**3GPP TSG-SA3 Meeting #102e *draft\_S3-210101-r1***

**e-meeting, 18 - 29 January 2021, online**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.517** | **CR** | **0006** | **rev** | **1** | **Current version:** | **16.1.0** |  |
|  | | | | | | | | |
| *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:*** | Protection policies test case | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell, NTT Docomo, Huawei, HiSilicon | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | SCAS\_5G | | | | |  | ***Date:*** | | | 2021-01-29 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-16 |
|  | *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:*** | | Test case is only described for the case that both modification and protection policies are set to a different value, but this test should also cover the cases of one of the policies being different at peer SEPP and SEPP under test. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Update to allow all variants of different policies that do not match. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Testing may bring wrong result. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.2.2.6 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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

4.2.2.6 Correct handling of protection policy mismatch

*Requirement Name:* Correct handling of protection policy mismatch

*Requirement Reference*: TS 33.501 [3], clause 13.2.3.6

*Requirement Description*:

"When a SEPP receives a data-type encryption or modification policy on N32-c as specified in clause 13.2.2.2, it shall compare it to the one that has been manually configured for this specific roaming partner and IPX provider. If a mismatch occurs for one of the two policies, the SEPP shall perform one of the following actions, according to operator policy:

- Send the error message <TBD> to the peer SEPP

- Create a local warning"

*Threat References:* TR 33.926 [4], clause G.2.3.2, Incorrect handling for protection policy mismatch

*Test case*:

**Test Name:** TC\_SEPP\_POLICY\_MISMATCH

**Purpose:**

Verify that the SEPP under test is able to identify the mismatch between the protection policies manually configured for a specific roaming partner and IPX provider and the protection policies received on N32-c connection, and take action accordingly.

**Procedure and execution steps:**

**Pre-Conditions:**

- Test environment with a peer SEPP instance (as cSEPP), which may be simulated.

- The SEPP under test and the peer SEPP have mutually authenticated and already established N32-c connection.

- Exchanging of Data-type encryption policies and Modification policies is required to be performed between the SEPP under test and the peer SEPP.

- The tester shall have access to the interfaces of the SEPP under test and the peer SEPP.

- The tester has configured on the SEPP under test the policies for receiving messages, i.e. the Data-type encryption policy *d* of the peer SEPP and the Modification policy *m* for the peer SEPP and an IPX provider *I* used for the peer SEPP.

- The tester has configured on the peer SEPP the policies for sending, i.e. the peer SEPP's Data-type encryption policy *d'* and the Modification policy *m'* for the IPX provider *I* used for the peer SEPP.

- There are three cases to test:

a) the data encryption policies *d* and *d'* are identical, the modification policies *m* and *m'* are different

b) the data encryption policies *d* and *d'* are different, the modification policies *m* and *m'* are identical

c) both the data encryption policies *d* and *d'* and the modification policies *m* and *m'* are different

NOTE: The test case below only applies in case the SEPP under test supports manual configuration of the data encryption policy and/or modification policy for the specific roaming partner and IPX provider.

- The tester has configured on SEPP under test the action to be taken for policy mismatch, which is sending error message.

**Execution Steps:**

For each of the three cases above, the following is executed

1. The peer SEPP sends a Security Parameter Exchange Request message to the SEPP under test including the peer SEPP's Data-type encryption policy *d'*, and the Modification policy *m'*.

2. The SEPP under test stores the received Data-type encryption policy *d'* and the Modification policy *m'*, then compare them with the Data-type encryption policy *d* and the Modification policy *m* configured on it.

**Expected Results:**

- The SEPP under test sends an error signalling message to the peer SEPP on the N32-c connection or logs the error.

**Expected format of evidence:**

Logs and the communication flow saved in a .pcap file.

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