**SA WG2 Meeting #S2-141E S2-2007309r19**

**12 – 23 October, 2020, Electronic, Elbonia *was S2-2007309+7324+7356+7589+7759***

**Source: Ericsson, (Intel, China Telecom, MediaTek Inc., Nokia), Huawei, HiSilicon**

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

**Document for: Agreement**

**Agenda Item: 8.2**

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

*Abstract of the contribution: This paper updates the KI#4 Interim conclusions* *by resolving some of the ENs*

# 1. Discussion

## 1.1 DCS Discovery

In the KI#4 interim conclusions, the following conclusion and associated EN is written:

*- The SNPN, which directly interacts with DCS, determines the corresponding DCS identity or address/domain based on the input from the UE.*

*Editor's note: It is FFS whether some alternative way to identify the DCS is to be added.*

The DCS is defined as:

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

The default UE credentials are defined as:

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

If the UE has been provisioned default UE credentials, then these should contain enough information for finding the DCS i.e. if the UE provides such information to the network (e.g. the ON), the network should be able to find the DCS. At DCS discovery, the network also should verify that the DCS is authorized or trusted by the ON.

If the UE is not provisioned with any default UE credentials, then it is not possible to make the UE "uniquely identifiable and verifiably secure" i.e. there is no way to authenticate the UE and there is in such case no need for any DCS.

The onboarding SNPN may use the Default UE credentials provided by the UE as part of the registration procedure to determine the DCS identity.

Default UE credentials is assumed to include UE onboarding identity. Such UE onboarding identity type may be, for instance, in the form of SUCI as specifed in TS 33.501 clause 6.12.2. Home Network Identifier is included in SUCI. The UE does not conceal the Home Network Identifier. The exact details for UE onboarding identity such as type, format, for instance NAI format, or protection scheme are subject to SA3 decision.

In specific, critical SNPN deployments, where the DCS is also locally deployed, the onboarding SNPN may be locally provisioned the required DCS identity information and it may desirable for onboarding SNPN not to rely on such information provided by the UE at initial access.

Until SA3 has determined whether primary authentication is required during initial access, it is premature to omit an option for a lightweight registration procedure without primary authentication.

It is proposed to complete the conclusion and remove the associated EN.

## 1.2 NG-RAN impacts

The following text is written in the KI #3 conclusions:

The NG-RAN of the Onboarding network includes information in the SIB so that the UE can discover and select an appropriate O-SNPN.

*Editor's note: whether an explicit indication towards the network from the UE is used indicating that the registration is for onboarding is FFS.*

*Editor's note: Whether new RRC information is needed or existing RRC information can be used (e.g. NSSAI information) for an AMF selection during Registration procedure is FFS.*

With respect to the first EN, it is already agreed that NG-RAN nodes broadcast SIB information enabling the UE to discover and select an appropriate O-SNPN.

The minimum SIB information that NG-RAN should broadcast consists of a single bit indicating that the O-SNPN supports onboarding procedures. This helps the UE to discriminate and eliminate from the list of candidate O-SNPNs those networks that do not support onboarding.

Additionally, NG-RAN could broadcast some sort of identifier that allows the UE to univocally select the appropriate O-SNPN that can accept the onboarding in the SO-SNPN. However, a number of open issues are not yet resolve. For example, how is the UE provisioned with the identifier; or how is the O-SNPN provisioned with the identifier that the UE is searching for; or how does the SO-SNPN influences any of the previous. It is suggested to continue with more investigation for resolving this aspect.

It is assumed that the ON can be executed by any SNPN and that NG-RAN supporting Onboarding also can be connected to AMFs used for other services. Therefore, there is a need to be able to select an AMF that supports Onboarding, i.e. the NG-RAN will need to know that the UE requests the RRC connectivity for Onboarding as to select an AMF supporting Onboarding. The AMF also need to be able to restrict the functionality for the UE to only on-boarding service, i.e. the AMF needs to be Onboarding aware.

