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

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

**Source: Huawei, HiSilicon**

**Title: Network Slice Access Control Functionalities and Services**

**Document for: Discussion**

**Agenda Item: 8.4.2**

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

*Abstract: This contribution provides some further clarification on the TR conclusion related to the slice access control, especially on the collocated case.*

# 1. Introduction

FS-eNS\_Ph2 (TR23.700-40) study and conclude the need of network slice access control functionalities and services in 5G System. It is concluded that a new functionality of network slice access control can be deployed as a standalone or **co-located within existing NF.** So in case that the new NF is collocated within the existing NF, what does it means?

# 2. Discussion

## 2.1 General

To support Network Slice-Specific Access Control functionalities in 5G System, there are at least two options as described in clause 8.1 TR23.700-40 in realization of these new functionalities in 5G System.

Option #1: Identify a new (standalone) NF

This option identifies a new and dedicated NF for Network Slice-Specific Access Control functionalities. By introducing a new 5GC NF, the specifications of a new NF (i.e., the interactions with other 5GC NFs, services and information flows) must be defined and supported in Access Control procedures.

Option #2: New NF Co-located within existing 5GC NF

This option allows reuse of existing interactions, services and information flows by hosting/identifying Network Slice-Specific Access Control functionalities at an existing 5GC NF.

In the following description we try to give some detail analysis on these two approaches and further clarify the meaning of the option #2.

## 2.2 Option #1 - Network Slice-Specific Access Control Service Operations Information Flow by introducing a new NF

Network Slice-Specific Access Control function (NSACF) is defined to control the quota management of Network Slice-Specific quota in access control procedure. In particular, the quota management of slice SLA parameters on maximum number of registered UEs or maximum number of established PDU Sessions of an S-NSSAI, subject to the quota management, shall apply in registration or session management procedure, respectively.

NOTE: the below call flow of the option 1 is an example to show how it works. The concrete call flow is to be decided in the normative work phase.

### 2.2.1 Network Slice-Specific Access Control in Registration

The services and information flows to be supported by AMF to NSACF during a general registration procedure is described in Figure 2.2.1-1.



Figure 2.2.1-1: call flows for standalone NSACF during registration procedure

1. AMF receives UE request on registration to a set of S-NSSAIs as per Clause 4.2.2.2.2 in TS23.502.
2. During registration procedure as per Clause 4.2.2.2.2 in TS23.502 the AMF triggers the Network Slice quota checking on the maximum number of registered UEs via the service operation < Nnsac\_regUEQuotaCheck\_Request > with the NSACF. The request shall include a set of Network Slices which are subjected to the quota management in access control and the UE ID.

If NSACF is not configured in the AMF, the AMF performs NSACF discovery and selection.

1. The NSACF checks the status of the slice quota of requested S-NSSAI(s), determines the acceptance or rejection of the registration request to the specific S-NSSAIs and updates the counter of the S-NSSAIs, if necessary. The NSACF maintain a table of the UE ID and the associated registered S-NSSAI.

When the quota is exceeded or has been consumed, the decision of the acceptance or rejection shall apply according to the NSACF policies.

1. The NSACF sends the decision (e.g., accept) response via the service operation < Nnsac\_regUEQuotaCheck\_Response > to the AMF.
2. The AMF checks the response of the NSACF.
3. Registration procedure continues as per clause 4.2.2.2.2 in TS23.502, if the NSACF decides to accept the UE registration request to the specific S-NSSAI(s).
4. Alternatively, the NSACF sends the decision (e.g., reject) response via the service operation < Nnsac\_regUEQuotaCheck\_Response > to the AMF.
5. The AMF handle the rejection of the specific S-NSSAI(s) to the UE.

If there are multi S-NSSAI is to be registered, the NSACF actions are performed for a number of S-NSSAIs in parallel.

NOTE: In option 1, during deregistration of S-NSSAI or UE initiates the registration procedure to update the allowed S-NSSAI(s) or during NSSAA procedures, the additional specific service operations and information flows to be supported by AMF to the NSACF.

