**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* [***HELP***](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:*** | New SCAS test on valid UE security capability encoding while AS security establishment | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Federal Office for Information Security (BSI) | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | eSCAS\_5G | | | | |  | ***Date:*** | | | 2023-05-08 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | B |  | | | | | ***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:*** | | TS 33.501 states that the UE 5G security capabilities shall be sent to the gNB/ng-eNB by the AMF to establish the AS security context. TR 33.926 highlights the risk of invalid encoding of UE security capabilities on the NG interface. Currently there is no SCAS test case available yet that tests the correct behaviour of the AMF for the incorporation of the UE 5G security capabilities in the NGAP Context Setup Request. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Added test case to verify the correct incorporation of UE 5G security capabilities in the NGAP Context Setup Request. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | In the worst case, the AMF implements an incorrect encoding function for the security algorithms used for AS security, resulting in incorrectly negotiated security algorithms on the air interface. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | | **X** |  | Other core specifications | | | | TR 33.926 CR 0065.. | | |
| ***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 \*\*\*\*\*\*\*\*\*\*

4.2.2.6.X Correct transfer of UE security capabilities in AS security establishment

*Requirement Name:* Correct transfer of UE security capabilities in AS security establishment

*Requirement Reference:* TS 33.501 [2], clause 6.7.3.0.

*Requirement Description*: “When AS security context is to be established in the gNB/ng-eNB, the AMF shall send the UE 5G security capabilities to the gNB/ng-eNB.” as specified in TS 33.501 [2], clause 6.7.3.0

*Threat References:* TR 33.926 [4], clause K.2.6.2 Invalid encoding of UE security capabilities on the NG interface

*Test Case:*

**Test Name:** TC\_UE\_SEC\_CAPS\_AS\_CONTEXT\_SETUP

**Procedure and execution steps:**

**Purpose:**

Verify that the UE security capabilities sent by the UE in the initial NAS registration request are the same UE security capabilities sent in the NGAP Context Setup Request message to establish AS security.

**Pre-Conditions:**

- Test environment with UE, gNodeB, AUSF and UDM. All of them may be simulated.

- The tester configures valid UE 5G security capabilities.

- The tester captures the NGAP traffic between the gNodeB and AMF on the N2 interface.

**Execution Steps:**

The tester triggers the initial NAS registration procedure with valid UE security capabilities.

**Expected Results:**

The NGAP Context Setup Request contains the same UE 5G security capabilities as sent in the initial NAS registration request.

**Expected format of evidence:**

- List of configured UE 5G security capabilities

- Network trace (\*.pcap file) containing the captured messages.

\*\*\*\*\*\*\*\*\*\* END OF CHANGE \*\*\*\*\*\*\*\*\*\*