The question is if we define a network slice for Onboarding or if we define separate indications to enable the Onboarding logic. The following are some considerations:

- If we define an Onboarding Slice and re-uses the network slice selection information then:

- we are overloading the semantics of network slices for indicating that the UE is requesting an onboarding procedure. Actually, the UE is not requesting to be registered in a particular network slice, but just be provisioned with credentials.

- we get S-NSSAI information in RRC, NGAP and NAS as required;

- we are restricted to use an Onboarding network slice i.e. it is not possible to use eMBB Network Slice also for Onboarding;

- UE, NG-RAN are just slightly impacted

- we would need procedures for UEs that request this onboarding network slice but not for onboarding, as well as those requesting onboarding outside this onboarding network slice

- If we define new indications to enable the Onboarding, then:

- New IE required in RRC (msg 5), NGAP and new indication in NAS Registration;

- A network can re-use any Network Slice also for Onboarding; Some networks can steer the UE into a specific network slice for onboarding procedures; others may split and have multiple onboarding network slices, or none at all (e.g., eMBB network slice). Flexibility is achieved.

- Slightly impacts in UE, NG-RAN, and AMF.

- The network has the control for steering the UE however it wants.

It is proposed to enable the explicit indication of the UE’s procedure for Onboarding.

The information provided by the UE to the AMF can be re-used the default UE credentials which contains the information can be used by the AMF either to initiate the onboarding registration or to re-direct to a suitable AMF which can trigger the onboarding registration.

**Proposal:** the onboarding information provided by the UE to the AMF can be the default UE credentials which contain the necessary information for the AMF to trigger the onboarding registration or to re-direct to a suitable AMF for the onboarding registration

## 1.3 Onboarding registration

For component 1 (SNPN), there is an EN stating:

*Editor's note: Further conclusions how to enable on-boarding registration is FFS e.g., based on default ON profile at UDM (e.g. When PLMN is used) or UE indication or local policy.*

UDM usage in SNPN for Onboarding:

- The SNPN acting as ON may also be serving normal users, i.e. the ON acts also as a regular SNPN. As such, the ON acting as an SNPN may have a deployed UDM, however, this UDM is provisioned with the subscription data pertaining to the SNPN regular usage, not related to onboarding procedures;

- There is no need for the AMF in the ON to down-load subscription data as the UE does not yet have any subscription to be downloaded;

- When possible, the Onboarding functionality should not impact normal services.

- The information needed by the AMF for restricting the registration to Onboarding service can be locally configured in AMF or retrieved from another NF:

- The other NF can be UDM, PCF, NRF, …

If UDM: The UDM should not be the same used for normal services, but a special UDM can be provisioned with a default subscription to be used for Onboarding;

If PCF: The PCF could have the information, but there seems not to be a need for policy differentiation as such.

If NRF: The information is not related to any NF profile but rather information about Onboarding restrictions as such.

The NFs (AMF, SMF, PCF, etc.) at onboarding SNPN are locally configured with onboarding specific configuration data to enable SNPN to restrict UE to consume only onboarding service. There is no subscription at onboarding phase, thus no UDM services to be consumed at SNPN.

It seems like the most suitable and optimal option is to use local configuration in the AMF Set when ON is S-SNPN. It is proposed to remove the related EN.

When PLMN supports as Onboarding Network (ON):

- Sol#31 proposes that UE selects and registers to the onboarding PLMN using default operator profile (subscription and credentials to the onboarding PLMN for the UE to be "uniquely identifiable and verifiably secure"), and the AMF restricts this registration only for onboarding service only based on UDM indication, SMF restricts the PDU session for remote provisioning only based on UDM subscription. The UE shall initiate de-registration from the on-boarding network after finishing the remote provisioning or the on-boarding network shall initiate the de-registration based on timer configured for on-boarding service.

