# 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.

Revision history:

Ver2 includes changes addressing comments to the questions from Convida, Orange, Qualcomm, OPPO, Huawei and Futurewei.

As questions are added and changed, please re-send your proposed answers.

Ver3 slightly modifies KI#1-Q5.

Combined version includes input from:

- Ericsson

- Intel

- Alibaba

- OPPO

- Samsung

- MediaTek

- Deutsche Telekom

- China Mobile

- Convida Wireless

- LGE

- Orange

- Qualcomm

- Sony

- Futurewei

- Lenovo

- InterDigital

- vivo

- AT&T

- Nokia

- Cisco

- Philips

- ZTE

- China Telecom

# 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 | We foresee the following type of SPs:  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. |
| Intel | SP can be an SNPN or a PLMN.  The SNPN can either have a full-fledged 5GC or only have AAA architecture. In the latter case there may be a need for protocol interworking between SBA and Radius/Diameter interfaces.  “Home routed”-like architecture (as in Solution #1) should be supported to enable session continuity as UE moves between the SNPN and the PLMN. |
| Alibaba | PLMNs being SP, which have a complete EPC, using the EPC credentials for SNPN, in case there is no 5G PLMN available. |
| OPPO | Have to have SPs that are separate and outside the SNPN or PLMN and provide the credentials that are for that vertical sector that that SP caters for. There can be different types of SPs but interactions to SP should be through off the shelf "open" non-proprietary protocols. |
| Samsung | PLMN/SNPN with at least AUSF/UDM for authentication.  Verticals with an AAA server |
| MediaTek | Only PLMN or SNPN which has full or partial 5GC functionalities (e.g., AUSF/UDM) can be SP.  Given the above, a Service Provider need not be defined. |
| Convida Wireless | The Service Provider could be the MNO/PLMN.  The Service Provider might only have certain parts of a 5GC. A common scenario will be that the Service Provider has an SMF, UPF, and a AAA Infrastructure.  The Service Provider might only have a AAA Infrastructure. |
| LGE | SP can be an SNPN or a PLMN, and also partial or complete 5GC. |
| Orange | The entity owning SNPN credentials not specified by 3GPP has AAA infrastructure not specified by 3GPP. |
| Qualcomm | In this context Service Provider (SP) is assumed to refer to the entity separate from the SNPN that issued the UE's subscription.  SP can be a PLMN or SNPN that has a full or partial 5GC (partial = at least AUSF and UDM).  Partial refers to the case that the SP supports authenticating the UE in the SNPN but does not offer any services so that network functions required for "home-routed" traffic scenarios are not needed. |
| Sony | Verticals could be the SP   1. Complete 5GS 2. Complete 5GC+ shared RAN 3. Partial 5GS 4. Only AAA infrastructure   PLMNs could be a SP |
| Futurewei | 1. PLMN: has 5GC and RAN 2. Verticals providing over-the-top service or other SNPN operators.    1. For the authentication issues of KI #1, this kind of service providers at less have to support AAA functions and may support non-3GPP credential and mechanism. The solution needs to have minimum impact on their existing AAA functions.    2. For mobility scenarios, SMF/UPF are needed, AMF/N3IWF may be needed. |
| Lenovo | PLMNs (deploying 5GS)  SNPNs or Verticals (deploying at least AUSF/UDM, and optionally N3IWF/SMF/UPF).  Verticals with an AAA infrastructure. |
| 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. |
| vivo | SP can be PLMNs, SNPNs with 5GC, or other SP which has its own AAA and doesn’t have 5GC.  SP provide authentication/security for UE to access SNPN. |
| Nokia | Option 1: UDM, AUSF, UDR; Option 2: SP could own all NFs that may be present in an HPLMN); Option 3: light weight SP with just a AAA type server (variant of AUSF)  (In general, we should allow flexibility for different deployment models to avoid too many constraints in the specifications) |
| Cisco | SP can be an SNPN or a PLMN. SP can be an "Identity Provider".  Use of the most commonly deployed authentication and accounting protocols should be allowed, i.e RADSEC authentication and RADSEC accounting. Interworking between SBA protocol on the hosting SNPN and partners should be supported. |
| Philips | The service provider for an NPN may be a mobile operator, MVNO, factory owner, office IT department or any other “3rd party or vertical” interested in operating or making use of an NPN. It can be assumed that the service providers operates a partial or full 5GC. |
| ZTE | For the key issue 1, the Service Provider (SP) has the credentials which is owned by an entity separate from the SNPN.  So at least, the SP may have AAA, or have the UDM and AUSF. The SP can have more NF depend on the services can be provided. (e.g. the SP is a SNPN, so it can have the whole 5GC) |

# 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 for verticals. |
| Intel | Architecture similar to roaming architecture (Solution #1) is sufficient.  In our view, MOCN is not a solution for KI#1 because implying that RAN is owned by one administration while the 3rd party is the 5GC is a stretch.  Assume a shared RAN provides access to 5GC from MNO A, B and C, while the RAN is owned (administered) by MNO A. The MOCN solution implies that all subscribers of MNO B or C are in a situation of “credentials being owned by a 3rd party”, which is in our view not the problem that needs to be solved. |
| OPPO | An architecture that supports external SP and external credential providers (for verticals). As far as possible, keep UE transparent to such architectures if different architectures are to be accepted, e.g. if more than one architecture is chosen, the UE must not need to distinguish one architecture from another. |
| Samsung | Roaming architectures for PLMN  AAA interface to verticals |
| MediaTek | Roaming-like architecture to be re-used for PLMN or SNPN being SP. |
| LGE | Roaming-like architecture |
| Orange | Roaming like architecture should be kept reserved for roaming between PLMNs in order not to disrupt the current roaming model. An SNPN should not expose the interfaces defined for VPLMNs. |
| Qualcomm | Existing 5GS home-routed roaming and local-break out (LBO) architectures with the V-SNPN taking the role of the V-PLMN and the SP taking the role of the HPLMN.  LBO applies to the case where an SP supports authenticating the UE in the V-SNPN but does not offer any services so that network functions required for "home-routed" traffic scenarios are not needed. |
| Sony | Networks sharing (MOCN) and roaming architectures for PLMNs as SPs.  Roaming architectures for verticals.  SNPN with AAA only interface to SP. |
| Futurewei | MOCN, roaming like architecture (this option needs to support non-3gpp credential and AAA mechanism) and AUSF connecting to “AAA” should all be considered as valid options to satisfy different deployment scenarios. |
| Lenovo | Existing roaming architecture (e.g. when SP is PLMN).  Enhancements to roaming architecture (e.g. when SP is SNPN).  New/enhanced architecture for SP with AAA only interfaces.  We do not consider MOCN as valid solution to this KI#1. |
| InterDigital | Roaming architecture. |
| vivo | For SP as PLMNs, or SNPNs with 5GC, roaming architecture is applied.  For SP which has its own AAA and doesn’t have 5GC, whether need an AAA-proxy in the visited SNPN to connect the SP’s AAA is TBD.  MOCN is deployment choice and seems not need to be specified. |
| AT&T | Current roaming model should be preserved and be kept between PLMNs. |
| Nokia | Merge of solution #1 and #2 – our views were reflected in S2-200xxxx-eNPN-Solution2-Update-v1.docx |
| Cisco | Architecture such as Solution #4 is required. For MNOs, architecture as in Solution #1 may be used, but this architecture is not applicable to non-MNO identity providers.  In addition interface for providing subscription/policy information either via the NEF and/or directly to PCF and UDM are needed.  LBO should be the base model. |
| Philips | No preference at this point in time. Requires further evaluation of the different solutions. |
| ZTE | It depends on what entities the SP have in the Q1.  If the SP only have UDM and AUSF, LBO can be applied  If the SP have whole 5GC, home routed or LBO can be applied |

# Question KI#1-Q3: Identifying the Service Providers

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 how to identify these separate entities also called Service Providers

