**3GPP TSG-SA3 Meeting #109AdHoc-e *draft\_ S3-230023-r1***

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

**Source: BSI, Nokia, Nokia Shanghai Bell, Deutsche Telekom**

**Title: KI12 solution 19 update on hosted SEPP**

**Document for: Approval, Information, Discussion**

**Agenda Item: 5.24**

# 1 Decision/action requested

***In this box give a very clear / short /concise statement of what is wanted.***

# 2 References

[1] TR 33.875

# 3 Rationale

*Improvement of solution description. More precise wordings for the proposed normative text that forms part of the solution. Also, added a requirement to support certificate pinning.*

# 4 Detailed proposal

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

## 6.19 Solution #19: Hosted SEPP requirements

### 6.19.1 Introduction

This solution addresses key issue #12. It provides input for text that needs to be adapted for clarification of a deployment option for SEPP of a PLMN, if hosted by an entity external to the PLMN.

### 6.19.2 Solution details

This solution is addressing the Hosted SEPP as described in KI#12.

If the Hosted SEPP provider is contracted by several PLMNs, it hosts several distinct Hosted SEPP instances for the different PLMNs.

A PLMN can have a Local SEPP (managed by the PLMN) and a Hosted SEPP (instance), both handling disjoint sets of roaming relations.

It is proposed to add the following definitions to 33.501:

**“Hosted SEPP:** A SEPP that is hosted and operated by a provider outside the PLMN, for example an IPX provider. From the perspective of roaming partners, PLMN trust extends to the Hosted SEPP instance representing this PLMN. A Hosted SEPP provider can operate Hosted SEPPs for multiple PLMNs.

**Local SEPP:** A SEPP of a PLMN that is operated by an MNO.

Each SEPP type serves a set of roaming relations that is disjoint from the set of roaming relations served by other SEPP types.”

It is further proposed to have an addition to the general requirements in 33.501 clause 5.9.3 (Requirements for e2e core network interconnection security) as follows:

“From the roaming partner’s point of view, a Hosted SEPP shall behave in the same way as the SEPP.

All SBI messages transmitted between the PLMN and the Hosted SEPP deployment shall be confidentiality, integrity, and replay protected.

A Hosted SEPP provider shall isolate the processing for each PLMN from the processing for other PLMNs.

A Hosted SEPP provider shall use a different TLS certificate per PLMN, as the MNC and MCC of that PLMN are encoded in the certificate (as specified in TS 23.003, Table 6.1.3c.3-1). This certificate shall be issued to the Hosted SEPP provider under its own unique name, and hence shall contain both the PLMN-ID and its own unique identifier.

A Hosted SEPP shall only be able to obtain a certificate with an MCC/MNC combination if the affected MNO has previously authorized this.”

As roaming with hosted SEPPs potentially increases the number of root CAs in the overall system, the need to support certificate pinning also increases. Having in mind the trust establishment mechanism communicated by the GSMA in and acknowledged by 3GPP in SA3-223910, it is proposed to add the following requirement to 33.501.

*“The SEPP shall support Certificate Pinning in the following way: It shall maintain a set of lists containing root CA certificates, as well as a mapping of PLMN-IDs to this set. The mapping associates each PLMN-ID with a given root CA certificate list. During N32-c connection setup, the SEPP shall map the PLMN-ID of the remote SEPP leaf (server or client) certificate to the associated root CA certificate list for the purposes of certificate chain verification. Only the root CA certificates in the associated list shall be treated as trusted during certificate chain verification. If the remote SEPP certificate contains multiple PLMN-IDs that are mapped to different root CA certificate lists, then that certificate shall be rejected.”*

Finally, it is proposed to have an additional NOTE referring to Hosted SEPP concept in 33.501 clause 13.1.2 (Protection between SEPPs) as follows:

“If a Hosted SEPP is deployed as the edge of one PLMN and in the same security zone, the same protection requirements apply to this Hosted SEPP as they apply to a SEPP in general. Furthermore, the Hosted-SEPP-specific protection requirements in clause 5.9.3 apply.”

### 6.19.3 Evaluation

Whether to use a Hosted SEPP is a business decision. Nevertheless, it is important to provide a minimal set of requirements covering this deployment option.

Guidelines for naming are provided for Hosted SEPP by GSMA already and 3GPP TS 33.310 may need to be checked for consistency with respect to new security requirements. Such requirements may need to be communicated to GSMA as well.

Editor’s Note: Further evaluation is FFS.

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