**SA WG2 Meeting SA2-140e S2-2005837r07**

**19th August – 2nd September, 2020, E-meeting (revision of S2-201xxxx)**

**Source: Deutsche Telekom**

**Title: eNPN KI #1 & K2 discussion and proposals for evaluations and conclusions**

**Document for: Discussion / Approval**

**Agenda Item: 8.2**

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

*Abstract of the contribution: This document discusses stage 1 requirements, their applicability to evalutions and consclusions for key issue 1 and key issue 2 and proposes a way forward for evaluations and conclusions.*

# 1 Discussion

**Following observations and proposals based on stage 1 requirements in 22.261 and 22.263:**

*The 5G system shall support operator controlled alternative authentication methods (i.e. alternative to AKA) with different types of credentials for network access for IoT devices in isolated deployment scenarios (e.g. for industrial automation).*

**Observation 1: Although this requiremetn does not use called private network here, it makes clear alternative authentication methods are for isolated deployments only.**

*The 5G system shall enable an NPN to be able to request a third-party service provider to perform NPN access network authentication of a UE based on non-3GPP identities and credentials supplied by the third party service provider.*

**Observation 2: This requiement opens up NPN authentication based on non-3GPP identities and credentials to be possible via a third party service provider.**

**Observation 3: There are no requirements on service contintinuity based on non-3GPP identities and credentials. Only service for this use case which is required is authentication.**

*A non-public network subscriber to access a PLMN service shall have a service subscription using 3GPP identifiers and credentials provided or accepted by a PLMN.*

**Observation 4: This requirements makes clear that PLMN services can only be accessed using 3GPP identifiers and credentials provided or accepted by a PLMN.**

*The 5G system shall enable an NPN to be able to request a PLMN to perform NPN access network authentication of a UE based on 3GPP identities and credentials supplied by the PLMN.*

**Observation 5: This requirement makes clear that when a PLMN is the third party service provider only 3GPP identities and credentials supplied by the PLMN can be used.**

**Proposal 1: Evalution and conclusions (ideally already solutions) shall clearly separate in specific sections the cases when non-3GPP identifiers and credentials are used and when 3GPP identifiers and credentials are used.**

*The 5G system shall support a mechanism for a PLMN to control whether a user of a UE can manually select a non-public network hosted by this PLMN that the UE is not authorized to select automatically.*

**Observation 6: This requirement is applicable to PNI-NPNs only.**

The 5G system shall support a mechanism for a UE to identify and select a non-public network.

NOTE: Different network selection mechanisms may be used for physical vs virtual non-public networks.

**Observation 7: This requirement is applicable to both PNI-NPNs and SNPNs. It does not explicitly mention manual or automatic selection. It is unclear whether PLMN network selection mechnism can include SNPN selection or not.**

**Proposal 2: Send an LS to SA1 to clarify this point.**

**On service continuity (KI#2):**

The 5G system shall support uplink and downlink service continuity maintaining acceptable performance requirements while switching between co-located PLMN and NPN (e.g., due to mobility).

**Observation 8: Based on the above requirements and observations service continuity can**

1. **only be based on 3GPP identifiers and credentials.**
2. **be between a PNI-NPN and its hosting PLMN or**
3. **PLMN subscribers using their services moving from PLMN to SNPN and vice versa.**
4. **be based on dual subscription (via N3IWF).**

**Conclusions to KI#2 therefore can only consider solutions that fulfill above criteria.**

**Proposal 3: Consider above observation as evalution criteria for conclusions to KI#2.**

*The 5G system shall support a mechanism to prevent a UE with a subscription to a non-public network from automatically selecting and attaching to a PLMN or non-public network it is not authorized to select.*

*The 5G system shall support a mechanism to prevent a UE with a subscription to a PLMN from automatically selecting and attaching to a non-public network it is not authorized to select.*

**Proposal 4: Evalution and conclusion shall make sure the above requirements are fulfilled.**

# 2 Proposal

**It is asked to agree on proposals below.**

**Proposal 1: Evalution and conclusions (ideally already solutions) shall clearly separate in specific sections the cases when non-3GPP identifiers and credentials are used and when 3GPP identifiers and credentials are used.**

**Proposal 2: Send an LS to SA1 to clarify whether PLMN network selection mechnism can include SNPN selection or not.**

**Proposal 3: Consider the observation that service continuity can**

1. **only be based on 3GPP identifiers and credentials.**
2. **be between a PNI-NPN and its hosting PLMN or**
3. **PLMN subscribers using their services moving from PLMN to SNPN and vice versa.**
4. **be based on dual subscription(via N3IWF)..**

**as evalution criteria for conclusions to KI#2.**

**Proposal 4: Evalution and conclusion shall make sure that mechanisms are in place to prevent a UE**

1. **with a subscription to a non-public network from automatically selecting and attaching to a PLMN or non-public network it is not authorized to select.**
2. **with a subscription to a PLMN from automatically selecting and attaching to a non-public network it is not authorized to select.**

It is also proposed to update TR 23.700-07 as indicated below.

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

# 7 Evaluation

## 7.1 Key Issue #1: Enhancements to Support SNPN along with credentials owned by an entity separate from the SNPN

### 7.1.1 Evaluation of solutions based on 3GPP identifiers and credentials

Editor’s note: to be completed.

### 7.1.2 Evaluation of solutions based on non-3GPP identifiers and credentials

Editor’s note: to be completed.

**\* \* \* \* Next Change \* \* \* \***

# 8 Conclusions

## 8.1 Key Issue #1: Enhancements to Support SNPN along with credentials owned by an entity separate from the SNPN

### 8.1.2 Conclusions for UEs with an SNPN subscription

Editor’s note: to be completed.

In the conclusion the entity owning the credentials is called Home SNPN (HSNPN) and the owner is a SNPN (identified with PLMN ID + NID).

HSNPN subscriptions are provisioned in the UE.

Editor's note: It is FFS which information is configured in the UE for doing network selection.The information configured in the UE for doing network selection can be updated using any of the existing procedures UE configuration update or UE parameter update or other provisioning methods can be considered by Stage 3 WGs. SIB enhancements to enable the above are FFS.

After UE registers to a SNPN, UE may reselect and register to another SNPN with the new network selection information from HSNPN.

For SNPN subscriptions, non-AKA authentication procedure can be used as described in annex B of TS 33.501 [7].

Editor’s note: An architecture to support AAA interfaces to service provider (SNPN) is pending input from SA3. The recommended architecutre will be decided based on SA3's feeback.

Editor’s note: Registration procedure to support AAA interfaces to service provider (SNPN) is pending input from SA3 and is FFS including the subscription data V-SNPN should use in this scenario.

##  Access to HSNPN services via SNPN is supported following the same architectural principles as specified in TS 23.501 [4] clause 4.2.8 and the SNPN taking the role of "Untrusted non-3GPP access".

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