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

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

**Source: TELUS, [tbd]**

**Title: ACME and Client Identity Validation**

**Document for: Approval**

**Agenda Item: 5.4**

# 1 Decision/action requested

***Approve this contribution to add text in the Key Issue clause for ACME TR***

# 2 References

[1] S3-235090 Study of ACME for Automated Certificate Management in SBA

[2] S3-240XXX TR 33.776 Skeleton for Automated Certificate Management Environment (ACME) for the Service Based Architecture (SBA) Specification

[3] 3GPP TS 33.501 “Security architecture and procedures for 5G system”

[4] 3GPP TS 33.310 “Network Domain Security (NDS); Authentication Framework (AF)”

[5] ETSI GS NFV-IFA 010 “Network Functions Virtualisation (NFV) Release 5; Management and Orchestration; Functional requirements specification”

[6] IETF RFC 8555, “Automatic Certificate Management Environment (ACME)”, 12 Mar 2019

[7] IETF draft-ietf-acme-client-07 “ACME End User Client and Code Signing Certificates” published 3 Aug 2023

[8] W3C WebAuthn “Web Authentication: An API for accessing Public Key Credentials Level 2”

[9] IETF RFC 6125 “Representation and Verification of Domain-Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS)” Mar 2011

[10] ETSI GS NFV-IFA 026 “Network Functions Virtualisation (NFV) Release 4; Management and Orchestration; Architecture enhancement for Security Management Specification” Oct 2023

# 3 Rationale

The SID for Study of ACME for Automated Certificate Management in SBA has been approved in SA3#113 in S3\_235090. The contribution adds text in the Key Issues clause for ACME for Automated Certificate Management in SBA TR.

# 4 Detailed proposal

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

## 5.X Key issue #X: ACME and Client Identity Validation

### 5.X.1 Key issue details

Confidentiality for machine-to-machine communications requires confidence in both the encryption algorithm and key management system which authenticates the identity of the relying parties. The current mTLS and certificate management specifications seem to not validate the client identity, which leaves open the server to client identity spoofing.

mTLS prescribed in [3] clause 13.1 requires client certificates for a NF to identify itself to a Services Based Interface such that the TLS server can validate the calling client identity. ACME is traditionally a server-side automation scheme, and provides for validation of the end entity as described in [4] clause 10.2.2 via an initial trust known as Identifier Validation Schemes.

CMPv2 is a protocol between the requesting client entity and the CA/RA entity, dealing with enrollment, issuance operations. CMPv2 is mandated in [4] clause 7.2. CMPv2 has no identity validation mechanism. ACME would extend the 3GPP specifications to validate the 5G Core NF identities, including the client identity.

Explicit clarity is required regarding the separation of client identity from server identity. Client certificate identities are only mandated to be established in the CN field (ref: [4] clause 6.1.1 Note 3). In [4] clause 6.1.3c.3, it defines [9] as the baseline for client profiles but [9] clause 1.7.2 defines client identities as out of scope. In [4] clause 6.1.3c3 goes on to define inclusion of server address identities in the SAN of client certificates.

The clarity issue affects the validation of client certificates and the extended issue of using multiple CA’s to provide mutual exclusivity for independence in trust zones. Independence in trust zones enables operators to ensure plane separation, such as signalling and OA&M planes. Another application is security zone separation on the same plane, for example the AMF’s Namf SBI vs its N2 interface. The N2 interface is specified to use DTLS for security. In the case of the AMF, it is unclear if the client certificate should carry the SAN of the N2 reference point address or the Namf services based interface. The AMF certificate cannot have both server references without combining the SBI zone with the RAN signalling zone.

The ability to have different CAs made authoritative for each independent entity should be retained. This arrangement enables mutual-exclusive trust relationships. If the client identity of the NF should be untethered to NF server interface identity such that it can be independently validated, it supports the case where a separate Server CA and Client CA issue the certificates as identified in [4] clause 5.1.1.2. This also supports the case where a NF hosts at least two interfaces, each being in different trust zones. However this does pose problems for client identity validation.