- Sol#33 proposes the similar mechanism as solution #31, with the following differences:

- no details on how to support the functionality to restrict usage to only on-boarding service

- further describe that new NPN operator profile can be provided at the eUICC inside the device on top of the established PDU Session by using eSIM-based UE onboarding procedure between eUICC and eUICC platform as specified in GSMA

- Sol#39 proposes the similar mechanism as solution #31, with the following differences:

- further describe the attach procedure to any onboarding PLMN using the default operator profile, that is used only for UE onboarding, e.g., contain a default Subscribed S-NSSAI and a default DNN that are appropriate to reach the PS

- further describe the procedure on identifying the UE and the subscription/configuration/credential for remote provisioning using GPSI at PS

When PLMN supports as Onboarding Network and UE initiates the onboarding, a default PLMN operator profile needs to be used to support the functionality to restrict usage to only on-boarding service. So when PLMN supports as Onboarding Network and UE initiates the onboarding, a default PLMN operator profile needs to be used to support the functionality to restrict usage to only on-boarding service. UDM indicates that this operator profile is only for onboarding service. A default subscribed DNN, S-NSSAI is supported for the PDU session to reach to the PS.

## 1.4 UE Parameters Update during the registration procedure

Currently the UPU can only be sent after the Registration procedure. As long as the UE is kept in CM-CONNECTED there is no immediate need to execute the UPU during the Registration procedure i.e. the UPU can be executed directly after the Registration procedure. It is proposed to remove the EN:

*Editor's note: It is FFS whether the UE Parameters Update container can be delivered to the UE during the registration procedure.*

## 1.5 Need to pre-configure the S-NSSAI and DNN in the UE

The following EN can be found:

*Editor's note: the need to pre-configure the S-NSSAI and DNN in the UE and to send it to the UE is FFS as default DNN and S-NSSAI could be used for provisioning to an SNPN. Also, if needed, whether to progress one or more options into normative phase is FFS.*

Whether the UE need to send the S-NSSAI depends if a special network slice is defined for Onboarding, see e.g. clause 1.2.

If a special network slice is defined for Onboarding e.g. SST=Onboarding (no need for SD), then such SST will be described in TS 23.501 Table 5.15.2.2-1 - Standardised SST values. In such case the UE should be hardcoded with the SST of the Onboarding slice to be requested for onboarding procedures. Such SST could not be ever modified. Therefore, there is no need to pre-configure the UE

If there is no special network slice defined for Onboarding and instead a separate indication is defined, then the network slice to use can be decided by the network (as access is restricted to Onboarding there is no need for the UE to provide it).

For DNN, unless the DNN is used to differentiate the PDU Session towards a specific PS, the DNN can be decided by the network i.e. UE can assume "default DNN" is used.

There can be two types of UE in the context of this KI for Onboarding i.e.,

a) an off the shelf UE provisioned with default credentials and a unique UE identifier or a UE may be pre-configured

b) provisioned with initial default configuration including PLMN ID and NID of the SNPN, S-NSSAI, DNN needed to access the provisioning server.

The Editor’s Note mentioned above is applicable for case b. If the UE is pre-configured with the S-NSSAI for the purpose of Onboarding only, then a new SST value needs to be standardized for the purpose of Onboarding. In our view, it is up to the network to decide selecting the AMF and the DNN for the purpose of Onboarding purpose based on an indication provided by the UE. Similar to RLOS, there should be one RRC indication that allows the NG-RAN to select a dedicated AMF for onboarding, and there should be one NAS indication that allows the AMF to e.g. select a dedicated SMF for onboarding and perform other onboarding-related configuration. Given that the solution needs to work for off-the-shelf UE, we do not see the need to use a different mechanism for UEs with additional pre-configuration and propose deleting the corresponding EN on the use of S-NSSAI and DNN. Moreover, we propose to close the Editor’s note on the need for Onboarding indication.1.6 Provisioning of NPN credentials in UDM/UDR

The following EN is written:

*Editor's note: Whether the specific procedure for provisioning of UDM (or AAA) with the UE credentials/subscription data is in scope of 3GPP is FFS.*

The provisioning aspects of regular NPN credentials are not part of the scope of KI #4, nor they typically are part of the scope of SA2. It is therefore proposed to remove the EN and add text indicating these aspects.

