**3GPP TSG-SA3 Meeting #107-e *S3-221115***

e-meeting, 16 - 20, May 2022

**Source: MITRE**

**Title: KI#27 update - requirements**

**Document for: Approval**

**Agenda Item: 5.2**

# 1 Decision/action requested

***This pCR proposes to update the security requirements for KI #27***

# 2 References

[1] 3GPP TR 33.848 v0.11.0 "Study on Security Impacts of Virtualisation"

# 3 Rationale

KI #27 is concerned with stored secrets (e.g., hardcoded passwords, keys) in NF container image and/or VNF package.

Potential security requirements within KI #27 suggests that *The VNF images shall not be packaged with embedded secrets* *such as passwords or credentials, or any other critical configuration data*.

The key issue is intended to study the cases where secrets are stored in NF container images. However, this requirement prohibits any solutions that embed secrets in the VNF images.

The secrets *such as passwords or credentials, or any other critical configuration data* are still needed by VNF images. Therefore, it is proposed to update the security requirement to capture these cases where VNF images are not packaged with embedded secrets.

# 4 Detailed proposal

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of Changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 5.28 Key Issue 27: Secrets in NF container images

### 5.28.1 Key issue detail

There are scenarios which benefit from including configuration and secrets, such as passwords or credentials in NF container images. For e.g. containers require to be able to connect to other containers within the deployment as well as with external entities. All these connections need to be authenticated and secured. One way of achieving this is to provide the requisite secrets or keys to the containers which allow them to authenticate and be authenticated and secure the communication channel. A common but in-secure means of providing secrets to the containers is by packaging the secrets or the keys with the image itself. There is the risk that the same can be extracted, read or manipulated before the container is deployed and the secret used.

### 5.28.2 Security threats

With a long supply chain, container images are vulnerable to outside scrutiny. With container images containing secrets or keys, this becomes a serious threat vector. Adversaries can extract them by obtaining a copy of the image and they can be potentially shared with third parties for illicit gain.

- Secrets embedded within a container image can be stolen.

- Secrets embedded within a container image can be modified

### 5.28.3 Potential security requirements

The embedded secrets such as passwords or credentials, or any other critical configuration data in VNF images shall be properly protected.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of Changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*