**3GPP TSG-SA3 Meeting #109AdHoc-e *commenting - draft\_S3-230316-r1***

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

**Source: Nokia, Nokia Shanghai Bell**

**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.

- Outsourced SEPP: The SEPP is outsourced by the PLMN but deployed within the same PLMN domain. Several PLMNs operated under the same PLMN domain can use this SEPP. This scenario refers to the usage of an Operator Group Roaming Hub operating a SEPP on behalf of all group PLMNs. It has been addressed by GSMA NG.113 [X].

- Hosted SEPP: The SEPP is outsourced by the PLMN and deployed outside the PLMN

The scenario, in which the operator decides to let its SEPP being operated by an external entity is called the “Hosted SEPP” scenario and subject of this key issue.

The Hosted SEPP scenario introduces security requirements which must be fulfilled by N32 between 2 SEPPs and by the connection between PLMN network functions and a SEPP if hosted outside the PLMN.

### 5.12.2 Key issue details

The decision of an operator to let a SEPP being operated by an external entity can be independent of whether and which IPX providers are used, and whether and which roaming hub(s) are used. See KI#10 for this topic.

In case an operator uses a Hosted SEPP, the security perimeter of the PLMN as described in TS 33.501, clause 4.2.1, extends to an entity external to the PLMN.

The following requirements specified in TS 33.501 still apply:   
"The 5G System architecture introduces a Security Edge Protection Proxy (SEPP) as an entity sitting at the perimeter of the PLMN for protecting control plane messages." and   
"The SEPP enforces inter-PLMN security on the N32 interface."

Hosted SEPP functions among others are:

(1) Terminating the N32c/f interface and authenticating the roaming partner (TLS, PRINS). See [1] clause 5.9.3.2 requirement:   
"The SEPP shall protect application layer control plane messages between two NFs belonging to different PLMNs or SNPNs that use the N32 interface to communicate with each other." and   
"The SEPP shall perform mutual authentication and negotiation of cipher suites with the SEPP in the roaming network."

(2) Roaming Security Functions (Topology Hiding and Firewalls) [1] clause 5.9.3.2   
"The SEPP shall perform topology hiding by limiting the internal topology information visible to external parties."

(3) Shielding PLMN external CAs towards the PMN internal NFs. [1] clause 5.9.3.2   
"The SEPP shall protect application layer control plane messages between two NFs belonging to different PLMNs or SNPNs that use the N32 interface to communicate with each other."

(4) Bridging between PMN external and internal IP addressing schemas (private, public) [1] clause 5.9.3.2   
"As a reverse proxy the SEPP shall provide a single point of access and control to internal NFs."

(5) Enforcement of market specific regulatory requirements to have a SEPP PLMN internally within HPLMN. [3] clause "1) Roaming Hub"   
"Furthermore, regulation in some countries may require that the PLMN SEPP be deployed in the PLMN and located in the country where the PLMN operates."

According to GSMA LS SA3-221737, a PLMN may 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 where an entity external to the PLMN operates all or some of the SEPPs of a PLMN new risks may arise. These include:

- attacks on the traffic between PLMN and Hosted SEPP,

- missing edge protection at the PLMN,

- lack of a way to attribute the cause of a security issue to a specific actor (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 different 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 outsourcing a 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 \*\*\*