# FS\_eNPN - SA2 Open issues related to KI#1 and KI#4 and questions for resolving the open issues – moderated e-mail discussion…

Author: Rapporteur

These questions and answers will be used to progress the SA2 work for FS\_eNPN KI#1 and KI#4.

Questions for open issues that require SA3 input has so far been excluded.

# Question KI#1-Q1: Service Providers

**Question**: What different types of service providers can be supported and what network functions can be assumed that these different types of service providers have?

|  |  |
| --- | --- |
| **Company** | **Comments** |
| Ericsson | PLMNs being SP, which have a complete 5GC  Verticals being SP and only have AAA infrastructure.  Verticals being SP and have partial or complete 5GC. Partial would mean AUSF/UDM and possibly SMF/UPF/N3IWF if home routing is needed. |
| InterDigital | Service Provider can be PLMNs or SNPNs which have complete 5GC infrastructure, or “Non-3GPP-network-based” organizations which can issue and verify credentials. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Question KI#1-Q2: Architectures

Several solutions exist proposing different existing or enhanced architectures to support KI#1 and we need to come to conclusions on which of these architectures we should agree on in this study. Example "architectures" proposed are e.g. MOCN, roaming like architecture, and AUSF connecting to "AAA".

**Question**: What existing architectures can be used to support KI#1 and what enhancements are needed on top of these architectures?

|  |  |
| --- | --- |
| **Company** | **Comments** |
| Ericsson | Networks sharing (MOCN) and roaming architectures for PLMNs as SPs.  Roaming architectures for verticals.  SNPN with AAA only interface to SP. |
| InterDigital | Roaming architecture. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Question KI#1-Q3: Service Provider identities

A separate entity providing the subscription can according to existing solutions be PLMNs or verticals that don't have a PLMN id. We should agree on what extra identity or identities that are required and the different formats of these.

**Question**: How to identify the separate entity providing the subscription?

|  |  |
| --- | --- |
| **Company** | **Comments** |
| Ericsson | Introduce a new identity SP-ID.  SP-ID can be in the same form as PLMN id as well as PLMN id + NID i.e., same as SNPN id. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Question KI#1-Q4: Service Providers supported in a SNPN

In release 16 the UE had a subscription tied directly the SNPN identity resulting in that UE could read SIB1 network identities and directly know that it can register to a network with matching SNPN identity. In this key issue the subscription is owned by a separate entity with an identity according to question 1. There need to be a mechanism enabling the UE to make an efficient network selection so that it selects a suitable SNPN.

**Question**: How do UE know what Service Providers are supported in a SNPN?

|  |  |
| --- | --- |
| **Company** | **Comments** |
| Ericsson | Configuration in the UE as described in solution 1 in TR 23.700-07 clause 6.1.  As a complement the NG-RAN can support to broadcast one bit indicating SNPN supports SP credentials as described in solution #2. For further study if NG-RAN also need to support the broadcast of specific SP-IDs for the scenario where the UEs configuration is not up to date. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Question KI#1-Q5: Network Selection

Network selection is defined by CT1 but SA2 should set the requirements for it. We need to understand how to handle multiple subscriptions and based on what subscription is used, what networks should be possible to select.

**Question**: What enhancements to Network selection are required?

|  |  |
| --- | --- |
| **Company** | **Comments** |
| Ericsson | UE with SP subscription need to be able to select SNPN where the SP is supported.  UE with PLMN subscription need to be able to select both PLMN native network and SNPN with support for PLMN as SP.  Priority per SP between different SNPNs and between SNPN and native PLMN network is to be configurable.  Support for multiple subscriptions in the UE and how the UE select what subscription to use. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Question KI#4-Q1: Credentials in scope of provisioning

SA1, in [S1-201087](http://www.3gpp.org/ftp/TSG_SA/WG1_Serv/TSGS1_89e_ElectronicMeeting/Docs/S1-201087.zip), replied to the SA2 question whether provisioning requirement applies to SNPNs for:

