**3GPP TSG-SA3 Meeting #116 *S3-242398-r1\_was\_S3-242189***

Jeju, South Korea, 20 – 24 May 2024

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.527** | **CR** | **0002** | **rev** | **1** | **Current version:** | **18.0.1** |  |
|  | | | | | | | | |
| *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:*** | Revision on the TS 33.527 according to the scope | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Huawei, HiSilicon | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | VNP\_SECAM\_SCAS | | | | |  | ***Date:*** | | | 2023-05-09 |
|  |  | | | |  | |  | | |  |
| ***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:*** | | The expected result does not belong to the VNF. Hence, the non-VNF related party shall be removed. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Clarify the unclear test cases. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Some of the content is out of the scope of VNF test. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 4.2.3.3.5.2, 4.2.7.2, 4.2.7.3, | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\*\*\* BEGIN of the first CHANGE \*\*\*

##### 4.2.3.3.5 Virtualized Network product software package integrity

##### 4.2.3.3.5.1 Overview

All text from TS 33.117 [1], clause 4.2.3.3.5 applies to GVNP of type 1.

In addition, VNF package and VNF image integrity shall be validated when on board, and VNF image integrity shall be validated when in instantiated. The detailed potential security requirements and related test cases are as following.

###### 4.2.3.3.5.2 VNF package and VNF image integrity

*Requirement Name*: VNF package and VNF image integrity

*Requirement Description*:

1) VNF package and image shall contain integrity validation value (e.g. MAC).

2) VNF package shall be integrity protected during on boarding.

*Threat Reference*: Clause 5.3.2.5.1 of the TR 33.927[2], "Software Tampering ";

*Test case*:

**Test Name:** TC\_VNF PACKAGE AND IMAGE\_ INTEGRITY

**Purpose:**

1. To test whether the VNF package has been integrity protected or not.

2. To test whether the VNF image has been integrity protected or not.**Procedure and execution steps:**

**Pre-Condition:**

- The virtualized network product document describes information that the VNF package and VNF images is integrity protected.

- A valid VNF package and a not-valid VNF package (e.g. a tampered image in VNF package) are available.

- A valid VNF image (i.e. a correct HASH value is attached) and a not-valid VNF image (i.e. an incorrect HASH value is attached, e.g. the VNF image can be tampered when the VNF image is sent from the NFVO to the VIM or when the VNF image is stored in the image repository) are available in the image repository of VIM.

- There are NFVO and VIM, or simulated NFVO and VIM. The certificate or the public key which is used to verify the digital signature of VNF package and image has been pre-configured in the NFVO.

NOTE: The NFVO and VIM may be renamed or collocated with other components in the simulated environment based on the various deployment options.

**Execution Steps**

Execute the following steps:

1. Review the documentation provided by the vendor describing how VNF package integrity is verified;

2. During VNF package on boarding, the tester uploads a valid VNF package into a NFVO. The NFVO verifies the integrity of the VNF package by validating the digital signature of the VNF package using the pre-configured certificate according to the documentation;

3. During VNF package on boarding, the tester uploads a not-valid VNF package into a NFVO. The NFVO validates the digital signature of the VNF package using the pre-configured certificate;

4. During VNF instantiation, the VIM selects a VNF image with a correct integrity protection value from the image repository to instantiate the VNF image.

5. During VNF instantiation, the VIM selects a VNF image with an incorrect integrity protection value from the image repository to instantiate the VNF image.

**Expected Results:**

1. The VNF package is successfully verified;

2. The verification of not-valid VNF package is failure. ;

3. The VNF image with a correct integrity protection value is successfully verified;

4. The verification of VNF image with an incorrect integrity protection value is failure. .

**Expected format of evidence:**

Snapshots containing the result of the VNF package on boarding and the VNF image instantiation.

\*\*\* BEGIN of the second CHANGE \*\*\*

#### 4.2.7.2 Security functional requirements on executive environment provision

*Requirement Name*: secure executive environment provision

*Requirement Description*:

The VNF shall support to compare the owned resource state with the parsed resource state from VNFD (VNF Description) by the VNFM. The VNF can query the parsed resource state by the VNFM from the OAM. The VNF shall send an alarm to the OAM if the two resource states are inconsistent. This comparing process can be triggered periodically by the VNF, or the administrator can manually trigger the VNF to perform the comparing process.

