**3GPP TSG-SA3 Meeting #112S3-253025**

**Goteborg, Sweden, 14 - 18 August 2023**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.512** | **CR** | **0048** | **rev** | **2** | **Current version:** | **19.0.0** |  |
|  | | | | | | | | |
| *For* ***HE******LP*** *on using this form: comprehensive instructions can be found at  http://www.3gpp.org/Change-Requests.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Add test cases to ensure protection of initial NAS message in registration procedure | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | BSI (DE), Montsecure | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | SCAS\_5GA | | | | |  | ***Date:*** | | | 2025-08-11 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-20 |
|  | *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. | | | | | | | | *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 requirement of the initial NAS message retransmission was not yet covered by any AMF SCAS test case. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Adds a test case which verifies that the AMF requests and uses the retransmitted (and protected) initial NAS message. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | If the AMF does not use the retransmitted initial NAS message and simply proceeds with the registration procedure based on the original Registration Request, then the AMF could be vulnerable to Bidding Down attacks. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.2.2.3.X | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 \*\*\*\*\*\*\*\*\*\*

4.2.2.3.X NAS Protection of initial NAS message

*Requirement Name*: Protection of initial NAS message

*Requirement Reference:* TS 33.501 [2], clause 6.4.6

*Requirement Description*: The UE sends the NAS Security Mode Complete message to the network in response to a NAS Security Mode Command message. The NAS Security Mode Complete message is ciphered and integrity protected. Furthermore the NAS Security Mode Complete message includes the complete initial NAS message in a NAS Container if either requested by the AMF or the UE sent the initial NAS message unprotected. The AMF uses the complete initial NAS message that is in the NAS container as the message to respond to, as stated in TS 33.501, clause 6.4.6, step 4.

*Threat References*: TR 33.926 [6], clause K.2.3.1, Bidding Down

*Test Case:*

**Test Name:** TC\_AMF\_NAS\_INITIAL\_MESSAGE\_RETRANSMISSION

**Purpose:**

Verify that the AMF requests the security protected retransmission of the initial NAS message from the UE in the NAS Security Mode Complete message and does proceed with the registration procedure based on the retransmitted,protected NAS Registration Request message.

**Pre-Conditions:**

- AMF network product is connected in emulated/real network environment.

- UE does not have a 5G NAS security context

- The Tester is able to intercept and modify the NAS signalling packets sent between UE and AMF over the N1 interface.

**Execution Steps:**1. The tester triggers the UE to conduct an initial registration procedure.

2. The tester intercepts the unprotected Registration Request message sent from the UE to the AMF and modifies either the Requested NSSAI or Registration Type.

3. The AMF initiates the Security Mode Command Procedure after receiving the unprotected Registration Request (initial NAS message) from the UE. The AMF sets the RINMR bit (Retransmission of the initial NAS message requested) to 1 in the Security Mode Command message sent to the UE.

4. The UE sends a Security Mode Complete message with a retransmitted and protected Registration Request message to the AMF.

5. The tester observers the AMFs consecutive behaviour.

**Expected Results:**

The RINMR bit is set to 1 in the Security Mode Command message sent from the AMF to the UE.

The AMFs consecutive messages (e.g. NSSAI modified: Nnssf\_NSSelection\_Get or Nudm\_SDM\_Get; Registration Type modified: Nudm\_UECM\_Registration; for Emergency Registration: Nsmf\_PDUSession\_CreateSMContext) are based on the contents of the retransmitted and protected Registration Request message of the UE.

**Expected format of evidence:**

Evidence suitable for the interface, e.g., packet captures of the N1 interface or application log files of the AMF containing the operational results.

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