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

|  |  |
| --- | --- |
| **Company** | **Comments** |
| Ericsson | For some solutions e.g. MOCN and AAA-type of solutions there is no need for any separate identifier.  A separate identifier for the Service Provider may be used in relation to roaming architecture solutions.  Introduce a new identity to identify the Service Providers, for the solutions that need it, e.g. SP-ID. Using the same name would make it easier to read and understand the solutions.  SP-ID can be in the same form as PLMN id as well as PLMN id + NID i.e., same as SNPN id.  The SP-ID can be used in relation to SNPN selection, but should be further described in the solutions. |
| Intel | We believe there is no need for any SP-ID to be broadcasted on Uu.  An “SP-ID” is only used in the UE configuration (refer to Solution #1) and can be either a PLMN ID or a (PLMN ID + NID) pair (for PLMN and SNPN, respectively). Also, the realm part of the Network Specific Identifier (encoded as user@realm) may be encoded in a way that uniquely identifies the SP’s realm. |
| OPPO | Use of a new SP-ID, wherein the SP that UE selects is conveyed by UE to AMF AMF to select intended SP.  Resolving the format of the SP-ID can be deferred till a(some) settled architecture(s) is(are) agreed. |
| Samsung | For PLMN, use the PLMN id  For verticals and SNPN, use the PLMN id + NID (same as SNPN id) |
| MediaTek | PLMN ID (PLMN being SP) or PLMN ID + NID (SNPN being SP) are sufficient.  There is no need to distinguish SP from PLMN/SNPN. |
| Convida Wireless | We think that an SP-ID is necessary. Furthermore, it should be possible to resolve the UE Identifier to an SP-ID. |
| LGE | No new format on SP-ID, PLMN ID (PLMN being SP) or PLMN ID + NID |
| Orange | Existing naming schemes to identify a AAA server can be reused. This identity does not need to be broadcast over Uu. |
| Qualcomm | No additional identifiers are needed to identify the separate entity.  PLMN ID (SP = PLMN) or PLMN ID + NID (SP = SNPN) is sufficient to identify the entity. For PLMN ID also MCC 999 can used (i.e. there is no need for a unique PLMN ID). Unqiue NIDs can easily be configured even for verticals by requesting, free of charge, a Private Enterprise Number (PEN) from IANA and by using the PEN to derive a unique NID (see related CT4 specs for details). |
| Sony | Rel-16 format should be sufficient, no need for new SP-ID format. |
| Futurewei | Support to have SP-ID to differentiate with the network ID in order to identify the service provider who may not directly provide the communication service. |
| Lenovo | The service provider ID (SP-ID) can be one of:  - PLMN ID;  - SNPN ID (i.e. PLMN Id + NID); or  - (in case of SUPI defined as NSI), the SP-ID can be the "realm" part of NSI. |
| vivo | The existing SUPI/SUCI (IMSI or NAI format) are sufficient. |
| AT&T | Existing naming schemes to identify a AAA server can be reused. |
| Nokia | Should be identified by SP ID |
| Cisco | The mobile is configured to camp on certain PLMN-IDs based on configuration.  The realm part of the Network Specific Identifier (encoded as user@realm) may be encoded in a way that uniquely identifies the SP’s realm. DNS is used to lookup the SP (Identity provider) for authentication purposes. |
| ZTE | The existing mechanism can work, i.e. The PLMN ID + NID  The NID part may include the SP information |

# Question KI#1-Q4: SNPN selection

In release 16 the UE had a subscription tied directly to the SNPN identity so 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 needs to be a mechanism to enable the UE to make an efficient network selection so that it selects a suitable SNPN.

## Question KI#1-Q4.1: SNPN selection based on UE pre-configuration

**Question**: Should it be possible to pre-configure the UE with the preferred SNPNs to select?

|  |  |
| --- | --- |
| **Company** | **Comments** |
| Ericsson | Yes, we assume configuration in the UE as described in solution 1 in TR 23.700-07 clause 6.1. |
| Intel | Yes. UE pre-configuration with network lists in priority order should be the default.  Today the pre-configured lists in the UE or USIM (e.g. “Operator Controlled PLMN Selector” list or “Equivalent Home PLMN” list) are the fundamental ingredients that drive network selection when UE’s Home PLMN is not advertised on the radio.  In our view pre-configured network lists shall remain the fundamental mechanism that drives network selection even when the serving network is an SNPN.  To support all possible cases (e.g. SP is a PLMN, SP is another SNPN, service continuity, etc.) a common network selection mechanisms is used based on UE configuration (refer to Solution #1) regardless whether the UE has PLMN or SNPN subscription.  If UE has multiple subscriptions, we expect that the user needs to activate the subscription(s) they wish to use simultaneously and the network selection is performed separately for each activated subscription (similar to a Multi-USIM device). |
| OPPO | YES, pre-configuration. |
| Samsung | The UE may have pre-configured info about preferred SNPN, which is similar to operator/user controlled PLMN selector list |
| MediaTek | Yes the UE can be pre-configured with a list of the preferred SNPNs.  Given an SNPN can be a service provider, this list can be used for this purpose as well. |
| Convida Wireless | Yes |
| LGE | YES, UE pre-configuration. |
| Orange | Yes. |
| Qualcomm | Yes, this will help in scenarios where it is possible to pre-configure the UE with preferred SNPNs to select. Given that it is however not possible to pre-configure the UE with preferred SNPNs to select in all scenarios (see also next question), other solutions are needed in addition. |
| Sony | Yes |
| Futurewei | Yes, the prefer SNPN can be pre-configured to UE or updated by service provider who own the UE subscription via the connecting network. |
| Lenovo | Yes, the UE can be pre-configured with a list of the preferred SNPNs. |
| vivo | Yes, it is possible to pre-configure the UE which allowed/preferred SNPN to access with the SP’s credential, like the roaming PLMN. |
| AT&T | Yes. |
| Nokia | See our views under answers to Q1. Pre-configuration as one option is OK but not as the only option. |
| Cisco | Yes, it should be possible for the UE to be pre-configured with preferred SNPNs to select. |
| Philips | Yes, it should be possible to pre-configure this information. |
| ZTE | Pre-configuration can be one option. It also may have other option |

## Question KI#1-Q4.2: Support for SNPN selection in case UE does not have correct or sufficient information for SNPN selection

**Question**: Are there scenarios where the stored configuration information in the UE may not be sufficient to select the suitable SNPN and should those scenarios be supported?

|  |  |
| --- | --- |
| **Company** | **Comments** |
| Ericsson | It is hard to judge when the configuration would not be enough, but we at least need to protect the deployments that has not been updated with support for Rel-17 work. The exact scenarios that requires additional support is FFS. |
| Intel | No.  Today, if during network selection the UE has exhausted all the PLMN IDs in the configured list without finding a match with the information advertised on the radio interface, the UE will nevertheless attempt to register with one of the detected PLMNs.  However, for SNPN subscribers there is the following stage 1 requirement in 22.261: “*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.*”  Because of this requirement we think that the UE must stop the network selection if the information advertised on the radio does not match any of the configured lists. |
| OPPO | It is difficult to quantify what is "sufficient", so we consider the question is about having correct information.  This is quite solution dependent and likely to be FFS. |
| Samsung | No need to consider such an error scenario in detail. However, In such cases manual selection mode or steering of roaming-like mechanism can be used to provide some updated UE configuration for SNPN selection if possible. |
| MediaTek | It is unclear what this question means, i.e. what “correct information” stands for and what “insufficient information” stands for.  Without clarity, this question is irrelevant. |
| Convida Wireless | Yes, there are scenarios where the stored configuration information in the UE may not be sufficient to select a suitable SNPN. However, we see no need to specify something in this scenario, other than to say that the UE should not attempt to connect to any network. Of course, the user might change the UE’s configuration locally. |
| Orange | In such case the UE shall not connect to any SNPN until it has been properly configured. The UE can attach to a PLMN using normal procedures to obtain connectivity and reach a provisioning server. |
| Qualcomm | Yes, these scenarios exist and should be supported.  One example is audio/video recording equipment that is transported directly from a storage facility to a venue (e.g. stadium or theater) where the AV equipment needs to be temporarily installed and connected to the venue's SNPN.  In this scenario it is not possible to pre-configure the A/V equipment (the UE) with a list of preferred SNPNs to select (here: the venue's SNPN) before powering up the UE in the venue.  The ability to guide the UE to the desired SNPN without having to pre-configure the UE with preferred SNPNs is key to enabling these scenarios (see also reply to the next question). |
| Sony | Yes |
| Futurewei | Yes, there are valid scenarios, such as a event company moves their concert equipment to a new concert within a short period time, and no time for reconfigure all the UEs for the new SNPN selection. |
| Lenovo | Yes, such scenarios should be considered and supported.  Some possible solutions can be used:  - manual selection of SNPN; of  - steering/re-direction of UE has to be supported, e.g. from currently selected SNPN (which does not have SLA with the SP) to another SNPN having SLA with the SP. |
| vivo | Similar as roaming, UE pre-configuration should be sufficient.  Furthermore, the PS can update the provision on the UE based on UE’s provision request. E.g. If a UE wants to access to an SNPN but has no information about which credential to be used, the UE can request credential provisioning from PS, as key issue4 request. |
| AT&T | No |
| Nokia | Yes, UE should have the possibility to read the SIB to determine SNPN, SP information to perform selection. Access network should be able to broadcast/provide the list of SP IDs and RG IDs with which access is allowed.  That way the UE does not need to be pre-provisioned with serving SNPN IDs directly, but it is enough it knows its SP ID or optionally a Roaming Group ID. |
| Cisco | This is a configuration issue, and should be solved by onboarding. Special handling is not required. |
| Philips | Such scenarios don’t seem to be useful. |
| ZTE | Yes, the scenario is possible. Example, moving all the equipment to a new place where there is a new SNPN deployed, it is impossible to pre-configure all the possible SNPN in the UE. |

