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

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

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.537** | **CR** | **XXXX** | **rev** | **-** | **Current version:** | **18.0.1** |  |
|  |
| *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:*** | 4.2.2.1, 4.2.3.2.4.1, 4.2.3.4.2 |
|  |  |
|  | **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\*\*\*\*

#### 4.2.2.1 AKMA key storage and update

*Requirement Name*: AKMA key storage update

*Requirement Reference:* TS 33.535 [4], clause 6.1

*Requirement Description*: The AAnF is expected to store the latest information sent by the AUSF. After receiving the new generated A-KID and KAKMA, the AAnF deletes the old A-KID and KAKMA and stores the new generated A-KID and KAKMA as specified in TS 33.535[4], clause 6.1.

*Threat References*: TR 33.926 [6], clause X.2.2.Y, AKMA key storage and update

*Test Case*:

**Test Name:** TC\_AKMA\_Key\_Storage\_Update

**Purpose:**

Verify that the AAnF stores only the latest AKMA context received by the AUSF.

**Pre-Conditions:**

- Test environment with AUSF and AF. The AUSF and the AF may be simulated.

- AAnF network product is connected in emulated/real network environment.

**Execution Steps**

Test A:

1) Primary authentication is simulated for a specific UE, leading to the simulated AUSF pushing SUPI, A-KID1, KAKMA1 to the AAnF.

2) The AF requests a KAF from the AAnF by proving A-KID1 and AF\_ID.

3) Another primary authentication is simulated for the same UE, leading to the simulated AUSF pushing SUPI, A-KID2, KAKMA2 to the AAnF.

4) The AF requests a KAF by providing A-KID1 to the AAnF.

5) The AF requests a KAF by providing A-KID2 to the AAnF.

**Expected Results:**

The AF received an error message indicating the AKMA context related to A-KID 1 is not found after step 4). After step 5), the AF received a KAF which is different from the KAF that received after step 2).

**Expected format of evidence:**

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

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

##### 4.2.3.2.4.1 Confidentiality, integrity and replay protections over SBA interface

*Requirement Name*: Confidentiality, integrity and replay protections over SBA interface

*Requirement Reference:* TS 33.535 [4], clause 4.4.0

*Requirement Description*: The SBA interface between the AAnF and the AUSF is expected to be confidentiality, integrity and replay protected as specified in TS 33.535 [4], clause 4.4.0.

*Threat References*: TR 33.926 [3], Annex X.2.2.1, Control plane data protection with AUSF

*Test Case:*

**Test Name:** TC\_PROTECT\_SBA\_AAnF\_AUSF

**Purpose:**

Verify that the transported data between AAnF and AUSF are confidentiality, integrity and replay protected over SBA interface.

**Pre-Conditions:**

- AAnF and AUSF network products are connected in simulated/real network environment.

- Network product documentation containing information about supported TLS protocol and certificates is provided by the vendor.

- Tester shall have access to the SBA interface between AAnF and AUSF.

**Execution Steps:**

The requirement mentioned in this clause is tested in accordance with the procedure mentioned in clause 4.2.2.2.2 of TS 33.117 [2].

**Expected Results:**

The user data transported between AAnF and AUSF is confidentiality, integrity and replay protected.

**Expected format of evidence:**

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

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

##### 4.2.3.2.4.2 Confidentiality, integrity and replay protections over SBA interface

*Requirement Name*: Confidentiality, integrity and replay protections over SBA interface

*Requirement Reference*: TS 33.535 [4], clause 4.4.0

*Requirement Description*: The SBA interface between AAnF and AF/NEF is expected to be confidentiality, integrity and replay protected as specified in TS 33.535 [4], clause 4.4.0.

*Threat References*: TR 33.926 [3], Annex X.2.2.2, Control plane data protection with AF/NEF

*Test Case*:

**Test Name**: TC\_PROTECT\_AAnF\_AF\_NEF

**Purpose**:

Verify that the transported data between AAnF and AF/NEF are confidentiality, integrity and replay protected over SBA interface.

**Pre-Conditions**:

- AAnF and AF/NEF network products are connected in simulated/real network environment.

- Network product documentation containing information about supported TLS protocol and certificates is provided by the vendor.

- Tester shall have access to the SBA interface between AAnF and AF/NEF.

**Execution Steps**:

The requirement mentioned in this clause is tested in accordance with the procedure mentioned in clause 4.2.2.2.2 of TS 33.117 [2].

**Expected Results**:

The user data transported between AAnF and AF/NEF is confidentiality, integrity and replay protected.

**Expected format of evidence**:

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

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