanisms;

- For the provisioning of IMSI accompanied by AKA credentials, GSMA RSP is used, Provisioning Server (PS) can provision the credential to UE over either the aforementioned Control Plane (CP) or User Plane (UP) procedure; and other configuration parameters (NSSAI, DNN used to connect to SNPN) should be transmitted over CP to UE.

- For the provisioning of Non-3GPP credentials, the credentials can be provided to UE over either UP or CP based procedure and other configuration parameters (NSSAI, DNN used to connect to SNPN) should be transmitted over CP to UE;

- Editor’s note: in case DCS is deployed, the architecture to support DCS, e.g. the DCS is connected to SO-SNPN or O-SNPN, may related to security issue and should be decided after receive feedback from SA3. On the other hand, in case DCS is not deployed, the architecture to support authentication for default credentials is related to security issue and should be decided after receive feedback from SA3.

- It shall be possible to pre-configure the Provisioning Server (PS) address, on the UE and it also shall 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 provided by the network is prioritized, if configured and overrides any PS and/or SO-SNPN identity stored in the UE. For this purpose, the PS address shall be part of the onboarding configuration data, which are made available to PCF and/or SMF dedicated to onboarding;

- For User plane method is used, based on local configuration or UDM subscription the remote provisioning can be supported via a PDU session dedicated to the remote provisioning.

- UDM of SO-SNPN may synchronize UE credentials/subscription data with the PS accordingly when remote provisionging is successfully performed;

- If upon succesful restricted access PDU session the UE still does not have a PS address, the device uses a well-known FQDN to perform PS discovery.

NOTE: SA3 may evaluate these mechanisms and provide guidance on appropriateness of use for SNPNs.**UE Onboarding for PNI-NPN (Component 1 of KI#4)**

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

Editor's note: whether an extra security layer for protection of credentials between PS and UE is needed should be decided by SA3.

- 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 SA2;

- The PS address may be provided to the UE during the Registration procedure.

Editor's Note: How the PS address is provided to the UE is FFS.

* Editor’s note: The vertical may verify the UE before PNI-NPN credential is provisioned to UE, and howthis is done should be decided by SA3.
* After the 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.

>>>>END OF CHANGES<<<<