**3GPP TSG-SA3 Meeting #102bis-eS3-210839**

**e-meeting, 01 - 05 March 2021**

**Source:** **Nokia****, Nokia Shanghai Bell**

**Title:** **Update on Ki#27 Image Snapshot and VNF Mobility.**

**Document for: Approval**

**Agenda Item: 5.04**

# 1 Decision/action requested

***The contribution proposes a solution to protect the privacy of the UE identity.***

# 2 References

[1] 3GPP TR 33.848:” Study on Study on Security Impacts of Virtualisation”

# 3 Rationale

In the last SA3 meeting Key Issue 27 related to Image Snapshot and VNF Mobility has been added to [1]. This pCR adds one more level of detail and proposes specific points, which should be addressed during the study and resolution of this Key Issue.

# 4 Detailed proposal

It is proposed that SA3 agree the below pCR for inclusion in the TR [1].

**\*\*\*\* START OF CHANGES \*\*\*\***

## 5.28 Key Issue 27: Image Snapshot and VNF Mobility

### 5.28.1 Key issue detail

Starting, checkpointing, restarting or migration of virtual workloads are fundamental operational tasks in a cloud environment.

Potential security risks are related to a migration of a virtual workload from a secure environment to a less secure environment or to attacking data while on rest (e.g., as part of a snapshot file) or while in transit (e.g., during live migration).

In general, these threats can be handled using appropriate mechanism, i.e., ensuring that source and target environment are secure, that snapshot files are protected, that the mechanism used during migration is secure, or that the underlying operational processes are secure.

This approach, however, assumes that the cloud environment is trustworthy, i.e., the operator, who deploys VNFs in a cloud environment trusts that the cloud operator has secure mechanisms and processes in place with respect to lifecycle management of virtual workloads.

If, however, a cloud environment is regarded as potentially malicious, things are different. In such a case typically remote attestation techniques can be used to verify that a VNF is running in a trustworthy execution environment. Such a setup makes migration of VNFs more complicated, since the attestation is valid only for the source environment and not for the target environment, i.e., some form of re-attestation needs to be executed for the target environment. Furthermore, data (including security credentials) used by the VNF in the source environment are protected ("sealed") so that they are readable and usable only in the source environment. Thus, the migration needs to include a mechanism, which allows unsealing (on the source environment) and sealing (on the target environment) of the data to be transferred (i.e., the persistent state) in a secure way without opening the possibility of running several copies of a VNF with different persistent state (so called forking or roll-back attacks).

### 5.28.2 Security threats

An attacker might initiate migration of a VNF from a trustworthy execution environment into a non-trustworthy environment. The non-trustworthy environment might be under the control of the attacker and might be used for direct attacks against a VNF.

An attacker might attack VNF data, while they are at rest as part of a VNF snapshot or in transition during live migration.

An attacker, who has control over the deployment of VNFs (i.e., the attacker can start, pause, restart, or migrate a VNF), could run several instances of the same VNF with different persistent state. While not trivial, this kind of fork or roll-back attacks can be used to initiate complex attacks against the overall integrity of the 5G system.

### 5.28.3 Potential security requirements

Migration of a VNF from a trustworthy environment to an untrustworthy environment shall not be possible, e.g., the access to virtualization management operations, like starting, stopping, pausing, restarting, live migration of a VNF, shall be subject to authentication and authorization.

VNF data shall be confidentiality protected when stored as part of a VNF snapshot or during migration of the VNF to another execution environment.

Where VNF sub-components are in different trust domains, the snapshot shall maintain security and isolation requirements for each trust domain within the snapshot of the VNF.

The ability of a VNF to verify the trustworthiness of another VNF (as described in KI#13) shall not be impeded by pausing, stopping, restarting, or migrating a VNF.

All VNF Snapshot and VNF mobility operations shall preserve the persistent state of the VNF in order to prevent forking or roll-back attacks.

It shall be possible to protect and prevent sensitive VNF or VNF-components from being subject to snapshot or migration without explicit authorization.

All system snapshots events shall be subject to secure logging.

Snapshots shall be securely deleted, once they are no longer required or after a specified maximum snapshot age has been reached.

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