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

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** |  | **Current version:** |  |  |
|  | | | | | | | | |
| *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 | **x** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Clarification of RES\* verification failure handling | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Federal Office for Information Security (BSI) | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** |  | | | | |  | ***Date:*** | | | 2023-05-08 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | F |  | | | | | ***Release:*** | | | Rel-17 |
|  | *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:*** | | The Requirement Description states how the SEAF/AMF correctly handles a missing Nausf\_UEAuthentication\_Authenticate Response message from the AUSF. This is not covered by a SCAS test case yet.  For Test A and B, the expected behaviour of the AMF/SEAF should be to send a null value RES\* in the Nausf\_UEAuthentication\_Authenticate Request message to the AUSF as stated in TS 29.509 [10], clause 5.2.2.2.2. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Added reference to TS 29.509.  Corrected Requirement Description to match 33.501 (changed “Request” to “Response”).  Added 3rd purpose to check for SEAF/AMF correctly handling a missing Nausf\_UEAuthentication\_Authenticate Response message.  Added Test case E and F to check for SEAF/AMF correctly handling a missing Nausf\_UEAuthentication\_Authenticate Response message.  Added Expected Results for Test case E and F.  Modified Expected format of evidence. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Not all requirements stated in the Requirement Description are fulfilled. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 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 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 nonspecific.

- 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 (Release 15): "Security architecture and procedures for 5G system".

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

[4] 3GPP TS 23.003: "Numbering, addressing and identification".

[5] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[6] 3GPP TR 33.926: "Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes".

[7] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[8] 3GPP TS 23.501: "System Architecture for the 5G System".

[9] 3GPP TS 38.413: "NG-RAN; NG Application Protocol (NGAP)".

[10] 3GPP TS 29.509: “5G System; Authentication Server Services”

\*\*\*\*\*\*\*\*\*\* END OF 1st CHANGE \*\*\*\*\*\*\*\*\*\*

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

##### 4.2.2.1.2 RES\* verification failure handling

*Requirement Name*: RES\* verification failure handling

*Requirement Reference:* TS 33.501 [7], clause 6.1.3.2.2

*Requirement Description*:

"The SEAF shall proceed with step 10 in Figure 6.1.3.2-1 and after receiving the Nausf\_UEAuthentication\_Authenticate Response message from the AUSF in step 12 in Figure 6.1.3.2-1, proceed as described below:

- If the AUSF has indicated in the Nausf\_UEAuthentication\_Authenticate Response message to the SEAF that the verification of the RES\* was not successful in the AUSF, or

- if the verification of the RES\* was not successful in the SEAF,

then the SEAF shall either reject the authentication by sending an Authentication Reject to the UE if the SUCI was used by the UE in the initial NAS message or the SEAF/AMF shall initiate an Identification procedure with the UE if the 5G-GUTI was used by the UE in the initial NAS message to retrieve the SUCI and an additional authentication attempt may be initiated.

Also, if the SEAF does not receive any Nausf\_UEAuthentication\_Authenticate Response message from the AUSF as expected, then the SEAF shall either reject the authentication to the UE or initiate an Identification procedure with the UE."

As specified in TS 33.501 [7], clause 6.1.3.2.2.*Threat References*: TR 33.926 [6], clause K.2.2.3, RES\* verification failure

*Test Case*:

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

**Purpose:**

1) Verify that the SEAF/AMF correctly handles RES\* verification failure detected in the SEAF/AMF or/and in the AUSF, when the SUCI is included in the initial NAS message.

2) Verify that the SEAF/AMF correctly handles RES\* verification failure detected in the SEAF/AMF or/and in the AUSF, when the 5G-GUTI is included in the initial NAS message.

3) Verify that the SEAF/AMF correctly handles a missing Nausf\_UEAuthentication\_Authenticate Response message from the AUSF.

**Procedure and execution steps:**

**Pre-Conditions:**

Test environment with UE and AUSF. The UE and the AUSF may be simulated.

**Execution Steps**

A. Test Case 1

1) The UE sends RR with SUCI to the SEAF/AMF under test, to trigger the SEAF/AMF under test to initiate the authentication, i.e. to send Nausf\_UEAuthentication\_Authenticate Request to the AUSF.

2) The AUSF, after receiving the request from the SEAF/AMF under test, responds with a Nausf\_UEAuthentication\_Authenticate Response message with an authentication vector to the SEAF/AMF under test.

3) The UE, after receiving the Authentication Request message from the SEAF/AMF under test, returns an incorrect RES\* to the SEAF/AMF under test in the NAS Authentication Response message, which will trigger the AMF to compute HRES\*, compare HRES\* with HXRES\* and send an authentication request to the AUSF. The tester captures the value of RES\* in the request.

4) The AUSF returns to the AMF under test the indication of RES\* verification failure.

