**3GPP TSG-SA3 Meeting #108e *draft\_S3-221862-r2***

**e-meeting, 22 - 26 August 2022**

**Source: Nokia, Nokia Shanghai Bell**

**Title: Solution update and conclusion on KI#6 on access token usage by NFs of an NF Set**

**Document for: Approval**

**Agenda Item: 5.24**

# 1 Decision/action requested

**KI6 related update for solution #7 and conclusion for KI#6**

# 2 References

[1] 3GPP TR 33.875

# 3 Rationale

*Clarifications added for the handling of NF Sets / NF Service Sets, since handling of sets on NF Service Consumer side is equal to the handling of sets on NF Service Producer side,. The latter is already specified in TS 23.501.*

# 4 Detailed proposal

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

6.7 Solution #7: Access token request for NF Set

6.7.1 Introduction

This solution addresses KI#6.

3GPP introduces the concepts of NF Set and NF Service Set which allows essentially for a group of interchangeable NF instances/NF Service instances of the same type, supporting the same services and the same Network Slice(s). Rel-16 also allows re-selection of a NF instance or a NF Service instance within the Set for subsequent transaction.

5G SBA architecture design allows for the concept of stateless NFs.

To support the NF Set concept, ie. a group of interchangeable NF instances or NF Service instances providing the same service, the context needs to be accessible to all NFs of the set.

The solution addresses NF Sets or NF Service Sets on the consumer side. It assumes that each NF Service Consumer of a set is known at NRF also with its NF Set ID or the NF Service Set ID. Thus, verification of the correctness of a set id is done when authenticating the NF Service Consumer as OAuth 2.0 client when registering at NRF. Thus, if NRF is then issuing an access token with a distinct set id related to the NF Service Consumer's NF Set IF or NF Service Set ID, the NF Service Producer can trust the correctness, or do another verification, if the set id is also included in CCA or NF certificate.

A NF Service Producer can also indicate in its profile, if it is allowing the NRF to provide access tokens for NF Sets or NF Service Sets.

NOTE: Whether to have this feature allowed per operator policy configured at NRF or per NF Service Producer or NF Service Producer Set is a deployment decision.

The solutions objective is to avoid that a NF from a NF Set needs to request a new access token, when targeting a service of an existing resource requested before by another NF of the NF Set, it is proposed that any NF in a NF Set can request an access token for the NF Set. Thus, any NF Service Consumer targeting a service of an existing resource it can use the access token provided to a NF Set of NF Service Consumers. All NFs of a NF Set need to retrieve the current status from the same place to allow for the same access token to be used by different NFs of the set.

NOTE: For any NF to make use of this solution, that NF is required to register its profile with the NRF.

6.7.2 Solution details

The NF Service Consumer belonging to a NF Set, it includes its NF Set ID in the Access Token Request message to NRF and also in the CCA or the NF certificate.

When the Access Token Request is processed by the NRF and a NF Set ID is included, the NRF knows that the NF Service Consumer requests an access token to be useable by all NF Service Consumer instances within the NF Set. If NRF authorization of the NF Service Consumer is successful, ie. the NF Service Producer has indicated that an access token for a NF Set or NF Service Set can be issued, and the NF Set ID in the CCA matches the NF Set ID in the access token or in the NF certificate, NRF includes as claim the NF Set ID of the expected NF Service Consumer instances to allow the access token generated for usage by all NF Service Consumers in the NF Set. NRF sends the access token back to the requester. The request needs to put the context information of such common token at a place from which all NFs of the NF Set can retrieve it.



**Figure 6.7.2-1 – Access Token Request procedure (TS 33.501 Figure 13.4.1.1.1-1) enhanced with NF Set ID in the Access Token Request message**

How NFs of a NF Set or a NF Service Set manage the distribution of an access token issued for set or service set and their availability to other NFs within the NF Set, is for implementation and out of scope.

When a service is requested, the requester (NF Service Consumer or SCP) includes the NF Set ID of the NF Service Consumer in the Service API Request, as well as in the CCA, if the CCA is sent, in addition to the access token obtained from the NRF. NF Set ID in CCA is only reliable if the NF Set ID is included in the certificate related to the private key that the NF Service Consumer used to sign the CCA.

The NF Service Producer checks whether the Consumer NF Set Id in the Service Request matches with the NF Set ID claim in the Access token. If CCA is sent, it also verifies, if the NF Set ID matches the NF Set ID in the CCA. If included in NF certificate, it can also match the NF Set ID with the NF Set ID in the NF certificate. If yes, it proceeds with serving the request, otherwise it rejects the request.

There is always one NF representing a set at a given time. Only one NF of the NF Set or NF Service Set shall be able to use the access token issued for a set at a given time. The management of which NF within the set is currently the leader and using the OAuth token is for implementation and out of scope.

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 enables 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 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 should be destroyed and not used. A new access token is required.

Since NF Service Producers can indicate in their profile allowedxxx IEs, configuration effort is necessary so that they are consistent with the NF sets.

Editor's Note: FFS whether it is the same effort managing an access token used by different NFs of the same NF Set of Service Producers.

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

## 7.6 KI#6: Access token usage by all NFs of an NF set

### 7.6.1 Analysis

Only solution #7 is provided for this key issue. When implementing NF Sets a common context storage needs to be organised, from which all NFs of the set can retrieve the same status. There is no difference in this handling for NF Service Producer and NF Service Consumer.

The main hurdle is that a NF Service Consumer is not necessarily a NF Service Producer, in which case no NF profile registration at NRF is needed. However, NF Service Consumers need to register with the OAuth 2.0 server and as described in the solution, the NF Set ID or NF Service Set ID is needed to be known at the NRF for the solution to work.

The NF Set management is out of scope but not different from using services of different NF Service Producers within the same set by the same token.

Editor's Note: Further analysis is FFS.

### 7.6.2 Conclusion

TBD

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