**3GPP TSG-SA3 Meeting #109AdHoc-e *draft\_S3-230252-r1***

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

**Source: Nokia, Nokia Shanghai Bell**

**Title: solution for KI#3 network slice admission control**

**Document for: Approval**

**Agenda Item: 5.12**

# 1 Decision/action requested

***Approve the new solution to TR33.886***

# 2 References

[1] 3GPP TR 23.700-41 “Study on enhancement of network slicing; Phase 3”

[2] 3GPP TR 33.886 "Study on enhanced security for Network Slicing Phase 3"

# 3 Rationale

The contribution proposes solution for KI#3 to mitigate security risks caused by potential threats triggered by malicious/compromised NSACFs in specific serving areas.

All content in the change part is new.

# 4 Detailed proposal

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 1st change \*\*\*\*\*\*\*\*\*\*\*\*

## 5.X Solution #X: Protect NSAC procedure in multiple NSACFs deployment scenario

### 5.X.1 Introduction

The solution addresses KI#3 network slice admission control (NSAC), in which malicious/compromised NSACF(s) in specific area(s) of a PLMN or in a VPLMN may launch DoS attack towards the Primary NSACF. The solution suggests the primary NSACF to validate the number of UEs or PDU sessions for a S-NSSAI when received the numbers from a NSACF .

When received NSAC number update request from a NSACF in a serving area/VPLMN, based on pre-configured policy the Primary NSACF may cross check with UDM to confirm the number reported by the NSACF is matched to actual number recorded in UDM for a network slice.

If the numbers are not matched, the primary NSACF may stop normal NSAC procedure with the identified NSACF and may send event to management system.

### 5.X.2 Solution details



**Figure 5.x.2-1 workflow to validate number reported by NSACF**

**Precondition**:

* Policies, which related to whether trigger cross check with UDM after received number update request from a NSACF, are pre-configured in a primary NSACF. The policies may be defined according to threat surface, security control and security posture of the VPLMN or specific serving area the NSACF located, or other criteria.

**Procedure**:

0a. After received UE registration request and completed primary authentication and authorization for the UE , the AMF sends Nudm\_UECM\_Registration request to UDM. Once Nudm\_UECM\_Registration is completed and AMF decides on allowed slice, the AMF sends registration update message or Ack message to UDM to inform about the allowed slices list. The S-NSSAI in this list is the HPLMN mapping of the S-NSSAI in allowed NSSAI of the registration.

0b. After creating PDU session for a UE on a slice, the SMF sends Nudm\_UECM\_Registration request to UDM to register the PDU session with parameters including a S-NSSAI.

1. A NSACF in a VPLMN or specific serving area sends Nnsacf\_NSAC\_NumberOfUEsUpdate\_Request or Nnsacf\_NSAC\_NumberOfPDUsUpdate\_Request to the Primary NSACF. That implies the local maximum or upper threshold number of UEs/PDUs is reached.

2. The primary NSACF check the local policies pre-configured as described in precondition. If cross check with UDM is not needed according to the policies, the primary NSACF goto step 10a directly to perform NSAC for the S-NSSAI and update quota for the NSACF if needed.

3. If cross check with UDM is needed according to the policies, the primary NSACF either scans all possible UDMs of the HPLMN or probably discover UDMs based on pre-configured rules.

4. The primary NSACF sends request to each UDM to get number of registered UEs/PDU sessions in specific VPLMNs or AMFs/SMFs for the S-NSSAI.

5. The UDM generates report for number of registered UEs /number of PDU sessions in a VPLMN/AMF/SMF List for the S-NSSAI.

6. The UDM returns the report to the primary NSACF.

7. The primary NSACF consolidates the numbers collected from all impacted UDMs, and gets the total number of registered UEs/PDU sessions in specific VPLMN/serving area for the S-NSSAI.

8. The primary NSACF compares the total number of registered UEs/PDU sessions based on UDM reports and the maximum number in the Nnsacf\_NSAC\_NumberOfUEsUpdate\_Request (or may be stored locally in primary NSACF).

9a. If the two numbers are matched or deviation is not crossing the configured threshold, the primary NSACF performs NSAC for the S-NSSAI and update quota for the NSACF if needed.

9b. If the two numbers don't match or deviation is crossing the configured threshold, the primary NSACF stop NSAC procedure with the potential malicious NSACF, and may adjust the quota for the NSACF, and report the anomaly to OAM.

10. The primary NSACF sends update response to the NSACF, with success or failure.

### 5.X.3 Evaluation

TBD

\*\*\*\*\*\*\*\*\*\*\*\*\* End of the changes \*\*\*\*\*\*\*\*\*