**3GPP TSG-SA3 Meeting #115 *S3-240997-r1***

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

**Source: Google**

**Title: New key issue on Secure Transport of Messages**

**Document for: Approval**

**Agenda Item: 5.4**

# 1 Decision/action requested

***Approve this contribution to add the proposed key issue for TR 33.776***

# 2 References

[1] IETF RFC 8555: “Automatic Certificate Management Environment (ACME)”, March 12, 2019

# 3 Rationale

As 5G SBA evolves to incorporate use of ACME [1] for automated management of certificates, it is crucial that ACME messages are transported securely. Secure transport of ACME messages is crucial in a service based architecture where network functions may be self contained and independent. Secure transport of ACME messages involves confidentiality and integrity protection and protects against replay attacks. Therefore, for secure transport of messages, 5G SBA should be able to leverage the capabilities offered by ACME, which implements secure HTTP protocol and digital signatures.

# 4 Detailed proposal

\*\*\* BEGINNING OF CHANGE \*\*\*

## 5.X Key issue #X: Secure Transport of Messages

### 5.X.1 Key issue details

The ACME automated certificate management protocol provides procedures and recommendations to support different aspects of the certificate lifecycle [1]. Using ACME for automated certificate management in SBA, would require messages to be integrity protected, confidentiality protected, replay protected, and mutually authenticated.

### 5.X.2 Security Threats

Not Applicable

### 5.X.3 Potential security requirements

Not applicable

\*\*\* END OF CHANGE \*\*\*