**3GPP TSG-SA3 Meeting #119** draft\_S3-245211-r3\_was\_**S3-244657-r2**

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

**Source: Google,**

**Title: Conclusion for KI#4 (Certificate enrolment)**

**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#4 in TR 33.776.

# \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* BEGINNING OF CHANGES - ALL NEW TEXT \*\*\*\*\*\*\*\*\*\*\*\*\*

## 7.x KI#4: Certificate enrolment

### 7.x.1 Analysis

This key issue is addressed by Solution #5 (Using ACME protocol for certificate enrolment) which is the only solution that explicitly focuses on the KI#4. The solution includes two different methods of ACME client authorization for certificate enrolment: the ‘challenge-response’ process and the ‘pre-authorization’ process, wherein pre-authorization process is largely optional.

### 7.x.2 Conclusion

Given that the ‘pre-authorization’ process is largely optional for client authorization for certificate enrolment, the ‘pre-authorization’ portion of the certificate enrolment procedure can be excluded from the normative phase of the study. The normative phase can begin based on the rest of the procedure described in Solution #5.

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