**3GPP TSG-SA3 Meeting #114e *ad-hoc S3-240039-r1***

Electronic meeting, online, 22 - 26 January 2024

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.117** | **CR** | **0154** | **rev** | **1** | **Current version:** | **18.2.0** |  |
|  | | | | | | | | |
| *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 |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | Update to the clause 4.2.3.4.1.1 - System functions shall not be used without successful authentication and authorization | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Samsung | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | SCAS | | | | |  | ***Date:*** | | | 2023-12-09 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | F |  | | | | | ***Release:*** | | | Rel-18 |
|  | *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:*** | | Execution Steps of clause 4.2.3.4.1.1 states the following:  The accredited evaluator's test lab is required to execute the following steps:  1. The tester verifies, based on his/her own experience, that the list is adequate.  This is subjective, what constitutes an "adequate list” is not clear in the specification Therefore, it is recommended to provide further clarification on the adequate list. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Based on the pre-conditions specified i.e., “The manufacturer shall supply the list of system functions which include network services, local access via a management console, local usage of operating system and applications.”, the tester should have the adequate list of system functions to perform the further verifications. Without an adequate list tester will not be able to perform the test case. Hence, step 1 need not be performed by the tester as the understanding is, in order to perform the test case tester should be in possession of adequate list of system functions. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Unclear test cases in TS 33.117. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.2.3.4.1.1 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 \*\*\*\*\*\*\*\*\*\*\*\*\*

4.2.3.4.1.1 Successful authentication and authorization of system functions

*Requirement Name:* Authentication and authorization forSystem functions

*Requirement Reference: In accordance with industry best practice*

*Requirement Description*:

The usage of a system function without successful authentication on basis of the user identity and at least one authentication attribute (e.g. password, certificate) shall be prevented. System functions comprise, for example network services (like SSH, SFTP, Web services), local access via a management console, local usage of operating system and applications. This requirement shall also be applied to accounts that are only used for communication between systems. An exception to the authentication and authorization requirement are functions for public use such as those for a Web server on the Internet, via which information is made available to the public.

*Threat References: TR 33.926 [4]Test case*:

**Test Name**: TC\_SYS\_FUN\_USAGE

**Purpose:**

To ensure that system functions shall not be used without successful authentication and authorization.

**Procedure and execution steps:**

**Pre-Conditions:**

1. The vendor shall supply the list of system functions which include network services, local access via a management console, local usage of operating system and applications.

2. The vendor shall supply the list of access entries for system functions.

**Execution Steps**

The tester is required to execute the following steps:

1. The tester verifies that the access entries to use system functions, which are listed by the vendor, require successful authentication on basis of the user name and at least one authentication attribute. The tester also verifies that the access entries to use system functions require authorization via an access control mechanism (e.g. Discretionary access control/Ownership/Capabilities or Mandatory access control). This applies to both system functions that are locally accessible and those that are remotely accessible via a network interface.

**Expected Results:**

1. The network product does not allow access to any system function provided by the vendor without a successful user authentication and authorization.

**Expected format of evidence:**

A testing report provided by the testing agency which will consist of the following information:

- Description of executed tests and commands

- Relevant output (e.g. Screenshot)

- Test result (Passed or not)

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