**3GPP TSG-SA3 Meeting #115  *draft\_S3-24XXXX***

**Athens, 26 February - 1 March 2024**

**Source: Johns Hopkins University APL, Cisco, TBD**

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

**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] 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, renewing certificates over their multiple lifecycles can become quite intensive and could lead to potential outages and service impacts as a result of expired certificates (e.g., if forgotten or not renewed in time). This can become a significant concern if the lifecycle period becomes shorter and shorter resulting in more frequent renewals over a shorter period of time. There are benefits for certificate renewals of digital certificates during their lifecycle that are automated, secure, scalable and interoperable with certificate management protocols. Therefore, renewal of certificates that is automated and fully interoperable with ACME in the 5GC SBA could have security, efficiency and reliability benefits [1].

# 5 Key issues

*\*\*\*\*Start of Change 1\*\*\*\**

## 5.X Key Issue X: Certificate revocation

## 5.X.1 Key Issue Details

The ACME automated certificate management protocol provides procedures and recommendations to support different aspects of the certificate lifecycle [2]. Certificate renewal is the process of issuing a new digital certificate for an existing certificate that needs to be reissued (e.g., when a certificate is about to expire or if the certificate has been compromised). Certificate renewal may be conducted for a variety of other reasons, such as if a certificate needs to be changed or updated due to changes in the NF or network domain. In addition, the certificate that was replaced is revoked to prevent the potential for unauthorised use.

This KI is to identify ACME certificate renewal procedures and solutions in the 5GC SBA. In addition, the certificate expiration period and renewal interval need to be set appropriately against potential security threats while reducing certificate management overhead and associated risk (e.g., certificates expiring prior to being renewed).

### 5.X.2 Security Threats

A scenario where a long-lived certificate (i.e., long duration before expiration) becomes compromised without being detected could remain a threat and an attack vector against the network and NFs for a long period of time. Therefore, short-lived certificates with an appropriate validity period or expiration can reduce such potential threats and their impact.

In addition, certificate renewal without proper authentication and authorization could lead to issuance of invalid and compromised certificates.

### 5.X.3 Potential Security Requirements

To minimise risk and to expedite resolution of potential threats due to compromised digital certificates or other scenarios for certificate renewal, an automated and secure solution to renewing certificates that is secure and interoperable with ACME is needed in the 5GC SBA. In addition, certificate expiration and renewal period need to be appropriately defined so that potential security threats are minimised without undue impact to automated certificate management operations and the 5GC. Solution to this KI need to only allow authorised and approved certificate renewal to be supported.

*\*\*\*\*End of Change1\*\*\*\**