**3GPP TSG-SA3 Meeting #115 *S3-240824 – r1***

**Athens, Greece, 26th February – 1st March 2024**

**Source: Google**

**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] IETF RFC 8226, Secure Telephone Identity Credentials: Certificates, February 2018

[4] IETF RFC 9475, Messaging Use Cases and Extensions for Secure Telephone Identity Revisited (STIR), December 2023

[5] ATIS-1000074, ATIS/SIP Forum IP-NNI Task Group, "Signature-based Handling of Asserted information using toKENs (SHAKEN)", January 2017

# 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 such as the STIR [3, 4] / SHAKEN [5] ecosystem 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.

### 5.X.2 Security Threats

Poorly implemented challenge validation opens the door to unauthorized certificate issuance. Malicious entities may exploit this vulnerability to obtain certificates without properly demonstrating control or ownership of the associated resources.

There is also an increased risk of attackers intercepting and manipulating communication between the certificate requester and the certificate authority leading to Adversary in The Middle (AiTM) attacks, replay attacks, identity spoofing, certificate tampering and other risks such as domain hijacking.

### 5.X.3 Potential security requirements

The identification, evaluation and integration of suitable new ACME challenge types and features are required for automated certificate management in the 5G SBA.

Assessment of integration and interoperability implications for standard ACME challenge validation processes is required within the existing security mechanisms (i.e., authentication and authorization) in the 5G SBA. Study of other suitable challenge and validation mechanisms such as the STIR/SHAKEN protocol utilizes is required to maximizes the efficacy of ACME for the 5G SBA.

In addition, the challenge validation should consider dynamic challenge-response interactions with temporal validity attributes as part of the authentication and authorization processes within the 5G SBA to enhance the security of accessing and utilizing services within the architecture.

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