**3GPP TSG-SA3 Meeting #108e-AdHoc *S3-222545r2***

**e-meeting, 10 - 14 October 2022** merger of 2545, 2546, 2830, 2650, 2745, 2899

**Source: Huawei, HiSilicon, Nokia, ZTE, Lenovo, Xiaomi**

**Title: Update to key issue 1**

**Document for: Approval**

**Agenda Item: 5.12**

# 1 Decision/action requested

***Approve the new KI proposal to eNS3 TR33.886***

# 2 References

[1]

# 3 Rationale

The contribution proposes to update key issue 1 with security threats and requirments. Specifically, this key issue addresses security issues related to the downlink only, i.e. the link from the network side (UDM) to the UE. As to the uplink, it will be addressed in a separate key issue.

# 4 Detailed proposal

pCR

\*\*\* BEGINNING OF CHANGES \*\*\*

## 4.1 Key Issue #1: providing VPLMN slice information to roaming UE

### 4.1.1 Key issue details

The following requirement for a 5G network is specified in TS 22.261[2] in order to support a roaming UE activating network slice services

*For a roaming UE activating a service/application requiring a network slice not offered by the serving network but available in the area from other network(s), the HPLMN shall be able to provide the UE with prioritization information of the VPLMNs with which the UE may register for the network slice*

A related key issue is also being studied in TR 23.700-41 [3] for possible procedure changes to automatic PLMN selection for a roaming UE requiring a network slice not offered by the serving network but available in the area from other network(s). It is expected that the corresponding security procedure will be affected (e.g. Steering of Roaming in TS33.501 [4]) in order to support the HPLMN to provide a roaming UE the VPLMN slice information.

A few solutions in TR 23.700-41 [3] are considering that a roaming UE can send a container (transparent for AMF) to its HPLMN, e.g. in a UE initiated procedure to indicate the UPU/SoR capabilities, a new container (transparent for AMF) may be included from a roaming UE. The container may contain UE information that is pertinent to triggering the HPLMN service providing the UE with slice-specific prioritization information of VPLMNs, to which the UE may register. Security aspects on protecting the container or information therein provided by the UE need to be studied as well.

In this key issue, the following aspects will be studied:

- Would security procedures be impacted? If so which security procedures are impacted in support of HPLMN proving a roaming UE with information about prioritization information of the VPLMNs with which the UE may register for the network slice?

- How to secure the procedures impacted.

- How the UE can securely send UE information (e.g. UE UPU/SoR capabilities, capability to handle Slice-Aware SoR information, UE location, Requested NSSAI, information on network slice not offered by the serving network) to the home network via the visited network when required.

- If the serving network does not offer the network slice requested by the UE, how the UE can securely report to the HPLMN.

### 4.1.2 Security threats

As specified in TS33.501 [4], the network-specific steering-of-roaming information sent to a UE is integrity protected to prevent tampering from VPLMN. Besides, the information is only sent to the UE after authentication and authorization. However, if slice-specific information for steering of roaming is not integrity protected, it may be tampered by the VPLMN. If the information is sent to an unauthorized UE, it may cause leakage of the information.

If a roaming UE needs to send the triggering information to the HPLMN that is not protected, the information may be tampered or discarded by the VPLMN. The HPLMN will not be able to provide the UE with prioritized VPLMN information.

The HPLMN will not be able to provision the UE with prioritized VPLMN information if the serving network hides the information about rejected services or services could not be offered by the VPLMN, which can further lead to service failure.

### 4.1.3 Potential security requirements

The 5G system shall secure procedures (integrity protection, protection from siliently dropping messages) for the HPLMN to provide a roaming UE with information about slice availability and network prioritization.

The 5G system shall secure the procedure of a roaming UE sending information to its HPLMN in order for the HPLMN to provide VPLMN information about slice availability and network prioritization.

Editor's note: Whether a roaming UE needs to send triggering information (and also content details) or rejected slice information to its HPLMN so that the HPLMN can provide slice availability and prioritization information in VPLMNs should be aligned to the conclusions in TR 23.700-41 [3].

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