1. IMSI accompanied by AKA credentials, both used for SNPN authentication
2. IMSI accompanied by AKA credentials, the IMSI being used to derive a Network Specific Identifier that will be used for SNPN authentication with the AKA credentials

SA1 reply:

"*A1) The quoted requirement applies to non-3GPP identities and credentials only, while SA2’s question refers to 3GPP identities and credentials. As such, the answer is no, the above-quoted requirement does not include provisioning of the mentioned identities and credentials to SNPNs. However, SA1 would like to point out that a requirement for remote provisioning has been included in TS 22.261, clause 6.14.2, since Release 15:*

*The 5G system shall support a secure mechanism for a home operator to remotely provision the 3GPP credentials of a uniquely identifiable and verifiably secure IoT device.*"

The KI#4 describes provisioning of e.g. "information" and "NPN subscription".

**Question**: Is there a need to accommodate the Key Issue description for Onboarding?

Answers:

|  |  |
| --- | --- |
| **Company** | **Comments** |
| Ericsson | The KI description is generic i.e. it allows any type of credentials to be provisioned (i.e. as per SA1 requirements - 3GPP and non-3GPP credentials). There is therefore no need to amend the KI description. |
| InterDigital | Agree that the KI allows both 3GPP and Non-3GPP credentials to be provisioned. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Question KI#4-Q2: Provisioning for PNI-NPN

SA2 also asked about provisioning for PNI-NPN and SA1, in [S1-201087](http://www.3gpp.org/ftp/TSG_SA/WG1_Serv/TSGS1_89e_ElectronicMeeting/Docs/S1-201087.zip), provided answers to the SA2 questions as follows:

*Q2) SA2 would like to verify with SA1 whether the above-quoted requirement applies to PNI-NPN, which is the NPN “hosted by a PLMN” as described in TS 22.261 clause 6.25.1, or not, and what would be the corresponding use cases.*

*A2) SA1 requests clarification on the question from SA2, specifically, is SA2 asking if the above quoted question is related to primary or secondary authentication for the PNI-NPN.*

*Q3) If SA1 confirm the above-quoted requirement applies to PNI-NPN in Q2, SA2 have further Q3 as below.*

*For PNI-NPN, a UE may perform secondary PDU session authentication using 3rd party credentials, if the NPN is integrated in PLMN by means of dedicated DNNs, and/or a UE may perform Network specific slice authentication and authorisation (NSSAA) using 3rd party credentials if the NPN is integrated in PLMN by means of network slice. Given the authentication procedures already specified in TS 23.501, TS 24.501 and TS 33.501, SA2 would also like to ask whether provisioning for identities and credentials used for Network specific slice authentication and authorisation (NSSAA) and secondary PDU session authentication should be considered to be covered as part of NPN service requirement for onboarding and remote provisioning solution.*

*A3) SA1 requests clarification on the question from SA2, specifically, is SA2 asking whether 3rd party credentials may be used for secondary network slice authentication and authorization or*

*Is SA2 asking whether these 3rd party credentials for secondary authentication can be provisioned via the 3GPP system, or is SA2 asking something else.*

**Question**: is it in scope of the study to provision identities and credentials for PNI-NPN (e.g. used for NSSAA or secondary authentication)?

Answers:

|  |  |
| --- | --- |
| **Company** | **Comments** |
| Ericsson | TBD |
| InterDigital | We still think the KI should not apply to PNI-NPN. UE already has PLMN subscription, any procedure to provide additional PNI-NPN related information should not be considered part of “remote provisioning” or “onboarding”. But for the sake of progress, we are OK to accept PNI-NPN in the scope if that’s the majority view and there is no further SA1 guidance. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Question KI#4-Q3: Initial access – AS support

The initial access for onboarding is meant to enable means to achieve connectivity from an Onboarding Network for the purpose of a subsequent provisioning.