Assuming client identity is independent of NF service interface identity, ACME [6] standardised Identifier Validation Challenges for validation of entities before certificate issuance. The methods HTTP-01, DNS-01, TLS-SNI-01 and TLS-ALPN-01 are designed for server certificate acquisition and leverage validation of the requestor by service address or server identifier. If client and server identity are independent, then they are insufficient for client identity validation. These cannot validate (by means other than ceremony) that the calling NF is in possession of the client certificate’s private key.

ACME client validation specifications have extensions before IETF in [7] and are required to be standardised in the ACME protocol before client certificates can be issued in automated fashion via ACME.

The following are analysis of the proposed client challenge types detailed in the proposed extensions of [7]:

**Option - ppkp-01 - WebAuthn or Public/Private Key Pairs**

WebAuthn, as defined in [8], is defined for the purpose of strongly authenticating users, which typically are inappropriate for device identity or machine-to-machine communications.

**Option - cert-01 - Public Key Cryptography**

This is the specification to use yet another existing X.509 based PKI system to authenticate the 3GPP based identity binding. This method assumes that there is an existing system in place for client identity from which to bootstrap. It is expected that 3GPP would want to avoid an obvious circular dependency for identity assurance.

**Inappropriate Option - HOTP-01 - HMAC-Based One-Time Password**

One time passwords are typically deployed as a Turing test for human beings and are inappropriate for device identity or machine-to-machine communications.

**Inappropriate Option - TOTP-01 - Time-Based One-Time Password**

One time passwords are typically deployed as a Turing test for human beings and are inappropriate for device identity or machine-to-machine communications.

**Inappropriate Option - OTP-01 - Generic One-Time Password**

One time passwords are typically deployed as a Turing test for human beings and are inappropriate for device identity or machine-to-machine communications.

**Other Options**

Raw public/private key pairs may be useful in this context at commissioning time of the newborn NF. A NF may be commissioned with an initial token that is recorded in the ACME server by the NF-commissioning OAM agent as shown in [4] clause 10.2.2. This functions as the “pre-established trust”. The OAM agent could include the ETSI Certificate Management Function as specified in clauses 5.9 and 6.12 of [5] and fulsomely in clause 5.2 of [10]. The commissioned token would be used by the ACME client to provide the CA proof of ownership in the pre-established trust scheme.

### 5.X.2 Security Threats

Without client certificate automation, there is no mTLS. Without mTLS an adversary with possession of network communications can spoof client identity to the server. The server cannot validate identity (i.e. simple TLS vs mTLS). This is a risk of spoofing to achieve repudiation of an unauthorised command, information leakage, unauthorised access, escalation of privilege.

A mTLS client with an expired client certificate will be unable to make required API calls for smooth operations of the 5G core. This is a risk of denial of service by accidental expiry.

An adversary on the same network as the SBI can spoof a client if a server does not validate the client certificate.

An adversary with a runtime image on the same network as another NF can spoof a client NF on the SBI and obtain unauthorised access via subscription to API publications or make API calls to change configurations.

In the case where clarification of mutually exclusive CAs is not provided, the following threats are possible:

* Use of core SBI certificate to spoof identity to a management host.
* Use of core SBI certificate to spoof identity to a gNB or ng-eNB on N2.
* Use of 5G-AN N2 certificate to spoof identity to a management host.
* Use of 5G-AN N2 certificate to spoof the identity of one MOCN member element to another.
* Use of 5G-AN N2 certificate to spoof the identity for unauthorised access to a PLMN’s core SBI.
* Use of 5G-AN N2 keys to spoof the identity of one MOCN member element to another.
* Use of 5G-AN N2 keys to spoof the identity of an AMF to a management host.
* Use of 5G-AN N2 keys to spoof the identity of one MOCN member to another.
* Use of 5G-AN N2 keys to spoof the identity for unauthorised access to a PLMN’s core SBI.

### 5.X.3 Potential security requirements

Operators should define the client identity as independent of NF service interface identity to have different CAs made authoritative for each independent entity.

Operators should ensure plane separation, such as signalling and OA&M planes extend to the application messaging layer.

Operators should ensure security zone separation on the same plane, for example, within the signalling plane, the AMF’s Namf service based interface, and its N2 interface should each be provided different and independent identities.

Operators should consider mutually exclusive PKI CA for issuing client certificates and server certificates for authorization segmentation.

Operators should consider mutually exclusive PKI CA for issuing certificates to different planes and different security zones within a plane for authorization segmentation.

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