**3GPP TSG-SA3 Meeting #123 S3-253027**

Goteborg, Sweden, 25 – 29 August 2025

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.518** | **CR** | **DraftCR** | **rev** | **-** | **Current version:** | **19.0.0** |  |
|  |
| *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:***  | Living document 33.518 |
|  |  |
| ***Source to WG:*** | Huawei, HiSilicon,BSI (DE), Montsecure |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | SCAS\_5GA |  | ***Date:*** | 2025-07-29 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***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:*** | S3-253026:TC\_CLIENT\_CREDENTIALS\_ASSERTION\_VALIDATION in 33.117 includes tests for validating the properties in the CCA but it does not consider the timestamp (iat) value because this is NRF specific. |
|  |  |
| ***Summary of change:*** | S3-253026:Add a test case for validating the timestamp (iat) in the CCA value as an addition to TC\_CLIENT\_CREDENTIALS\_ASSERTION\_VALIDATION in 33.117. |
|  |  |
| ***Consequences if not approved:*** | S3-253026:See section TR 33.926 [4], clause 6.3.4.1 for threats that could occur, if the CCA value is not validated correctly. |
|  |  |
| ***Clauses affected:*** | 4.2.2.X(new), 4.2.2.X.1(new) |
|  |  |
|  | **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:*** | The merger of S3-253026 |

\*\*\*\*\*\*\*\*\*\* START OF 1st CHANGE \*\*\*\*\*\*\*\*\*\*

##### 4.2.2.X Authentication for Indirect Communication

###### 4.2.2.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 [10], clause 13.3.8.3: TS 29.500 [21], clause 6.7.5

*Requirement Description*:

The verification of the Client credentials assertion is 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 [16].

- It validates the timestamp (iat) and/or the expiration time (exp) as specified in RFC 7519 [17].

- If the receiving node is the NRF, 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 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 6.3.4.1, Incorrect validation of client credentials assertion

NOTE 1: The following test case only applies if the NF under test implements verification of client credentials assertions.

NOTE 2: This test case is an extension to TC\_CLIENT\_CREDENTIALS\_ASSERTION\_VALIDATION in TS 33.117 [2] and only includes the NRF-specific test for the validity of the iat value.

If the verification of the CCA fails at the receiving entity (e.g. NRF or NF service producer), a "403 Forbidden" response is returned with the cause attribute set to "CCA\_VERIFICATION\_FAILURE", as stated in TS 29.500 [21], clause 6.7.5.

*Test Case*:

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

**Purpose:**

Verify that the NF under test correctly handles client credentials assertion validation failure. This test case specifically verifies that the NRF under test verifies that the iat value is valid.

**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 NRF under test is preconfigured with the certificate of the consumer NF.

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

- The NRF under test has implemented the client credentials assertion (CCA) authentication method as specified in TS 33.501 [10], clause 13.3.8.3.

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

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

**Execution Steps**

1. The tester computes a client credentials assertion correctly, except that the timestamp (iat) value is in the future. The tester should make sure that the expiration time is greater than the timestamp (iat) value.

2. The tester includes the client credentials assertion in the service request sent from the consumer NF to the NRF under test via the SCP.

3. The tester captures the response sent back by the NRF under test.

**Expected Results:**

The NRF under test rejects the consumer NF's service request with a 403 Forbidden HTTP status code and sends back an error message according to the description TS 29.500 [21], clause 6.7.5.

**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 should at least contain the messages sent between the NRF and the NF service consumer.

\*\*\*\*\*\*\*\*\*\* END OF CHANGES \*\*\*\*\*\*\*\*\*\*