**3GPP TSG-****SA3 Meeting #104-e *S3-213028r1***

**e-meeting, 16 – 27 August 2021**

**Source: Philips International B.V., Lenovo, Motorola Mobility**

**Title: Addressing Editor’s notes of KI#2**

**Document for: Approval**

**Agenda Item: 5.12**

# 1 Decision/action requested

***We request SA3 to consider incorporating the suggested updates to KI#2 of TR 33.857.***

# 2 Rationale

Key Issue #2 “Provisioning of credentials” in TR 33.857 still has various Editor’s notes. Because these have not been discussed since they were introduced, this effectively blocked progress on any solutions for this key issue, despite the statement in one of the Editor’s notes that it is possible to study solutions for this key issue in this TR. In this pCR we propose to address the Editor’s notes and/or clarify why these can be removed.

Editor’s note: The entity granting the authorization is FFS.

* Analysis and proposed resolution: The owner of the credential to be provisioned to allow a UE to access a Subscription Owner SNPN (SO-SNPN) has the ultimate authorization authority to enable provisioning. Since the credential owner wants to allow the UE to gain access to the SO-SNPN it can be assumed that there must be some business/trust relation between them. According to the SA2 architecture for onboarding and provisioning to SNPNs, granting the authorization by the Credential owner/SO-SNPN is configured and delegated to the Provisioning Server (PS). The interface between the credential owner and the PS regarding this delegation is out of scope of 3GPP. However, it can be assumed that if the PS is not configured to allow the provisioning of one or more of the involved UEs, the provisioning will fail. Note that it can be further assumed that the PS is not authorized to just provision any arbitrary UE, only those UEs that have been authenticated by the DCS with their known default credentials. We propose to clarify these aspects in the text of KI#2 and in this way address the Editor’s note from the PS point of view.

From the UE point of view, the authorization to allow the UE to be provisioned may require explicit user consent or the UE may have implemented some form of implicit consent (e.g. to enable provisioning when the UE is powered up for the first time and encounters an Onboarding SNPN (O-SNPN) that enables onboarding and provisioning, e.g. after receiving the respective broadcasted information as specified in Section 5.30.2.10.2.3 of TS 23.501). The implementation details for explicit user consent and implicit consent can be assumed to be out of scope of 3GPP. As specified in 5.30.2.10.3 it can be further assumed that in case the onboarding network is a PLMN, and not an O-SPNP, that the UE needs to have the relevant PLMN subscription to do so (e.g. to be able to access the DNN/S-NSSAI used for user plane remote provisioning). We propose to clarify this in the text of KI#2 to address the UE part of the Editor’s Note.

Editor's Note: User intent to authorize the provisioning is ffs.

* Analysis and proposed resolution: This relates to the above analysis of the Editor’s note about which entity grants the authorization. As mentioned above it is an implementation decision on whether to require explicit user consent or implicit consent. Since the UE explicitly initiates an onboarding connection, and the UE even has to include some attributes to indicate that it is an onboarding connection (e.g. as specified in Section 5.30.2.10.2.6 of TS 23.501), it can be assumed that a UE implementation does not arbitrarily initiates such onboarding connection, and initiates it only based on user intent (e.g. pressing some button or external trigger out of scope of 3GPP). A UE can even implement an additional confirmation step to accept the provisioning or not accept any provisioning after it has already been provisioned (and e.g. require a factor reset before it can be provisioned again). All these implementation options seems to be out-of-scope of 3GPP, so the attributes included in the onboarding connection should be sufficient to indicate that the user intends to provision the device. We propose to clarify this in the text of KI#2 to address this Editor’s Note.

Editor’s note: The end points for the protection in the above requirement (i.e. *”Credentials shall be confidentiality protected, integrity protected, and replay protected during remote provisioning”*) are FFS.

* Analysis and proposed resolution: Two cases can be distinguished:
1. PS and O-SNPN do not have a trust relationship (likely the most common case): in this case it clear that the credentials should not in any way be exposed to the O-SNPN, hence the end points for the protection are the UE and the PS.
2. PS and O-SNPN do have a trust relationship: even though a trust relationship may exist between the PS and O-SNPN it is still safest to have end-to-end confidentiality, integrity and replay protection directly between the UE and the PS. This simplifies the solution, otherwise the various interfaces would need to be protected individually. At least for release 17 we can assume the end points to be the UE and the PS.

We propose to clarify the text of KI#2 accordingly in order to address this Editor’s note.

Editor's Note: Whether the solution covers all type of devices (e.g. MEs with limited resources not able to run certain types of security protocols) is ffs.

