**3GPP TSG-SA3 Meeting #109AdHoc-e *commenting - draft\_S3-230316-r4***

**Electronic meeting, 16 - 20 January 2023**

**Source: Ericsson, Nokia Shanghai Bell, Mavenir**

**Title: Update of Key issue #12: Security in Hosted SEPP scenarios**

**Document for: Approval**

**Agenda Item: 5.24**

# 1 Decision/action requested

***Approve the pCR to TR 33.875 [1] below.***

# 2 References

[1] 3GPP TR 33.875: "Study on enhanced security aspects of the 5G Service Based Architecture (SBA)"

# 3 Rationale

This paper provides an update of “Key issue #12: Security in Hosted SEPP scenarios”.

# 4 Detailed proposal

\*\*\* BEGIN CHANGE 1 \*\*\*

## 5.12 Key issue #12: Security in Hosted SEPP scenarios

### 5.12.1 Introduction

It has been discussed that SEPPs can be deployed in different ways:

- Local SEPP: The SEPP is deployed within the PLMN. This is the deployment as specified by TS 33.501.



Figure 5.12.1-1 Local SEPP deployment

- Outsourced SEPP: The SEPP is outsourced by the PLMN and deployed within the PLMN infrastructure and considered within the PLMN secure domain Several PLMNs which form an Operator Group can use the same outsourced SEPP. This scenario is described as an Operator Group Roaming Hub in KI#10 and GSMA NG.113 [X].



Figure 5.12.1-2 Outsourced SEPP deployment

- Hosted SEPP: The SEPP is outsourced by the PLMN to an external entity and deployed outside the PLMN.



Figure 5.12.1-3 Hosted SEPP deployment

The “Hosted SEPP” scenario is subject of this key issue.

In hosted SEPP deployment scenario, the hosted SEPP will still be responsible for

- Terminating the N32c/f interface (TLS, PRINS) - N32 side

- Roaming Security Function - Topology Hiding - N32 side

- Roaming Security Functions – Filtering criteria and capabilities – N32 side

- Security Function – Filtering criteria and possible Firewall – NF side. This applies if HPLMN consider this as PLMN edge..

### 5.12.2 Key issue details

 Following issues are required to be worked through in hosted SEPP scenario.

- Whether the IPX, which hosts the SEPP, uses certificates from its own CA or uses certificates issued from the Home PLMN and whether the Home PLMN is willing to consider and use the IPX's CA as trusted CA

- Whether the Hosted SEPP can handle private addresses of the Home PMN

- Whether the Hosted SEPP is trusted to enforce market specific regulatory requirements

- In addition, the edge of the HPLMN deployments may need protection, e.g., Topology Hiding, filtering criteria and firewall, etc.

The PKI infrastructure can be deployed in different ways for issuing the digital identities to the hosted SEPP’s PLMN facing SBI and external facing N32.

According to GSMA LS SA3-221737, a PLMN can use both Local SEPPs (managed by PLMN) and Hosted SEPPs, i.e., the PLMN has Local SEPPs each handling a set of roaming relations, while the Hosted SEPPs handle a different set of roaming relations.

In a scenario of Hosted SEPP additional risks arise. These include:

- attacks on the traffic between PLMN and Hosted SEPP,

- insufficient protection of the PLMN core,

- lack of a way to attribute the cause of a security issue to a specific actor (e.g., the operator or the Hosted SEPP provider),

- an unauthorized actor claiming to be a Hosted SEPP provider of an operator towards its roaming partners, and

- risks due to one actor operating Hosted SEPPs for multiple PLMNs.

### 5.12.3 Security requirements

Existing requirements in TS 33.501 on the SEPP shall apply in the Hosted SEPP scenario, unless there are explicit exceptions. Specifically, edge protection requirements can differ from the existing requirements since the hosted SEPP is not deployed at the edge of the PLMN.

Existing NFs and SCPs should be impacted as least as possible.

For the scenario of hosted SEPP, the following requirements shall apply:

- The Hosted SEPP providers shall use their own unique credentials to authenticate themselves. Moreover, it shall be possible for operators that receive signalling from a Hosted SEPP provider pertaining to a roaming partner to verify that the Hosted SEPP provider has been authorised by the roaming partner.

- The connection between the PLMN and the Hosted SEPP provider shall be confidentiality, integrity, and replay protected.

- The solution should enable the Hosted SEPP providers to operate SEPPs for multiple PLMNs in a way that isolates the SEPP instances operated for different PLMNs from each other for security reasons. Specifically, if one of the instances gets corrupted or otherwise malfunctions, other instances should remain unaffected as much as possible.

\*\*\* END CHANGE 1 \*\*\*