**3GPP TSG-SA3 Meeting #104-e *S3-21xxxx***

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

**Source: Nokia, Nokia Shanghai Bell**

**Title: OAuth 2.0 Misalignment discussion**

**Document for: Discussion**

**Agenda Item: 4.22**

1 Decision/action requested

Misalignment issues between SA3 and CT4 need to be clarified

Status of discussion after offline telco 10.9.

2 References

[1] 3GPP

3 Rationale

## **Status on OAuth client registration**

* **discussion on frozen Rel-15/Rel-16**
* 33.501 has a mandatory requirement that Oauth clients shall be registered using Nnrf\_NFMangement register service, which was debated and not accepted by CT4 since Rel15
* Thus, status in 29.5xx: this feature is not available in stage 3
* Situation: some companies followed stage 2 and want to keep the feature, even without stage 3
* Compromise so far discussed: make it optional, add a clarification

**The NF Service registration procedure, as defined in clause 4.17.1 of TS 23.502 [8], may~~shall~~ be used to register the OAuth 2.0 client (NF Service Consumer) with the OAuth 2.0 Authorization server (NRF), …**

**Ongoing debate is on the additional clarification**

Is it sufficient to say:

**Any other Oauth2.0 client registration mechanism is out of scope of this document.** (S3-212451)

Or is it necessary to clarify, what happens if Oauth client is known to NRF by different means?

**A Network Function that does not implement this option shall be able to get an access token from the NRF as long as the NRF is able to authenticate and authorize the Network Function during the NF access token get service request.** (S3-212895)

**Offline discussion 10.8.:** in general, Oauth clients need to be known to NRF to allow the OAuth server to respond; it was discussed whether to mandate in Rel17 to register Oauth clients and/or NF Consumers

**Open:**

* What exactly to mandate in Rel-17? OAuth client reg. or NF Consumer registration?
* how to deal with cases, when consumers are not producers and therefore do not have a NF profile?
* How to deal with cases, when the requesting NF (consuming) is not registered at same NRF as where the NF producer‘s profile is available, ie. not registered at the token issuing NRF?

## **Status on NRF services using OAuth**

* **discussion on frozen Rel-15/Rel-16**
* 33.501 has the following note 13.3.1

**NOTE 1: When a NF accesses any services (i.e. register, discover or request access token) provided by the NRF, the OAuth 2.0 access token for authorization between the NF and the NRF is not needed.**

* 29.501 has the optional feature of usage of the OAuth 2.0 access token for authorization between the NF and the NRF for Nnrf\_NFManagement or the Nnrf\_NFDiscovery services

Ongoing debate: allow or not allow NRF services with OAuth

Difference to OAuth client discussion: stage 3 available and usefulness of the feature was seen

**From the offline discussion 10.8.**

Service mesh can have all information to add oauth tokens. This can be used for NRF management and discovery services. Service mesh allows a token to come from a different place.

Having the ability to have tokens, provides more security value.

**2 proposals on the table**

S3-212451: “shall not be required” -> meant is: do not allow NRF services with OAuth

NOTE 1: void.

When a NF accesses any services (e.g., management, discover, request access token) provided by the NRF, the OAuth 2.0 access token for authorization between the NF and the NRF shall not be required.

S3-212895: split and align NRF services on management and discovery with stage 3

NOTE 1: When a NF consumes the Nnrf\_AccessToken Service provided by the NRF, the OAuth 2.0 access token for authorization between the NF and the NRF is not needed.

When a NF consumes the Nnrf\_NFManagement or the Nnrf\_NFDiscovery services provided by the NRF, the usage of the OAuth 2.0 access token for authorization between the NF and the NRF is optional.