**3GPP TSG-SA3 Meeting #116 *S3-241952***

Jeju, South Korea, 20th - 24th May 2024 (revision of S3-24xxxx)

**Source: Huawei, HiSilicon**

**Title: Addressing EN in Solution #3**

**Document for: Approval**

**Agenda Item: 5.4**

# 1 Decision/action requested

***Approve the pCR to TR 33.776***

# 2 References

None

# 3 Rationale

This contribution is to address the EN below in the solution #3.

Editor’s Note: A more detailed description of the new ACME identifier, new challenge type, and proof of control over the NF instance ID, as assumed by this solution, are FFS.

As requested by the EN, more detains are provided at the relevant steps of the solution procedure.

# 4 Detailed proposal

pCR

\*\*\* Start of 1st CHANGE \*\*\*

## 6.3 Solution #3: Using NF instance ID as ACME identifier

### 6.3.1 Introduction

This solution addresses the key issue #3.

The ACME protocol defined in the RFC 8555 [2] uses domain names or IP addresses as the ACME identifier. In this solution, the NF instance ID, which is the unique identifier of an NF, is used as the ACME identifier. The ACME procedure is amended accordingly.

### 6.3.2 Solution details

In this solution, the initial trust is used to prove ownership of resources to ACME server. It supports all three optional initial trust mechanisms specified in TS 33.310 [3].

### 6.3.2.1 Initial trust

In this solution, the initial trust schema defined in clause 10.2.2 of TS 33.310 [3] is reused. As shown in Figure 6.3.2.1, the NF acts as the ACME client, the Operator CA/RA acts as the ACME server, and the OAM system acts as a validation information Authority.

A new identifier “NF instance ID” is introduced in this solution, A new ACME challenge-type is also introduced, named as "NF instance ID". In this challenge type, the initial trust is used to prove ownership of resources to ACME server. The trust relationship between a CA and OAM (validation information authority) is assumed.



Figure 6.3.2.1 Initial trust schema

### 6.3.2.2 Procedure

Prerequisites of the procedure: the same as the prerequisites stated in clause 10.2.2 of TS 33.310 [3]

Figure 6.3.2.2 shows the amended ACME procedure when using an NF instance ID as the ACME identifier. It is assumed that the NF takes the role of an ACME client for simplicity (i.e. the ACME client may be a separate entity).

NOTE: If NF and ACME client are separate entities, communications between the NF and the ACME client shall be protected, e.g. TLS. This may require reuse of mechanisms defined in TS 33.310 [3] for the initial trust setup and communications between the end entity (NF) and OAM.

For simplicity, the CA is assumed to be co-located with the ACME server. It is also assumed that the communication between the NF and the ACME server is protected, e.g. TLS.

The amended ACME procedure is as follows:

1. An NF creates its account on the ACME server as described in RFC 8555 [2].

2. The NF sends a newOrder request as in RFC 8555 [2]. In addition, the request message includes the NF instance ID as the identifier.

NOTE 1: A new identifier “NF instance ID” is introduced as opposed to RFC 8555 [2]. 3. The ACME server sends a challenge to the NF with the challenge type "NF instance ID".

NOTE 2: A new challenge type “NF instance ID” is introduced as opposed to RFC 8555 [2]. More details are described in step 4.

4. The NF sends the challenge response to the ACME server, which includes the NF instance ID and validation information for the ACME server to validate the NF (i.e. to prove the NF has control over the NF instance ID). The validation information can be any of the three options of NF initial trust information as in clause 10.2 of TS 33.310 [3], i.e. 1) OAM issued certificates, 2) an Initial Authentication Key (IAK), or 3) OAM issued signature of certain NF profile parameters, at least including the NF instance ID. All the mandatory parameters, e.g. NF Type etc as defined in the NF certificate profile in 33.310 [3] are included in the validation information.

5. The ACME server validates the challenge response as in RFC 8555 [2]. In addition, the ACME server validates the validation information in the challenge response.

The ACME server validates the validation information the same way as verifying the initial trust options specified in clause 10.2 of TS 33.310 [3],

NOTE 3: The steps 2 to 5 contain changes to the RFC 8555 [2] (e.g. NF instance ID identifier, NF instance challenge, proof of NF control over the NF instance ID based on verifying the initial trust) that are not possible as of now.

6. NF sends to the ACME server a CSR request for its certificate. The ACME server verifies the CSR based on the outcome in step 5 and, if successful, issues the NF certificate including the NF instance ID.

**

Figure 6.3.2.2 ACME procedure with an NF instance ID as the ACME identifier

### 6.3.3 Evaluation

This solution requires a new ACME identifier "NF instance ID", a new challenge type for the "NF instance ID" identifier, and proof of NF control over the NF instance ID. This is currently not possible in RFC 8555 [2] as described from the step 2 to the step 5. Therefore, additional work is required in IETF.

\*\*\* END OF 1st CHANGE\*\*\*