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

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

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.512** | **CR** | **<CR#>** | **rev** | **<Rev#>** | **Current version:** | **17.3.0** |  |
|  | | | | | | | | |
| *For* [***HE***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)***LP*** *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:*** | Clarification of | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Federal Office for Information Security (BSI) | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eSCAS\_5G | | | | |  | ***Date:*** | | | 2023-05-08 |
|  |  | | | |  | |  | | |  |
| ***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-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | The Expected Results of several test cases contain instructions for the tester. In general, Expected Results must not include tester instructions. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Moved the tester instructions from the Expected Results to the Execution Steps. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Test cases are not conformant with TR 33.916 | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.2.2.4.1, 4.2.2.4.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 1st CHANGE \*\*\*\*\*\*\*\*\*\*

##### 4.2.2.4.1 Bidding down prevention in Xn-handover

*Requirement Name*: Bidding down prevention in Xn-handovers

*Requirement Reference:* TS 33.501 [7], clause 6.7.3.1

*Requirement Description*: "In the Path-Switch message, the target gNB/ng-eNB shall send the UE's 5G security capabilities received from the source gNB/ng-eNB to the AMF. The AMF shall verify that the UE's 5G security capabilities received from the target gNB/ng-eNB are the same as the UE's 5G security capabilities that the AMF has locally stored. If there is a mismatch, the AMF shall send its locally stored 5G security capabilities of the UE to the target gNB/ng-eNB in the Path-Switch Acknowledge message. The AMF shall support logging capabilities for this event and may take additional measures, such as raising an alarm."

as specified in TS 33.501 [7], clause 6.7.3.1.

*Threat References*: TR 33.926 [6], clause K.2.4.1, Bidding down on Xn-Handover

*Test Case*:

**Test Name:** TC\_BIDDING\_DOWN\_XN\_AMF

**Purpose:**

Verify that bidding down is prevented by the AMF under test in Xn handovers.

**Pre-Conditions:**

Test environment with (source and target) gNBs may be simulated.

The AMF under test is configured with the UE’s security context for the UE.

The AMF under test is configured to log UE security capability mismatch.

**Execution Steps**

1) The tester sends 5G security capabilities for the UE, different from the ones stored in the AMF, to the AMF under test using a Path-Switch message.

2) The tester captures the Path-Switch Acknowledge message sent by AMF under test to the target gNB.

3) The tester examines the AMF log regarding the capability mismatch.

**Expected Results:**

The Path-Switch Acknowledge message sent by AMF under test to the target gNB includes the locally stored 5G security capabilities in the AMF under test for that UE.

Thelog entry shows that the capability mismatch is logged.

**Expected format of evidence**

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

\*\*\*\*\*\*\*\*\*\* END OF 1st CHANGE \*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\* START OF 2nd CHANGE \*\*\*\*\*\*\*\*\*\*

##### 4.2.2.4.2 NAS protection algorithm selection in AMF change

*Requirement Name*: NAS protection algorithm selection in AMF change

*Requirement Reference:* TS 33.501 [7], clause 6.7.1.2

*Requirement Description*: "If the change of the AMF at N2-Handover or mobility registration update results in the change of algorithm to be used for establishing NAS security, the target AMF shall indicate the selected algorithm to the UE as defined in Clause 6.9.2.3.3 for N2-Handover (i.e., using NAS Container) and Clause 6.9.3 for mobility registration update (i.e., using NAS SMC). The AMF shall select the NAS algorithm which has the highest priority according to the ordered lists (see sub-clause 6.7.1.1 of the present document)."

as specified in TS 33.501 [7], clause 6.7.1.2.

*Threat References*: TR 33.926 [6], clause K.2.4.2, NAS integrity protection algorithm selection in AMF change

*Test Case*:

**Test Name:** TC\_NAS\_ALG\_AMF\_CHANGE \_AMF

**Purpose:**

Verify that NAS protection algorithms are selected correctly.

**Pre-Conditions:**

Test environment with source gNB, target gNB and source AMF. Source and target gNBs and source AMF may be simulated.

**Execution Steps**

Test case 1: N2-Handover

1) The AMF under test receives the UE security capabilities and the NAS algorithms used by the source AMF from the source AMF. The AMF under test selects the NAS algorithms which have the highest priority according to the ordered lists. The lists are configured such that the algorithms selected by the AMF under test are different from the ones received from the source AMF.

2) The tester captures the NGAP HANDOVER REQUEST message containing the NASC IE (NAS Container) sent by the AMF under test to the gNB.

Test case 2: Mobility registration update

The AMF under test receives the UE security capabilities and the NAS algorithms used by the source AMF from the source AMF. The AMF under test selects the NAS algorithms which have the highest priority according to the ordered lists. The lists are configured such that the algorithms selected by the AMF under test are different from the ones received from the source AMF.

**Expected Results:**

For Test case 1, the NASC IE of the captured NGAP HANDOVER REQUEST message sent by the AMF under test to the gNB includes the chosen algorithm.

For Test case 2, the AMF under test initiates a NAS security mode command procedure and includes the chosen algorithms.

**Expected format of evidence:**

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

\*\*\*\*\*\*\*\*\*\* END OF 2ndCHANGE \*\*\*\*\*\*\*\*\*\*