## 1.7 Reference to industry-based mechanisms for user plane provisioning of SNPN credentials.

In the following highlighted agreed interim conclusion, for the case of UP provisioning of SO-SNPN credentials the UP remote provisioning protocol used is out of scope of SA2. However, the sentence also includes reference to industry developed mechanisms without any clarification on what type of provisioning will be supported as part of the industry developed mechanisms. For example, in TR 23.700-07, an example user plane protocol in Solution 35 refers to reusing CMPv2 protocol. Though certificate-based provisioning is one of the possible UP provisioning mechanisms that may be used, it is unclear if the industry developed mechanisms can support other EAP-compatible authentication methods (e.g. pre-shared secret, identity-based cryptography, etc.). So, we propose to remove uses industry developed mechanisms from the interim conclusion without specific reference to the industry protocol and leave that discussion to SA3.

When User Plane is used for provisioning of SO-SNPN credentials, the User plane remote provisioning protocol used and how the UE downloads the SNPN credential from the Provisioning Server (PS) after PDU session establishment in the O-SNPN is out of scope of SA2 and uses industry developed mechanisms.

## 1.8 Configuration PDU session

For the Configuration PDU session, all related solutions propose that this PDU session is used only for provisioning of the new subscription/credential.

- Sol#5 uses a well-known or pre-configured S-NSSAI or DNN, or a combination of S-NSSAI and DNN, which is used just for provisioning purposes and has limited connectivity capabilities. The AMF selects a designated SMF, which in turn selects a designated PSA that provides a data connection restricted only to the Provisioning Server. The PCF may in addition provision URSP rules for the UE that restrict communication only to the provisioning server and/or specific applications.

- Sol#27 is similar as Sol#5, with more description on subscription profile (e.g., a list of triplets (IP address, port number, protocol)) that restrict the connectivity of the Onboarding PDU Session. The SMF can get the subscription profile for onboarding PDU Session from local configuration, PS or AMF.

- Sol#31 is similar as Sol#5, with more details on subscription profile (e.g. port ID, valid period, allowed destination address list and QoS information). Further, it describes how the SMF gets from the UDM the restriction information of the onboarding PDU Session in case the ON is PLMN or PNI-NPN.

- Sol#33 is similar as Sol#31 in case the ON is PLMN.

- Sol#35 is similar as Sol#5.

- Sol#39 is similar as Sol#31 in case the ON is PLMN.

- Sol#40 is similar as Sol#5.

It is clear that the PDU session within the ON should be used only for remote provisioning. When User Plane is used for provisioning of SO-SNPN credentials, a restricted PDU session is supported to be dedicated for the remote provisioning based on local configuration or UDM subscription.

# 2. Proposed changes

\*\*\* Start of changes \*\*\*

## 8.4 Key Issue #4: UE onboarding and remote provisioning

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

### 8.4.1 Conclusions for SNPN case

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

- It should be possible to support a registration procedure that enables support for UE onboarding using Default UE credentials and with an O-SNPN as the Onboarding Network (ON).

Editor's note: In order to support UE onboarding using Default UE credentials and O-SNPN as the Onboarding Network (ON) the distribution of security functions when primary authentication is used should be decided by SA WG3, e.g. whether and how to support the primary authentication based on default credential in case DCS is deployed or not.

- It should be possible that one SNPN can take the role of both Onboarding Network (ON) and SO (Subscription Owner), and it should be possible that the ON and SO are different SNPNs i.e. O-SNPN and SO-SNPN.

