**3GPP TSG-SA3 Meeting #115AdHoc-e  *S3-241149\_r2***

**Electronic meeting, online, 15 – 19 April 2024**

**Source: Johns Hopkins University APL, Cisco Systems, Google Inc.**

**Title: New key issue on certificate revocation**

**Document for: Approval**

**Agenda Item: 5.4**

# 1 Decision/action requested

***It is requested to approve a key issue for TR 33.776***

# 2 References

[1] TR 33.776, v0.1.0, "Study of Automated Certificate Management Environment (ACME) for the Service Based Architecture (SBA)".

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

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

# 3 Rationale

As the use of digital certificates and virtualized environments continue to expand in the 5GC, revoking certificates across a large number of network functions and services can become quite intensive. If not automated, it could lead to delays in revoking certificates that have been compromised. If revoking certificates require extensive manual procedures, the potential for certificates to be improperly revoked could increase and lead to negative network and service impacts (e.g., unexpected outages) or vulnerabilities if compromised certificates are not revoked. There are benefits for certificate revocation of digital certificates that are automated, secure, scalable and interoperable with certificate management protocols such as ACME [2].

# 5 Key issues

*\*\*\*\* Start of Change \*\*\*\**

## 5.X Key Issue X: Certificate revocation

## 5.X.1 Key Issue Details

The ACME automated certificate management protocol [2] provides procedures and recommendations to support automated certificate revocation. Certificate revocation is the process of revoking a digital certificate so that it can no longer be used prior to expiration. ACME will use existing certification revocation status checking profiles that have been specified in TS 33.310 [3] such as CRL specified in clause 6.1a and OCSP specified in clause 6.1b. Revocation may be conducted for a variety of reasons, such as a compromise of the certificate’s private key or changes to underlying parameters such as the domain name. This KI is to study the ACME automated certificate revocation procedures, namely certificate revocation requests from the ACME client, as part of the management lifecycle in the 5GC SBA.

Note: Study on new certification revocation status procedure profiles beyond the existing set in clause 6.1 in TS 33.310 are out of scope.

### 5.X.2 Security Threats

Not applicable.

### 5.X.3 Potential Security Requirements

Not applicable.

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