**3GPP TSG-SA3 Meeting #104-e *S3-212897r1***

**e-meeting, 16 - 27 August 2021**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.501** | **CR** | **1191** | **rev** | **-** | **Current version:** | **17.2.1** |  |
|  | | | | | | | | |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network | **x** |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | | |
| ***Title:*** | | Oauth2.0 misalignment | | | | | | | | | |
|  | |  | | | | | | | | | |
| ***Source to WG:*** | | Nokia, Nokia Shanghai Bell, Ericsson, AT&T, Interdigital, Xiaomi, HPE, Lenovo, Motorola Mobility | | | | | | | | | |
| ***Source to TSG:*** | | S3 | | | | | | | | | |
|  | |  | | | | | | | | | |
| ***Work item code:*** | | 5G\_eSBA | | | | |  | ***Date:*** | | | 2021-08-27 |
|  | |  | | | |  | |  | | |  |
| ***Category:*** | | **F** | **A** | | | | | ***Release:*** | | | Rel-17 |
|  | | *Use one of the following categories:* ***F*** *(correction)* ***A*** *(mirror corresponding to a change in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)*  Detailed explanations of the above categories can be found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | | | | | | | | *Use one of the following releases: Rel-8 (Release 8) Rel-9 (Release 9) Rel-10 (Release 10) Rel-11 (Release 11) Rel-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  | |  | | | | | | | | | |
| ***Reason for change:*** | Change 1  Stage 3 specification allows since Rel-15 conditionally: if OAuth is used, NRF services for Management and Discovery can be consumed by presenting an access token (see 29.510).  33.501 states:  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.  The informative note in 33.501 may lead to misinterpretation – “not needed” can be interpreted to not used or being optional.  The proposed change aligns TS 33.501 (stage-2) with TS 29.510 (stage-3). The motivation is the following:   * As a general rule, in case of stage-2/3 misalignments, stage-3 should be followed by default, if not there are strong reasons against. * In the LS S3-212409/CP-211326, CT plenary tasks SA3 (responsible stage-2 group) with the resolution of the misalignment, not CT4 (responsible stage-3 group). * CT4 saw it as beneficial to employ the authorization for NRF-specific APIs as well, so the optional support of OAuth 2.0 for Nnrf\_NFManagement and Nnrf-NFDiscovery services should not be removed. * Otherwise a Rel-17 NRF that would be provisioned to use OAuth for certain NRF services is able to reject requests not including a token with a 401 Unauthorized to a Rel-15/16 NF. NRF can only reject with a 401 if the feature is optionally allowed.   Change 2  Current specification text mandates OAuth 2.0 client registration by using the NRF service, i.e. NnrfManagement NFRegister request. But not all NFs need to register at NRF.  OAuth client registration is needed for providing an access token.  Register an OAuth client can be done in several ways.RFC 6749 also enables client reg. without interaction, or by local configuration, e.g. by OAM  From RFC 6749  Client registration does not require a direct interaction between the  client and the authorization server. When supported by the  authorization server, registration can rely on other means for  establishing trust and obtaining the required client properties  (e.g., redirection URI, client type). For example, registration can  be accomplished using a self-issued or third-party-issued assertion,  or by the authorization server performing client discovery using a  trusted channel.  Also note, an “Oauth2 client profile” might be totally different to the existing “NF Profile” of NF Service Producers.  Examples of NFs that are purely NF Service Consumers, for which it makes no sense to be required to register in NRF with NFManagement\_Register:   * From Rel-15 onwards; CBCF, possibly GMLC, possibly NEF (Standard Rel-15 NEF just offers one interface within the network, towards the PCF; if this interface is not deployed, there is no need for NEF to register) * From Rel-16 onwards: I-CSCF, S-CSCF, TAS, and SCC-AS are service consumers, but not service producers; a Rel-16 P-CSCF may also consume N5 services before supporting service registration   Examples of NFs that produce / register services in one NRF and may consume services discovered from different NRFs:   * Scenarios where an NF registers its services to an NRF X but need to discover other NF services from an NRF Y, e.g., AMF registering to a PLMN-level NRF but performing discovery requests to network slice specific NRFs (e.g., to discover an SMF/PCF).   **Thus, in the scenarios above, an NF Service Consumer SHALL NOT be forced to issue an NFManagement\_Register operation simply to be able to issue an NFDiscovery\_Request operation.**  Therefore, it is unclear why 33.501 mandates to use NFRegister for OAuth 2.0 client registration. Since there may be however already implementations, it is proposed to update “shall” to “may”. But making it only optional is not sufficient. A Network Function that does not implement this option must also 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.  Thus it is proposed to add such clarification as well. | | | | | | | | | | |
|  |  | | | | | | | | | | |
| ***Summary of change:*** | Change 1:  To align with frozen stage 3, the use of Oauth2.0 access token by a NF when consuming NRF services Nnrf\_NFManagement or the Nnrf\_NFDiscovery is optional.  Change 2:  Optionally allow the use of NFRegister for registering an OAuth client, but clarify that a Network Function that does not implement this option must also 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. | | | | | | | | | | |
|  |  | | | | | | | | | | |
| ***Consequences if not approved:*** | Misalignment and interoperability issues. | | | | | | | | | | |
|  |  | | | | | | | | | | |
| ***Clauses affected:*** | 13.3.1.3, 13.4.1.1.1 | | | | | | | | | | |
|  |  | | | | | | | | | | |
|  | **Y** | | | **N** |  | | | |  | | |
| ***Other specs*** |  | | | **x** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** |  | | | **x** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** |  | | | **x** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  |  | | | | | | | | | | |
| ***Other comments:*** |  | | | | | | | | | | |
|  |  | | | | | | | | | | |
| ***This CR's revision history:*** |  | | | | | | | | | | |

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

\*\*\*\*\*\*\*\*\* CHANGE 1

#### 13.3.1.3 Authorization of discovery request and error handling

When NRF receives message from unauthenticated NF, NRF shall support error handling, and may send back an error message. The same procedure shall be applied vice versa.

After successful authentication between NRF and NF, the NRF shall decide whether the NF is authorized to perform discovery and registration.

In the non-roaming scenario, the NRF authorizes the Nnrf\_NFDiscovery\_Request based on the profile of the expected NF/NF service and the type of the NF Service Consumer, as described in clause 4.17.4 of TS23.502 [8].

In the roaming scenario, the NRF of the NF Service Producer shall authorize the Nnrf\_NFDiscovery\_Request based on the profile of the expected NF/NF Service, the type of the NF Service Consumer and the serving network ID.

If the NRF finds NF Service Consumer is not allowed to discover the expected NF instances(s) as described in clause 4.17.4 of TS 23.502[8], NRF shall support error handling, and may send back an error message.

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.

\*\*\*\*\*\*\*\*\* CHANGE 2

13.4.1.1.1 OAuth 2.0 roles

OAuth 2.0 roles, as defined in clause 1.1 of RFC 6749 [43], are as follows:

a. The Network Repository Function (NRF) shall be the OAuth 2.0 Authorization server.

b. The NF Service Consumer shall be the OAuth 2.0 client.

c. The NF Service Producer shall be the OAuth 2.0 resource server.

**OAuth 2.0 client (NF Service Consumer) registration with the OAuth 2.0 authorization server (NRF)**

The NF Service registration procedure, as defined in clause 4.17.1 of TS 23.502 [8], may be used to register the OAuth 2.0 client (NF Service Consumer) with the OAuth 2.0 Authorization server (NRF), as described in clause 2.0 of RFC 6749 [43]. The client id, used during OAuth 2.0 registration, shall be the NF Instance Id of the NF.

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