**3GPP TSG-SA3 Meeting #115 *S3-24XXXX***

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

**Source: Google, CableLabs, John Hopkins University APL, Cisco Systems**

**Title: Scope for TR 33.776**

**Document for: Approval**

**Agenda Item: 5.4**

# 1 Decision/action requested

***Approve this contribution to add text in the Scope clause for TR 33.776***

# 2 References

[1] TR 33.876 v18.0.1 Study on automated certificate management in Service-Based Architecture (SBA)

# 3 Rationale

The SID for Study of ACME for Automated Certificate Management in SBA has been approved in SA3#102 in SP-231787. The contribution adds text in the Scope clause for ACME for Automated Certificate Management in SBA TR.

# 4 Detailed proposal

\*\*\* BEGINNING OF CHANGE #1 \*\*\*

# 1 Scope

The scope of this document is to identify key issues and study solutions addressed using ACME for automated certificate management in SBA.

Areas of study include:

* Automated certificate management protocol and procedures for certificate life cycle events (i.e., enrolment,  renewal, and revocation) within 5G SBA (i.e., to be used by operator CAs and all 5GC NFs including NRF,  SCP, SEPP, etc.), including the following:
	+ ACME transport and request/response messages for 5G SBA use cases
	+ ACME certificate profiles for all 5G SBA entities
* Mechanisms for establishing initial trust and chain of trust of Certificate Authority hierarchies, including the  following:
	+ Existing ACME challenge types and if any new challenge types are needed for 3GPP use cases:
		- Creation, deletion, rotation, revocation and storage of the certificates
	+ Ability to automate ACME challenge validation
	+ Suitability of existing mechanisms when 5G SBA is for standalone NPN (SNPN)
* Call flow of the messages exchanged between different entities in the chain of trust.
* The certificate management framework in the 5G core should consider the coexistence of ACME and CMPv2.
	+ Identifying potential requirements and solutions in a multi-vendor environment where either CMPv2 or ACME may be selected for automated certificate management, specifically
		- Operators CA supporting CMPv2 and/or ACME.
		- 5GCs NF supporting CMPv2 and/or ACME.

NOTE: Certificate management for the external interface of the SEPP is out of scope.

\*\*\* END OF CHANGES #1 \*\*\*

\*\*\* BEGINNING OF CHANGES #2 \*\*\*

# 3.3 Abbreviations

CA Certificate Authority

NPN Non-Pubic Network

NRF Network Repository Function

SCP Service Communication Proxy

SEPP Security Edge Protection Proxy

SNPN Stand-Alone Non-Public Network

\*\*\* END OF CHANGES #2 \*\*\*