**3GPP TSG-SA3 Meeting #123 S3-253015**

Goteborg, Sweden, 25 - 29 August 2025

|  |
| --- |
| *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 |  |

|  |
| --- |
|  |
| ***Title:***  | Add test case on access token subject verification |
|  |  |
| ***Source to WG:*** | MITRE-FFRDC, US National Security Agency |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** |  |  | ***Date:*** | 2025-08-25 |
|  |  |  |  |  |
| ***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](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:*** | For clause 4.2.2.2.3.1Access token verification tests do not include verification of the access token subject (i.e., NF service consumer).The token verification steps in TS 33.501 clause 13.4.1.1 are not aligned with the token verification steps in the test case in clause 4.2.2.2.3.1 TC\_AUTHORIZATION\_TOKEN\_VERIFICATION\_FAILURE\_ONE\_PLMN. Two token verification checks are not addressed in this test case including:1. *In the direct communication case, it checks that the NF Instance ID in the subject claim within the access token matches the NF Instance ID in the subjectAltName in the NF Service Consumer's TLS client certificate.*
2. *If the CCA is present in the service request, it may verify the CCA as specified in clause 13.3.8.3 and that the subject claim (i.e., the NF Instance Id of the NF Service Consumer) in the access token matches the subject claim in the CCA.*

Two new test cases F & G are added to this test case to address these access token verification steps that are specified in TS 33.501.Since this test case applies to direct communication in NF-NF communications, the token verification check in 1) is applicable under the pre-condition that TLS is used for authentication. Thus, a pre-condition of mutual authentication using TLS is added for test case F only.Similarly, the token verification check in 2) is applicable under the pre-condition that a *CCA is present in the service request*. Thus, a pre-condition of CCA being present in the service request is added for test case G only.This test case is applicable to both Direct and Indirect communication modes. Thus, the pre-condition that requires mutual authentication cannot hold true in indirect communication according to the specified text in TS 33.501 clause 13.3.2.2 Indirect Communication which says in *NOTE 0: Mutual authentication between NF Service Consumer and NF Service Producer is not achieved with hop-by-hop security.* Therefore, this pre-condition must be altered to hold true in indirect communication. To this end, the network product under test can utilize implicit authentication of the NF service consumer, according to TS 33.501 clause 13.3.2.2 which states *In indirect communication scenarios, the NF Service Producer and NF Service Consumer shall use implicit authentication by relying on authentication between NF Service Consumer and SCP, and between SCP and NF Service Producer, provided by the transport layer protection solution, NDS/IP, or physical security.* Therefore, the pre-condition on mutual authentication is changed to say, “The network product under test has already authenticated the NF service consumer.” |
|  |  |
| ***Summary of change:*** | The following changes are made to clause 4.2.2.2.3.1:1. The Requirement Description is modified to align to the requirements in TS 33.501.
2. The pre-conditions are unified for both Indirect and Direct communication modes by replacing the mutual authentication pre-condition with client authentication performed by the network product under test.
3. Additional Pre-conditions are added, which are only applicable for test cases F & G.
4. Two new test cases F & G are added to the test case in clause 4.2.2.2.3.1, to address the access token subject verification steps that are specified in TS 33.501.
 |
|  |  |
| ***Consequences if not approved:*** | The required token verification steps in TS 33.501 clause 13.4.1.1, including verification of access token subject, are not met in the test case for NF access token authorization. Additionally, the test case pre-conditions do not hold true for both Indirect and Direct Communications mode. |
|  |  |
| ***Clauses affected:*** | 4.2.2.2.3.1 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **N** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **N** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **N** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 1st Change\*\*\*\*\*\*\*\*\*\*\*\*\*\*

###### 4.2.2.2.3.1 Authorization token verification failure handling within one PLMN

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

*Requirement Reference:* TS 33.501 [10], clause 13.4.1.1

*Requirement Description*:

According to TS 33.501 [10], clause 13.4.1.1, the NF Service producer verifies 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 verifies the claims in the access token as follows:

NOTE: Void.

- In the direct communication case, it checks that the NF Instance ID in the subject claim within the access token matches the NF Instance ID in the subjectAltName in the NF Service Consumer's TLS client certificate.

- 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 checks that it serves the corresponding slice(s).

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

- 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.

- If scope is present, it checks that the 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.

- If the CCA is present in the service request, it can verify the CCA as specified in clause 13.3.8.3 and that the subject claim (i.e., the NF Instance Id of the NF Service Consumer) in the access token matches the subject claim in the CCA.

- If the verification is successful, the NF Service producer executes the requested service and responds back to the NF Service consumer. Otherwise, it replies based on OAuth 2.0 error response defined in RFC 6749 [12]. The NF service consumer optionally stores 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:**

- The tester shall know if the network product supports the following optional access token verification claims. If an optional claim is not supported, the associated sub-test case does not apply:

- S-NSSAI (Test Case H)

- NSI (Test Case I)

- NF Set ID (Test Case J)

- additional scope (Test Case K)

- Test environment with a NF service consumer.

- The NF service consumer may be simulated.

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

- If either of the following pre-conditions are met, the associated sub-test case applies:

- The network product under test has already mutually authenticated with the NF service consumer using TLS certificate, as specified in TS 33.501[10] clause 13.1.0 (Test Case F).

- A Client Credentials Assertion (CCA) is present in the service request and verified as specified in TS 33.501[10] clause 13.3.8.3, and the Network product supports CCA based authentication (Test Case G).

- The tester has 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 A~G are tests on failure handling by the network product under test when the mandatory claims in access token failed verification.

Test Case A: No access token

1) The tester sends a request without a token to the network product under test.

2) The network product under test recognized the absence of the access token and the verification of the access token fails.

Test Case B: 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 C: 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 D: 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 E: 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 Case F: Access token subject claim does not match the TLS certificate

1) The tester computes an access token correctly, except that the subject claim does not match the corresponding field in the TLS certificate, i.e., the NF Instance ID in the subject claim within the access token does not match the NF Instance ID in the subjectAltName in the NF Service Consumer's TLS client certificate (which was used to establish the TLS connection), 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. However, the subject claim in the access token does not match the subjectAltName in the TLS certificate of the NF service consumer.

NOTE: Test case F is applicable only for direct communication case.

Test Case G: Access token subject claim does not match the CCA

1) The tester computes a Client Credentials Assertion (CCA) correctly for the NF Service Request from the NF service consumer to the network product under test.

2) The tester computes an access token correctly, except that the subject claim (i.e., the NF Instance Id of the NF Service Consumer) in the access token does not match the subject claim in the CCA, and then includes the access token and the CCA in the NF Service Request sent from the NF service consumer to the network product under test.

3) The network product under test verifies that the integrity of the access token, the audience, scope, and expiration time claims are all valid. However, the subject claim in the access token does not match the subject claim in the CCA.

Test Cases H~K 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 optional claims in the received access token.

Test Case H: 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 I: 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 J: 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 K: 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 A~G 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 H~K 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., packet trace (pcap file).

\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 1st Change\*\*\*\*\*\*\*\*\*\*\*\*\*\*