**3GPP TSG-SA3 Meeting #101-e *S3-20xxxx***

**e-meeting, 9th - 20th November 2020 revision of S3-203117**

|  |
| --- |
| *CR-Form-v12.0* |
| **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:***  |  |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** |  |  | ***Date:*** | 30-10-2020 |
|  |  |  |  |  |
| ***Category:*** |  |  | ***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 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-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)* |
|  |  |
| ***Reason for change:*** | In TS 29.510 R16, the definition of the specific claims within an access token has been updated. Hence, the requirements of access token verification were updated accordingly in TS 33.501 R16.Therefore, the referenced requirements and test details for access token verification failure handling in TS 33.117 R16 needs to be updated for TS 33.117 R17 accordingly. |
|  |  |
| ***Summary of change:*** | Updated the requirement and test details for access token verification failure handling in clause 4.2.2.2.3.1 of TS 33.117 R17. |
|  |  |
| ***Consequences if not approved:*** | The test case cannot fully serve the test purpose. |
|  |  |
| ***Clauses affected:*** | 2, 4.2.2.2.3.1 |
|  |  |
|  | **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 the 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 TR 41.001: "GSM Specification set".

[3] IETF RFC 3871: "Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure".

[4] 3GPP TR 33.926: "Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes".

[5] CVE-1999-0511, http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0511

[6] "Practical recommendations for securing Internet-connected Windows NT Systems", <https://support2.microsoft.com/default.aspx?scid=kb;%5BLN%5D;164882>.

[7] X-Force Vulnerability Report, <http://www.iss.net/security_center/static/193.php>

[8] IETF RFC 2644: "Changing the Default for Directed Broadcasts in Routers."

[9] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[10] 3GPP TS 33.501 v15: "Security architecture and procedures for 5G system".

[11] IETF RFC 7540: "Hypertext Transfer Protocol Version 2 (HTTP/2)".

[12] IETF RFC 6749: "OAuth2.0 Authorization Framework".

[13] 3GPP TS 29.501: "Principles and Guidelines for Services Definition".

[xx] 3GPP TS 33.501: "Security architecture and procedures for 5G system" (Release 16)

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of the 2nd Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

###### 4.2.2.*2*.3.1 Authorization token verification failure handling wthin one PLMN

*Requirement Name*: Authorization token verification failure handling wthin one PLMN

*Requirement Reference:* TS 33.501 [xx], clause 13.4.1.1

*Requirement Description*:

"13.4.1.1 Service access authorization within the PLMN

2. The NF Service producer shall verify the access token as follows:

 - The NF Service producer ensures the integrity of the access token by verifying the signature using NRF’s public key or checking the MAC value using the shared secret. If integrity check is successful, the NF Service producer shall verify the claims in the access token as follows:

NOTE: Void.

- It checks that the audience claim in the access token matches its own identity or the type of NF service producer. If a list of NSSAIs or list of NSI IDs is present, the NF service producer shall check that it serves the corresponding slice(s).

- If an NF Set ID present, the NF Service Producer shall check the NF Set ID in the claim matches its own NF Set ID.

- If scope is present, it checks that the scope matches the requested service operation.

- If the access token contains "additional scope" information (i.e. allowed resources and allowed actions (service operations) on the resources), it checks that the additional scope matches the requested service operation.

- It checks that the access token has not expired by verifying the expiration time in the access token against the current data/time.

3. If the verification is successful, the NF Service producer shall execute the requested service and responds back to the NF Service consumer. Otherwise it shall reply based on Oauth 2.0 error response defined in RFC 6749 [43]. The NF service consumer may store the received token(s). Stored tokens may be re-used for accessing service(s) from producer NF type listed in claims (scope, audience) during their validity time."

*Threat References*: TR 33.926 [4], clause 6.3.3.1, Incorrect Verification of Access Tokens

*Test Case*:

**Test Name:** TC\_AUTHORIZATION\_TOKEN\_VERIFICATION\_FAILURE\_ONE\_PLMN

**Purpose:**

Verify that the NF service producer does not grant service access if the verification of authorization token from a NF service consumer in the same PLMN fails.

**Procedure and execution steps:**

**Pre-Conditions:**

- Test environment with a NF service consumer.

- The NF service consumer may be simulated.

- The network product under test has already mutually authenticated with the NF service consumer.