B. Test Case 2

1) The UE sends RR with a 5G-GUTI to the SEAF/AMF under test, to trigger the SEAF/AMF under test to initiate the authentication, i.e. to send Nausf\_UEAuthentication\_Authenticate Request to the AUSF.

2) The AUSF, after receiving the request from the SEAF/AMF under test, responds with a Nausf\_UEAuthentication\_Authenticate Response message with an authentication vector to the SEAF/AMF under test.

3) The UE, after receiving the Authentication Request message from the SEAF/AMF under test, returns an incorrect RES\* to the SEAF/AMF in the NAS Authentication Response message, which will trigger the AMF to compute HRES\* and compare HRES\* with HXRES\*, and send an authentication request to the AUSF. The tester captures the value of RES\* in the request.

4) The AUSF returns to the AMF under test an indication of RES\* verification failure.

C. Test Case 3

1) The UE sends RR with SUCI to the SEAF/AMF under test, to trigger the SEAF/AMF under test to initiate the authentication, i.e. to send Nausf\_UEAuthentication\_Authenticate Request to the AUSF.

2) The AUSF, after receiving the request from the SEAF/AMF under test, responds with a Nausf\_UEAuthentication\_Authenticate Response message with an authentication vector to the SEAF/AMF under test.

3) The UE returns RES\* to the SEAF/AMF under test in the NAS Authentication Response message, which will trigger the AMF to compute HRES\*, compare HRES\* with HXRES\*, and send to the received RES\* to the AUSF.

4) The AUSF returns to the AMF under test an indication of RES\* verification failure.

D Test Case 4

1) The UE sends RR with 5G-GUTI to the SEAF/AMF under test, to trigger the SEAF/AMF under test to initiate the authentication, i.e. to send Nausf\_UEAuthentication\_Authenticate Request to the AUSF.

2) The AUSF, after receiving the request from the SEAF/AMF under test, responds with a Nausf\_UEAuthentication\_Authenticate Response message with an authentication vector to the SEAF/AMF under test.

3) The UE returns RES\* to the SEAF/AMF under test in the NAS Authentication Response message, which will trigger the AMF to compute HRES\*, compare HRES\* with HXRES\*, and send to the received RES\* to the AUSF.

4) The AUSF returns to the AMF under test an indication of RES\* verification failure.

Test E:

1) The tester triggers the UE to send a Registration Request with SUCI to the SEAF/AMF under test, to trigger the SEAF/AMF under test to initiate the authentication, i.e. to send Nausf\_UEAuthentication\_Authenticate Request to the AUSF.

2) The AUSF, after receiving the request from the SEAF/AMF under test, responds with a Nausf\_UEAuthentication\_Authenticate Response message with an authentication vector to the SEAF/AMF under test.

3) The UE returns RES\* to the SEAF/AMF under test in the NAS Authentication Response message, which will trigger the AMF to compute HRES\*, compare HRES\* with HXRES\*, and send the received RES\* to the AUSF.

4) The tester prepares the AUSF to not return the Nausf\_UEAuthentication\_Authenticate Response message and therefore trigger a timeout at the SEAF/AMF.

Test F:

1) The tester triggers the UE to send a Registration Request with 5G-GUTI to the SEAF/AMF under test, to trigger the SEAF/AMF under test to initiate the authentication, i.e. to send Nausf\_UEAuthentication\_Authenticate Request to the AUSF.

2) The AUSF, after receiving the request from the SEAF/AMF under test, responds with a Nausf\_UEAuthentication\_Authenticate Response message with an authentication vector to the SEAF/AMF under test.

3) The UE returns RES\* to the SEAF/AMF under test in the NAS Authentication Response message, which will trigger the AMF to compute HRES\*, compare HRES\* with HXRES\*, and send the received RES\* to the AUSF.

4) The tester prepares the AUSF to not return the Nausf\_UEAuthentication\_Authenticate Response message and therefore trigger a timeout at the SEAF/AMF.

NOTE: The timeout timer is the NAS timer T3520.

**Expected Results:**

For test case 1 and 3, the SEAF/AMF rejects the authentication by sending an Authentication Reject to the UE.

For test case 2 and 4, the SEAF/AMF initiates an Identification procedure with the UE to retrieve the SUCI.

For test case E and F, the SEAF/AMF rejects the authentication to the UE or initiate an Identification procedure with the UE.

For test case A and B, a null value RES\* is in the Nausf\_UEAuthentication\_Authenticate Request message sent from the SEAF/AMF to the AUSF. (stated in TS 29.509 [10], clause 5.2.2.2.2)

**Expected format of evidence:**

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

\*\*\*\*\*\*\*\*\*\* END OF 2nd CHANGE \*\*\*\*\*\*\*\*\*\*