**3GPP TSG-SA3 Meeting #123S3-252974**

**Goteborg, Sweden, 25 - 29 August 2025**

|  |
| --- |
| *CR-Form-v12.1* |
| **CHANGE REQUEST** |
|  |
|  | **33.117** | **CR** | **0223** | **rev** | **1** | **Current version:** | [**19.2.0**](https://www.3gpp.org/ftp/Specs/archive/33_series/33.117/33117-j20.zip) |  |
|  |
| *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 |  |

|  |
| --- |
|  |
| ***Title:***  | Firmware/BIOS access to Privileged Users |
|  |  |
| ***Source to WG:*** | DoT, India |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** |  SCAS\_5G\_Maint  |  | ***Date:*** | 2025-08-26 |
|  |  |  |  |  |
| ***Category:*** | F |  | ***Release:*** | Rel-19 |
|  | *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 canbe 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:*** | Access to firmware should be given to the privileged users only post succesful authetication. |
|  |  |
| ***Summary of change:*** | In the current version of specification, access to firmware/boatloader is given after successful authentication. In worst case, this might be used by a ‘normal user’. From security perspective, the access to write/modify should be given to privilged user only upon successful authentication. |
|  |  |
| ***Consequences if not approved:*** | 3GPP specification is ambigious which may lead to security consequences, if not addressed as proposed. |
|  |  |
| ***Clauses affected:*** | 4.2.3.3.2 |
|  |  |
|  | **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:*** | Initial draft and presentation |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

##### 4.2.3.3.2 Boot from intended memory devices only

*Requirement name*: Boot from intended memory devices only

*Requirement reference*: In accordance with industry best practice

*Requirement Description*:

The network product can boot only from the memory devices intended for this purpose.

*Test case:*

**Test Name:** TC\_BOOT\_INT\_MEM\_1

**Purpose:**

Verify that the network product can only boot from memory devices intended for this purpose (e.g. not from external memory like USB key).

**Procedure and execution steps:**

**Pre-Conditions:**

A document which contains information regarding the firmware access mechanism supported by the product and about the memory devices from which the network product can boot.

**Execution Steps**

1. The tester verifies that the network product is configured to boot from memory devices declared in the network product document only.

2. The tester verifies that the network product does not boot from any undeclared memory device by preparing a bootable medium for every class of bootable memory device (e.g. CD, USB key, network boot) present in and accessible at the network product and trying to boot from this medium.

3. The tester verifies that attempts to access and modify the firmware of the network product are permitted following successful authentication but prevented without prior successful authentication.

4. The tester verifies that the boot sources can be modified only by administrator/root user.

**Expected Results:**

The network product cannot boot from a memory device that is not configured in its firmware, and access to the firmware is only possible with the correct authentication.

**Expected format of evidence:**

Screenshot of the actual boot device configuration of the network product and firmware access mechanism/authentication.

Textual description of the attempts of booting from prepared memory devices.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 1st Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*