- The tester shall have access to the interface between the NF service consumer and the network product under test.

- The tester has the NRF’s private key or the shared key.

- The network product under test is preconfigured with the NRF’s public key or the shared key.

**Execution Steps**

The network product under test receives the access token sent from the NF service consumer, verifies the access token based on Oauth 2.0.

Test Cases 1~4 are tests on failure handling by the network product under test when the mandatory claims in access token failed verification.

Test Case 1: Verification failure of the access token integrity

1) The tester computes an access token correctly, except that the signature or the MAC is incorrect, e.g., the signature or the MAC is randomly selected, and then includes the access token in the NF Service Request sent from the NF service consumer to the network product under test.

2) The integrity verification of the access token by the network product under test fails.

Test Case 2: Incorrect audience claim in the access token

1) The tester computes an access token correctly, except that the audience claim is incorrect, i.e., the audience claim in the access token does not match the identity or the type of the network product under test, and then includes the access token in the NF Service Request sent from NF service consumer to the network product under test.

2) The network product under test verifies that the integrity of the access token is valid. However, the audience claim in the access token does not match its identity or type.

Test Case 3: Incorrect scope claim in the access token

1) The tester computes an access token correctly, except that the scope is incorrect, i.e., the scope does not match the requested service operation, and then includes the access token in the NF Service Request sent from the NF service consumer to the network product under test.

2) The network product under test verifies that the integrity of the access token and the audience claim are valid. However, the scope does not match the requested service operation.

Test Case 4: Expired access token

1) The tester computes an access token correctly, except that the expiration time has expired against the current data/time, and then includes the access token in the NF Service Request sent from the NF service consumer to the network product under test.

2) The network product under test verifies that the integrity of the access token, the audience and scope claims are all valid. However, the expiration time in the access token has expired against the current data/time.

Test Cases 5~8 are tests on failure handling by the network product under test when the optional claims in access token failed verification.

NOTE: The test cases below only apply to the NFs which support identifying and understanding the optioanl claims in the received access token.

Test Case 5: Incorrect list of S-NSSAIs in the access token

1) The tester computes an access token correctly, except that the list of S-NSSAIs is incorrect, i.e., the network product under test does not serve the slices indicated in the list of S-NSSAIs, and then includes the access token in the NF Service Request sent from NF service consumer to the network product under test.

2) The network product under test verifies that the integrity of the access token, the audience, scope and expiration time claims are all valid. Then it further checks the list of S--NSSAIs included in the access token.

Test Case 6: Incorrect list of NSIs in the access token

1) The tester computes an access token correctly, except that the list of NSIs is incorrect, i.e., the network product under test does not serve the slices indicated in the list of NSIs, and then includes the access token in the NF Service Request sent from NF service consumer to the network product under test.

2) The network product under test verifies that the integrity of the access token, the audience, scope and expiration time claims are all valid. Then it further checks the list of NSIs included in the access token.

Test Case 7: Incorrect NF Set ID in the access token

1) The tester computes an access token correctly, except that the NF Set ID is incorrect, i.e. the NF Set ID in the claim does not match the NF Set ID of the network product under test, and then includes the access token in the NF Service Request sent from NF service consumer to the network product under test.

2) The network product under test verifies that the integrity of the access token, the audience, scope and expiration time claims are all valid. Then it further checks the NF Set ID included in the access token.

Test Case 8: Incorrect additional scope in the access token

1) The tester computes an access token correctly, except that the additional scope information is incorrect, i.e. the allowed resources and allowed actions on the resources do not match the requested service operations, and then includes the access token in the NF Service Request sent from the NF service consumer to the network product under test.

2) The network product under test verifies that the integrity of the access token, the audience, scope and expiration time claims are all valid. Then it further checks the additional scope included in the access token.

**Expected Results:**

For test cases 1~4 on verification failure of mandatory claims in the access token, the network product under test rejects the NF service consumer’s service request based on Oauth 2.0 error response defined in RFC 6749 [12].

For test cases 5~8 on verification failure of optional claims in the access token, if the network product under test understands these optional claims (list of S-NSSAIs, list of NSIs, NF Set ID, additional scope), it rejects the NF service consumer’s service request based on Oauth 2.0 error response defined in RFC 6749 [12].

**Expected format of evidence:**

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

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