## Question KI#1-Q4.3: SNPN selection in case UE does not have correct or sufficient information for SNPN selection

**Question**: If there is a need to support scenarios where the UE is not pre-configured with the correct and sufficient information about which specific SNPN to select, is it sufficient that the UE selects (in any order) an available SNPN that supports accessing using credentials from a separate entity or should there be support to guide the UE which SNPN or PLMN to select?

|  |  |
| --- | --- |
| **Company** | **Comments** |
| Ericsson | As stated in the question, we at least need broadcast to support 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. Would be good to discuss the scenarios to understand whether manual selection or UE trying the available SNPNs is enough or not e.g. do we envision large amount of SNPNs supporting this kind of solution in an area? |
| Intel | No, there is no need to support such scenarios. See answer to Question KI#1-Q4.2. |
| OPPO | As with our answer to Q4.2 |
| Samsung | manual selection mode or steering of roaming-like mechanism can be used to provide some updated UE configuration for SNPN selection if possible. |
| MediaTek | It is unclear what this question means, i.e. what “correct information” stands for and what “insufficient information” stands for.  Without clarity, this question is irrelevant. |
| Convida Wireless | We do not think that a UE should select an SNPN without first receiving some indication that it is an SNPN that it has credentials for or that it is an SNPN that can onboard the UE. |
| Orange | This should not be permitted. |
| Qualcomm | No, it is insufficient to let the UE select any available SNPN that supports accessing using credentials from a separate entity since this will likely result in the UE not selecting the desired SNPN.  For instance audio/video recording equipment that is transported directly from a storage facility to a venue (e.g. stadium or theater) may for example select the SNPN of an adjacent factory or other enterprise instead of the venue's SNPN.  It also needs to be considered that there may be a significantly larger number of private networks (SNPNs) than PLMNs today.  Having UEs try to find the "correct" visited network by trial and error will create significant amount of unnecessary signaling for SNPNs and will also significantly increase the time until the UE will be successfully registered.  To avoid this and to guide the UE to select the desired SNPN, SNPNs can broadcast the identities of Home SPs that the SNPN has an agreement with.  Alternatively, SNPNs may broadcast the identities of Roaming Groups that the SNPN has an agreement with.  The same Roaming Group ID could for instance be assigned to all national broadcasting companies and configured to their audio/video equipment. If a venue broadcasts the Roaming Group ID assigned to the national broadcasters, then the AV equipment will be able to automatically select the venue's SNPN without having to be pre-configured with the venue's specific SNPN ID. See Solution 2 in TR 23.700-07 for further details. |
| Sony | The UE need to be re-configured with the correct preferred SNPN. It should be enough for the UE to connect to any SNPN that is willing to allow data traffic for re-configuration of the UE and possible also new credentials to be used when register to this new preferred SNPN. |
| Futurewei | Randomly selecting and accessing a SNPN should be avoided, otherwise this will violate the requirement from SA1 regarding preventing unauthorized UE to accessing the SNPN. There should be mechanism to guide UE to select the proper SNPN in that situation. |
| Lenovo | If the UE configuration is not sufficient, the UE can select any available SNPN supporting network access for separate SP.  Steering to another SNPN should be supported (see answer to Q4.2). |
| vivo | Please see the answer in Q4.2. |
| AT&T | No |
| Nokia | It should be possible for the SNPN to provide the UE an explicit list of Service Provider IDs and Roaming Group IDs with which access is possible, to prevent “trial and error” based access selection. |
| Cisco | The mobile should select based on configuration. There is no need to guide the UE which SNPN or PLMN to select. User interaction may be needed. User interaction may be used. |
| Philips | See KI#1-Q4.2 |
| ZTE | No. It will result in the unnecessary retry signaling burden to the network. Specially, if there are multi available SNPN can be selected. |



# Question KI#1 – (new) Q5: Mobility and service continuity

For KI#1, TR mentions for mobility and service continuity

- UE moving from SNPN#1 with separate entity#1 to SNPN#2 with separate entity#1 available; and

- UE moving between SNPN#1 (where separate entity=PLMN) and PLMN.

However, some of the present available solutions are unclear on how such mobility and service continuity requirements are met. Are clarifications required before evaluation of solutions are done or will work be done in normative phase or is it not necessary to work on these requirements in this release.

**Question**: Should mobility and service continuity scenarios be studied and detailed in this study phase?

|  |  |
| --- | --- |
| **Company** | **Comments** |
| Ericsson | Perhaps not the most important aspect, but preferably solutions should state whether and how service continuity is supported. |
| Intel | Yes, service continuity (actually – session continuity) should be studied for the case described in the second bullet above.  Solution #1 clearly describes how service continuity requirements are met:  *- When the service provider of the UE is a PLMN, the standalone non-public network selects the session management function and PDU Session Anchor (PSA) in the PLMN to support PDU sessions that require service continuity using the home-routed roaming architecture.*  *- Mobility in the absence of the N14 interface between SNPN and PLMN is handled by the "Existing PDU Session" indication in the PDU Session Establishment Request.*  The description focuses only on the case where the SP is a PLMN (i.e. second bullet above) because we are not sure if there is a requirement to handle the case described in the first bullet, but the principle would be the same. |
| OPPO | If some solutions are clear on meeting those requirements and some are not, making a choice at solution selection phase is not balanced. SO unless those requirements are void, then all solutions need to identify the way they meet those requirements. |
| Samsung | Negative |
| MediaTek | A decision is to be taken in study phase whether and how to move forward in normative phase. This should not be left to normative phase discussion.  A starting point could be the second scenario that “UE moving between SNPN#1 (where separate entity=PLMN) and PLMN and leave the first scenario out. |
| Convida Wireless | Yes |
| Orange | No. Mobility scenarios are in the scope of KI#1 but this is not stated as a requirement of this KI. Therefore a solution not addressing mobility should still be considered in the evaluation phase. |
| Qualcomm | We do not see any architectural gaps to support mobility and service continuity for the scenarios listed above. Therefore we do not see any need to continue studying solutions for these scenarios. |
| Futurewei | Yes, service mobility and continuity need to be studied in this phase, as network selection will not only considering the initial network selection, but also the target SNPN selection during the mobility.  Also because we have new 3rd party service provider, as well as SNPN has different deployment models than traditional PLMN (such as high number of SNPN networks, small area of each SNPN, providing more specialized or dedicated services, so on), we should also consider the service mobility triggered by either UE or Service providers, such as SP can guide UE to select and move from the service SNPN to another overlapping SNPN or PLMN if there is need from SP. |
| Lenovo | Mobility and service continuity requirements may be met for scenarios where home-route-like connection is used (E.g. when the SP is PLMN/SNPN deploying SMF/UPF functionality). |
| vivo | No, the existing specification seems sufficient to support the mobility and service continuity. |
| AT&T | Yes |
| Nokia | Yes. it is important to determine if the solution has restrictions to support mobility and service continuity prior to being selected for conclusion. |
| Cisco | Mobility and service continuity scenarios do not need to be studied in the study phase. SNPN should be treated as a Wi-Fi hotspot, a bit like LADN.  There should be no requirement for an interface between two SNPNs to support mobility. IP@ continuity may not need to be provided in this phase. |
| Philips | If some solutions do not meet those requirements and others do, this may be taken into consideration during solution evaluation. |
| ZTE | The mobility and service continuity shall be supported for above scenario.  But whether the existing mechanism or new solution can met this requirement is FFS |

# 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.*

This requirement was acknowledged as being part of "Existing features partly or fully covering the use case functionality" during FS\_AVPROD study (see TR 22.827)."

