**3GPP TSG-SA3 Meeting #108Adhoc-e draft\_S3-222498-r4**

**e-meeting, 10th – 14th October, 2022**

**Source: Huawei, HiSilicon**

**Title: New solution for KI #2 and #8 in NF certificate enrolment procedure**

**Document for: Approval**

**Agenda Item:** **5.5**

# Decision/action requested

***This contribution proposes a new solution in TR 33.876***

# References

None

# Rational

This contribution proposes a new solution for KI#2 and KI#8. As proposed in security threat, if certificate enrolment parameters are tempered by attacks, the CA may issue an incorrect certificate.

This pCR proposes a solution to focus on the validation and protection of key parameters on NF profile in order to prevent the misuse certificate request by misbehaviours. CA/CeEF should verify the integrity of the related parameters in certificate enrolment request before issuing the certificate.

# Detailed proposal

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of 1st Change (All Text New) \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## 6.Y Solution #Y: Enhance the security protection for Certificate parameters

### 6.Y.1 Introduction

This solution addresses KI#2 and KI#8.

After an NF is instantiated, it needs to request a certificate from the Certificate Enrolment Function (CeEF)/CA. As highlighted in the security threat, it is important that CeEF/CA can verify the NF’s parameters in the NF profile before issuing the certificate.

The solution proposes that the NF is involved and provides the signature of NF profile in order to give the necessary assurance to the CeEF/CA for issuing a certificate.

### 6.Y.2 Solution details

#### 6.Y.2.1 General

The NF profile is configured by the operation, administration, maintenance (OAM). It is assumed that when applying for a certificate, the NF provides some parameters from the NF profile, e.g. NF instance ID, NF type, FQDN/IP address, PLMN ID, etc.

Editor’s Note: Whether the signature should be applied to the entire NF profile or only to limited parameters on NF profile is ffs.

CeEF/CA verifies the integrity of the provided parameters during the certificate enrolment procedure to make sure a correct certificate can be issued. To accomplish the verification. The NF shall provide the signature of the parameters in NF profile in certificate enrolment request to build trust.

#### 6.Y.2.2 Procedure



**Figure** 6.Y.2.2-1 The Procedure of CeEF/CA verifying NF profile

1. The NF is pre-configured with the signature of the parameter in NF profile (e.g., NF instance ID, NF type, etc.), which is used in certificate enrolment procedure. The signature can be generated by OAM. For example, OAM can establish a trust relationship with the CeEF/CA in advance by obtain the certificate from CeEF/CA, and then the OAM can configure its signature for the NF.

NOTE: the signature can be either sent to NF with its profile or requested by NF after the instantiation phase in case of some parameters are NF self-generated (e,g., NF instance id).

Editor’s Note: Alignment of presentation of messages in the OAM interface and in the certificate request, and alignment in computation of the signatures in two interfaces is FFS

Editor’s Note: How the OAM initially evaluates the NF profile to provide a signature is FFS.

1. The NF sends certificate enrolment request to CeEF/CA including the signature of NF profile to request a new certificate. For example, in case of CMPv2 Initialization Request (ir) [10], the signature can be included in the senderKID or any extended Fields of ir, as long as the CeEF/CA can verify the integrity of the NF profile in the enrolment procedure. How an NF establishes the security connection with CeEF/CA is left to implementation or reference to other solutions.

2. The CeEF/CA verifies the received parameters, including the NF profile signature. If the verification is not successful, the CeEF/CA sends a failure response.

Editor’s Note: Based on what information the CeEF/CA verifies the signature of NF profile is FFS.

3. If the NF profile signature is verified successfully, CeEF/CA continue the certificate enrolment procedure with NF (e.g., NF and CeEF/CA can use CMPv2 as specified in IETF RFC 4210 [10] or specified in other solutions).

### 6.Y.3 Evaluation

TBD

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of 1st Change (All Text New) \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*