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

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

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

**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] 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, revoking certificates over their lifecycles can become quite intensive and could lead to increase likelihood of negative network and service impacts (e.g., misconfiguration, introduction of vulnerabilities, unexpected outages). This can become a significant concern if the lifecycle period becomes shorter and shorter which would require more frequent revocation of certificates. There are benefits for certificate revocation of digital certificates during their lifecycle that are automated, secure, scalable and interoperable with certificate management protocols. Therefore, certificate revocation 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\*\*\*\**

## 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 certificate revocation [2]. Certificate revocation is the process of revoking a digital certificate that has been issued so that it can no longer be used. Revocation may be conducted for a variety of reasons, such as if the certificate is no longer needed, certificate has expired or is about to expire, and a new certificate has been issued/renewed. Other reasons for revocation could be for a compromise of the certificate private key or changes to underlying parameters such as the domain name.

This KI is to identify ACME certificate revocation supported procedures and solutions in the 5GC SBA.

### 5.X.2 Security Threats

Compromised certificates if not revoked can be used to attack the network such as impersonating and gaining unauthorised access to NFs, breaking encryption, and/or be used to introduce other potential threats. In addition, revocation needs to be supported in a timely manner to reduce the amount of time that vulnerabilities remain exposed.

Manual methods to revoke certificates can be time consuming and error prone which can introduce potential delays and prolong network and service outages. These types of threats and others can be reduced or eliminated by using industry supported standards such as ACME for automated certificate revocation.

Lastly, certificate revocation without proper authorization could lead to unauthorised revocation of valid certificates and a wide range of unexpected network outages and service disruptions.

### 5.X.3 Potential Security Requirements

To minimise risk and to expedite resolution of potential threats due to compromised digital certificates or other valid reasons for certificate revocation, an automated and secure certificate revocation solution that is secure and interoperable with ACME is needed in the 5GC SBA. Solution to this KI shall only allow authorised and approved certificate revocation to be supported.

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