**3GPP TSG-SA3 Meeting #104-e *draft\_S3-212451r2***

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

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **<Spec#>** | **CR** | **1146** | **rev** | **1** | **Current version:** | **<Version#>** |  |
|  |
| *For* ***[HE](http://www.3gpp.org/3G_Specs/CRs.htm%22%20%5Cl%20%22_blank)******LP*** *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:*** | <Source\_if\_WG>, Huawei, HiSilicon, Deutsche Telekom AG, China Mobile, CableLabs, Verizon, Samsung |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | 5GS\_Ph1-SEC |  | ***Date:*** | 2021-08-16 |
|  |  |  |  |  |
| ***Category:*** | F |  | ***Release:*** |  Rel-15 |
|  | *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 canbe 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:*** | This change is to address the misalignment between TS33.501 and TS29.510 with respect to the requirement of a NF having an Oauth2.0 access token before consuming the NRF NFManagement and NFDiscovery services. In the current TS33.501, in clause 13.4.1.1.1, there is misalignment between the text of the call flow and the call flow steps captured in the figure.Oauth2.0 (NF service consumer) may use the NF registration procedure for reqistering with the NRF. However, security enhancement on the Oauth2.0 authorization when consuming NRF services is not identified. Furthermore, since Rel-15 and Rel16 are frozen all other enhancements are out of scope. |
|  |  |
| ***Summary of change:*** | In Rel-15 and Rel-16 the use fo Oauth2.0 access token by a NF when consuming NRF services shall not be required. |
|  |  |
| ***Consequences if not approved:*** | Misalignment which could lead to misinterpretation and vulnerable implemntation and interoperability issues. |
|  |  |
| ***Clauses affected:*** | 13.3.1, 13.4.1.1 |
|  |  |
|  | **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 Change No. 1 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 13.3.1 Authentication and authorization between network functions and the NRF

NRF and NF shall authenticate each other during discovery, registration, and access token request. If the PLMN uses protection at the transport layer as described in clause 13.1, authentication provided by the transport layer protection solution shall be used for mutual authentication of the NRF and NF.

If the PLMN does not use protection at the transport layer, mutual authentication of NRF and NF may be implicit by NDS/IP or physical security (see clause 13.1).

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 TS 23.502 [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.

NOTE 1: void.

When a NF consumes the Nnrf\_NFManagement or the Nnrf\_NFDiscovery services provided by the NRF, the OAuth 2.0 access token for authorization between the NF and the NRF may be supported. The mechanism for the Oauth2.0 authorization of NRF services is not specified in this document.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change No. 1 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of Change No. 2 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#### 13.4.1.1 Service access authorization within the PLMN

##### 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.

The OAuth 2.0 client can also be registered by other means. .

Also NF Service Consumers which do not use the NF Service registration procedure for OAuth 2.0 client registration as specified above may get an access token from the NRF.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of Change No. 2 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*