The impacts to the Access Stratum for the initial access (assuming so far that there is no impacts for subsequent procedures e.g. for provisioning) is FFS.

Question: What impacts do you foresee needed to the AS to support UE Onboarding?

Answers:

|  |  |
| --- | --- |
| **Company** | **Comments** |
| Ericsson | SIB information to indicate support for onboarding per network.  RRC (e.g. in msg 5) information sent by the UE should identify the need for an onboarding session, in order to enable the NG-RAN node the selection of AMF used for onboarding. |
| InterDigital | SIB information to indicate support for onboarding.  Having additional indication in UE’s RRC message, which advertises the UE is seeking onboarding and remote provisioning, may cause potential security/privacy concerns and needs to be studied by SA3. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Question KI#4-Q4: Assumptions regarding DCS

A DCS has been "defined" as:

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

The ownership of the DCS is FFS e.g. it can be owned by the device manufacturer or a 3rd party affiliated with the device manufacturer or by the ON. The ownership may imply a need for certain functionality or interfaces.

Also, the interfaces used by the DCS is FFS e.g. if SBA services can be assumed to be used by the DCS.

**Question**: What assumptions can be made with regards to the DCS e.g. ownership and type of interfaces/protocols supported?

Answers:

|  |  |
| --- | --- |
| **Company** | **Comments** |
| Ericsson | The architecture should not assume a specific ownership i.e. it should allow for a flexible deployment. Therefore, the DCS should be possible to be deployed without requiring SBA support.  Wherever possible, the architecture should assume that the DCS need not implement 3GPP-specific services, i.e., the architecture should assume support for standardized non-3GPP application-level protocols, e.g., RADIUS, EAP, etc. |
| InterDigital | Agree with Ericsson on the ownership. The interface/protocol between the 3GPP NW and DCS should use “off-the-shelf” protocols.  And in our understanding the default credential authentication may be part of PS so it doesn’t have to be a separate DCS in the architecture.  As a recent development (related to NSSAA) in SA3(incoming LS S3-200821), interface between AUSF and AAA servers is ruled out because of the security requirement to fully isolate different authentication types. This needs to be taken into consideration too. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Question KI#4-Q5: Assumptions regarding Provisioning Server

A PS has been "defined" as:

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

The ownership of the Provisioning Server is FFS, e.g. it can be owned by the device manufacturer or a 3rd party affiliated with the device manufacturer or by the ON.

**Question**: What assumptions can be made with regards to the PS e.g. ownership and type of interfaces/protocols supported?

Answers:

|  |  |
| --- | --- |
| **Company** | **Comments** |
| Ericsson | The architecture should not assume a specific ownership i.e. it should allow for a flexible deployment. However, to enable e.g. appropriate security some relationships between PS and the SO can be assumed. |
| InterDigital | Agree with Ericsson that the ownership should be flexible. An onboarding network may be connected to multiple PSs owned by different parties, and a PS may be connected to multiple onboarding networks. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Question KI#4-Q6: UP or CP used for provisioning?

Solutions for UP and for CP have been discussed and added to the TR.

**Question**: Should UP or CP be used for provisioning, or both be possible?

Answers:

|  |  |
| --- | --- |
| **Company** | **Comments** |
| Ericsson | Both should be possible as they may fit different type of deployments e.g. UP when existing provisioning means defined outside of 3GPP is used and CP when for some reasoning UP cannot be used or is not required to be used. |
| InterDigital | 3GPP should not be burdened with interfaces/protocols for interacting with Provisioning Server in different deployment scenarios and thus UP is preferred. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Question KI#4-Q7: Assumption of subscription in the network

It is FFS whether PEI or another UE identifier is used to identify a subscription that needs to be provisioned in the UE and how the list of UE identifiers is provisioned in the SNPN owning the subscription.

**Question**: How is the subscription that needs to be provisioned in the UE identified and how is it provisioned in the network.

