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

**e-meeting, 9th - 20th November 2020 revision of S3-203085**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *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:*** | F |  | | | | | ***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:*** | | According to TS 29.510, the producerPlmnId claim in an access token is a conditional claim, which shall be ignored if an NF service producer receiving this IE in an access token does not understand this IE.  The producerPlmnId claim is included by the NRF in an access token for an NF consumer requesting services across PLMN. When an NF producer does not understand this IE if present, it is not able to provide services to an NF consumer in another PLMN.  Therefore, it is proposed to add a note to restrict the test case in TS 33.117 clause 4.2.2.2.3.2 to the NFs supporting the producerPlmnId claim only, and correct the test case accordingly. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Added a note and corrected the test case of token verification failure handling in different PLMNs in TS 33.117 clause 4.2.2.2.3.2. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The network product under test may not pass the test based on the execution steps and expected results as currently specified. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.2.2.2.3.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

###### 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 shall 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 4.2.2.2.3.1, 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.

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