**3GPP TSG-SA WG3 Meeting #98e *S3-200201***

**e-meeting, 2-6 March 2020**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v11.2* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.512** | **CR** | **005** | **rev** | **-** | **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 | **X** | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | New test case on NAS integrity protection | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, Hisilicon | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | SCAS\_5G | | | | |  | | ***Date:*** | | 2020-01-09 |
|  |  | | | |  | | |  | |  |
| ***Category:*** | **B** |  | | | | | | ***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:*** | | 33.926 has defined threat “NAS integrity selection and use” which states “if NAS does not use the highest priority algorithm, NAS layer risks being exposed and/or modified or being exposed to denial of service”.  No test case is available in current 33.512 referencing this threat. This contribution proposes to add the test case for the threat. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Adding a new test case on NAS integrity protection. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Registration of UE will never be successful and hence UE is denied service. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.2.2.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\*\*\* START OF 1st CHANGES \*\*\*

##### 4.2.2.3.X NAS integrity algorithm selection and use

*Requirement Name*: NAS integrity algorithm selection and use

*Requirement Reference:* TS 33.501 [2], clause 6.7.1

*Requirement Description*: "The AMF shall then initiate a NAS security mode command procedure, and include the chosen algorithm and UE security capabilities (to detect modification of the UE security capabilities by an attacker) in the message to the UE (see sub-clause 6.7.2 of the present document). The AMF shall select the NAS algorithm which have the highest priority according to the ordered lists." as specified in TS 33.501 [2], clause 5.5.2.

*Threat References*: TR 33.926 [6], clause K.2.3.2, NAS integrity selection and use

*Test Case:*

**Test Name:** TC\_NAS\_INT\_SELECTION\_USE\_AMF

**Purpose:**

Verify that the AMF selects the NAS integrity algorithm which has the highest priority according to the ordered list of supported integrity algorithms and the 5G security capabilities supported by the UE.

Verify that the selected NAS security algorithm is being used.

**Pre-Conditions:**

Test environment with a UE containing its 5G security capabilities, AUSF and UDM. The UE, AUSF and UDM may be simulated.

**Th**e list of ordered NAS integrity algorithms are configured on the AMF under test.

**Execution Steps:**

1) The UE sends a Registration Request with Initial Registration typeto the AMF unders test.2) The tester filters the Security Mode Command and Security Mode Complete messages.

3) The tester examines the selected integrity algorithm in the SMC against the list of ordered NAS integrity algorithm, and the MAC verification of the Security Mode Complete at the AMF under test..

**Expected Results:**

The selected integrity algorithm has the highest priority according to the list of ordered NAS integrity algorithm and is contained in the UE 5G security capabilities.

The MAC verification of the Security Mode Complete message is successful.

**Expected format of evidence:**

Logs and communication flow saved in a .pcap file.

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