**3GPP TSG-SA3 Meeting #119** **draft\_S3-244658-r2**

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

**Source: Google**

**Title: Conclusion for KI#5 (Certificate Renewal)**

**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#5 in TR 33.776.

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

## 7.x. KI#5: Certificate renewal

### 7.x.1 Analysis

This key issue is addressed by two solutions, namely Solution #4 (Reuse solution about policy-based certificate renewal), which proposes to reuse the solution adopted in the study of FS\_ACM during Release 18, and Solution #9 (Using ACME protocol for certificate renewal). Solution #4 depends on the preconfigured policy. Similarly, in solution #9 the NF initiates certificate renewal procedures based on the trigger from pre-configured certificate renewal policies. While both solutions intend to adopt policy-based certificate renewal principles, solution #9 also includes the procedure by which certificate renewal is carried out. Solution #9 involves two different methods of ACME client authorization for certificate renewal: the ‘challenge-response’ process and the ‘pre-authorization’ process, wherein pre-authorization process is largely optional.

### 7.x.2 Conclusion

It is proposed to use Solution #4 and Solution #9 as the basis for the normative phase. Additionally, the “pre-authorization” aspect of Solution #9 can be excluded for the normative phase.

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