**3GPP TSG-SA3 Meeting #111 *S3-23xxxx***

**Berlin, Germany, 22 - 26 May 2023**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.518** | **CR** | **XXXX** | **rev** | **-** | **Current version:** | **17.0.0** |  |
|  |
| *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 |  |

|  |
| --- |
|  |
| ***Title:***  | SCAS release reference corrections |
|  |  |
| ***Source to WG:*** | Huawei, HiSilicon |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | SCAS\_5G\_Ph2 |  | ***Date:*** | 2023-05-22 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***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 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:*** | SA3 has been adding the release numbers explicitly to any of the references pertaining to the network function targeted by the SCAS work, for example reference 2 in TS 33.511. This is because the SCAS work has always been one "release late" since it is challenging to develop the SCAS requirements and tests in parallel to targeted new features within the same release timeline. The references have not been regularly updated and some SCAS specifications include more than one reference to the same specification, for example references 2 and 7 in TS 33.512. This practice is neither future proof nor it is documented anywhere. Furthermore, for SCAS evaluation of network products, this dependency on previous releases in SCAS documents turned out to be not very useful anyway. This issue has been discussed several times in previous SA3 meetings and the proposed resolution is documented in [S3-231050](https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_110_Athens/docs/S3-231050.zip). |
|  |  |
| ***Summary of change:*** | Removal of the release number from the relevant references and minor reformulations to avoid verbatim content copies from other specifications |
|  |  |
| ***Consequences if not approved:*** | Unnecessary dependencies on previous releases and risk for confusion on scope of SCAS specifications |
|  |  |
| ***Clauses affected:*** | 2, 4.2.2.2.1 |
|  |  |
|  | **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\*\*\*\*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 33.117: "Catalogue of general security assurance requirements".

[3] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[4] 3GPP TS 23.502: "Procedures for the 5G System".

[5] 3GPP TS 29.510: "5G System; Network function repository services; Stage 3".

[6] 3GPP TR 33.926: "Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes".

\*\*\*\* Next Changes\*\*\*\*

##### 4.2.2.2.1 NF discovery authorization for specific slice

*Requirement Name*: NF discovery authorization for specific slice

*Requirement Reference:* TS 33.501 [3], clause 5.9.2.1, TS 23.502 [4], clause 4.17.4, and TS 29.510 [5], clause 6.2.3.2.3.1.

*Requirement Description*:

NRF is expected to be able to ensure that NF Discovery and registration requests are authorized as specified in TS 33.501 [3], clause 5.9.2.1.

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, the NRF determines whether the NF service consumer is allowed to discover the expected NF instance(s). If the expected NF instance(s) or NF service instance(s) are deployed in a certain network slice, NRF authorizes the discovery request according to the discovery configuration of the Network Slice, e.g. the expected NF instance(s) are only discoverable by the NF in the same network slice as specified in TS 23.502 [4], clause 4.17.4.

If included, the requester-snssais IE is expected to contain the list of S-NSSAI of the requester NF. The NRF is expected to use this to return only those NF profiles of NF Instances allowing to be discovered from the slice(s) identified by this IE, according to the "allowedNssais" list in the NF Profile and NF Service as specified in TS 29.510 [5], clause 6.2.3.2.3.1.

*Threat References*: TR 33.926 [6], clause H.2.2.1, No slice specific authorization for NF discovery

*Test Case*:

**Test Name:** TC\_DISC\_AUTHORIZATION\_SLICE\_NRF

**Purpose:**

Verify that the NRF under test does not authorize slice specific discovery request for the NF instance which is not part of the requested slice, according to the slice specific discovery configuration of the requested NF instance.

**Procedure and execution steps:**

**Pre-Conditions:**

- Test environment with the NF1 and NF2, which may be simulated.

- The NF2 is configured with a list of S-NSSAI, which contains slice A but not slice B.

- The NF1 is configured as a NF instance belonging to slice B and is connected in emulated/real network environment.

- The NF1 and NF2 is successfully authenticated with the NRF under test.

**Execution Steps**

1. The NF2 registers at the NRF under test with a list of S-NSSAI.

2. The NF1 sends an Nnrf\_NFDiscovery\_Request to the NRF under test with the expected service name of NF2, NF type of the expected NF2.

3. The NRF under test determines that NF2 instance only allows discovery from NFs belonging to slice A, according to the "allowedNssais" list stored in NF2 Profile.

**Expected Results:**

The NRF under test returns a response with "403 Forbidden" status code, as specified in clause 5.3.2.2.2 of TS 29.510 [5].

**Expected format of evidence:**

Evidence suitable for the interface, e.g., evidence can be presented in the form of screenshot/screen-capture.

\*\*\*\* End of Changes\*\*\*\*