**3GPP TSG-SA3 Meeting #123 S3-252706-r3**

Goteborg, Sweden, 25 – 29 August 2025

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.516** | **CR** | **0008** | **rev** | **-** | **Current version:** | **18.0.0** |  |
|  |
| *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 test case that verifies if the AUSF processes RES\* failures correctly |
|  |  |
| ***Source to WG:*** | BSI (DE), Montsecure |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | SCAS\_5GA |  | ***Date:*** | 2025-08-15 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-20 |
|  | *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. | *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:*** | The AMF has a test case named TC\_RES\_STAR\_VERIFICATION\_FAILURE that verifies whether RES\* verification failure is handled correctly. TS 33.501, clause 6.1.3.2.2 also requires the AUSF to perform the RES\* verification.Especially in a roaming scenario, this verification is done in the AUSF network function for the home network, since the AMF/SEAF is part of the visiting network in such case.If verification in the AUSF is not correctly implemented, this might have security implications, as seen in some open source implementations. |
|  |  |
| ***Summary of change:*** | Added a test case TC\_RES\_STAR\_VERIFICATION\_FAILURE\_AUSF that tests whether RES\* verification is correctly implemented in the AUSF. |
|  |  |
| ***Consequences if not approved:*** | Security key K\_SEAF might be leaked if the AUSF network function does not implement RES\* verification correctly (more information in TR 33.926). |
|  |  |
| ***Clauses affected:*** | 4.2.2.X |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** | **X** |  |  Other core specifications  | TR 33.926 CR 0108  |
| ***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 \*\*\*\*\*\*\*\*\*\*

#### 4.2.2.X RES\* verification failure handling

*Requirement Name:* RES\* verification failure handling of AUSF

*Requirement Reference:* TS 33.501, clause 6.1.3.2.0 and TS 29.509, clause 5.2.2.2.2.

*Requirement Description*:

As specified in TS 33.501, clause 6.1.3.2.0, step 11, AUSF compares the received RES\* with the stored XRES\*. If the RES\* and XRES\* are equal, the AUSF considers the authentication as successful from the home network point of view. AUSF informs UDM about the authentication result.

*Threat Reference*: TR 33.926, clause F.2.2.X, RES\* verification failure

*Test case*:

**Test Name:** TC\_RES\_STAR\_VERIFICATION\_FAILURE\_AUSF

**Purpose:**

Test case 1: Verify that the AUSF correctly handles RES\* verification when the XRES\* value is the same as the RES\* value.

Test case 2: Verify that the AUSF correctly handles RES\* verification when the XRES\* value is set an incorrect value (value not equal to RES\*).

Test case 3: Verify that the AUSF correctly handles RES\* verification when the XRES\* value is set to null.

**Pre-Conditions:**

- AUSF network product is connected in simulated/real network environment including a UDM and AMF. The UDM and AMF may be simulated.

- The tester has access to the user credentials.

- The SUPI is provisioned in the UDR.

- Tester can derive expected RES\* from RAND, AUTN, and subscriber credentials.

- Serving Network Name is consistently configured.

**Execution Steps:**

1. The tester triggers an Nausf\_UEAuthentication request message (POST /ue-authentications) sent from AMF to AUSF containing the SUCI derived from the SUPI and Serving Network Name.

2. The tester captures the Nausf\_UEAuthentication response message (HTTP 201 Created) sent from AUSF to AMF containing HXRES\*, AUTN and RAND values.

NOTE: Steps 1 and 2 are to be executed for Test case 1, 2 and 3.

Test case 1 (RES\* equals XRES\*):

3. The tester computes a valid RES\* value based on the observed RAND.

4. The tester triggers an Nausf\_UEAuthentication\_Authenticate request message (UT /ue-authentications/{authCtxId}/5g-aka-confirmation) sent from AMF to AUSF containing the computed RES\* value.

5. The tester captures the Nausf\_UEAuthentication\_Authenticate response message (HTTP 200 OK) sent from AUSF to AMF containing AUTHENTICATION\_SUCCESS, SUPI and Kseaf.

Test case 2 (RES\* incorrect and not null):

3. The tester computes an incorrect RES\* value (not the expected value and not all zeroes).

4. The tester triggers an Nausf\_UEAuthentication\_Authenticate request message sent from AMF/SEAF to AUSF containing the incorrect RES\* value.

5. The tester captures the Nausf\_UEAuthentication\_Authenticate response message sent from AUSF to AMF/SEAF.

Test case 3 (RES\* set to null):

3. The tester triggers an Nausf\_UEAuthentication\_Authenticate request message sent from AMF/SEAF to AUSF containing only zeroes as the RES\* value.

4. The tester captures the Nausf\_UEAuthentication\_Authenticate response message sent from AUSF to AMF/SEAF.

**Expected Results:**

For test case 1, the AUSF responds with a successful authentication response. Additionally, the AUSF notifies the UDM of the successful authentication over the N13 interface.

For test cases 2 and 3, the AUSF responds with an unsuccessful authentication response. Additionally, the AUSF notifies the UDM of the unsuccessful authentication over the N13 interface.

**Expected format of evidence:**

Evidence suitable for the interface, e.g., evidence can be presented in the form of log messages or a packet trace. A packet trace contains at least the messages sent between the AMF/SEAF and AUSF and the messages sent between the AUSF and UDM on the N13 interface.

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