**3GPP TSG-SA3 Meeting #100e *S3-20xxxx***

**e-meeting, 17 - 28 August 2020 *revision of S3-201892***

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.117** | **CR** | **DraftCR** | **rev** | **-** | **Current version:** | **16.5.0** |  |
|  | | | | | | | | |
| *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:*** | eSCAS\_5G | | | | |  | ***Date:*** | | | 01-08-2020 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **B** |  | | | | | ***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-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | In order to address the threat analysed in S3-201891, a test case needs to be defined for testing the relevant requirement defined in TS 33.501.  Therefore, it is proposed to add the requirement and corresponding test case in TS 33.117 for generic NFs. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Added a new clause for the requirement and test case on generic NFs for correct handling of client credentials assertion validation. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | No test case for security assurance of the authentication for indirect communication. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | clause 2, new clauses 4.2.2.2.x, 4.2.2.2.x.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: "Security architecture and procedures for 5G system" (Release 15).

[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.x Authentication for Indirect Communication

###### 4.2.2.2.x.1 Correct handling of client credentials assertion validation failure

*Requirement Name*: Correct handling of client credentials assertion validation failure

*Requirement Reference:* TS 33.501 [xx], clause 13.3.8.3

*Requirement Description*:

"The verification of the Client credentials assertion shall be performed by the receiving node, i.e., NRF or NF Service Producer in the following way:

* It validates the signature of the JWS as described in RFC 7515 [45].
* If validates the timestamp (iat) and/or the expiration time (exp) as specified in RFC 7519 [44].

If the receiving node is the NR F, the NRF validates the timestamp (iat) and the expiration time (exp).

If the receiving node is the NF Service Producer, the NF service Producer validates the expiration time and it may validate the timestamp.

* It checks that the audience claim in the the client credentials assertion matches its own type.

It verifies that the NF instance ID in the client credentials assertion matches the NF instance ID in the public key certificate used for signing the assertion".

*Threat References*: TR 33.926 [4], clause 6.3.x.1, Incorrect validation of client credentials assertion

Note: The following test case only applies if the NF under test implements verification of client credentials assertions.

*Test Case*:

**Test Name:** TC\_CLIENT\_CREDENTIALS\_ASSERTION\_VALIDATION

**Purpose:**

Verify that the NF under test correctly handles client credentials assertion validation failure.

Editor's Note: This test case applies for Rel-16 NFs. The formulation for indicating the applicable release may need to be updated.

**Procedure and execution steps:**

**Pre-Conditions:**

- Test environment with a consumer NF and a SCP, which may be simulated. (Potentially simulated) consumer NF and (potentially simulated) SCP can be combined for the testing purpose.

- The NF under test is preconfigured with the certificate of the consumer NF.

- The NF under test is configured to require assertions for NF consumer authentication for at least one of its services.

- The tester has the private key of the consumer NF.

- The tester has access to the interface between the consumer NF and the NF under test.

**Execution Steps**

Test Case 1: Failed verification of the client credentials assertion integrity

1) The tester computes a client credentials assertion correctly, except that the signature is incorrect, and then includes the client credentials assertion in the service request sent from the consumer NF to the NF under test via the SCP.

2) The integrity verification of the client credentials assertion by the NF under test fails.

Test Case 2: Incorrect audience claim in the client credentials assertion

1) The tester computes a client credentials assertion correctly, except that the audience claim is incorrect, i.e., the audience claim in the client credentials assertion does not match the type of the NF under test, and then includes the signed client credentials assertion in the service request sent from the consumer NF to the NF under test via the SCP.

2) The NF under test verifies that the audience claim in the client credentials assertion does not match its type.

Test Case 3: Expired client credentials assertion

1) The tester computes an access token correctly, except that the expiration time (exp) has expired against the current time, and then includes the signed client credentials assertion in the service request sent from the consumer NF to the NF under test via the SCP.

2) The NF under test verifies that the expiration time in the client credentials assertion has expired against the current time.

**Expected Results:**

For test cases 1~3, the NF under test rejects the consumer NF’s service request and sends back an error message.

Editor's Note: the result needs to be aligned with the relevant error handling description to be added in TS 29.500.

**Expected format of evidence:**

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

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