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. |
| Intel | 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. |
| OPPO | The KI#4 on Onboarding should be a broad church, and not get stuck on what precise and nature of credentials are included and excluding those kinds of credentials e.g. even IMS credentials, e.g. 3rd party credentials, that has already have provisioning means. This way forward also allows for future – as yet not designed credentials to be provisioned by onboarding. |
| Samsung | For the clarification, we can add it as NOTE for this “Any type of credentials should be provisioned for SNPN” if required. |
| MediaTek | The current description in KI#4 is sufficient. |
| Deutsche Telekom | The KI generally relates to NPN, while the clarification is specifically for SNPNs. A note clarifying the case for SNPNs would make this otherwise “overgeneric” KI better understandable |
| China Mobile | It is better to clarify that in this key issue, what type of UE’s subscription for SNPN will be studied. |
| LGE | NO |
| Orange | Yes, since we have received a clear answer from SA1 that the requirement in TS 22.263 does not apply for IMSI accompanied by AKA credentials, this should be reflected in KI#4 description. |
| Qualcomm | No need to amend the KI description; as per SA1 requirements, both 3GPP and non-3GPP credentials can be provisioned. |
| Sony | 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. |
| Futurewei | Credential should be in the scope of the provisioning. The current KI description is general enough to cover that and no need to be updated. |
| Lenovo | We understand that KI#4 includes provision of both types of credentials, 3GPP and non-3GPP credentials. If needed, this can be explicitly clarified in the KI. |
| InterDigital | Agree that the KI allows both 3GPP and Non-3GPP credentials to be provisioned. |
| vivo | Yes, “credential” and “NPN subscription” are not exactly same. And the UE can be provisioned with either 3GPP credential or non-3GPP credential. |
| AT&T | Yes. |
| Nokia | Yes |
| Cisco | The external credentials providers will belong to one of two classes: (a) Service Providers who has IMSI and AKA credentials pre-configured on the mobile , or (b) non-SPs who will not require IMSI based credentials.  Hence, we do not need to consider the case of provisioning IMSI and AKA credentials on the mobile. |
| Philips | It is important that the onboarding solutions allows provisioning of all the necessary identity and credential information to enable access to the SNPN. The term “Information” is sufficiently broad to capture all these aspects, so no need to update KI#4. If desired the term “NPN subscription” may be replaced with “NPN access credentials and identity information” |
| ZTE | Yes. SA1 has confirmed the requirement, and the “information” is too general. |

# 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 | If a UE got a PLMN subscription (provisioned with any existing means), and there is a need for secondary authentication or NSSAA, then the UE would not be able to access the NPN. It would therefore be valuable to allow such solutions. |
| Intel | In our view this is not part of the UE onboarding proper. PNI-NPN related information can be configured either over the top or using UE Configuration Update. |
| OPPO | Same as answer to KI#4, Q1. |
| Samsung | Negative |
| MediaTek | No. If the UE can register to a PNI-NPN successfully, UE related information could be updated via UE Configuration Update procedure before UE establishes any PDU Session to a network slice or to a dedicated DNN of PNI-NPN. |
| Deutsche Telekom | No. But it should be in the scope to check that existing methods can already be employed for that, i.e. it should not be omitted from the evaluation for KI#4.  It is very important to clearly separate the SNPN and PNI-NPN case. This KI should not end up defining how to provide access to PLMNs with default credentials. |
| China Mobile | We insist that PNI-NPN is in the scope of key issue 4. We should have clear standardization to facilitate the provision of UE’s identity and credentials for PNI-NPN through a flexible method, which is supporting the implementation of NSSAA and secondary authentication. |
| LGE | NO |
| Qualcomm | No, unless SA1 answers otherwise. NSSAA and PDU session secondary authentication are orthogonal mechanisms to PNI-NPNs i.e. they can be used without PNI-NPNs and PNI-NPNs can be deployed without NSSAA and PDU session secondary authentication. In rel.15/16 it was agreed that the credentials used for NSSAA and PDU session secondary authentication are out of scope of 3GPP and therefore we don’t see why this needs to be changed in rel.17. |
| Futurewei | Yes. |
| Lenovo | Yes, we understand that provisioning of credentials for NSSAA or secondary authentication is in the scope. |
| 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. |
| vivo | Wait for SA1’s answer |
| Nokia | Neutral. |
| Cisco | We share the same view as Intel. This is not part of the UE onboarding. PNI-NPN related information can be configured either over the top or using UE Configuration Update. |
| Philips | Yes, it is important that the onboarding solutions allows provisioning of all the necessary identity and credential information (incl. secondary credentials) to enable access to a PNI-NPN. If it is not defined how this is done, the solutions would be incomplete. |
| ZTE | Yes. |
| China Telecom | Yes. PNI-NPN may be deployed with NSSAA and PDU session secondary authentication, thus there should be a mechanism to provision corresponding identity and credential to UE, otherwise UE may not access PNI-NPN successfully. |

# Question KI#4-Q3: AS impacts to support UE Onboarding

Question: What impacts do you foresee needed to the AS (Access Stratum) 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. |
| Intel | A new 1-bit SIB indication (“Support for Onboarding”) broadcasted by the NG-RAN indicates that the SNPN provides access to onboarding service. The UE determines that the cell supports onboarding service over NG-RAN via the broadcast indicator in AS and subsequently initiates the Registration procedure. During the registration procedure, the UE provides information in both RRC and NAS registration request indicating that the registration is only for restricted onboarding service based on which the NG-RAN selects an AMF in the O-SNPN. |
| OPPO | Information in SIBs to indicate the "associated" SPs/Provisioning servers seems inevitable. But more can only be ascertained when it is clearer about the solutions i.e. answer is solution dependent. |
| Samsung | Broadcasting the information for selection of ON |
| MediaTek | User Plane (UP) onboarding does not have any impact to the AS while Control Plane (CP) onboarding may affect the AS as described in the solutions in current TR. |
| Deutsche Telekom | Anything added for AS would have following effects:   * If it is specific for SNPNs, it is not clear how RAN sharing would be impacted. Our assumption is that SNPN + PNI-NPN RAN sharing will then not be possible * If it is generically added for NPNs in general, how any added parameter is used would need to be added to PLMN network selection, which we would not be OK with   Our view for the PNI-NPN case is that there is no need for AS changes. Changes required by SNPNs should not impact non-SNPNs. RAN aspects of SNPN-specifica like this should be assessed by RAN before being decided, as they may also end up having an effect on non-SNPNs-related functionality |
| Convida Wireless | At least SIB Information so that the UE can determine what network can onboard it.  Also, some RRC information so that NG-RAN can select the onboarding network’s AMF. |
| LGE | SIB information to indicate support for onboarding. |
| Orange | AS shall not be impacted to support onboarding. |
| Qualcomm | We foresee the following AS impacts:   * Per-network SIB indication of support for onboarding * RRC indication sent by the UE to indicate the need for an onboarding session so that NG-RAN can select an AMF used for onboarding. |
| Sony | SIB information to indicate support for onboarding per network.  Adding a new “cause value” for onboarding would be useful. |
| Futurewei | Because we may consider both CP and UP based solution, this require the capability support from UEs, so the AS can be enhanced to support those 2 options. Need to decide after we studying all the potential solutions. |
| Lenovo | We foresee impact to the information broadcast (e.g. SIB) to indicate support of 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. |
| vivo | TBD |
| AT&T | AS should not be impacted to support onboarding. |
| Nokia | Indicating support for UE onboarding in the broadcast so that the UE knows whether to camp in the cell or not. |
| Cisco | Impacts similar to PARLOS with the advertisement of a bit in RAN stating un-authenticated restricted access is allowed. |
| Philips | Depends on the solution. |
| ZTE | It depends on the solution.  No AS impact is preferred |

