**3GPP TSG-SA3 Meeting #119** draft\_**S3-244656-r2**

**Orlando, Florida, 11 – 15 Nov 2024**

**Source: Google**

**Title: Evaluation update for solution #9 (Using ACME protocol for certificate renewal)**

**Document for: Approval**

**Agenda Item: 5.4**

# 1 Decision/action requested

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

# 2 References

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

[2] IETF RFC 8555: “Automatic Certificate Management Environment (ACME)”, 2019

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

# 3 Rationale

This contribution proposes a solution evaluation update for solution #9 in TR 33.776.

# 4 Detailed proposal

\*\*\* BEGINNING OF CHANGES \*\*\*

## 6.9 Solution #9: Using ACME protocol for certificate renewal

### 6.9.1 Solution overview

This solution addresses KI#5 in TR 33.776 [1].

#### 6.9.1.1 5G NF/ACME client-initiated certificate renewal procedure

This section describes a client-based certificate renewal request process. The certificate renewal proceeds with the same flow of messages as certificate enrolment as depicted and described in Figure 6.5.2.2.1 (Solution #5) of TR 33.776 [1].

It is assumed that the 5G NF, an ACME client has been through a certification enrolment (issuance) process and has received a signed certificate from the CA/RA (ACME server) as described in Solution #5 of TR 33.776 [1].

The 5G NF has been configured with certificate renewal policies.

The CA/RA (ACME server) may have a set of 5G NFs (ACME clients) pre-authorized for certificate renewal, as detailed in RFC 8555 [2]. The CA/RA may have a pre-populated list of such objects. The certificate renewal follows the following steps.

1. The ACME client initiates a request for certificate renewal to the ACME server based on a trigger from certificate renewal policy. The renewal request is a newOrder request as described in Solution #5 of TR 33.776 [1].
2. Upon receiving the certificate renewal request, the ACME server checks if the ACME client is pre-authorized for certificate renewal.
3. The ACME server builds a response including any pre-existing authorization objects marked as valid. These are either from the pre-populated list, if it is a pre-authorized 5G NF, or from previous successful challenge-responses. It includes authorization objects marked as pending and requiring challenge-response if needed.

As discussed in the Step 1 of the solution described herein, the certificate renewal request is a newOrder request. This means that the new certificate request for certificate renewal is the same as the new certificate request in certificate enrolment (issuance) procedure. Clause 7.4.1 in RFC 8555 [2] defines the pre-authorization procedure for certificate enrolment (issuance) and therefore, applies to certificate renewal procedure as well.

Note that pre-authorization may be limited by time (time interval). In other words, the ACME server may keep track of a time interval. If the renewal request is outside of the time interval, the CA/RA sends an authorization challenge to the ACME client as described in Solution #5 of TR 33.776 [1]. For example, if the renewal interval constraint is set as a week (336 hours) and if an ACME client sends a renewal request after 336 hours of the last certificate issuance, the ACME server may send a challenge validation request to the ACME client.

1. The ACME client completes any required challenge.

If the challenge is not completed successfully prior to the expiration time initially provided by the server or updated by the server, the client may start a wait timer and re-start the certificate renewal procedure from Step 1. The wait timer may be pre-configured with appropriate wait time (e.g., 0 seconds).

1. The ACME client sends a Certificate Signing Request to the ACME server as described in Solution #5 of TR 33.776 [1].

Note that if the challenge is not completed successfully prior to the expiration time initially provided by the ACME server or updated by the ACME server, the order will eventually be dropped by the ACME server.

1. The ACME client sends a POST-as-GET request and downloads the certificate, as described in Solution #5 of TR 33.776 [1].

### 6.x.3 Evaluation

This solution addresses KI#5.

This solution impacts 5G core network functions and 5G OAM system.

Pre-defined certificate renewal policies in the 5G NF (ACME client) trigger the process for certificate renewal. A 5G NF sends the certificate renewal request to a trusted CA/RA (ACME server).

A 5G NF may be pre-authorized by a CA/RA for certificate renewals. The pre-authorization objects are marked as valid either as a pre-populated list of NFs or the NF may be pre-authorized based on a previous successful challenge-response. In such a scenario, the CA/RA does not involve challenge validation steps. However, pre-authorization may be constrained by a time interval within which the CA/RA expects to receive a certificate renewal request for it to issue a certificate without challenging the client.

If the 5G NF is not pre-authorized for certificate renewal, the CA/RA sends challenge validation objects to the 5G NF, which it needs to complete successfully.

The CA/RA may resend a challenge validation request to the 5G NF if the previous challenge was unsuccessful.

If the challenge validation procedure couldn’t be completed within expiration time initially provided by the server, then the 5G NF may restart the certificate renewal process. After a successful validation of the challenge, the 5G NF sends a certificate signing request to the CA/RA. The CA/RA generates a certificate, which the 5G NF then downloads.

.

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