* Analysis and proposed resolution: Given that for access to NPNs currently only two primary authentication mechanisms have been defined, i.e. either based EAP-AKA or EAP-TLS, it seems reasonable to assume that in scope of release 17 at a minimum EAP and AKA or TLS needs to be supported by the onboarding device. Otherwise, the UE after onboarding would not be able to access the SO-NPN anyway. In order to make progress we can assume provisioning of EAP-AKA related credentials to be out-of-scope, and only consider provisioning of EAP-TLS related credentials. This could cover a fair amount of different devices that would be able to support such type of credentials, and certainly beats the alternative of not specifying any secure provisioning in release 17. Given the importance to look at lightweight solutions, this implies that we should not only look at user plane solutions, but also control plane type of solution. This is anyway an open issue that SA2 asked SA3 to look into in their liaison, i.e. whether control plane solutions can provide sufficient protection. We propose to clarify the text of KI#2 regarding these aspects in order to address this Editor’s note.

Editor’s note: It is FFS whether the protection in the above requirement requires to specify a solution in normative phase or whether it is left to implementation. However, it is possible to study solutions for this key issue in this TR.

* This Editor’s note seems to document common practice in SA3 studies. After the solutions are documented and evaluated in the TR, depending on the conclusions it can then be decided which solutions (if any) would be specified as part of the WID or not. We can leave this Editor's note in for now, if companies are not ready yet to take it out. The Editor’s note anyway states very clearly that this particular Editor’s note cannot and should not be used to block solution proposals and evaluation of the solutions in the TR. It is certainly important that solutions and evaluation of those studies are allowed to continue, because in order to try to address the release 17 service requirements in TS 22.261 3GPP should at least define one working solution for provisioning of UEs to gain access to an SNPN.

Editor's Note: Further requirements is ffs.

In principle we can leave it in, but given the limited time left for release 17 to take new requirements on board and since no company has submitted new requirements for this KI for several meeting, we propose to remove it.

# 3 Detailed proposal

We ask SA3 to kindly consider including the following change to TR 33.857 to address the above mentioned editor’s notes KI#2 and to provide some clarifications.

**\*\*\*\* START OF CHANGES \*\*\*\***

## 5.2 Key Issue #2: Provisioning of Credentials

### 5.2.1 Key issue details

This Key Issue aims at addressing security implications introduced in solutions related to Key Issue #4 in TR 23.700-07 [3].

The objective of Key Issue #4 in TR 23.700-07 [3] is twofold, UE onboarding and then remote provisioning of non USIM credentials for SNPN and PNI-NPN This Key Issue aims at studying the corresponding security implications related to the provisioning. For PNI-NPNs, only credentials for secondary and slice-specific authentication need to be considered.

The UE can perform the onboarding procedure with an onboarding network, and then the UE may be remotely provisioned with the credentials by a Provisioning Server (PS). At least for release 17 it can be assumed that the security end points of the provisioning are the UE and the PS, and that the credentials should not be exposed to the O-SNPN. Furthermore in Release 17, it is assumed there is a trust relationship between the PS and the credential owners, and that the interfaces between the credential owner and PS are out of scope of 3GPP.. It can be assumed that the PS is properly configured to act on behalf of the credential owner for provisioning UEs to gain access to the SO-SNPN, including the configuration of limitations to prevent any arbitrary UE being provisioning. In case the onboarding network is a PLMN, and not an O-SPNP, then the UE in addition shall have the relevant PLMN subscription to so initiate an onboarding connection to enable provisioning (e.g. to be able to access the DNN/S-NSSAI used for user plane remote provisioning).

Designing completely new protocols is not in scope of this key issue.

### 5.2.2 Security threats

An unauthorized UE may be able to access PS for maliciously requiring remote provisioning service.

An unauthorized PS may be able to provide wrong remote provisioning service to the UE.

Unprotected provisioning of credentials may cause the SNPN credentials to be obtained or manipulated.

### 5.2.3 Potential security requirements

The UE and the PS should be authorized for remote provisioning.

NOTE: In release 17, it is assumed that the interface to authorize the PS by the credential owner is out-of-scope of 3GPP and that the PS is properly configured to act on behalf of the credential owner for provisioning UEs to gain access to the SO-SNPN. Furthermore, in release 17 it is assumed that any mechanism for explicit or implicit user consent for enabling remote provisioning is UE implementation specific and out-of-scope of 3GPP. These assumptions need to be clarified in any normative specification resulting from this key issue.

Credentials shall be confidentiality protected, integrity protected, and replay protected during remote provisioning between the UE and the PS.

NOTE: In release 17, remote provisioning is assumed to be restricted to credentials related to non-AKA key deriving EAP methods as defined in TS 33.501 (in case of SNPN), and remote provisioning of credentials for NSSAA or credentials for secondary authentication/authorization (in case of PNI-NPN).

Editor’s note: It is FFS whether the protection in the above requirement requires to specify a solution in normative phase or whether it is left to implementation. However, it is possible to study solutions for this key issue in this TR.

Editor's Note: Further requirements is ffs.

**\*\*\*\* END OF CHANGES \*\*\*\***