Editor's note: DCS is potentially introduced to authenticate a UE with default UE credentials or provide means to another entity to do it. There are two potential mechanisms for DCS to authenticate the UE. 1) DCS interacts with O-SNPN and Network Function in SO-SNPN (Subscription Owner SNPN) is not involved in the authentication procedure. As a result, the SO-SNPN is not directly involved with the authentication procedure but gets informed of its result and then performs remote provisioning. 2) DCS interacts with SO-SNPN and Network Function in SO-SNPN (Subscription Owner SNPN) is involved in the authentication procedure. As a result, the SO-SNPN is directly involved and aware of the result of authentication procedure and performs remote provisioning. SA WG3 needs to evaluate the two above mechanisms from security perspective and provide feedback.

Editor's note: The decision on whether primary authentication is required during initial access to the O-SNPN is dependent on SA WG3 feedback; until this feedback is received, it is assumed that such authentication is required.

- The SNPN, which directly interacts with DCS, may determine the corresponding DCS identity or address/domain based on the input from the UE or when primary authentication is used based on information (e.g. DCS address) locally provisioned at SNPN.

Editor’s note: SA3 should provide feedback on whether the UEs permanent identifier (SUPI or SUCI) may be used for finding the DCS identity or address/domain that can authenticate the UE, as well their security properties.

- The DCS can be an entity external to the 5GC of O-SNPN.

- The NG-RAN of the Onboarding network includes information in the SIB so that the UE can discover and select an appropriate O-SNPN. The UE may or may not be pre-configured with O-SNPN network selection information (e.g. O-SNPN network identifiers).

- Upon registration to an SNPN for Onboarding, the UE provides the information at RRC level which indicates the registration is for onboarding. This information will be specified only for SNPN and allows NG-RAN to select an appropriate AMF that supports onboarding procedures.

Editor’s note: Handling of RAN-level congestion is FFS.

- Upon registration to an SNPN for Onboarding, the UE provides the information at NAS level that the registration request is for onboarding to allow AMF to, e.g., select an appropriate SMF and perform other onboarding-related configuration.

- Using PLMN credentials for UE onboarding and PLMN as Onboarding Network (ON) is already possible.

- Onboarding network should support functionality to restrict usage to only on-boarding service.

- When Onboarding network is O-SNPN, the information required to restrict the usage to only onboarding service is locally configured in the AMF, and the AMF restricts the usage when the UE indicates that the registration is for Onboarding (e.g., onboarding registration type) or NG-RAN indicates that the access is for Onboarding.

- When Onboarding network is a PLMN, the functionality to restrict usage is activated for the UE by AMF based on received operator profile from the UDM.

Editor’s note: Whether there is a need to extend subscription information to support a restriction to only on-boarding service is FFS.

- The UE shall initiate de-registration from the on-boarding network after finishing the remote provisioning or the on-boarding network shall initiate the de-registration after successful completion of onboarding or based on timer configured for on-boarding service.

**Remote provisioning for SNPN credentials (Component 2 of KI#4)**

- Usage of a PLMN as Onboarding Network for a UE equipped with a USIM shall be possible. The SO-SNPN credentials can be transmitted to UE via UP connectivity. The UE shall be configured with Default credentials in USIM to register with a PLMN where the UE can register with the Default credentials in order to communicate with the provisioning server. When transmitting through a PLMN, it shall be possible that the SNPN credentials being provisioned are not accessible (e.g. by using an additional credential in the UE) by the PLMN;

- When User Plane is used for provisioning of SO-SNPN credentials, the User plane remote provisioning protocol used and how the UE downloads the SO-SNPN credential from the Provisioning Server (PS) after PDU session establishment in the O-SNPN is out of scope of SA2 ;

- Control Plane remote provisioning based on UE Parameters Update Procedure as defined in TS 23.502 [6] can be used for provisioning of credentials and other information to enable access to SO-SNPN. After Registration Complete, while onboarding is still in progress, UPU is imminent, thus, the NAS signalling connection shall not be released.

Editor's note: SA WG3 feedback will need to be taken into account for including of the CP based provisioning.

Editor’s note: When the PS is a stand-alone entity, how the PS is selected is for FFS.

Editor’s note: For remote provisioning via CP, when the PS is a stand-alone entity the role of PS (as UDM of SNPN or AF with respect to O-SNPN) is FFS.

