**3GPP TSG-WG SA2 Meeting #143E e-meeting  *S2-210xxxx***

Elbonia, 24 Feb – 09 Mar, 2021 (revision of S2-210xxxx)

**Source: Huawei, HiSilicon**

**Title: Architectural Support of Network Slice Access Control Functionalities**

**Document for: Discussion**

**Agenda Item: 8.4.2**

**Work Item / Release: eNS\_ph2 / Rel-17**

*Abstract: This contribution provides some further clarification on the evaluation of KI#1 and KI#2 in TR23.700-40 related to the architectural support of network slice access control functionalities.*

# 1. Introduction

FS-eNS\_Ph2 (TR23.700-40) study and conclude the need of network slice access control functionalities and services in 5G System. However there are no clear description on whether both centralized quota check and distributed quota check are needed even there may be some hint on it.

This contribution provides the discussion of the need of both centralized and distributed quota check for the network slice access control functionalities and services in 5G System.

# 2. Discussion

## 2.1 General

Depending on the operator's operational or deployment needs, the Network Slice Quota Access Control functionality should be deployed in both centralized and distributed to support distributed and scalable network deployment. The reason is explained in clause 2.2.

There may be some concern on whether the distributed network slice access control introduce some additional complexity comparing to the centralized approaches. Due to that we also give a call flow to show what the additional step it needs.

## 2.2 Centralized vs. Distributed Network Slice Access Control Model

In a centralized Network Slice Access Control model, every new access control requests (e.g., UE registration or PDU Session establishment request) is checked against the quota and the quota status at one centralized Network Slice Access Control check NF. The quota is kept at the central Network Slice Access Control check NF. Based on that, the enforcement of access control requests from UEs is performed. Apparently, the Network Slice Access Control in a centralized model is well suited for a small network and/or local slice deployment with not so many UEs (e.g., a local slice deployments for 10,000 UEs). However, this option is infeasible to handle a practical scenario of a large amount of quota of Network Slice (e.g., maximum number of registered UEs and maximum number of established PDU Sessions per S-NSSAI). An example of such a large-scale network deployment can be found at China. In this scenario, the amount of signalling and congestion at the centralized Network Slice Access Control check NF affects the quota checking and network operations. For example due to the congestion at the centralized Network Slice Access Control check point, the request of UE registration or PDU Session establishment of a specific S-NSSAI may be rejected even the request is still allowed per the available quota. Also for a larger network, the centralized option may also mean the huge signalling traffic and delay as all checking need to go to one dedicated central Access Control point.

In a distributed Network Slice Access Control model, the quota that is a subset of S-NSSAI quota is distributed to one or more NW Slice quota enforcement functionalities and where every new access control requests (e.g., UE registration or PDU Session establishment request) is checked against the quota available at one or more distributed Access Control points. For each distributed access control NF, when the distributed quota are consumed or no quota is available then the NW Slice quota enforcement functionality checks against the quota of NW Slice quota management functionality for additional instructions. Apparently, the Network Slice Access Control in a distributed model is well suited for a large network (e.g., a nationwide slice deployment with 1 million UEs covering an S-NSSAI). In this scenario, local quota is distributed to NW Slice quota enforcement functionality at several distributed access control check NFs by a NW Slice quota management functionality. Based on the local quota at the distributed access control check NFs, the enforcement of the access control requests from UEs (e.g., registration or PDU Session request) is performed. Comparing to a centralized Network Slice Access Control model, the distributed Network Slice Access Control model requires Network Slice quota distribution and management between distributed Network Slice Access Control points.

On one hand, the Network Slice quota distribution and management in a distributed model can be seen as overheads compared to a centralized model. On the other hand, this kind of overheads is unavoidable to support large-scale networks due to operator's operational or deployment needs.

**Conclusion 1: Per operator’s requirement both centralized and distributed slice access control are needed.**

## 2.3 Distributed Network Slice Access Control call flow



Figure 2.3-1: call flows for distributed slice access control

Comparing to the centralized approaches. We think that only following additional steps need to be extended for a distributed model:

0a. The primary NSAC configures the NW Slice local quota(s) of specific S-NSSAI(s) (e.g., number of allowed registered UEs) with secondary NSACs to perform access control of specific S-NSSAI(s). The secondary NSAC stores a NW Slice local quota information, which includes the maximum allowed number of registered UEs for the indicated S-NSSAI.

0b. The primary NSAC subscribes the network slice quota status from the secondary per specific event.So the secondary NSAC can send notification of the slice status to the primary NSAC, e.g. the local quota is nearly all consumed.

1. The primary NSAC is notified when the secondary NSAC detects the corresponding event exposure of the network slice quota status of the registered number of UEs of S-NSSAI.
2. The primary NSAC performs counting and collecting the number of registered UEs from the secondary NSAC that have been registered for an S-NSSAI.
3. The primary NSAC updates the configuration of the NW Slice local quota(s) of specific S-NSSAI(s) (e.g., number of allowed registered UEs) with secondary NSACs, if necessary.

**Conclusion 2: the distributed slice access control model can be easily extended on top of the centralized slice access control model.**

# 3. Conclusion and proposal(s)

In summary, we see the requirement to support distributed Network Slice Access Control model for a large network. The additional amount of complexity and signalling for the management of the local quota budgets is rather small. The savings in the transfer of signalling messages from all over the network to a single enforcement point (by handling most of the per UE signalling at the local enforcement point) should easily outweigh the signalling required for the management of the local budgets.

Hence, it is proposed the followings to be clarified in the normative work of KI#1 and KI#2 from FS-eNS\_Ph2.

* Network Slice-Specific Access Control functionalities in 5G System shall apply in both centralized and distributed Network Slice access control model to fulfil the business needs.