**3GPP TSG-SA3 Meeting #114e *ad-hoc draft\_S3-240051-r1***

Electronic meeting, online, 22 - 26 January 2024

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.117** | **CR** | **0166** | **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:*** | Addressing subjective comments from GSMA and comments in BSI AIS-N2 to 4.3.2.1 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei; HiSilicon | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | SCAS\_5G\_Ph3 | | | | |  | ***Date:*** | | | 2024-01-22 |
|  |  | | | |  | |  | | |  |
| ***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:*** | | GSMA commentted that there are some subjective descriptions in the test case, and recommended to remove the subjectivity.  The change is proposed to update the expected format of evidence from clause 2.3.1.29 of AIS\_N2 document which is for NESAS CCS\_GI. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Remove the subjectivity words.  Update the Expected format of evidence. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Misalignement with NESAS documents | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.3.2.1 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

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

#### 4.3.2.1 No unnecessary or insecure services / protocols

*Requirement Name*: No unnecessary or insecure services / protocols

*Requirement Reference:* In accordance with industry best practice

*Requirement Description*:

The network product shall only run protocol handlers and services which are needed for its operation, and which do not have any known security vulnerabilities. In particular, by default the following services shall be initially configured to be disabled on the network product by the vendor except if services are needed during deployment. In that case those services shall be disabled according to vendor’s instructions after deployment is done. Disabled protocols can still be enabled for other reasons by the network operators, e.g. remote diagnostics.

- FTP

- TFTP

- Telnet

- rlogin, RCP, RSH

- HTTP

- SNMPv1 and v2

- SSHv1

- TCP/UDP Small Servers (Echo, Chargen, Discard and Daytime)

- Finger

- BOOTP server

- Discovery protocols (CDP, LLDP)

- IP Identification Service (Identd)

- PAD

- MOP

NOTE 1: As an alternative to disabling the HTTP service, it is also possible for this service to remain active for reasons of user friendliness. In this case, however, queries to the web service are not answered directly on this port but from a redirected to HTTPS service.

Note 2: Full documentation of required protocols and services of the network product and their purpose needs to be provided by the vendor as prerequisite for the test case.

*Threat References:* TR 33.926 [4]

*Test Case*:

**Test Name**: TC\_NO\_UNNECESSARY\_SERVICE

**Purpose:**

To ensure that on all network interfaces, there are no unsecure services or protocols that might be running.

**Procedure and execution steps:**

**Pre-Conditions:**

A list of all required network protocols and services containing at least the following information shall be included in the documentation accompanying the Network Product:

- protocol handlers and services needed for the operation of network product;

- their open ports and associated services;

- and a description of their purposes.

The tool used shall be capable to detect and identify the protocol handlers and running services in the system.

**Execution Steps**

The tester is required to execute the following steps:

1. Verification of the compliance to the prerequisites:

a. Verification that the list of available network services and protocol handlers is available in the documentation of the Network Product.

b. Validation that all entries in the list are necessary for the operation of the Network Product class.

2. Identification of the network services and protocol handlers by means of tools or any other testing means.

3. Validation that there are no entries in the list of network services and handlers apart from the ones that have been mentioned for the operation of the Network Product in the attached documentation.

4. The tester shall reboot the network product and re-execute execution steps 2 and 3 without further configuration.

**Expected Results:**

The report will contain:

- The names and version of the tool(s) used.

- Information of all the protocol handlers and services running in the network product.

Result will show:

- There are no unnecessary services running in the network product except for the ones which are necessary for its operation.

- Any undocumented services running on the network product should be highlighted and brought out in the report.

- The network product behaves the same after reboot as before.

**Expected format of evidence:**

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

- The used tool(s) name and version information

- Settings and configurations, and commands used (if applicable)

- The output pertaining to the test case performed and

- The test results i.e. services existing or not existing in the Network Product

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