*Threat Reference*: Threats on interface between 3GPP VNF and virtualisation layer, in clause 5.3.2.3 of TR 33.927 [3].

*Test case*:

**Test Name:** TC\_SECURE EXECUTIVE ENVIRONMENT PROVISION

**Purpose:**

1. To test whether the VNF compares the owned resource state (e.g. scale) with the parsed resource state.

2. To test whether the VNF send an alarm to the OAM if the two resource states are inconsistent.

**Procedure and execution steps:**

**Pre-Condition:**

There are a VNF, a virtualization layer (or simulated virtualization layer), an OAM, a VNFM, a VIM (or simulated OAM, VNFM, VIM) on the test environment.

NOTE: This test case is applicable only for the scenario that the virtualization layer is able to change the resource state of VNF.

**Execution Steps**

**Execute the following steps:**

1. The tester utilizes the virtualization layer to change the resource state of VNF (e.g. change vCPU size of the VNF).

2. The tester uses the VNF to query the parsed resource state from the OAM.

3. The tester uses the OAM to query the parsed resource state of the VNF from the VNFM and send the received resource state to the VNF.

4. The tester checks whether the VNF sends an alarm to the OAM when the VNF receives the parsed resource state from the OAM and finds that the owned resource state and the parsed resource state are inconsistent.

**Expected Results:**

1. The VNF send an alarm to the OAM when the VNF receives the parsed resource state from the OAM and find that the owned resource state and the parsed resource state are inconsistent.

**Expected format of evidence:**

1. Screenshot contains the alarm on the OAM.

\*\*\* BEGIN of the third CHANGE \*\*\*

#### 4.2.7.3 Instantiating VNF from trusted VNF image

*Requirement Name*: Instantiating VNF from trusted VNF image

*Requirement Description*:

A VNF shall be initiated from trusted images in a VNF package. The VNF image(s) shall be signed by an authorized party. The authorized party is trusted by the operators.

*Threat Reference*: TR 33.926 [7], Clause5.3.4.1, "Software Tampering ";

*Test case*:

**Test Name:** TC\_INSTANTIATING VNF \_ TRUSTED IMAGE

**Purpose:**

To test whether the instantiating VNF from trusted VNF image.

**Procedure and execution steps:**

**Pre-Condition:**

- The virtualized network product document describes information that the VNF images is integrity protected.

- One VNF package included two trusted VNF images and the VNF package carries a correct digital signature of the VNF package.

- Another VNF package included untrusted VNF image which carry wrong digital signature of VNF image and the VNF package carries a correct digital signature of the VNF package.

- There are a NFVO, or a simulated NFVO. A certificate or public key which is used to verify the digital signature of VNF image has been pre-configured in the NFVO. This certificate is trusted by the operator. It means the digital signature of the VNF image is successfully verified by using the public key in the certificate trusted by the operator

NOTE: The NFVO and VIM may be renamed or collocated with other components in the simulated environment based on the various deployment options.

**Execution Steps:**

**Execute the following steps:**

1. Review the documentation provided by the vendor describing how digital signature of the VNF image is verified;

2. The tester uploads a VNF package included two trusted VNF images into a NFVO. The NFVO verifies the VNF images by validating each digital signature of the VNF image using the pre-configured certificate or the public key according to the documentation;

3. The tester uploads another VNF package included un-trusted VNF image into NFVO. The NFVO verifies the VNF image(s) by validating each digital signature of the VNF image using the pre-configured certificate or the public key according to the documentation.

Note: The digital signature validation of the image is also described in clause 4.2.3.3.5.2 VNF package and VNF image integrity, but the two test cases have the different test purposes. This test case focuses on VNF image credibility, while clause 4.2.3.3.5.2 is concerned with VNF image integrity.

**Expected Results:**

1. In the step 2, the signatures of the VNF images are successfully validated;

2. In the step 3, the signature of the un-trusted VNF image is failed to be validated;

**Expected format of evidence:**

Snapshots containing the result of the VNF package on boarding.

\*\*\* END CHANGES \*\*\*