**3GPP TSG-SA3 Meeting #119** draft\_**S3-244659-r1**

**Orlando, Florida, 11 – 15 Nov 2024**

**Source: Google**

**Title: Conclusion for KI #2 (Secure Transport of Messages)**

**Document for: Approval**

**Agenda Item: 5.4**

# 1 Decision/action requested

***Approve the pCR to TR 33.776***

# 2 References

[1] 3GPP TR 33.776: “Study of ACME for Automated Certificate Management in SBA”

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

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

# 3 Rationale

This contribution proposes a conclusion to KI#2 in TR 33.776.

# \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START OF CHANGES \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# 7 Conclusion

## 7.2. KI#2: Using ACME Secure Transport of Messages

### 7.2.1 Analysis

This key issue is addressed by Solution #7 (Using ACME protocol for secure transport of messages). Some ACME challenge types (e.g., dns-01, http-01) involve the ACME server initiating an exchange with the ACME client. How such exchanges are protected will need to be addressed by any solution that uses these challenge types.

### 7.2.1 Conclusion

The normative phase can begin based on Solution #7 and limited to challenge types that do not involve the ACME server initiating an exchange with the ACME client.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END OF CHANGES \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*