Answers:

|  |  |
| --- | --- |
| **Company** | **Comments** |
| Ericsson | Assume that the UE is able to build an onboarding SUPI derived from some unique UE identifier, such as PEI, MAC address, or Host ID.  Assume that the PS is provisioned with a list of onboarding SUPIs that need to be remotely provisioned. |
| InterDigital | The answer should depend on various solutions. Default credential may serve as UE identifier in the PS in some solutions.  As with SUPI, the UE identifier should be protected against privacy attacks. The solution has to protect the whole UE identifier (unlike SUPI where the routing information is not protected) |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Question KI#4-Q8: pre-configured information in the device

The device (UE) may have been pre-configured with information e.g. to ensure requirement "uniquely identifiable and verifiably secure" is satisfied and information related to e.g. Onboarding Network or Subscription Owner.

**Question**: What information is required to be available in the device prior to onboarding and what information *may* be available?

Answers:

|  |  |
| --- | --- |
| **Company** | **Comments** |
| Ericsson | Information to enable that the UE can be uniquely identifiable and verifiably secure is required to be available, e.g. credentials such that DCS can authenticate the UE.  Additional information may be available e.g. a list of PLMN ID + NID that the UE would use for finding Onboarding Networks to use, however, it must be noted that such assumption requires the UE to be provisioned prior to the onboarding procedure, defeating part of the goal of the onboarding procedure |
| InterDigital | UE may be preconfigured with the default credential(s) and this default credential will be used for authentication/authorization when UE tries to access the Provision Server.  UE doesn’t need to be configured with network selection parameters. UE can select any network that indicates support for onboarding and tries to access the Provision Server associated with the onboarding network. If it can pass the authentication with the Provision Server it means it has selected the right network, otherwise it may select another onboarding network. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Question KI#4-Q9: Restricted connectivity of initial access

**Question**: Is the initial access restricted and if yes, how is it ensured that the initial access is restricted such that it only can be used for onboarding?

Answers:

|  |  |
| --- | --- |
| **Company** | **Comments** |
| Ericsson | RRC information provided by UE makes NG-RAN select an AMF used for onboarding.  AMF controls such that only services required for UE onboarding are used.  For UP solution, the UP communication is restricted to 3-tuple information of available Provisioning Servers. The 3-tuple information can be provisioned in AMF and provided to SMF, pre-provisioned in SMF or by using a PCF. |
| InterDigital | PDU Session for remote provisioning should be controlled by the NW to only access provisioning server. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Question KI#4-Q10: Determination of Subscription Owner and Provisioning Server

**Question**: Who needs to determine the SO and the PS (UE and/or ON)? How is the SO and the PS determined?

Answers:

|  |  |
| --- | --- |
| **Company** | **Comments** |
| Ericsson | TBD |
| InterDigital | This depends on solutions. We should not assume that the UE is preconfigured with identifiers pointing to PS. In fact, having routing information as a part of the identifier (e.g., NAI format) creates an additional privacy threat. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Question KI#4-Q11: Duration of connectivity

**Question**: Is the time duration of the connectivity used for initial access and provisioned controlled by some means that requires standardization?

Answers:

|  |  |
| --- | --- |
| **Company** | **Comments** |
| Ericsson | There is no need to standardize additional means beyond what can be controlled with existing 5G connectivity. |
| InterDigital | Agree with Ericsson. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Question KI#4-Q12: UDM for Onboarding

A UE without any subscription is assumed to be able to perform some kind of registration in ON for the purpose of getting connectivity for UE onboarding.

**Question**: Is there a UDM used during the onboarding procedure and what is then the role(s) of such UDM?

Answers:

|  |  |
| --- | --- |
| **Company** | **Comments** |
| Ericsson | Since UDM is subscription oriented, and in the case of onboarding, there is not yet a subscription provisioned in the UE, our proposal is that UDM plays no role in onboarding procedures within SA2 scope. |
| InterDigital | Agree with Ericsson. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Question KI#4-Q13: Slicing considerations

It is FFS whether any specific slicing considerations are needed.

