**3GPP TSG-SA3 Meeting #104-e *S3-212466-r4***

**meeting, 16 – 27 Aug 2021**

**Source: MITRE**

**Title: New solution: Hardware Mediated Execution Enclave (HMEE)**

**Document for: Approval**

**Agenda Item: 5.4**

1 Decision/action requested

***This pCR proposes to solve Key Issue #6, 7, 15, and 25***

2 References

[3] ETSI GS NFV-SEC 009: "Network Functions Virtualisation (NFV); NFV Security; Report on use cases and technical approaches for multi-layer host administration".

3 Rationale

This solution aims to address KI 6, 7, 15, and 25 by proposing to standardize the use of Hardware Mediated Execution Enclave (HMEE) when deploying a Network Function Virtualisation Infrastructure (NFVI). From ETSI GS NFV-SEC 009 [3] *A hardware-mediated execution enclave is defined as an area of process space and memory within a system environment within a computer host which delivers confidentiality and integrity of instructions and data associated with that enclave. This enclave is protected from eavesdropping, replay and alteration attacks as the programs within the enclave are executed.* Utilizing an HMEE within the NFVI may solve the issue of Virtual Network Function (VNF) isolation, memory introspection, and confidentiality of data-in-use in both virtualized and containerized environments.

Use of an HMEE in the NFVI provides means to support at least the following security controls:

* Security of data-in-use. When code is executed on a shared physical host it is at risk of being modified or inspected by co-located VNFs or the host itself. With HMEE, code is executed in a secure environment, protecting the code and data from co-located VNFs and the host.
* Data integrity. HMEE is resistant to unauthorized modifications of information inside HMEE.

To scale across 5G NFV this solution proposes to utilize the trust domains from solutions to key issue #1. For example, trust domains that have security critical functions shall only be deployed on hosts that have HMEEs enabled. Meanwhile, less sensitive functions belong to a lower trust domain and do not need to be deployed on HMEE enabled hosts.

4 Detailed proposal

SA3 is kindly requested to agree to the below pCR to TR 33.848.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* First Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 6.XX Solution #XX: Hardware Mediated Execution Enclave (HMEE)

### 6.XX.1 Introduction

This solution aims to address KI 6, 7, 15, and 25 by proposing to standardize the use of Hardware Mediated Execution Enclave (HMEE) when deploying a Network Function Virtualisation Infrastructure (NFVI). From ETSI GS NFV-SEC 009 [3] *A hardware-mediated execution enclave is defined as an area of process space and memory within a system environment within a computer host which delivers confidentiality and integrity of instructions and data associated with that enclave. This enclave is protected from eavesdropping, replay and alteration attacks as the programs within the enclave are executed.*

Utilizing an HMEE within the NFVI may solve the issue of Virtual Network Function (VNF) isolation, memory introspection, and confidentiality of data-in-use in both virtualized and containerized environments. HMEE solutions offer protection from co-located VNFs running on the same physical host as well as protection from the host itself. General purpose HMEE can be equipped with Commercial Off The Shelf (COTS) hardware that may be used to host the NFVI.

Use of an HMEE in the NFVI provides the means to support at least the following security controls:

* Security of data-in-use. When code is executed on a shared physical host it is at risk of being modified or inspected by co-located VNFs or the host itself. With HMEE, code is executed in a secure environment, protecting the code and data from co-located VNFs and the host.
* Data integrity. HMEE is resistant to unauthorized modifications of information inside HMEE.

To scale across 5G NFV this solution proposes to utilize the trust domains from solutions to key issue #1. For example, trust domains that have security critical functions shall only be deployed on hosts that have HMEEs enabled. Meanwhile, less sensitive functions belong to a lower trust domain and do not need to be deployed on HMEE enabled hosts.

### 6.XX.1 Solution details

This solution proposes to equip the NFVI with one or more HMEEs, where an HMEE can be deployed for a single VNF or a group of VNFs. If the HMEE is shared, it shall provide isolation from collocated VNFs.

The HMEE is to be used for executing sensitive functions within the VNF, such as information elements marked as private (e.g., the SIDF de-concealing the SUPI from the SUCI). Other operations should use the existing security measures for NFV deployment.

When deploying an HMEE on a NFV environment the following should be considered:

* The NFVI shall be deployed using hardware resources that have an HMEE enabled. NFVI hosts should be able to attest trusted execution of VNFs. If the NFVI is deployed on the cloud in an Infrastructure as a Service (IaaS) model, then the operator shall be able to attest the root of trust on demand.

NOTE 1: How the attestation can occur is up to key issue #13. Additionally, some HMEEs have remote attestation capabilities.

Editor’s Note: Availability of VNF attestation is FFS.

* The NFVI shall be assessed to determine risk and based on this, it shall be designated an appropriate trust domain for VNF deployment. HMEE enabled hosts provide security guarantees that reduce security risks and therefore shall belong to higher trust domains.

NOTE 2: Establishment of trust domains is based on solutions for key issue #1

* Data-in-use shall be inaccessible by either other VNFs or the virtualisation layer (container engine or hypervisor). VNF sensitive data and functions shall be executed using the HMEE.

### 6.XX.1 Evaluation

TBD

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