- Control Plane remote provisioning procedure assumes a Provisioning Server that communicates with the 5GC using 3GPP-defined protocols.

- For the provisioning of IMSI accompanied by AKA credentials, GSMA RSP is used, Provisioning Server (PS) can provision the credential to UE over User Plane (UP) connectivity;

- For the provisioning of Non-3GPP credentials, the credentials can be provided to UE over UP connectivity;

- It shall be possible to pre-configure the Provisioning Server (PS) address, SO-SNPN identity on the UE, and it shall also be possible that the O-SNPN provides the PS address to the UE after successful authentication and authorization. The PS address from the O-SNPN shall be integrity protected. The PS address provided by the network is prioritized, if configured and overrides any PS address stored in the UE. Configuration of PS address to the UE can be supported using one of the following methods:

a. SMF may deliver onboarding configuration data as part of extended Protocol Configuration Options (PCO) in PDU Session Establishment Response to UE. This is similar to use of PCO to configure Autoconfiguration server for UE in Wireless and Wireline Convergence (TR 23.716 [28] clause 6.10).

b. Alternatively, onboarding configuration data may be configured in the UE during Registration Procedure.

c. In addition, onboarding configuration data may be configured in the UE using service specific policies subject to UE capabilities similar to what is used for V2X communications as specified in TS 23.287 [29] clause 5.1.1 for ways how parameters may be made available to the UE and TS 23.287 [29] clause 6.2.5 for AF-based service parameter provisioning and TS 24.587 [30] clause 5.2.4 for configuration parameters such as validity timer, server address and geographical area.

- It is assumed that the UDM (or AAA) of SO-SNPN is provisioned with UE credentials/subscription data when remote provisioning is successfully performed. Existing mechanism for provisioning of UDM/UDR can be reused.

- When User Plane is used for provisioning of SO-SNPN credentials, a restricted PDU session is supported to be dedicated for the remote provisioning. Upon successful establishment of restricted access PDU session, if the UE still does not have a PS address, the device uses a well-known FQDN to perform PS discovery.

NOTE: SA WG3 may evaluate these mechanisms and provide guidance on appropriateness of use for SNPNs.

### 8.4.2 Conclusions for PNI-NPN case

**UE Onboarding for PNI-NPN (Component 1 of KI#4)**

- No enhancement for the UE onboarding (component 1 of KI#4) with PLMN credentials used for primary authentication and PLMN network selection are needed for the case of PNI-NPN credentials provisioning.

**Remote provisioning for PNI-NPN credentials (Component 2 of KI#4)**

- At least network initiated remote provisioning of credentials to allow access to PNI-NPN services should be supported in Rel-17;

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

Editor's note: SA WG3 feedback for the suitability of the procedure will need to be taken into account.

Editor's note: whether an extra security layer for protection of credentials between PS and UE is needed should be decided by SA WG3.

- For User Plane remote provisioning:

- The protocol for provisioning of PNI-NPN credentials used for NSSAA and/or PDU Session secondary authentication, i.e. how the UE download the NPN credential from the PS after PDU session establishment in PNI-NPN, is out of scope of SA WG2;

- The PS address and DNN/NSSAI used to access PS may be provided to the UE during or after the Registration procedure;

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

Editor's note: The vertical may verify the UE before PNI-NPN credential is provisioned to UE, and how this is done should be decided by SA WG3.

- Upon successful remote provisioning of the UE, the UE Subscription Data in the UDM/UDR may be updated to enable the access to the PNI-NPN.

Editor's note: for PNI-NPN credentials remote provisioning, whether the 3GPP operator could decide to update the UE Subscription Data (e.g., S-NSSAI, DNN, CAG information) in the UDM/UDR used to access to the PNI-NPN based on the input from the vertical which may be outside 3GPP operator domain should be decided by SA WG3.

- For Control Plane remote provisioning:

- It is assumed that the PS communicates with the 5GC using 3GPP defined protocols.

\*\*\* End of changes \*\*\*