**3GPP TSG-SA3 Meeting #106-e *draft\_S3-220078-r2***

**e-meeting, 14 - 25 February 2022**

**Source: Johns Hopkins University APL, US National Security Agency, CISA ECD, InterDigital**

**Title: Updates to Solution #5**

**Document for: Approval**

**Agenda Item: 5.2**

# 1 Decision/action requested

***It is requested to approve this update to solution #5 in TR 33.848***

# 2 References

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

# 3 Rationale

Solution 5: Solution Using Boot Time Attestation for NF Registration [1], clause 6.6 modifies the NF Service Registration procedure by verifying attestation results of a new VNF as part of the NRF registration. To support attestation, signing the NF profile provides assurance that a VNF cannot send an altered NF profile with a registration request.  Otherwise, a rogue VNF could send the NF profile of another successfully attested NF instance to circumvent the attestation process.

# 4 Detailed proposal

*\*\*\*\*Start of Change \*\*\*\**

#### 6.6.3.5 NF Service Registration Procedure with Remote Attestation

This solution proposes to provide proof to the 3GPP functional domain that a new VNF has been successfully attested before registration occurs in the 5G Core.

Once successfully instantiated, a new VNF will register with the NRF. The original NF Service Registration procedure is detailed in [13], clause 4.17.1. The modified NF Service Registration procedure shown in Figure 6.6.3.5-1 includes attestation by adding steps 2, 3, and 4. Steps 1, 5, and 6 are steps from the original procedure.

The modified NF Service Registration procedure retrieves attestation results based on the NF Instance ID in the NF profile. This solution proposes the use of digital signatures to enable integrity protection and verification of the NF profile sent in the registration request by the VNF. The NF profile should be signed by the entity that configures the profile (e.g., NFV MANO or OAM). Signing the NF profile prevents the registering VNF from altering the NF profile by forging the NF Instance ID of a successfully attested VNF.

NOTE: A signed NF profile is within alignment of TS 23.502 [13] clause 4.17.1. TS 23.502 clause 4.17.1, NOTE 2 states: the NF profile is configured by OAM system and NOTE 3 states: that whether the NF profile sent by NF service consumer to NRF needs to be integrity protected by the NF service consumer and verified by the NRF is to be decided by SA3.

**Figure 6.6.3.5-1: NF Service Registration Procedure with PACF**

When an NF requires attestation results to register, the following steps are proposed for the registration procedure:

Step 1: NF service consumer, i.e. an NF instance, sends Nnrf\_NFManagement\_NFRegister Request message to NRF to inform the NRF of its NF profile when the NF service consumer becomes operative for the first time.

NOTE: The NF service consumer’s NF profile should be signed by the entity that configured the profile (e.g., NFV MANO, or OAM)

Step 2: The NRF initiates a request for attestation results and sends the signed NF profile to the PACF.

Step 3: The PACF verifies the signature on the NF profile and retrieves attestation results from the Verifier using the NF Instance ID from the NF profile.

If signature verification fails, the NF service consumer cannot be trusted and an exception handling procedure should be activated to handle an untrusted NF.

Step 4: The PACF responds to the NRF with attestation results it received from the Verifier.

Step 5: If the attestation results affirm successful attestation, the NF service consumer can be trusted. The NRF stores the NF profile of NF service consumer and marks the NF service consumer available.

Otherwise, if the attestation results affirm an unsuccessful attestation, the NF consumer cannot be trusted and a recovery procedure should be activated to handle an untrusted NF.

Step 6: The NRF acknowledge NF Registration is accepted via Nnrf\_NFManagement\_NFRegister response.

There can also be interactions between NFs with MnF (as defined in TS 28.533) for NF management service.

Besides the above procedures defined in 3GPP, the NFs can also interact with domains defined in other SDOs, e.g., MANO defined in ETSI.

The main idea is requiring the Remote Attestation server to exposure the RA report/result of different layers to the network entities (NRF, NFp, PS, MnF, MANO, OAM, etc.) which will interact with the attested NF, then, on receiving the interaction from the NF, these network entities can invoke the RA report/result and take further actions.

NOTE: The RA server itself can also be distributed in different layers. The network entities can communicate with the RA server directly or via a unified proxy

### 6.6.4 Evaluation

Editor’s Note: To be added.

Editor’s Note: In cases where the NF does not need to register to NRF, the NRF cannot perform verification of the attestation results as proposed in the solution. Evaluation of this case is FFS.

Editor’s Note: NF profile signing is FFS.

Editor’s Note: The linkage between provisioning certificates and OAuth tokens to remote attestation is FFS.

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