# Question KI#4-Q4: Assumptions regarding DCS

To address some solutions for KI#4, 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**: In the solutions making use of a DCS, 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. |
| Intel | The standard should be defined for the most generic case where each of the logical entities can be owned by a different administration. For instance, a device manufacturer may own the DCS, but it might as well delegate the ownership to a major consumer electornics vendor. The interface between 5GC and DCS does not need to be service-based. |
| OPPO | Separate DCS ownership must be supported and without requiring SBA services. Protocol to be used towards DCS should be open application level protocols, details for Stage 3 to decide. |
| Samsung | the assumption on DCS is that there is contract between DCS and ON |
| Deutsche Telekom | A very valid assumption to consider would be “existing technologies that can be reused” and to separate the SNPN and PNI-NPN cases, as they may end up not having the same needs. |
| Convida Wireless | The architecture should not assume a specific ownership of the DCS.  The interface between the 5GC and DCS should be a 3GPP defined service-based interface. The interface between the DCS and Provisioning Server does not need to implement 3GPP-specific services. |
| Orange | Existing technologies and standards should be reused. No CP interface between 5GC and DCS is needed. |
| Qualcomm | We prefer that the interfaces are the same irrespective of whether AKA or non-AKA methods are used in O-SNPN for authentication using “default credentials”.  For security reasons certain parts of the AUSF functionality are needed in O-SNPN, while the rest of the security functions (UDM/UDR/ARPF) can be accomplished by DCS. The main issue that needs to be addressed is where to terminate EAP. We prefer towards DCS – in which case, Kausf & Kseaf need to be derived (which is responsibility of AUSF currently) by the DCS (as EMSK, key from which these keys are derived, cannot be sent outside of the EAP server per EAP RFC). |
| Sony | 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. |
| Futurewei | Due to the nature of vertical NPN deployment, the DCS may be closer to the SP or subscription owner rather than the device manufacturer. So, the DSC should be considered to have close collaboration with ON. Some SLA/trust relationship exist between them.  No preference on the interface protocol. |
| Lenovo | Regarding ownership: flexible deployment of DCS should be supported (e.g. DCS can be in the manufacturer domain, device owner domain or operator domain).  Regarding type of interfaces/protocols: no need to standardize the interface to DCS (i.e. SBA cannot be used, but rather AAA protocols areused). |
| 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. |
| vivo | It is assumed not to define new authentication methods and reuse existing protocol, e.g.   * If the DCS owner is out of 3GPP, e.g. EAP AKA, EAP TLS defined by SA3 can be reused. Whether need an AAA-P for AUSF to connect DCS’s AAA is TBD.   If the DCS owner is PLMN or SNPN, the existing protocol defined by SA3 can be reused. N12 is reused between AMF and DCS’s AUSF. |
| AT&T | Should reuse existing technologies and standards. |
| Nokia | Ownership answer depends on the deployment model. 3GPP can specify SBA for DCS. It would be best not to make a strict assumption thus avoid restrictions in 3GPP spec. |
| Cisco | Same as Ericsson.  The standard should be defined for the most generic case where each of the logical entities can be owned by a different administration. If UP solution is used, there may not be an interface between 5GC and DCS. |
| Philips | The DCS will typically be owned or operated by the target NPN for which the UE needs to be onboarded, or the target NPN has access to the DCS that may be owned by a device vendor. It is unlikely that the onboarding network owns or operates the DCS, and hence it requires a standardized interface and a secure protocol between the onboarding network and the target NPN to access/request/copy information from the DCS owned or operated or accessed by the target NPN. |
| ZTE | It depends on where the DCS is deployed.  If the DCS is deployed in the operator network, it can be SBA based. Otherwise, there is no mandatory to use the SBA interface. |

# 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? How do we consider the compatibility with existing Provisioning Servers?

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. |
| Intel | The standard should be defined for the most generic case where each of the logical entities can be owned by a different administration. The Provisoning Server may be owned e.g. by the O-SNPN operator, by the SNPN owning the subscription or by a 3rd party. |
| Alibaba | The architecture should not assume a specific ownership. The architecture should allow the PS to have interface with the relevant entity in the SNPN in order to dynamically generate and provision credentials to the UE and the correspondent entity in the SNPN (e.g. vertical AAA in the case of non-3GPP credential based authentication.) after successful onboarding.  Note: This is very useful for IoT type of UE since it is difficult to preconfigure credentials for a large number of IoT UE in real deployment. Allowing the PS to dynamically generate credentials will provide maximum flexibility. For example, it allows the SNPN provider to purchase commercial off-the-shelf IoT type of UE without preconfiguring credential for it. This will simplify the deployment. |
| OPPO | In principle same answer as for KI#4-Q4 |
| Samsung | the assumption on PS is that there is contract between PS and DCS and between PS and SO-SNPN. |
| Deutsche Telekom | As in KI#4-Q2, the SNPN and PNI-NPN cases must be clearly distinguishable. The requirements are not the same |
| Convida Wireless | The architecture should not assume a specific ownership of the PS. |
| Orange | Existing technologies and standards should be reused. |
| Qualcomm | We believe that the security mechanisms used and where the provisioned credentials are stored will determine the ownership. In general we prefer that SA2 does not spend much time on the UE-to-provisioning server interface and procedures and leaves it to SA3 and even leaving use of protocols outside of 3GPP is acceptable from our perspective. |
| Futurewei | Prefer provisioning server locates in ON or the 3rd domain affiliated with the service provider or the ON. |
| Lenovo | Regarding ownership: flexible deployment of PS should be supported (e.g. PS can be in the manufacturer domain, device owner domain or operator domain).  Regarding type of interfaces/protocols: no need to standardize the interface to PS in 3GPP (e.g. other SDOs may standardize the protocols between PS and secure storage in UE). |
| 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. |
| vivo | UP based solution doesn't require to specify the interfaces/protocols detail.  For CP based solution, the interfaces/protocols are the scope of SA3. |
| AT&T | Should reuse existing technologies and standards. |
| Nokia | Most likely owned by respective SNPNs and/or service providers. Again, ownership answer depends on the deployment model. 3GPP can specify SBA for DCS. It would be best not to make a strict assumption thus avoid restrictions in 3GPP spec. |
| Cisco | No assumption need to be made regarding the ownership of the PS. There should be security agreement between the Provisioning Server and the subscription owner. |
| Philips | Same answer as for KI#4-Q4 |
| ZTE | In general, the Provisioning server is owned by SNPN.  The interface/protocol for PS depends on the solution, i.e. UP or CP.  If with UP solution, no specific work is required. |

