**3GPP TSG-SA3 Meeting #106-e *draft\_S3-220396-r4***

**e-meeting, 14 – 25 February 2022**

|  |
| --- |
| *CR-Form-v12.1* |
| **CR CHANGE REQUEST** |
|  |
|  | **33.501** | **CR** | **1335** | **rev** | **1** | **Current version:** | **17.4.0** |  |
|  |
| *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:***  | NRF deployments |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell, Ericsson, Mavenir, Huawei, HiSilicon |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** |  |  | ***Date:*** | 2022-02-25 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***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 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-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | Multiple NRFs can be deployed in a PLMN, optionally using a hierarchical structure whereby an NRF may redirect or forward service requests to another NRF. One (or more) NRF can serve the entire PLMN, a set of network slices, or a single network slice. Also 33.875 identified in KI#8 as deployment model assumes that NFc needs to be registered at a local NRF or that NFc is known (as Oauth client) at a local NRF. It also assumes that one NRF is trusting the other NRF in the same PLMN. When requesting an access token, NFc goes first to its local NRF, which authenticates NFc and then forwards or redirects the request to the target NRF, where a NFp has registered its services. In this case the local NRF authenticates the NFc and the target NRF (holding the policy for NFp services) provides the access token for NFp service.Clarification text is required to address the various NRF deployments and how the NFc behaves when it has discovered a local NRF or if the NF Service Consumer requests an NRF, where the NF Service Producer is not registered.  |
|  |  |
| ***Summary of change:*** | Adding deployment options for NRFs as a new clause.Clarfiy that the NF Service Consumer may have discovered a specific NRF in advance, e.g. a slice specific NRF, and can send its request directly to that NRF. If the NF Service Consumer requests an NRF, where the NF Service Producer is not registered (see NRF deployment options in 13.4.1.1.1a), the requested NRF needs to redirect/forward the service request to that NRF. Further clarify that in a local NRF deployment, the NF Service Producer only gets the certificate of the local NRF. Thus, the local NRF would need to check if the NF Service Consumer is authorized and the NRF where the NF Service Producer is registered would need to trust the NRF which has verified the NF Service Consumer.  |
|  |  |
| ***Consequences if not approved:*** | Some NRF deployment scenarios are missed in 33.501, no alignment with CT4 29.510 |
|  |  |
| ***Clauses affected:*** | 13.4.1.1.x (new) |
|  |  |
|  | **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:*** | ***S3-214594, S3-214194-r10*** |

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

##### 13.4.1.1.x Access token requests in deployments with several NRFs

As described in clause 6.2.6.1 of TS 23.501 [1], an operator network can deploy multiple NRFs, for example due to network slicing or network segmentation.

An NF Service Consumer shall send its access token requests to the NRF where it is registered as OAuth 2.0 client. The NRF that receives the access token request from the NF Service Consumer authenticates the NF Service Consumer, and may verify the input parameters in the access token request as described under Step 1 in clause 13.4.1.1.2. After successful authentication and verification of the input parameters, the NRF may forward the access token request to another NRF.

If an NRF receives an access token request for an NF Service Producer that is not registered at this NRF, the NRF forwards the access token request to the NRF where the NF Service Producer is registered. The NRF determines to which NRF it forwards the access token request based on, e.g., the requested slices, the type of the NF Service Producer, the region of the potential NRFs, or the NF Profile of other NRFs which are registered with this NRF . There can also be several hops of NRFs between the NRF that receives the access token request from the NF Service Consumer and the NRF where the NF Service Producer is registered.

One possible hierarchical NRF deployment is the local NRF deployment. An NF Service Producer’s local NRF is the NRF where the NF Service Producer registered its NF profile. In the local NRF deployment, the NF Service Producer is configured with the public key which corresponds to the private key that its local NRF uses for signing the access token. Thus, when the local NRF receives an access token request for an NF service consumer, the local NRF checks if the NF Service Consumer is authorized to receive the requested service and, if yes, issues and signs the access token. In the case when the access token request for the NF service consumer was forwarded by another NRF, the local NRF of the NF service producer needs to trust the NRF which forwarded the access token request.

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