**3GPP TSG-SA3 Meeting #115 *S3-240870***

**Athens, Greece, 26th Feb 2024 - 1st Mar 2024**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.2* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.514** | **CR** | **draftCR** | **rev** | **1** | **Current version:** | **18.2.0** |  |
|  | | | | | | | | |
| *For* ***HE******LP*** *on using this form: comprehensive instructions can be found at  http://www.3gpp.org/Change-Requests.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Add UDM SCAS test case for checking the authentication verification of a synchronization failure message | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | BSI (DE) | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | TBD | | | | |  | ***Date:*** | | | 2024-02-16 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-19 |
|  | *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. | | | | | | | | *Use one of the following releases: Rel-8 (Release 8) Rel-9 (Release 9) Rel-10 (Release 10) Rel-11 (Release 11) … Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18) Rel-19 (Release 19)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | A test case for detecting the processing of an unverified AUTS parameter from synchronization failure messages is not yet specified in the UDM SCAS tests, resulting in a lack of test coverage for key security features. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Add UDM SCAS test case to check if a synchronization failure message with an AUTS parameter containing an invalid MAC-S will be rejected. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The UDM SCAS tests may fail to detect a significant security flaw. This could result in attacks affecting the user authentication and privacy. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | | **x** |  | Other core specifications | | | | TR 33.926 CR 0087  TS 33.102 CR 0284  TS 33.501 CR 1903 | | |
| ***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 1st CHANGE \*\*\*\*\*\*\*\*\*\*

# 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".

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

[6] 3GPP TS 23.003: "Numbering, addressing and identification".

[7] 3GPP TS 33.102: "3G security; Security architecture".

[8] 3GPP TS 29.503: "5G System; Unified Data Management Services; Stage 3".

\*\*\*\*\*\*\*\*\*\* START OF 2nd CHANGE \*\*\*\*\*\*\*\*\*\*

#### 4.2.2.X Authentication verification of synchronization failure messages

*Requirement Name:* Authentication verification of synchronization failure messages

*Requirement Reference:* TS 33.501 [2], clause 6.1.3.3.2;TS 33.102 [7], clause 6.3.5. and TS 29.503 [8], clause 5.4.2.2.2.2b

*Requirement Description:*

- When the UDM/ARPF receives an Nudm\_UEAuthentication\_Get Request message with a "*synchronisation failure indication*" it acts as described in TS 33.102 [9], clause 6.3.5 where ARPF is mapped to HE/AuC, as specified in TS 33.501 [2], clause 6.1.3.3.2

- The HE/AuC verifies *AUTS* (cf.subsection 6.3.3), as specified in TS 33.102 [7], clause 6.3.5 step 4.

- If the operation cannot be authorized due to e.g UE does not have required subcription data, none of the CAG IDs in the CAG cell match any of the subscribed and UE-acknowledged CAG IDs in the allowed CAG list, access barring or roaming restrictions, UDM receives an anonymous SUCI that does not contain the realm part, HTTP status code "403 Forbidden" should be returned including additional error information in the response body (in "ProblemDetails" element). If the cellCagInfo is not received, the UDM shall not assume the UE is accessing from the PLMN and shall not stop the authenthcation if the UE is allowed to access 5GS via CAG cell(s) only, as specified in TS 29.503 [8], clause 5.4.2.2.2, 2b

- On failure, the appropriate HTTP status code indicating the error is returned and appropriate additional error information should be returned in the POST response body, as specified in TS 29.503 [8], clause 5.4.2.2.2

*Threat References*: TR 33.926 [4], clause E.2.2.X, Synchronization verification failure.

*Test Case:*

**Test Name:** TC\_VERIFY\_AUTH\_SYNC\_FAIL\_MSG\_UDM

**Purpose:**

Verify that the UDM validates the authentication of synchronization failure messages.

**Procedure and execution steps:**

**Pre-Condition:**

Test environment with an AUSF. The AUSF may be simulated.

**Execution Steps:**

1. The tester generates the parameters RAND and AUTS in such a way that the MAC-S contained in AUTS is invalid, for example, by randomly choosing the MAC-S value.

2. The tester sends an Nudm\_UEAuthentication\_Get message to the UDM with a "synchronisation failure indication" and the generated parameters.

**Expected Results:**

The UDM/ARPF rejects the AUTS parameter and sends a Nudm\_UEAuthentication\_Get Response message with anHTTP status code “403 Forbidden” and may include additional error information in the response body (in “ProblemDetails” element) as specified in TS 29.503 [8], clause 5.4.2.2.2, 2b.

NOTE: The “cause” attribute of the “ProblemDetails” element may be AUTHENTICATION\_REJECTED as described in TS 29.503 [8], clause 6.3.3.2.4.2-2.

The UDM/ARPF could also log the rejection of the AUTS parameter.

**Expected format of evidence:**

Evidence suitable for the interface, e.g., evidence can be presented in the form of packet trace (e.g., pcap file).

### \*\*\*\*\*\*\*\*\*\* END OF CHANGE \*\*\*\*\*\*\*\*\*\*