**3GPP TSG-SA3 Meeting #116 *S3-242439-r3***

Jeju, Republic of Korea, 20th – 24th May 2024

**Source: Huawei, HiSilicon**

**Title: Reuse solution about policy-based certificate renewal**

**Document for: Approval**

**Agenda Item: 5.4**

# 1 Decision/action requested

***Approve the pCR to TR 33.776 [1]***

# 2 References

[1] 3GPP TR 33.776: " Study of Automatic Certificate Management Environment (ACME) for the Service Based Architecture (SBA)"

# 3 Rationale

This contribution proposes a solution for key issue #5.

During the R18 discussion for FS\_ACM\_SBA, we’ve proposed solutions about certificate renewal. And for the simultaneous update/renewal of a vast number of certificates, we have the conclusion that：

*" The update/renewal trigger, for example due to expiry, change in validity "status" or other events such as the sudden disclosure of broken cryptographic primitives, could be based on internal configuration, operator policies, etc. Therefore, no normative work is needed, and this aspect of the overall framework could be left to implementation. "*

So, in key issue #5, the issue that the certificate expiration period and renewal interval need to be set appropriately against potential security threats while reducing certificate management overhead and associated risk (e.g., certificates expiring prior to being renewed) can also reuse the solutions.

# 4 Detailed proposal

Approve the following assumptions for inclusion under clause 6.

\*\*\* Start of 1st Change \*\*\*

## 6.Y Solution #Y: Reuse solution about policy-based certificate renewal

### 6.Y.1 Introduction

This contribution addresses key issue #5, and in particular the requirement that the certificate expiration period and renewal interval need to be set appropriately against potential security threats while reducing certificate management overhead and associated risk (e.g., certificates expiring prior to being renewed).

### 6.Y.2 Solution details

This solution reuses the list of practical recommendations defined in Annex I.2 of TS 33.310[3] for NF certificate renewal expiration period and renewal interval. An NF can act as an ACME client and use ACME [2] to interact with an operator CA that acts as an ACME server to renew its certificate.

NOTE: The 1st sentence in the Annex I.2, i.e. “The normal procedure of update and renewal of 5GC NF certificates is managed by CMP protocol as described in clause X.3.1” does not apply.

### 6.Y.3 Evaluation

This contribution addresses key issue #5 and proposes to reuse the solution we adopted in the study of FS\_ACM during Release 18. The solution depends on the preconfigured policy and internal implementation of the NF/CA.

\*\*\* End of 1st Change \*\*\*