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

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

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.326** | **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, 4.2.1, 4.2.2 |
|  |  |
|  | **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 33.501: "Security architecture and procedures for 5G system".

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

[4] 3GPP TR 33.926: "Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes".

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

### 4.2.1 Routes the S-NSSAI to the right place

*Requirement Name*: Routes the S-NSSAI to the right place

*Requirement Reference:* TS 33.501 [2], clause 6.8.1.2.3

*Requirement Description*: If the AAA-P is present (e.g. because the AAA-S belongs to a third party and the operator deploys a proxy towards third parties), the NSSAAF forwards the EAP ID Response message to the AAA-P, otherwise the NSSAAF forwards the message directly to the AAA-S. NSSAAF routes to the AAA-S based on the S-NSSAI, as specified in TS 33.501 [2], clause 6.13.

Threat Reference: TBD

**Test Name:** TC\_NSSAAF\_CORRECT\_ROUTING

**Purpose:**

Verify that the NSSAAF forwards the NSSAA request to the right receiving end.

**Pre-Conditions:**

- Test environment with AMF, AAA-S and AAA-P, which may be simulated. The NSAAF under test is connected with AMF, AAA-S and AAA-P.

- A document describes the logic how the NSSAAF selects an AAA-S or AAA-P based on S-NSSAI.

- Preconfigure the NSSAAF under test with two routing entries, each for a NSSAI. One of the slice is a part of MNO and the AAA-S can be directly found by the NSSAAF, while the other slice serves 3rd party and the AAA-P will be used for NSSAA procedure.

**Execution Steps**

1. The AMF sends Nssaaf\_NSSAA\_Authenticate Req to the NSSAAF including one of the S-NSSAI.

2. The NSSAAF sends AAA message to an AAA-P.

3. Repeat step 1 and 2 with the other S-NSSAI, and the NSSAAF sends AAA message to an AAA-S.

**Expected Results:**

The NSSAAF forwards the NSSAA request to the correct AAA-S or AAA-P on the S-NSSAI.

**Expected format of evidence:**

Save the logs and the communication flow in a .pcap file.

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

### 4.2.2 AAA-S authorization in re-authentication and revocation scenarios

*Requirement Name*: AAA-S authorization in re-authentication and revocation scenarios

*Requirement Reference:* TS 33.501 [2], clause 16.4

*Requirement Description*: The NSSAAF checks whether the AAA-S is authorized to request the re-authentication and re-authorization by checking the local configuration of AAA-S address per S-NSSAI. If success, the NSSAAF requests UDM for the AMF serving the UE using the Nudm\_UECM\_Get (GPSI, AMF Registration) service operation. The UDM provides the NSSAAF with the AMF ID of the AMF serving the UE, as specified in TS 33.501 [2], clause 6.13.

Threat Reference: TBD

**Test Name:** TC\_NSSAAF\_AAAS\_AUTHORIZATION\_REAUTH\_REVOCATION

**Purpose:**

Verify that the AAA-S is authorized to send the re-authentication or revocation.

**Pre-Conditions:**

- Test environment with AAA-S and AAA-P, which may be simulated. The NSAAF under test is connected with AAA-S and AAA-P.

- A document describes the mapping between S-NSSAI and AAA-S server.

**Execution Steps**

1. The AAA-S sends Re-authentication or revocation message to the NSSAAF including the S-NSSAI and the GPSI.

2. The NSSAAF checks whether the AAA-S can be matched against with the S-NSSAI based on the mapping table.

**Expected Results:**

The NSSAAF rejects the re-authentication or revocation or pass the re-authentication or revocation.

**Expected format of evidence:**

 Save the logs and the communication flow in a .pcap file.

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