**3GPP TSG-SA3 Meeting #104-e *S3-212456***

**e-meeting, 16 - 27 August 2021**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.512** | **CR** | **0012** | **rev** | **1** | **Current version:** | **17.0.0** |  |
|  | | | | | | | | |
| *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:*** | AMF – NAS NULL integrity protection clarifications | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Keysight Technologies | | | | | | | | | |
| ***Source to TSG:*** |  | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | SCAS\_5G | | | | |  | ***Date:*** | | | 2021-07-16 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | A |  | | | | | ***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 preconditions and execution steps for the test case, do not cover the *Requirement Reference*. According requirement description and threat references, the test case in 4.2.2.3.2 is to verify that NIA0 can be disabled in AMF (if not required by the regulation to establish emergency calls).   1. The test case does not state that NIA0 must be disabled 2. The flow of the test case does not force the AMF to use NIA0, as the UE is not supporting NIA0 only | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Add step in pre-conditions to disable NIA0 in AMF  Divide test case in two, creating a new one to:   1. With an UE supporting NIA0, it is checked that AMF does not progress with the connection. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Incorrect specification in the test case. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.2.2.3.2 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 Change \*\*\*

##### 4.2.2.3.2 NAS NULL integrity protection

*Requirement Name*: NAS NULL integrity protection

*Requirement Reference:* TS 33.501 [2], clause 5.5.2

*Requirement Description*: "NIA0 shall be disabled in AMF in the deployments where support of unauthenticated emergency session is not a regulatory requirement." as specified in TS 33.501 [2], clause 5.5.2

*Threat References*: TR 33.926 [6], clause K.2.3.3, NAS NULL integrity protection

*Test Case:*

**Test Name:** TC\_NAS\_NULL\_INT\_AMF

**Purpose:**

Verify that NAS NULL integrity protection algorithm is used correctly.

**Pre-Conditions:**

Test environment with a UE. The UE may be simulated.

The vendor shall provide documentation describing how NIA0 is disabled and enabled in the AMF.

NIA0 is disabled in AMF for emergency calls.

**Execution Steps**

Test case A:

1. The UE only supports NIA0 as security capability.

2. The UE establish an unauthenticated emergency session

Test case B:

1. The UE support NIA0 and other integrity algorithms (NIA1, NIA2 and/or NIA3) as security capabilities.
2. The UE establish an emergency session.
3. The AMF derives the KAMF and NAS signalling keys after successful authentication of the UE.

4. The AMF sends the NAS Security Mode Command message to the UE containing the selected NAS algorithms.

**Expected Results:**

For Test case A: the session is rejected

For Test case B: the integrity algorithm selected by the AMF in NAS SMC message is different from NIA0 and

the NAS Security Mode Command message is integrity protected by the AMF.

**Expected format of evidence:**

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

\*\*\* End of Change \*\*\*