**3GPP TSG-SA3 Meeting #115 *S3-240984***

**Athens, Greece, 26th February – 1st March 2024 Merge of S3-240824, S3-240504, S3-240380**

**Source: Google, Huawei, HiSilicon, Telus, Cisco Systems**

**Title: New key issue on ACME Challenge Validation**

**Document for: Approval**

**Agenda Item: 5.4**

# 1 Decision/action requested

***Approve this contribution to add the proposed key issue for TR 33.776***

# 2 References

[1] IETF RFC 8555, Automatic Certificate Management Environment (ACME), March 12, 2019

[2] SP-231787, New Study of ACME for Automated Certificate Management in SBA

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

[4] IETF RFC 8738: " Automated Certificate Management Environment (ACME) IP Identifier Validation Extension".

[5] IETF RFC 8739: " Support for Short-Term, Automatically Renewed (STAR) Certificates in the Automated Certificate Management Environment (ACME) ".

[6] IETF RFC 8823: " Extensions to Automatic Certificate Management Environment for End-User S/MIME Certificates".

[7] IETF RFC 9448: " TNAuthList Profile of Automated Certificate Management Environment (ACME) Authority Token".

[8] IETF draft-ietf-acme-client-07: " ACME End User Client and Code Signing Certificates".

# 3 Rationale

Challenge validation is a crucial step in security protocols, especially in contexts like certificate issuance, to ensure that the requesting entity has control over the relevant resources or information. A weak challenge validation or the lack of such a measure pose many security risks such as issuance of unauthorized certificates. On the other hand, challenge validation requires entities to demonstrate control over a specific resource or piece of information. This serves as proof that the entity making a request has legitimate access and control over the necessary elements, enhancing the overall security of the process. Furthermore, it elevates security posture to prevent unauthorized access to resources or services, protection against replay attacks, mitigate identity spoofing and enhance authentication mechanisms. As the 5G system enhances the security infrastructure with automated digital certificates issuance methods, automated challenge validation methods in 5G SBA with ACME [1] need to be clarified.

# 4 Detailed proposal

\*\*\* BEGINNING OF CHANGE \*\*\*

## 5.X Key issue #X: Challenge Validation

### 5.X.1 Key issue details

Definition of one or more challenge validation mechanisms is needed for challenge types identified for use in SBA with ACME.

The objective of this key issue is to identify and evaluate the suitability of the ACME challenge types for use within the 5G SBA. The base ACME standard [1] supports standard challenges (DNS-01, HTTP-01, TLS-ALPN-01). Other ACME uses have implemented additional challenge types appropriate to their needs. The 5G SBA may benefit from defining new challenges and adding them to the "ACME Validation Methods" registry.

The ACME protocol supports the issuance of certificates with domain names, IP addresses, or email address as subject identifiers. More precisely, according to the current ACME protocol specifications [1][4][5][6], the protocol can be used for the following purposes: Issuance of Web PKI certificates attesting to domain name or IP addresses, issuance of Short-Term Automatically Renewed (STAR) X.509 certificates, issuance of certificates for use by email users (S/MIME), issuance of STI (Secure Telephone Identity) certificates, and issuance of end user client and code signing certificates. However, in SBA, the NF instance ID is used as the unique identifier for NF instances. In addition, based on the current provisions of TS 33.310 [3], the use of IP addresses only is not allowed.

Mutual TLS, as used between NFs in SBA, involves both client-side and server-side certificates. ACME is tailored for automated certificate validation for server-side certificates. Client-side as well as server-side needs to be considered for ACME in the context of SBA.

### 5.X.2 Security Threats

Not applicable

### 5.X.3 Potential security requirements

Not applicable

\*\*\* END OF CHANGE \*\*\*