**3GPP TSG-SA3 Meeting #104-e *draft\_S3-212886-r3***

**e-meeting, 16 - 27 August 2021** Revision of S3-21xxxx

**Source: Nokia, Nokia Shanghai Bell**

**Title: Access token request for NF Set – RFC clarification**

**Document for: Approval, Information, Discussion**

**Agenda Item: 5.20**

# 1 Decision/action requested

EN resolution by added evaluation.

# 2 References

[1] 3GPP 33.875

# 3 Rationale

*Reason for change: It was asked to clarify if the usage of the same access token for different OAuth 2.0 clients follows the OAuth 2.0 RFC and best practices.*

*Summary of changes: The following text has been added to the evaluation: The concept of NF Set and NF Service Set has been introduced by 3GPP. This concept is not part of the OAuth RFC, but in general it is common practice to also allow for project or group access tokens (see https://docs.gitlab.com/). RFC 6749 only mentions types of clients (public and confidential) and that a client can be implemented as a distributed set of components, each with a different client type and security context.*

# 4 Detailed proposal

*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START OF CHANGES*

## 6.7 Solution #7: Access token request for NF Set

Editor's Note: How does the NRF/NFp verify the correctness of NFc set ID is ffs.

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

### 6.7.3 Evaluation

 The solution proposed allows the authorization server, i.e., NRF, to issue an access token that can be used by all members of an NF Set or NF Service Set. The concept of NF Set and NF Service Set has been introduced by 3GPP. This solution enable optimization that is sought from the mutual redundancy among the NF instances of the set. It would be less optimized if each instance needs to request its own token.

Using the same access token for a NF Service Consumers belonging to one NF Set is not explicitly described by RFC 6749. Other literature mentions group access tokens, but further investigation on the impact managing an access token used by NF Service Consumers of the same set is needed.

According to RFC 6749, each NF instances needs to register with the authorization server (NRF) as a separate OAuth2.0 client before the authorization server is able to issue such a token which can be used by all members of the NF Set. Since this solution requires any NF which utilizes the mechanism proposed by this solution to register its NF profile with the NF set ID and/or NF service set ID the NF belongs to, the NRF will be able to authenticate the registering NF instance before accepting the NF registration and its profile. This mechanism provides the NRF with a secure mechanism of the NF set ID and/or the NF service set ID this NF belongs to. Therefore, when the NF sends an access token get for an access token with NF set ID and/or NF service set ID, the NRF is able to validate whether the NF instance belongs to the requested NF set ID and/or NF service set ID by validating the requested values to those in the NF instance profile. This mechanism is secure and does not require any new feature.

In order to ensure that the access token can reflect the identity of all NFs which belong to the NF set ID or the NF service set ID, it is also required that the NRF adds the NF Instance IDs of all NF instances which are members of the referenced NF Set ID and/or the NF service set ID as additional claims in tehaccess token. It is noted that all these NF Instances IDs are available to the NRF.

Since CCA is used for Indirect communications when SCP in the path between the NF Service Consumer and the NF Service Producer, including NF set ID and/or NF service set ID into the CCA only work for the case of indirect communication but not in the direct communication case.

Including NF set ID in the NF certificate is not a flexible mechanism which requires an intervension in case of the NF instance is removed from a specific NF set ID and/or NF service set ID or added to another NF set ID or NF service set ID. On the other hand, if any of these operations are done to any NF instance, the NF instance will update its profile with the NRF automatically and the update is almost dynamic for the rest of the processes.

This solution requires that in case of any change to the list of members of the NF set, all existing access token with the impacted NF set ID and/or NF service set ID shall be destroyed and not used. A new access token is required.

*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END OF CHANGES*