**3GPP TSG-SA3 Meeting #115  *draft\_S3-240367-r1***

**Athens, Greece, 26th February – 1st March 2024**

**Source: Johns Hopkins University APL, Cisco Systems, AT&T**

**Title: New key issue on Certificate Enrolment**

**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] SP-231787, New Study of ACME for Automated Certificate Management in SBA, 3GPP SA#102

[2] draft\_S3-240207, Proposed skeleton for TR 33.776 Study of Automated Certificate Management Environment (ACME) for the Service Based Architecture (SBA)

[3] IETF RFC 8555, Automatic Certificate Management Environment (ACME), March 12, 2019

# 3 Rationale

As the use of digital certificates and virtualized environments expand in the 5GC, resources needed to manually manage certificates can become quite intensive and could lead to increase likelihood of misconfiguration, vulnerabilities, and unexpected downtime. There are benefits for enrolment of digital certificates for such entities as operator CAs and 5GC NFs that are automated, secure, scalable and interoperable with certificate management protocols. Therefore, certificate enrolment that is automated and fully interoperable with ACME in the 5GC SBA should be supported [1].

Certificate enrolment is the process of obtaining a digital certificate from a CA. The process involves authentication, request submission, certificate generation, reception and installation. For this key issue for FS\_ACME\_SBA [2], the procedures and solutions for a NF and ACME client [3] to interoperate with the enrolling CA are required to support ACME in the 5GC SBA.

# 5 Key issues

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

## 5.X Key Issue: Certificate enrolment

## 5.X.1 Key Issue Details

The ACME automated certificate management protocol provides procedures and identifies solutions to support authentication to the enrolment server CA and secure message protocol to protect ACME message exchanges during the certificate enrolment process against replay and confidentially protection. To address the objectives of this study [1] there is a requirement to identify procedures and solutions to use ACME across the 5GC SBA for different scenarios (e.g., multi-vendor integration) and use cases (e.g., authentication of domain names, HTTPS, mutual TLS authentication). Procedures and solutions for automated certificate enrolment to consider for this key issue include:

* Support for ACME client and authentication
* Certificate signing request (CSR) – content and creation of request
* CSR Submission
* Certificate issuance

This KI is to identify ACME certificate enrolment procedures and solutions for different use cases for the 5GC SBA.

Editor’s note: Certificate revocation is out of scope for this key issue.

Editor’s note: Certificate renewal is out of scope for this key issue.

Editor’s note: ACME certificate enrolment and co-existence with CMPv2 is FFS.

### 5.X.2 Security Threats

Without the ability to automate the authentication of ACME clients, submission of CSRs, and reception of digital certificates in a timely and secure manner, automated certificate enrolment based on ACME protocol cannot be effectively supported in the 5GC SBA. Without automated certificate enrolment, operators who continue to rely on manual enrolment could increase the likelihood of negative network and service impacts (e.g., unexpected outages or potential introduction of network vulnerabilities due to expired or misconfigured certificates).

### 5.X.3 Potential Security Requirements

Network functions and services require automated and authenticated enrolment procedures and solutions supporting ACME to request/ obtain digital certificates from the enroling CA.

Editor’s note: Requirements for secure transport of messages is out of scope for this key issue.

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