**3GPP TSG-SA3 Meeting #117** **draft\_S3-243486-r1\_**

**Maastricht, Netherlands, 19 – 23 August 2024 revision of S3-243397**

**Source: Google, John Hopkins University APL, Cisco Systems, US National Security Agency**

**Title: Proposed solution for certificate enrolment**

**Document for: Approval**

**Agenda Item: 5.4**

# 1 Decision/action requested

***Approval of a new solution to address KI#4 in TR 33.776.***

# 2 References

[1] 3GPP TR 33.776: “Study of ACME for Automated Certificate Management in SBA”

2[3] 3GPP TS 33.310: “Network Domain Security (NDS); Authentication Framework (AF)”

[4] TS 23.003 “Numbering, addressing and identification”, 2020

# 3 Rationale

This contribution proposes a solution that addresses Key Issue #4 - Certificate enrolment, as defined in TR 33.776 [1]. The solution is based on use of the ACME protocol, as defined in RFC 8555 [2].

# 4 Detailed proposal

\*\*\* BEGINNING OF CHANGES (all text new) \*\*\*

## 6.x Solution #x: Using ACME protocol for certificate enrolment

### 6.x.1 Introduction

This solution proposes to use the ACME protocol to address the requirements in key issue KI#4 (Certificate enrolment).

### 6.x.2 Solution details

#### 6.x.2.1 Initial Trust

This solution can assume that the initial trust has already been established via the initial trust schema defined in TS 33.310 [3], which is briefly described as follows.

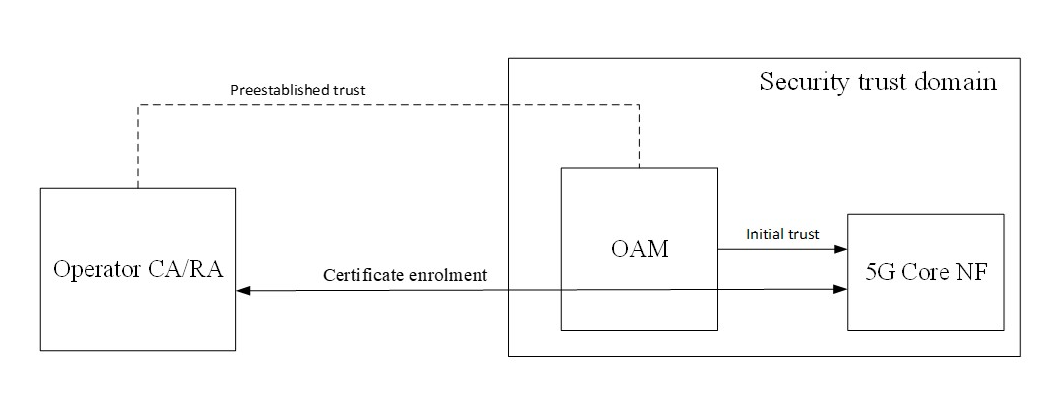


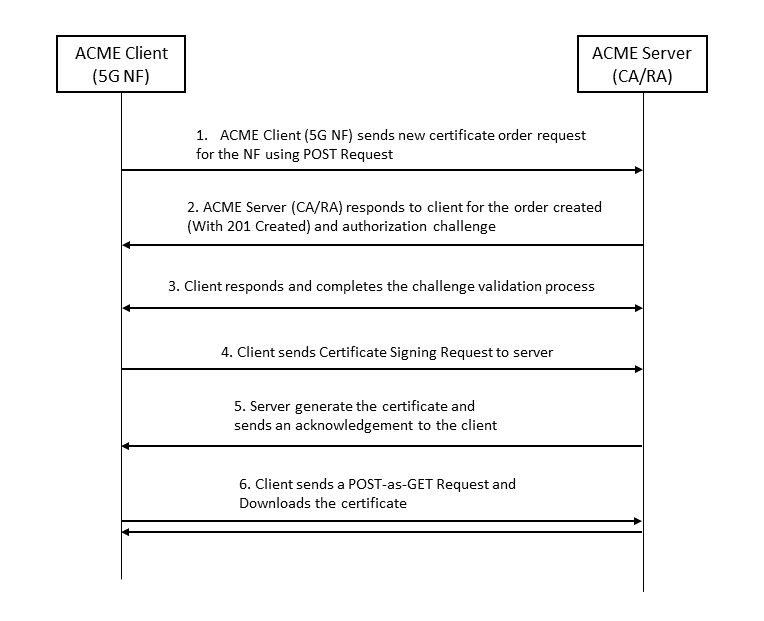
Figure 6.x.2.1-1 Initial trust schema

As depicted in Figure 6.x.2.1-1 Operation, administration and maintenance (OAM) system has a preestablished trust with Operator CA/RA. An operator CA/RA can be a trusted third-party CA/RA, with which the 5GS has a pre-established trust. The OAM can configure the 5G Core NF with a list of trust anchors and with a private/public key pair to be used for ACME account creation. Alternatively, the 5G Core NF can generate its own key pair.

Note that the Operator CA/RA behaves as an ACME server and the 5G Core NF acts as an ACME client.

##### 6.x.2.2 Certificate enrolment

Figure 6.x.2.2-1 describes the ACME certificate enrolment procedure for a 5G NF. Note that 5G Core NF can also be referred to as 5G NF.



**Figure 6.x.2.2-1 – ACME certificate enrolment**

1. The ACME client requests a certificate by sending a new order request for 5G SBA ACME Identifier to the CA’s newOrder resource using a POST request. 5G SBA ACME Identifier can be referred to as any ACME identifier shown to work with 5G SBA per this study. E.g., Solution #1, Solution #2, Solution #3 [1]. The request contains an indication of a new order. The request message is signed using the ACME client’s private key.
2. The ACME server responds with a 201 (Created) response back to the client indicating that the request has been fulfilled with further actions from the Client, which includes authorization objects with challenges to be satisfied as described in RFC 8555[2].
3. The ACME client checks the authorization objects within the response and completes the listed challenges before requesting the ACME server to sign the certificate as described in RFC 8555 [2]. Any challenge validation methods shown to work for 5G SBA can be included in this list.
4. Provided that the ACME client successfully completes the challenge validation procedure, the ACME server can generate a certificate for the 5G SBA ACME Identifier. At this point, authorizations are in the “valid” state and the order is “ready”. Upon receiving the acknowledgement, the client will send a Certificate Signing Request (CSR) to the ACME server.
5. If the call to finalize the order is valid, the server will issue the certificate and publish it in the corresponding resource directory to the URL provided in the order object.
6. The ACME client downloads the certificate by sending a POST-as-GET request to the certificate URL provided.

### 6.x.3 Evaluation

This solution addresses KI#4.

This solution impacts core network function, OAM and service protocols in the 5G core network.

The solution outlines how certificate enrolment in 5G SBA may be performed using the ACME protocol [2] with any ACME identifier type and corresponding ACME challenge validation types that are suited for use in 5G SBA deployments.

Editor’s Note: Further evaluation is FFS.

\*\*\* END OF CHANGES \*\*\*