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

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

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.117** | **CR** | **XXXX** | **rev** | **-** | **Current version:** | **17.3.0** |  |
|  |
| *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 |  |

|  |
| --- |
|  |
| ***Title:***  | SCAS release reference corrections |
|  |  |
| ***Source to WG:*** | Huawei, HiSilicon |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | SCAS\_5G\_Ph2 |  | ***Date:*** | 2023-05-22 |
|  |  |  |  |  |
| ***Category:*** | **F** |  | ***Release:*** | Rel-18 |
|  | *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:*** | SA3 has been adding the release numbers explicitly to any of the references pertaining to the network function targeted by the SCAS work, for example reference 2 in TS 33.511. This is because the SCAS work has always been one "release late" since it is challenging to develop the SCAS requirements and tests in parallel to targeted new features within the same release timeline. The references have not been regularly updated and some SCAS specifications include more than one reference to the same specification, for example references 2 and 7 in TS 33.512. This practice is neither future proof nor it is documented anywhere. Furthermore, for SCAS evaluation of network products, this dependency on previous releases in SCAS documents turned out to be not very useful anyway. This issue has been discussed several times in previous SA3 meetings and the proposed resolution is documented in [S3-231050](https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_110_Athens/docs/S3-231050.zip). |
|  |  |
| ***Summary of change:*** | Removal of the release number from the relevant references and minor reformulations to avoid verbatim content copies from other specifications |
|  |  |
| ***Consequences if not approved:*** | Unnecessary dependencies on previous releases and risk for confusion on scope of SCAS specifications |
|  |  |
| ***Clauses affected:*** | 2, 4.2.2.2.2, 4.2.2.2.3.1, 4.2.2.2.3.2, 4.2.2.2.4.1 |
|  |  |
|  | **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 Changes\*\*\*\*

# 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".

[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".

[14] void.

[15] 3GPP TS 33.210: "Network Domain Security (NDS); IP network layer security".

[x] IETF RFC 7515:"JSON Web Signature (JWS)"

[y] IETF RFC 7519:"JSON Web Token (JWT)"

\*\*\*\* Next Changes\*\*\*\*

##### 4.2.2.*2*.2 Protection at the transport layer

*Requirement Name:* Protection at the transport layer

*Requirement Reference:* TS 33.501 [10], clause 5.9.2.1, clause 13.1, clause 13.3.2

*Requirement Description*:

NF Service Request and Response procedure are expected to support mutual authentication between NF consumer and NF producer as specified in TS 33.501 [10], clause 5.9.2.1.

All network functions are expected to support TLS. Network functions are expected to support both server-side and client-side certificates. The TLS profile is expected to follow the profile given in Annex E of TS 33.310 [9] with the restriction to be compliant with the profile given by HTTP/2 as defined in RFC 7540 [11] as specified in TS 33.501 [10], clause 13.1.

Authentication between network functions within one PLMN is expected to use one of the following methods:

- If the PLMN uses protection at the transport layer as described in clause 13.1, authentication provided by the transport layer protection solution is to be used for authentication between NFs as specified in TS 33.501 [10], clause 13.3.2.

*Threat References*: TR 33.926 [4], clause 5.3.6.3, Weak cryptographic algorithms

*Test case*:

**Test Name:** TC\_PROTECT\_TRANSPORT\_LAYER

**Purpose:**

Verify that TLS protocol for NF mutual authentication and NF transport layer protection is implemented in the network products based on the profile required.

**Procedure and execution steps:**

**Pre-Conditions:**

Network product documentation containing information about supported TLS protocol and certificates is provided by the vendor.

A peer implementing the TLS protocol configured by the vendor shall be available.

The tester shall base the tests on the profile defined by 3GPP in Annex E of TS 33.310 [9] with the restriction that it shall be compliant with the profile given by HTTP/2 as defined in RFC 7540 [11].

**Execution Steps**

1. The tester shall check that compliance with the TLS profile can be inferred from detailed provisions in the network product documentation.

2. The tester shall establish a secure connection between the network product under test and the peer and verify that all TLS protocol versions and combinations of cryptographic algorithms that are mandated by the TLS profile are supported by the network product under test.

3. The tester shall try to establish a secure connection between the network product under test and the peer and verify that this is not possible when the peer only offers a feature, including protocol version and combination of cryptographic algorithms, that is forbidden by the TLS profile.

**Expected Results:**

- The network product under test and the peer establish TLS if the TLS profiles used by the peer are compliant with the profile requirements in TS 33.310 [9] Annex E and RFC 7540 [11].

- The network product under test and the peer fail to establish TLS if the TLS profiles used by the peer are forbidden in TS 33.310 [9] Annex E or RFC 7540 [11].

**Expected format of evidence:**

Provide evidence of the check of the product documentation in plain text. Save the logs and the communication flow in a .pcap file.

\*\*\*\* Next Changes\*\*\*\*

###### 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 [10], clause 13.4.1.1

*Requirement Description*:

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

- 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 verification is successful, the NF Service producer is expected to execute 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 optinally 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:**

- 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.

\*\*\*\* Next Changes\*\*\*\*

###### 4.2.2.2.3.2 Authorization token verification failure handling in different PLMNs

*Requirement Name*: Authorization token verification failure handling in different PLMNs

*Requirement Reference:* TS 33.501 [10], clause 13.4.1.2

*Requirement Description*:

The NF service producer is expected to check that the home PLMN ID of audience claim in the access token matches its own PLMN identity.

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

NOTE: The test case below only applies to the NFs which support identifying and understanding the producerPlmnId claim.

*Test Case*:

**Test Name:** TC\_AUTHORIZATION\_TOKEN\_VERIFICATION\_FAILURE\_DIFF\_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 a different PLMN fails.

**Procedure and execution steps:**

**Pre-Conditions:**

- Test environment with a NF service consumer and two SEPPs (one cSEPP, one pSEPP).

- The NF service consumer and SEPPs may be simulated.

- The network product under test has already mutually authenticated with the NF service consumer in a different PLMN via the SEPPs.

- 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.

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

**Execution Steps**

The network product under test receives the access token sent from the NF service consumer, verifies the access token in accordance with the execution steps in 4.2.2.1.2.1, with the following additional test cases:

Test Case 1: incorrect PLMN ID of the NF service producer in the access token

1) The test computes an access token correctly, except that the PLMN ID in the producerPlmnId claim of the access token is empty or different from the home PLMN ID of the network product under test, and then includes the access token in the NF Service Request sent from the NF service consumer to the network product under test through the SEPPs.

2) The network product under test receives the access token sent from the NF service consumer through the SEPPs, verifies that the PLMN ID in the producerPlmnId claim of the access token is different from its own home PLMN identity**.**

Test Case 2: absent PLMN ID of the NF service producer in the access token

1) The test computes an access token correctly, except that no producerPlmnId claim is included in the access token, and then includes the access token in the NF Service Request sent from the NF service consumer to the network product under test through the SEPPs.

2) The network product under test receives the access token sent from the NF service consumer through the SEPPs, verifies that the access token is not a token to be used by the NF service consumer in a different PLMN, based on the absence of PLMN ID of the NF service producer in the access token.

**Expected Results:**

For both test cases 1 and 2, 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].

**Expected format of evidence:**

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

\*\*\*\* Next Changes\*\*\*\*

###### 4.2.2.2.4.1 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

*Requirement Description*:

The verification of the Client credentials assertion is expected to 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 [x].

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

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 Changes\*\*\*\*