**3GPP TSG-SA3 Meeting #116 *S3-242554-r1***

Jeju, South Korea, 20th - 24th May 2024

**Source: Nokia, Nokia Shanghai Bell**

**Title: Solution to KI1 - Reuse SEG to protect N4**

**Document for: Approval**

**Agenda Item: 5.3**

# 1 Decision/action requested

***It is requested to approve the pCR for inclusion in TR 33.757***

# 2 References

# 3 Rationale

The pCR proposes a new solution to KI#1 which extends the SEG features to address the requirements.

# 4 Detailed proposal

Include the solution into TR 33.757 for KI 1.

**\*\*\*\*** START OF CHANGE **\*\*\*\***

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 22.261: "Service requirements for the 5G system;Stage 1".

[3] 3GPP TS 33.501: "Security architecture and procedures for 5G system"

[4] 3GPP TS 23.502: "Procedures for the 5G System (5GS)"

[5] 3GPP TS 29.244: "Interface between the Control Plane and the User Plane nodes"

[6] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)"

[7] IETF RFC 4303: "IP Encapsulating Security Payload (ESP)"

[8] 3GPP TS 23.273: " 5G System (5GS) Location Services (LCS); Stage 2"

[9] 3GPP TS 23.501: " System architecture for the 5G System (5GS); Stage 2"

[10] 3GPP TS 29.500: "Technical Realization of Service Based Architecture"

[11] 3GPP TS 33.210: "Network Domain Security (NDS); IP network layer security"

**\*\*\*\*** NEXT CHANGE **\*\*\*\***

## 7.Y Solution #Y: Extended SEG to support topology hiding and message inspection.

### 7.Y.1 Introduction

TS 33.210 [11] clause 4.5 specifies the SEG as the border component to which all IP traffic shall pass through when leaving or entering a security domain. As the NPN and PLNM domains are perceived as separate security domains this solution proposes to extend the SEG to support topology hiding and message inspection. As described in TS 33.501 [3] clause 9.9 the N4 interface already support IPsec ESP and IKE-v2 certificate-based authentication.

As SEG fulfils most of the requirements for KI#1, its proposed to reuse the SEG and extend the functionality to include message inspection and topology hiding.

### 7.Y.2 Solution detail

Figure 1 shows the architecture as described in TS 33.501 [3] clause 9.9 and TS 33.210 [11] clause 4.5. 

Figure 1: Architecture.

The solution proposes to utilise the IPsec ESP for confidentiality protection between the SEG’s in their respective domain. Mutual authentication and authorisation are enabled by IKE-v2 certificate-based authentication. In addition, message filtering can be supported. This is already specified in TS 33.210 [11] and TS 33.501 [3].

As the SEG’s terminates the IPsec tunnel, messages on the N4 interface are in plaintext between the SMF and SEG and SEG and UPF, which enables the SEG to enforce bi-directional topology hiding and message inspection. Therefore, it’s proposed to use the already specified architecture to protect the N4 interface but extend the feature set of the SEG to include topology hiding and message inspection. The enablement of feature set is based on configuration.

To support message inspection besides message filtering the SEG needs to be extended to be N4 message content aware.

### 7.Y.3 Evaluation

The solution solves the requirements stated in KI#1 by.

* Enabling mutual topology hiding by deploying a SEG in each domain and thereby enforcing the topology hiding prior to sending the message cross the boundary.
* Enhances the message filtering already embedded in the SEG to block malformed or incorrect messages.
* Utilises the already standardised means to mutual authenticate and authorise the endpoints to which the interface is established.

Editor’s note: Assessment of LI requirements is FFS.

**\*\*\*\*** END OF CHANGE **\*\*\*\***