**3GPP TSG-SA3 Meeting #106-e *draft\_S3-220389-r1***

**e-meeting, 14 - 25 February 2022**

**Source: Nokia, Nokia Shanghai Bell**

**Title: New KI on N32 security in Roaming Hub scenarios**

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

**Agenda Item: 5.11**

# 1 Decision/action requested

***KI on N32 security in Roaming Hub scenarios.***

# 2 References

[1] TR 33.875

# 3 Rationale

*Study has been extended to R18 to also cover N32 security topic. A new key issue is added on N32 security in Roaming Hub scenarios.*

# 4 Detailed proposal

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

## X.Y. Key issue #Y: N32 security in Roaming Hub scenarios

### X.Y.1 Introduction

Standardized N32 security mechanisms protect the communication between two SEPPs in two PLMNs if the SEPPS are either directly communicating with each other or communicating via IPX providers. The concept of roaming hub is traditionally a topic tackled by GSMA, having not been addressed by 3GPP so far.

A roaming hub is an entity that has commercial roaming agreements with many PLMNs. It sells access to these roaming agreements to interested home network operators, taking over the correct routing between PLMNs contracting the roaming hub, possibly also via interconnections, i.e., IPX providers. A roaming hub provides contracting network operators fast wide access to other network operators without the need for each network operator to establish a direct business relationship with the other network operators.

This key issue studies whether the current security mechanisms over N32 are sufficient to cover roaming hub scenarios or additions are needed.

### X.Y.2 Key issue details

The concept of N32 security assumes for N32-c the direct contact between two network operators to decide on the protocol used for sending service messages in N32-f. The N32-c direct contact is established via TLS. In the initial phase, the security protocol for N32-f is negotiated. I.e., if direct connection between the two communicating network operators exists or IPX providers are only routing messages, TLS can be used. Otherwise, application layer security with PRINS may be selected for N32-f, which allows an end-to-end control of information between two SEPPs, that can be visible and modifiable on the path between the two end points. In this application layer security case, N32-c is also used to negotiate protection and modification policies, before service messages between client and consumer can be sent via N32-f. In case of TLS used for N32-f, there is no way to modify any information on the path.

If network operators communicate with each other via roaming hubs, it depends on the deployment model how N32 security is applied. According to GSMA, several models of outsourcing a SEPP to IPX or having a SEPP in a roaming hub are discussed. Per definition N32 security is applied between 2 SEPPs. If both PLMNs (or their contracted IPX operate) their own SEPP and the communication is via a roaming hub that also operates a SEPP, then there are in fact two N32 connections, i.e., one N32 security connection would be established between Mobile Network Operator1 and roaming hub and another N32 secure connection is required between roaming hub and Mobile Network Operator2. In this case, there is no end-to-end security relation between the PLMNs anymore, since the roaming hub is able to manipulate messages in between. Also negotiation via N32-c can only be between one operator and the roaming hub.

This key issue investigates whether existing concepts for N32 security are sufficient and whether there is an additional need to specify N32 security for roaming hub scenarios.

### X.Y.3 Security requirements

### TBD

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