**3GPP TSG-SA3 Meeting #116 *draft\_S3-242451-r1***

Jeju, South Korea, 20th - 24th May 2024

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** | **2002** | **rev** | 1 | **Current version:** | **18.5.0** |  |
|  | | | | | | | | |
| *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:*** | Clarification on NFDiscovery Authorization | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon, BSI, Ericsson, Nokia | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TEI18 | | | | |  | ***Date:*** | | | 2024-05-08 |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***Release:*** | | | Rel-18 |
|  | *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-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | This CR is to address the CVD issue related to NFDiscovery in SBA raised in the LS from GSMA (S3-241764) as NFDiscovery Bypass Attack on 5G core.  Excerpts from LS:   * Summary of finding:   NRF finds target NFs that serve the sNssais as appeared in requestersNssais. A compromised consumer can obtain NF Profiles (with all sensitive metadata) of any producer, by using sNssais (to which the consumer wants access) and requestersNssais attributes (which the consumer presents) in the NF Discovery Request (TS 29.510, 6.2.3.2.3.1) towards NRF. The researchers claim there is a lack of cross-checking by NRF between requestersNssais received in the NF Discovery Request and the sNssais of the consumer NF Profile.   * Discussion/Observation:   Both information are provided by the same NF, hence even if compromised, this check does not bring anything. If NRF wants to check information against another source, it should be the NF certificate.  We believe there is a misunderstanding. NRF verifies the S-NSSAI in the requestersNssais (in the request message) with the allowed S-NSSAI in the producer’s NF profile at NRF, not the one in the request message of the consumer. NRF returns only those NF profiles of NF instances allowing to be discovered from at least one network slice identified by the requestersNssais attribute and if requested by the consumer in sNssais. Hence, the specification text may have been mis-interpreted by the researchers when stating that the requestersNssais could be checked by NRF against sNssais in Consumer NF Profile.   * Proposed action:   3GPP to consider whether clarification of the specification text on NRF behaviour is needed when providing a NF Discovery response.  Regarding NRF behaviour of handling authorization check during NF discovery, there are some details already specified in the stage 3 specification TS 29.510.  For example, in the TS 29.510 clause 6.1.6.2.2 it is stated that:  allowedRuleSet:  Map of rules specifying NF-Consumers allowed or denied to access the NF-Producer. The key of the map shall be a (unique) valid JSON string per clause 7 of IETF RFC 8259 [22], with a maximum of 32 characters.  This IE may be present when the NF-Producer and the NRF support Allowed-ruleset feature as specified in clause 6.1.9.  When NRF utilizes this parameter to determine if the NF-Consumers allowed or denied to access an NF-Producer, it matches the NF-Consumer's properties (PLMN, SNPN, nfType, NfDomain, S-NSSAIs) against each rule in decreasing order of priority (1 being the highest). When a matching rule is found, the search is stopped and the NF-Consumer is allowed/dis-allowed to access the NF-Producer (see Annex C).  And in the TS 29.510 clause 6.2.3.2.3.1, it is stated that:  NOTE 12: Based on operator's policies, a discovery request not including the requester's information necessary to validate the authorization parameters in NF Profiles may be rejected or accepted but with only returning in the discovery response NF Instances whose authorization parameters allow any NF Service Consumer to access their services. The authorization parameters in NF Profile are those used by NRF to determine whether a given NF Instance / NF Service Instance can be discovered by an NF Service Consumer in order to consume its offered services (e.g. "allowedNfTypes", "allowedNfDomains", etc.).  And in the TS 29.510 Annex C, it is stated that:  When scope of authorizations allowed to NF-Service-Consumers of different PLMNs, S-NSSAIs, SNPNs, NF-Domains etc. are different, it is not always possible for an NF (Service) Producer to register an authorization profile into NRF using allowedXXX parameters alone. The Allowed-ruleset feature addresses such requirements by extending the authorization policy with a prioritized list of RuleSets in the NF (Service) profile. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Added clarifying text on NRF behaviour during discovery request processing. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | May cause confusion. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.9.2, 13.3.1.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | | Intro sentence to list of requirements starts in new line (enter). | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | | Merger of S3-241949, S3-241798, and S3-242238 | | | | | | | | |

\*\*\*\*\*\*\*\*\*\*\*\* Start of changes\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#### 5.9.2.2 NRF security requirements

The Network Repository Function (NRF) receives NF Discovery Requests from an NF instance, provides the information of the discovered NF instances / NF service instance to the requesting NF instance or SCP, and maintains NF profiles.

The NRF receives from NF Service Consumers or SCPs access token requests for service consumption and provides authorization tokens.

The NRF shall act as authorization server.

The following NRF service-based architecture security requirements shall apply:

NRF and NFs that are requesting service shall be mutually authenticated.

NRF may provide authentication and authorization to NFs for establishing secure communication between each other.

\*\*\*\*\*\*\*\*\*\*\*\* next change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

#### 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. After successful registration, the NF Profile shall be stored at the NRF.

The NRF shall verify the parameters in the Nnrf\_NFDiscovery\_Request from the NF against the stored NF profile and decide whether the NF is authorized to perform discovery. NRF shall only return NF instances in the discovery response message for which the registered NF profile information (allowed parameters and rules) match the NF Service Consumer information received in the discovery request.

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.

NOTE 1: Void.

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.

\*\*\*\*\*\*\*\*\*\*\*\* End of changes\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*