**3GPP TSG-SA3 Meeting #116 *draft\_S3-241799\_r1***

Jeju, South Korea, 20th - 24th May 2024

**Source: Johns Hopkins Unversity APL**

**Title: Solution on certificate revocation**

**Document for: Approval**

**Agenda Item: 5.4**

# 1 Decision/action requested

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

# 2 References

[2] IETF RFC 8555: "Automatic Certificate Management Environment (ACME)".

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

# 3 Rationale

This contribution proposes a solution to address key issue #6 in TR 33.776.

# 4 Detailed proposal

*\*\*\*\*\*\*\*\* Start of Change (All new text) \*\*\*\*\*\*\*\**

6.Y Solution #Y: ACME automated revocation of certificates

6.Y.1 Introduction

This solution addresses key issue #6 on certificate revocation.

Certificate revocation is a necessary component of the certificate management lifecycle to address potential vulnerabilities that arise due to a compromise such as when the private key of the certificate has been exposed. There may be instances due to a misconfiguration or cyberattack or other events in which the private key of a valid certificate may have been compromised and the certificate needs to be revoked to mitigate potential threats.

The ACME protocol [2] defines automated revocation procedures of ACME enrolled and renewed certificates using established authenticated and authorized credentials (i.e., key pair) verified during ACME client account activation and certificate issuance. The end entity (e.g., ACME client in the NF) can use its account key pair or the key pair of the issued certificate to request revocation of its certificate from the CA (i.e., ACME server).

6.Y.2 Solution Details

This solution proposes certificate revocation procedure specified in RFC 8555 to revoke valid certificates before expiration.

The solution assumes:

* Initial trust between end entities (i.e., ACME client and ACME server) has been established based on clause 10.2 of 33.310.
* CRL and OCSP certificate revocation status checking profiles defined in TS 33.310 clause 6.1a and 6.1b, respectively, are reused [3].
* The certificate being requested for revocation has not expired.
* ACME client maintains the valid account key pair for the NF identifier for which the certificate was issued and/or access to the key pair of the issued certificate being requested for revocation to properly sign the revocation request.
* When the ACME client is co-located with the NF in 5G SBA, the ACME client does not have the privilege to request certificate revocation for other NFs.

Figure 6.y.1. 1 provides an overview of the ACME certificate revocation procedure, as summarized below:

1. To initiate the certificate revocation request, the ACME client generates a JWS object, in which the JSON payload contains the certificate to be revoked, using the account private key or the certificate private key.
2. The ACME client sends the revocation request to the ACME server.
3. The ACME server validates the revocation request by verifying that the private key used to sign the request is authorized to revoke the certificate. If the account private key was used, the request must come from the account that the certificate was issued or the account that holds the authorization for all the identifiers in the certificate
4. If the revocation request is deemed valid during on Step 3, the ACME server sends status is OK message. If revocation fails, the ACME server returns an error. If the certificate was already revoked, the ACME server returns status that it has been already revoked.

Note: When and how revoked certificates are added into the CRL and/or OCSP service is left to operator's implementation and out of scope of this solution.



Figure 6.y.1. 1: Overview of ACME-based automated certificate revocation

6.Y.3 Evaluation

Editor's Note: Evaluation of this solution is FFS

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