# 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? Is there any other potential provisioning mechanism?

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. |
| Intel | Focus on UP in Rel-17. |
| OPPO | Both CP and UP are needed.  What other potential provisioning mechanism will still go over either CP or UP and we consider it is a Stage 3 matter to consider such potential mechanism, if Stage 3 thinks fit to do so. |
| Samsung | both are possible |
| MediaTek | Prefer UP onboarding due to minimal impact to 5GS as mentioned in Q3. |
| Deutsche Telekom | See KI#4-Q2 |
| China Mobile | Both UP and CP methods can be considered in R17 study phase. |
| Convida Wireless | We do not see a need to support both.  We prefer the User Plane approach since it seems to have the least system impact. |
| LGE | Both possible |
| Orange | UP is sufficient. |
| Qualcomm | UP should be used  We also believe the CP provisioning solution requires evaluation by SA3 since the security association assumed is not clear to us. |
| Sony | UP based has highest priority |
| Futurewei | Both options should be considered as they may be suitable for different deployment cases, as well as can be up to the UE capability. |
| Lenovo | Both CP and UP are possible. |
| InterDigital | 3GPP should not be burdened with interfaces/protocols for interacting with Provisioning Server in different deployment scenarios and thus UP is preferred. |
| vivo | UP based solution. |
| AT&T | UP should be prefered |
| Nokia | TBD  Our considerations at this point:  At the minimum, UP based onboarding solution should at least be supported, as it allows the most flexibility for different credential provisioning methods that are not in scope of 3GPP itself.  Some existing provisioning solutions such as GSMA remote provisioning define HTTPS based access to Default Credential Server and Provisioning Server via user plane (UP). When Provisioning Server is external to access network used for onboarding the user plane (UP) based solution is the most flexibility for SNPN. It may be possible to define solution to combine Default Credential Server to control plane to provide enhanced security capabilities in terms of security key derivation for initial access based on “default UE credentials”. |
| Cisco | UP should be considered for provisioning. UP solution provides maximum flexibility in solution space. |
| Philips | No preference at this point in time. Requires further evaluation of the different solutions. |
| ZTE | In the R17, UP based solution is preferred.  It should be decided in the evaluation phase. |
| China Telecom | Both are possible in R17 study phase. |

# 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. |
| Intel | There are two cases to consider:  A) UE is a truly “off-the-shelf” device that has no configuration other than the default credential. In this case the user enters the PS identifier (and optionally the SO identifier). The PS selects the SO as follows:  A1) PS uses the SO identifier provided by the UE to select the SO.  A2) PS is provisioned with a list of UE identifiers for onboarding on per-SO basis; the UE identifier indirectly points to the SO.  B) There is an agreement in place between the UE vendor and the SNPN owning the subscription, so that the device is provisioned with some additional information (e.g. PS identity, SO identity). In this case the additional configured information is used to select the PS and the SO. |
| OPPO | PEI or SUPI |
| Samsung | based on the pre-configured information in the UE or in DCS. The subscription is also pre-configured in the network |
| Deutsche Telekom | See KI#4-Q2 |
| Convida Wireless | The subscription that needs to be provisioned in the UE is identified by an identifier that is part of, or formed from, the UE’s default credentials. For example, it can be a PEI or a combination of a PEI and a Service Provider ID.  We do not see a need to define how the subscription is provisioned in the network. For example, we do not define how a subscription is provisioned in the UDR. |
| Orange | This should be based on a trusted UE identity that cannot be cloned, e.g. SUPI or GPSI. PEI and MAC address shall not be used because they can easily be forged, allowing an illegitimate UE to be provisioned with the credentials that were intended for another UE. |
| Qualcomm | Depends on the “default credentials” and therefore the EAP methods that the UE will be using for onboarding access authentication. |
| Sony | The UE has (or derives) an initial ID used for onboarding that is unique and which the PS/DCS can verify. How this is done is outside of 3GPP |
| Futurewei | There can be a temporary UE identifier preconfigured in the UE for onboarding, this Identifier need to be tied to the service provider who own the subscriptions, e.g. the ID can be the combination of a serial number assigned from a range from the SP, the service provider ID who owning the subscription, and other info to differentiate this device and its SP(e.g IMEI).  Onboarding network and provisioning server can be provisioned from different service providers with the subscriptions basing on this temporary UE Id associating with the service provider. When ON and provisioning server receive request from the UE, will use that ID to identify the corresponding provisioning subscriptions. |
| Lenovo | Regarding identification of the subscription (btw. UE and PS): a subscription can be identified by application-specific ID or PEI. The PEI can be used for the UE identification and authentication, but not necessarily for subscription identification in the PS.  Regarding provisioning of the subscription in the network: it can be pre-provisioned in the UE's home network. Alternatively, it can be provisioned during or after the UE onboarding procedure. SA2 should not pose limitations. |
| 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) |
| vivo | SUPI, which can be derived from the UE ID associated with the provisioned 3GPP credential or N3GPP credential. |
| AT&T | This needs to be based on a trusted UE identity that cannot be tempered with, e.g. SUPI or GPSI. |
| Nokia | PEI, default credentials (certificates) |
| Cisco | An NAI based identity that can identify the realm of the SNPN owning the subscription and/or provisioning server. |
| Philips | TBD. |
| ZTE | PEI, and/or pre-configured information in the UE |

# 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 |
| Intel | The default credential shall be available in the UE.  Additional information (e.g. PS and/or SO identity) may be configured or may be entered by the user. |
| OPPO | At least default credentials and PEI. Others t.b.d with justification. |
| Samsung | Default credentials, which include their identifier. |
| MediaTek | Default subscription including identity and/or credentials to gain the initial connectivity to the DCS/Provisioning server |
| Deutsche Telekom | For the PNI-NPN case, preconfigured secondary credentials are an already possible option. Again, please clearly separate the SNPN and PNI-NPN cases clearly |
| China Mobile | For PNI-NPN, the pre-configured information in device is UE’s default subscription for access to the PLMN. |
| Convida Wireless | 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 to allow the UE to find the onboarding network is required.  Note that, in some cases, it might not be possible for a user to manually enter this information. Per KI#4: “*A TE might not have an interface that can be used to provision the MT*.” |
| LGE | Default credential |
| Orange | Information to enable that the UE can be uniquely identifiable and verifiably secure is required to be available, e.g. PLMN credentials. |
| Qualcomm | Information required to be available: Information to ensure that the UE can be uniquely identifiable and verifiably secure, e.g. credentials that enable the DCS to authenticate the UE.  Information that may be available: e.g. a list of PLMN ID + NID that the UE would use for finding onboarding networks to use. |
| Sony | The initial information could be related to the device manufacturer so the PLMN or SNPN can trust the device and the manufacturer could furthermore sponsor potential data use for performing the onboarding. |
| Futurewei | **The required default information:**  . a default temporary UE ID,  . Preferred SNPN list,  . Service provider Id,  . basic network configuration to allow to access the prefer ONs,  **The option default information:**  . PEI from the previous provisioning from previous network connection. (in case the UE has been used in the other network)  . Preferred Onboarding Network list.  . CP and UP based provisioning solution capability / preference indication  . default credential for onboarding operation  . prefer provisioning server address |
| Lenovo | Default credentials (e.g. ID and certificate) are required to ensure that the onboarding network can "uniquely identifiable and verifiably secure" prove the UE. |
| 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. |
| vivo | Default credential at least. |
| AT&T | PLMN credentials. |
| Nokia | Mandatory: PEI, default credentials (certificates)  May be available: Provisioning server IP address or FQDN |
| Cisco | An NAI based identity that can identify the realm of the SNPN owning the subscription and/or provisioning server. |
| Philips | At least some default credentials that are unique per device. |
| ZTE | Default credential,  additional information is FFS |

# Question KI#4-Q9: 3GPP connectivity used for UE Onboarding

**Question**: Is the 3GPP connectivity used for UE Onboarding restricted in some way and if yes, how is it ensured that it is restricted such that it only can be used for onboarding?

NOTE: KI#4-Q3 addressed AS impacts to support UE Onboarding in general i.e. this question is related to mechanisms to potentially restrict the use of the 3GPP connectivity for only UE Onboarding purposes, i.e. if restriction is seen needed.

