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

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.519** | **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 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:*** | | 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, 4.2.2.1.1, 4.2.2.1.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 TS 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[3] 3GPP TS 23.501: "System Architecture for the 5G System".

[4] 3GPP TS 33.122: " Security aspects of Common API Framework (CAPIF) for 3GPP northbound APIs".

[5] 3GPP TR 33.926: "Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes".

[6] 3GPP TS 33.117: "Catalogue of general security assurance requirements".

[x] 3GPP TS 33.210: "Network Domain Security (NDS); IP network layer security"

[y] IETF RFC 6749: "The OAuth 2.0 Authorization Framework"

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

4.2.2.1.1 Authentication on application function

*Requirement Name:* Authentication on application function

*Requirement Reference:* TS 33.501 [2], clause 5.9.2.3, and clause 12.2

*Requirement Description:* Mutual authentication between the NEF and Application Function is expected to be supported as specified in TS 33.501 [2], clause 5.9.2.3. For authentication between NEF and an Application Function that resides outside the 3GPP operator domain, mutual authentication based on client and server certificates is expected to be performed between the NEF and AF using TLS and Certificate based authentication is expected to follow the profiles given in TS 33.210 [x], clause 6.2 as specified in TS 33.501 [2], clause 12.2.

*Threat References*: TR 33.926 [5], clause I.2.2.1, No authentication on application function

***Test Case****:*

**Test Name:** TC\_CP\_AUTH\_AF\_NEF

**Purpose:** Toverify that the NEF can authenticate application function and establish TLS connection towards the application server with certificate based authentication, and may authenticate application function and establish TLS connection towards the application server with pre-shared key based authentication.

**Pre-Condition:**

- The NEF network product shall be connected in emulated/real network environments.

- In order to establish TLS connections to the NEF network product, the application function shall offer a feature that is supported by the NEF network product, including protocol version and combination of cryptographic algorithms.

- The application function and the NEF network product shall support certificate based authentication, and may support pre-shared key based authentication.

- If the NEF network product does not support CAPIF as specified in clause 6.2.5.1 in TS 23.501 [3], the certificates or the pre-shared key shall be provisioned in the NEF network product.

- If the NEF network product supports CAPIF, the certificates or the pre-shared key shall be provisioned in the CAPIF core function, the CAPIF core function shall be able to select appropriate authentication method as defined in the sub-clause 6.5.2 in TS 33.122 [4].

**Execution Steps:**

1. If certificate based authentication is used, provision correct certificate on the application function, if pre-shared key based authentication is used, provision same pre-shared key on the application function.

2. The application function shall initiate establishment of TLS connection towards the NEF network product, and check whether a TLS connection is established successfully.

3. If certificate based authentication is used, provision incorrect certificate on the application function, if pre-shared key based authentication is used, provision different pre-shared key on the application function.

4. The application function shall initiate establishment of TLS connection towards the NEF network product, and check whether no new TLS connection is established.

**Expected Results:**

Only one TLS connection is established at step 2.

**Expected format of evidence:**

Evidence suitable for the interface, e.g., Screenshot containing the operational results.

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

4.2.2.1.2 Authorization on northbound APIs

*Requirement Name:* Authorization on application function

*Requirement Reference:* TS 33.501 [2], clause 12.4

*Requirement Description:* The NEF is expected to authorize the requests from Application Function using OAuth-based authorization mechanism, the specific authorization mechanisms are expected to follow the provisions given in RFC 6749 [y]" as specified in TS 33.501 [2], clause 12.4.

*Threat References*: TR 33.926 [5], clause I.2.2.2, No authorization on northbound APIs

***Test Case****:*

**Test Name:** TC\_CP\_AUTHOR\_AF\_NEF

**Purpose:** Toverify that the NEF can authorize application function.

**Pre-Condition:**

- The NEF network product shall be connected in emulated/real network environments.

- The application function and the NEF network product shall support OAuth-based authorization mechanism.

- An authorization server (e.g. NRF, or CAPIF core function) that supports OAuth2 protocol to authorize NEF northbound APIs using the "Client Credentials" authorization grant has been deployed.

- The TLS connection between the NEF network product and the application function has been established.

- The authorization server is configured to grant the application function to access a northbound API of the NEF network product, called NEF northbound API A.

**Execution Steps:**

Test 1: without token:

1. The application function invokes Obtain\_Authorization service towards the authorization server to get a token from the authorization server for accessing the NEF northbound API A.

2. The application function invokes NEF northbound API A.

3. The tester triggers the application function to invoke another northbound API of the NEF network product, called NEF northbound API B, without token.

Test 2: With incorrect token:

1. The application function invokes Obtain\_Authorization service towards the authorization server to get a token from the authorization server for accessing the NEF northbound API A.

2. The application function invokes NEF northbound API A.

3. The tester triggers the application function to invoke the NEF northbound API B with a fake token.

**Expected Results:**

The invoking of NEF northbound API A succeeds, while the invoking of NEF northbound API B fails.

**Expected format of evidence:**

Evidence suitable for the interface, e.g., Screenshot containing the operational results.

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