**3GPP TSG-SA3 Meeting #116 *S3-242555-r2***

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

**Source: Nokia, Nokia Shanghai Bell**

**Title: Solution to KI2 – Extension of SCP**

**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

This pCR proposes a solution to KI#2 which extends the SCP to support topology hiding and message inspection.

# 4 Detailed proposal

Please include the solution into TR 33.757 for KI#2.

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

## 7.Y Solution #Y: Extended SCP

### 7.Y.1 Introduction

This solution proposes to extend the SCP to include topology hiding and message inspection. The precondition of the SCP configuration is communication type C or D where the SCP acts as an intermediate function and the network functions indirectly communicates through the SCP. More information concerning the communication types can be found in TS 23.501 [9] Annex E and G.

### 7.Y.2 Solution details

The solution extends the SCP functionality to include topology hiding and message inspection based on policy. The solution is explained through a simplified procedure, subscribe/notify from NPN to PLNM, but the solution also applies to requests from the PLNM to NPN, but in this case the NRF and SCP in the customer domain applies the topology hiding and message inspection. Figures 1 show the high-level procedure.

Figure 1: SCP based topology hiding.

1. The AMF in customer domain requestion to subscribe to a service in the UDM in the PLMN domain. In the CCA a distinct identifier of the AMF in customer premise is applied.

2. The SCP discovers the UDM and includes the CCA in the request.

3-4. The NRF verifies the CCA and according to policy, if the NF ID belongs to another domain verifies that the discovery request origins from the SCP.

5. The SCP requests an access token from the NRF.

6-7. The NRF reverifies the CCA according to the same steps as described in step 3. If Valid, the NRF include the NF ID in the access token.

8. The SCP applies topology hiding by substituting the callbacks provided by the AMF with callbacks local to the SCP. The SCP stores the mapping between the local callback and AMF callback.

9. The SCP registers with the local callbacks at the UDM services. It includes the access token in the request.

10-13. The UDM verifies the access token and according to policy, verifies that the origin of the request is from the SCP if the NF ID belongs to an external domain.

14-16: The UDM triggers the notification of the AMF. The initial callback terminates in SCP which based on translating triggers the callback provided by the AMF.

In all cases the SCP can apply message inspection before forwarding messages to the NRF or service producer.

### 7.Y.3 Evaluation

The solution fulfils the requirements for KI#2 by.

* Adding a distinct identifier of the NF consumer in the CCA which enables the producer network to authenticate and authorise the consumer.
* Reuses the SCP configured in communication type C or D as an intermediate function to apply topology hiding and message inspection.

Editor’s note: Evaluation of deployment of policies and policy enforcement points is FFS.

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