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. |
| Intel | The Configuration PDU Session is monitored by the O-SNPN so that it can only provide access to selected set of PSs. |
| OPPO | yes, need FFS on this. |
| Samsung | AMF may control onboarding-purpose registered UE’s access and services, e.g. restricted QoS, Dedicated DNN, timer for connectivity |
| MediaTek | See Q3, UP onboarding does not need the restriction while CP onboarding may need to restrict the 3GPP connectivity, .e.g., the UE may only establish a PDU Session restricted for onboarding. |
| Deutsche Telekom | For PNI-NPN cases, we do not foresee having devices with default credentials within the network and do not see the need to specify anything in this regard. Also see KI#4-Q2 |
| China mobile | For PNI-NPN case, the 3GPP connectivity used for UE onboarding is for provision UE with 3rd party’s identity and credentials for NSSAA and secondary authentication. |
| Convida Wireless | Per our answer to KI#4-Q3, NG-RAN should know that the UE is connecting to the network for onboarding and select an AMF accordingly. The AMF should prevent the UE from accessing services other than onboarding. |
| LGE | Depends on solution, like AMF-control |
| Orange | Normal procedures can be used and the subscription used for onboarding can be restricted to a specific DNN. |
| Qualcomm | AMF can determine that the request is for “onboarding” based on reserved S-NSSAI for this purpose or new NAS indicator (NAS). As part of the registration procedure URSP can be provided to the UE to allow only specific PDU session and in turn allow access to it only by specific application or IP address (i.e. using existing URSP mechanisms to bind traffic to S-NSSAI/DNN). |
| Sony | Yes, RRC information provided by UE makes NG-RAN select an AMF used for onboarding (and then an SMF for controlling the onboarding session). |
| Futurewei | The 3GPP connectivity can be restricted, but not the must, should be optional. This can be determined based on the connectivity policy associated with the ON and the UE, as well as the agreement between SP and ON. E.g. if the ON may allow the UE to send some service specific information to the SP during the provisioning.  This Question is also related to Q12, which UDM can store some different network configuration policies. |
| Lenovo | Yes, the 3GPP provided connectivity is restricted to onboarding.  Regarding "how" is it restricted: pre-configuration in the onboarding network (e.g. locally configured S-NSSAI/DNN, traffic filters, QoS) is sufficient. |
| InterDigital | PDU Session for remote provisioning should be controlled by the NW to only access provisioning server. |
| vivo | The existing FAR/URSP can be used, e.g. SMF can control UPF to only allow data for PS. The URSP can have the RSD as the 3-tuple of PS to only allow data for PS. |
| Nokia | UE should be offered limited services (= connectivity for onboarding) only.  The network advertises and the UE chooses this limited access at the network selection phase. Limitations can apply and potentially negotiate with the network e.g. PS only, data volume, duration etc. |
| Cisco | The restriction information for the onboarding PDN connection can be configured in the SMF for the onboarding DNN. |
| Philips | Yes, for security reasons the 3GPP connectivity used for UE onboarding has to be restricted. |
| ZTE | Similar mechanism which is used for Emergency service. (e.g. Limited service mode, emergency PDU session, etc) |

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

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

Answers:

|  |  |
| --- | --- |
| **Company** | **Comments** |
| Ericsson | ON determines the entities using the Onboarding SUPI as input, details TBD |
| Intel | There are two cases to consider:  A) UE is a truly “off-the-shelf” device that has no configuration other than the default credential. In this case the user enters the PS identifier (and optionally the SO identifier). The PS selects the SO as follows:  A1) PS uses the SO identifier provided by the UE to select the SO.  A2) PS is provisioned with a list of UE identifiers for onboarding on per-SO basis; the UE identifier indirectly points to the SO.  B) There is an agreement in place between the UE vendor and the SNPN owning the subscription, so that the device is provisioned with some additional information (e.g. PS identity, SO identity). In this case the additional configured information is used to select the PS and the SO. |
| OPPO | UE should be able to determine this, but if not some mechanism in NW to consider default be available. |
| Samsung |  |
| Deutsche Telekom | For PNI-NPN, we see no need to standardize anything in this regard (SA2 perspective). |
| Convida Wireless | The network needs to determine the DCS identity.  Depending on the solution, the UE or network needs to determine the PS.  Once the DCS and PS are determined, we do not see how the SO is relevant from a 3GPP specification perspective. |
| Qualcomm | We don’t understand the question |
| Futurewei | we can assume there is trust and SLA between these three if they are not the same entity. |
| 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. |
| vivo | DCS is determined by AMF based on the network ID in SUPI/SUCI or vendor info in PEI provided by the UE.  How to determine SO and PS is TBD. |
| Nokia | Subscription owner |
| Cisco | TBD |
| Philips | TBD. |
| ZTE | The serving AMF can determine the DCS. |

# Question KI#4-Q11: Duration of connectivity

**Question**: Is the time duration of the 3GPP connectivity used for UE Onboarding 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. |
| Intel | O-SNPN should monitor the time duration of the Configuration PDU Session. No need for standardization. |
| OPPO | No, but NW should have right to delete/deallocate/revoke resources for whatever reason, eg. congestion, inactivity? However, we do not see a need to standardize this? |
| Samsung | Negative |
| MediaTek | No if it is using UP onboarding. |
| Deutsche Telekom | For PNI-NPN, we see no need to standardize anything in this regard (SA2 perspective). |
| Convida Wireless | No |
| LGE | NO need on for standardization |
| Orange | There is no need to standardize additional means beyond what can be controlled with existing 5G connectivity. |
| Qualcomm | No, existing 5GS mechanisms are sufficient. |
| Sony | No, there should be no possibility to misuse the session for anything else than onboarding. |
| Futurewei | The standardization of time duration may not be needed. After the provisioning completes, the connectivity can be either torn down initiated by UE or the provisioning server, or the connectivity be modified and re-used in case the ON and SP are the same. |
| Lenovo | Local configuration in the onboarding network is enough (i.e. no standardization needed). |
| InterDigital | Agree with Ericsson. |
| vivo | No, in existing specification, when data transmission turns to inactive and inactive timer expiry, RAN will trigger the UE connection release to the AMF. |
| AT&T | No |
| Nokia | 3GPP could specify a mechanism for UE and network to negotiate duration allowed to offer connectivity for onboarding but not hard code a duration. |
| Cisco | There is no need to standardize the control of duration of connectivity for onboarding. This can be based on implementation. |
| Philips | For security reasons, the time duration needs to be restricted. However, does not necessarily be standardized. |
| ZTE | Not needed. |

# Question KI#4-Q12: UDM for Onboarding

A UE is assumed to be able to perform some kind of registration 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. However, some functionality similar to what UDM does today is required e.g. deconcealment of SUCI, involved in authorization of UE to proceed Registration. Whether the NF involved in such similar logic is called a UDM or a new NF is defined can be discussed. |
| Intel | 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. |
| Alibaba | UDM can play a role for SNPN credential distribution when there is no available Provisioning server and DCS for SNPN. The UDM is owned by a PLMN or a PNI-NPN. |
| OPPO | Yes, we see UDM has a role. Either for SNPN that does not deploy its 5GC – i.e uses the 5GC of PLMN – there will be some interactions with PLMN's UDM. Or if SNPN has its own (or access to) some subscription database, that is still a UDM role. |
| Samsung | Solution dependent |
| Deutsche Telekom | For PNI-NPN, we see no need to standardize anything in this regard (SA2 perspective). Secondary authentication can already perform this |
| Orange | Yes. The "pre-configured information in the device" can take the form of credentials of a PLMN intended to be used as HPLMN for the initial connectivity that will be used for onboarding; this PLMN's UDM is then used to authenticate the UE before onboarding. |
| Qualcomm | See answer to Q4. DCS needs to play the roles of UDM/UDR/AUSF and ARPF for the onboarding authentication. Probably not ALL the functionality currently supported in UDM is required – naming this entity DCS would allow us to flexibly determine which is the sub-set of functions of UDM that are needed |
| Futurewei | Yes, UDM needs to be involved if there will be differences network configuration for the provisioning of UE from different SPs, such as some use CP while others use UP. And even for same SP, there may be different provisioning category for different UEs. UDM can store those different user provision profile/subscription for the ON. |
| Lenovo | If the question is about the usage of UDM in the onboarding network (ON), then it can be solution specific. |
| InterDigital | Agree with Ericsson.  Editor's Note: was written based on initial Ericsson answer (i.e. based on first sentence from Ericsson). |
| vivo | DCS can only authenticate the UE is itself or a fake UE. Whether the UE is allowed for credential provisioning may need UDM to control.  E.g. UE vendor’s DCS can authenticate the PEI provided by the UE is the real PEI of the UE. But whether the UE is allowed for credential provisioned depend on SNPN. |
| AT&T | Yes. |
| Nokia | Yes it can be used for on boarding in conjunction with provisioning server.  UDM is used for Initiation of authentication and selection of authentication method (TS 33.501 clause 6.1.2 and TS 33.501 Annex B). If SUCI is provided, UDM/SIDF also performs de-concealment of SUCI. During Authentication procedure (TS 33.501 6.1.3 and TS 33.501 Annex B) UDM/ARPF provides the selected authentication method and authentication vectors or certificates for security key derivation. During onboarding procedure UE may have PEI, may not have SUPI and may have “non-3GPP credentials”. In order to allow deployment flexibility for SNPN Default Credential Server (DCS) should not be considered as functionality of UDM. |
| Cisco | Same as Ericsson. Editor's Note: was written based on initial Ericsson answer (i.e. based on first sentence from Ericsson). |
| Philips | Depends on whether the onboarding is done in the context of a PNI-NPN or SNPN. Also depends on solution. |
| ZTE | TBD |