### 2.2.2 Network Slice-Specific Access Control in Session Management

The service operations information flow(s) of NSACF in Session management are almost identical with the difference being the triggering procedure, message flow and the NF. In this case, the SMF triggers the Network Slice quota on the maximum number of established PDU Sessions via the service operation, e.g., < Nnsac\_estPDUSessionQuotaCheck\_Request > with the NSACF during the session management procedure as per clause 4.3.2 in TS23.502.

In the session management, the NSACF actions are performed for a single S-NSSAI only or for a number of S-NSSAIs requested by multiple UEs in parallel.

NOTE: In option 1, during PDU Session release of S-NSSAI, the additional specific service operation and information flows to be supported by SMF to the NSACF.

## 2.3 Option #2 - Network Slice-Specific Access Control Service Operations Information Flow by reusing an existing NF

Network Slice-Specific Access Control services are supported by an existing NF. For the sake of reusing the existing procedures, among all existing 5GC NFs, PCF is considered to host network slice access control functionalities.

### 2.3.1 Network Slice-Specific Access Control in Registration



Figure 2.3.1-1: call flows for collocated NSACF+PCF during registration procedure

1. AMF receives UE request on registration to a set of S-NSSAIs as per Clause 4.2.2.2.2 in TS23.502.
2. During registration procedure as per Clause 4.2.2.2.2 in TS23.502 the AMF triggers AM policy association establishment/Modification with the PCF via the service operation <Npcf\_AMPolicyControl\_Create>. Per clause 4.16.1.2 in TS23.502 the request include a set of allowed S-NSSAI, which may be subjected to the quota management in access control.
3. The PCF supported by access control functionalities checks the status of the quota of the requested S-NSSAI(s), determines the acceptance or rejection of the registration request to the specific S-NSSAIs and updates the counter of the related S-NSSAIs, if necessary.

When the quota is exceeded or has been consumed, the decision of the acceptance or rejection shall apply according to the internal policies.

1. The PCF sends the decision (e.g., accept) response via the service operation < Npcf\_AMPolicyControl\_Create response > to the AMF.
2. Registration procedure continues as per clause 4.2.2.2.2 in TS23.502, if the NSACF decides to accept the UE registration request to the specific S-NSSAI(s).
3. Alternatively, the NSACF sends the decision (e.g., reject) response via the service operation < Npcf\_AMPolicyControl\_Create response> to the AMF.
4. In case of rejection decision, the AMF handles the rejection of the specific S-NSSAI(s) to the UE.

### 2.3.2 Network Slice-Specific Access Control in Session Management

Per clause 4.16.4 in TS23.502 the SM Policy Association Establishment request, the SMF include the related S-NSSAI. In this case, PCF performs access control of maximum number of PDU Sessions of the requested S-NSSAI during the session management procedure as per clause 4.3.2 in TS23.502.

## 2.4 Pro and cons of introduce a new NF or reuse an existing NF

The pro and cons of introducing a new NF or reuse an existing NF are highlighted in the following table.

|  |  |  |
| --- | --- | --- |
|  | **Pro** | **Cons** |
| **A new (standalone) NF** | - Clear separation of services/functionality | - Impact on AMF/SMF due to support of new service interaction- Additional signalling necessary- Additional NF to be configured, or discovered and selected |
| **Co-located within existing 5GC NF, i.e. PCF** | - Minor impact on AMF (accept/reject per SNSSAI instead of per policy association)- No impact on SMF (should even work for Rel15/16 SMFs)- No additional signalling- Re-use of PCF (user/service specific) policy for exception handling (i.e. when slice SLA is fully used) | - New feature not visible to AMF/SMF/system due to PCF internal realization - Usage of PCF becomes mandatory for this feature |

Per the conclusion in S2#142E meeting, besides the standalone new NF case, the new NF can be collocated with the existing NF. As explained above, if the new NF is collocated with PCF, it can reuse the existing procedure with some minor update of the PCF internal behaviour. So it is suggested that in the collocated case, PCF is the best candidate to perform the Network Slice Access Control.

**Conclusion: in case of the new NF is collocated within an existing NF for the slice access control, the slice access control is executed by the PCF.**

# 3. Conclusion and proposal(s)

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

* If the new NF is deployed as co-located within existing NF, Network Slice-Specific Access Control functionalities is hosted by PCF.