**3GPP TSG-SA3 Meeting #109AdHoc-e *S3-23xxxx***

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

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

**Title: KI10 update on RHUB**

**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

*Removes inconsisteny in decription of roaming hub types, improves description of key issue.*

# 4 Detailed proposal

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

1st CHANGE

### 5.10.1 Introduction

In roaming scenarios, the communication between the visited network and the home network is sometimes mediated and routed through intermediaries. The following types of intermediaries exist.

**IPX providers:** While, traditionally, for some roaming relations, they simply route the traffic, for others they actively modify certain messages in order to establish or enhance interoperability.

**Roaming hubs:** There are two types of roaming hub, as follows.

* **Public Roaming Hubs**. offer a contractual and technical framework that enables operators to avoid entering a very large number of roaming agreements with individual other operators in order to achieve a large roaming coverage. By contracting the roaming hub, the operator obtains access to a large roaming footprint, without individually contracting the operators that are mediated through the hub. Apart from mediating the signalling, roaming hubs typically also mediate the billing. GSMA introduced the concept of roaming hubs to 3GPP in LS S3-213806.
* **Operator Group Roaming Hubs** offer similar services as public roaming hubs, and are special in that they are used by group network operator companies that reside in the same security domain to consolidate and secure operator group roaming.

The key issue looks at N32 security in intermediary scenarios, in particular roaming hub scenarios that have not been addressed in TS 33.501 so far.

2nd CHANGE

>>> PROPOSE TO SHIFT THIS CHANGE TO S3-230316

### 5.12.2 Key issue details

The decision of an operator to outsource the operation of a SEPP to 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. However, it is possible that an IPX provider, a roaming hub, or any other external entity takes the role of the Hosted SEPP provider.

In a Hosted SEPP scenario it is necessary to consider different perspectives when assessing the security perimeter boundaries. From the roaming partners’s perspective, the security perimeter of the PLMN extends to the Hosted SEPP provider, as described in TS 33.501, clause 4.2.1. From the perspective of the PLMN itself, the Hosted SEPP provider operates within its own security domain, especially since it may serve multiple PLMNs as a Hosted SEPP provider.

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.

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