**Question**: Are there any slicing considerations needed?

Answers:

|  |  |
| --- | --- |
| **Company** | **Comments** |
| Ericsson | A reasonable requirement is for operators to enable a specific network slice for onboarding procedures, so that the onboarding procedure is as much as possible isolated from regular traffic. Therefore, it should not be precluded the onboarding procedure to be executed through an onboarding network slice.  Such onboarding network slice is assumed not to be known by the UE (which is not yet provisioned). The assumption is that the NG-RAN node selects an AMF (perhaps in the onboarding network slice), the AMF selects an SMF and/or AUSF in the same onboarding network slice, the SMF selects a UPF also in the onboarding network slice.  We don't see the need for any additional standardization to enable the above. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Question KI#4-Q14: Assumptions regarding IMS subscription

KI#3 scope is to enable IMS services.

If 5GS level credentials are not available in the UE, then the UE likely got no IMS level credentials either.

**Question**: Can provisioning of IMS level credentials be regarded as in scope of KI#4, and if yes, what additional mechanisms are required to support the envisioned scenarios of IMS deployments?

Answers:

|  |  |
| --- | --- |
| **Company** | **Comments** |
| Ericsson | It can. The additional mechanisms are to be proposed through new or updated solutions to cover the scenarios:  1) 5GS and IMS provider is the same, and  2) 5GS and IMS provider is separate and can use separate credentials, but they have a business relation.  The additional mechanisms required is TBD.  NOTE: it should be also possible to re-use the 5GS level credentials to access IMS domain. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Question KI#4-Q15: Need for de-registration after provisioning?

It is FFS whether in case the ON and the SNPN owning the subscription are the same, there is a need for the UE to de-register, then select the SNPN and re-register or whether other procedures that does not result in de-registering would suffice

**Question**: Is there a need for de-registration after the UE been provisioned with a new subscription?

Answers:

|  |  |
| --- | --- |
| **Company** | **Comments** |
| Ericsson | For the case when UE is provisioned with a new subscription (i.e. UE didn't have one before), then the initial access is limited to UE onboarding and it is simpler to use de-registration e.g. as to ensure that the UE is registering to the appropriate network and to avoid the need to modify a restricted initial connectivity to a connectivity allowing access to normal services. Especially, because the registration is unaware of the regular SUPI, therefore, AMF, SMF, are not applying any regular services or policies to the regular SUPI. |
| InterDigital | Agree with Ericsson. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Question KI#4-Q16: PNI-NPN

Update of PLMN subscription by adding NPN parts of the PLMN subscription may be envisioned as per TS 22.263 requirement:

"*Based on MNO and NPN policy, the 5G system shall support a mechanism to enable MNO to update the subscription of an authorized UE in order to allow the UE to connect to a desired NPN. This on-demand mechanism should enable means for a user to request on-the-spot network connectivity which is authorized by its MNO.*".

**Question**: What interactions between UE and network is required for adding or updating NPN parts of PNI-NPN subscription? What procedures in the network are required that are in SA2 scope?

Answers:

|  |  |
| --- | --- |
| **Company** | **Comments** |
| Ericsson | We assume that updates of PLMN subscription in UDM/UDR is not in SA2 scope i.e. once PLMN subscription is updated based on input from NPN customer then SA2 can assume it is seen as subscription already been updated in UDM.  There are already procedures to provide required subscription data related to NPN to the UE e.g. CAG information and Network Slice information. Separate credentials possibly used for NPN in PNI-NPN case is part of question "Question KI#4-Q2: Provisioning for PNI-NPN". |
| Ericsson | Agree with Ericsson that PLMN subscription update is not in the scope. |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Rapporteur Summary

# Proposed Conclusions

The proposed conclusions will be used to identify solutions for the conclusions of the TR.

<conclusion X>

<conclusion X>

<conclusion X>

<conclusion X>

<conclusion X>