# 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. |
| Intel | 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.  We don't see the need for any additional standardization to enable the above. |
| OPPO | There will be some awareness of slice or some default slice considerations is applied if UE is not aware of slice to use. |
| Samsung | may specify the NS for on-boarding |
| MediaTek | No. The existing slicing architecture is suitable and sufficient. |
| Deutsche Telekom | As stated by Ericsson, there is no need for any additional standardization to enable KI#4 |
| China mobile | A default network slice maybe used for UE onboarding , but there is no standardization requirement. |
| Convida Wireless | An onboarding slice is proposed in some solutions. Other than that, we do not anticipate any significant slicing considerations as part of this KI. |
| LGE | Depends on solution |
| Qualcomm | No additional functionality needs to be standardized, it may be beneficial to reserve an SST for an onboarding slice to enable better interoperability. |
| Sony | No new additional functionality is needed. |
| Futurewei | Provisioning can be considered as one service belonging to a slice, and uses the existing slicing mechanism. No additional slicing consideration is needed |
| Lenovo | Please see KI#4-Q9 (i.e. network configuration in the ON is enough). |
| vivo | Specific slice/DNN for onboarding service can be considered. |
| Nokia | TBD |
| Cisco | Same as Ericsson. |
| Philips | Since some PNI-NPNs may depend on slices to isolate their traffic, so if slice specific credentials are needed for proper operation of the PNI-NPN, these should be provisioned as part of the onboarding procedure. |
| ZTE | Maybe one particular slice (S-NSSAI+DNN) is used for onboarding. |

# 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 might not have any 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. |
| Intel | It can. The onboarding solution should focus on provisioning the UE with IMS credentials. Whether the 5GS and IMS provider is the same or not should be discussed as part of KI#3 on support of voice.  For Rel-17, we are also fine to restrict the provisioning of IMS credentials for the case where the 5GS and IMS provider is the same. |
| OPPO | YES. Same principle as answer given in KI#4-Q1. |
| Samsung | In case of same operator b/w 5GS and IMS, yes  In case of different operator b/w 5GS and IMS, not sure in scope of KI#4 |
| Deutsche Telekom | The cases of SNPN and PNI-NPN need to be clearly separated. A statement applying to NPNs in general cannot be provided here |
| Convida Wireless | Yes. We do not see why additional mechanisms would be required from an SA2 perspective. |
| Orange | No. For PLMNs, 3GPP does not specify how IMS credentials are provisioned and the same should be assumed for NPNs. |
| Qualcomm | No. |
| Futurewei | No opinion |
| vivo | TBD |
| Nokia | NO, this was not in scope |
| Cisco | Provisioning of IMS level credentials should not be considered in Rel-17. |
| Philips | It is okay to leave this out-of-scope of KI#4 for release 17. |
| ZTE | No |

# 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. |
| Intel | Yes. At the end of onboarding the UE should deregister and subsequently register using the assigned network credentials. Given that the onboarding procedure is performed infrequently, we don’t see the need for achieveing signalling savings by trying to re-use the same registration. |
| OPPO | If UE is already on "correct" NW, there is no need to de-register, but if there is a need, then it should be NW forcing that deregistration and not a built into UE function. |
| Samsung | Positive |
| MediaTek | Yes, the UE should de-register from the current network and attempt registering to the desired NPN according to the NPN subscription provided during the onboarding procedure. |
| Deutsche Telekom | No view here if this only applies to SNPNs |
| Convida Wireless | Yes. The onboarding network and the network that is associated with the subscription might be different. Even if they are the same, the new subscription might impact NF selection. It seems easier to have the UE simply de-register and re-register, otherwise the UE will have to somehow be re-directed to the SNPN that owns the subscription. |
| LGE | Yes |
| Orange | Yes, the UE should de-register from the current network and attempt registering to the desired NPN according to the NPN subscription provided during the onboarding procedure. |
| Qualcomm | It can be based on policy indicated to the UE as part of the provisioning procedure. |
| Sony | For simplicity, the UE should deregister from the onboarding network and then re-register in the same or new network. |
| Futurewei | Deregistration may not be necessary in case the ON and the SNPN who owning the subscription are the same, e.g. the initial connectivity for provisioning can be modified after onboarding completed. |
| Lenovo | This can be solution specific |
| InterDigital | Agree with Ericsson. |
| vivo | If the UE turns to use the new UE ID associated with the new credential/subscription to access SNPN, de-registration and reregistration with new UE ID are needed. |
| AT&T | Yes. |
| Nokia | Yes. As the Onboarding procedure is allowed with limited service, de-registration may be needed so that the UE can re-register with appropriate credentials to get normal service. |
| Cisco | Yes the UE should de-register after the UE has been provisioned with a new subscription. |
| Philips | Since the onboarding connection has limited access to the core network, it would be most simple solution to close the onboarding connection and let the UE re-register with the provisioned credentials. |
| ZTE | Yes. For the Onboarding, there is restriction on the service (onboarding only)  After Onboarding, the UE can select the appropriate network to register. |

# 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". |
| Intel | 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. |
| OPPO | If UE is already on "correct" NW, there is no need to de-register, but if there is a need, then it should be NW forcing that deregistration and not a built into UE function. |
| Samsung | PNI-NPN related subscription update to UE can be done by UCU or registration accept procedure. |
| MediaTek | Any required information that should be updated to the UE registering to a PNI-NPN should use UCU procedure and no extra procedure is needed. |
| Deutsche Telekom | No need for any additional standardization |
| China Mobile | We assume that updates of PLMN subscription in UDM/UDR for PNI-NPN access maybe triggered by AF. The information which the AF provides to UDM through NEF should be specified, e.g. CAG ID or slice ID. |
| Orange | 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. |
| Qualcomm | See our answer in Q2. We don’t think we need anything more than what is already supported in rel.16 |
| Futurewei | The new update subscription may require PLMN to allow to establish a temporary connection for UE to get new NPN credential from a provisioning server affiliated with the NPN, then with the new credential, UE can access the NPN via PLMN after secondary authentication. This is in the scope of SA2. |
| Lenovo | As the SA1 requirement implies, in the following two scenarios 1) PNI-NPN subscription is added for the UE, or 2) the UE's subscription changes from PNI-NPN1 to PNI-NPN2, the TR should provide:  - description/mechanism how to update subscription in the network, i.e. the UE's subscription data in the PLMN in order to provide access to PNI-NPN; and  - description/mechanism how to update the UE, i.e. the UE configuration to use the PNI-NPN. |
| Ericsson | Agree with Ericsson that PLMN subscription update is not in the scope. |
| vivo | Once subscription data for PNI-SNPN is updated, it has already supported to update it to the UE. |
| Cisco | Same as Ericsson |
| Philips | If the UE configuration update procedure is reused, then it may need to be extended. |
| ZTE | The UCU is used to update UE for adding or updating NPN parts of PNI-NPN subscription. |

# 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>