**3GPP TSG-SA3 Meeting #115 *S3-240823-r1***

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

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

**Title: New key issue on Trust Anchors**

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

# 3 Rationale

The 5G System (5GS) has embraced a Service-Based Architecture (SBA) featuring self-contained, independently deployable entities that communicate seamlessly through well-defined APIs. As 5G evolves to incorporate automated certificate management, trust anchors take center stage in fortifying the foundation of secure communication. Trust anchors assume a critical function in safeguarding data and infrastructure, mitigating risks associated with unauthorized access, data tampering, and insecure communication, among other security concerns. The automation of certificate management is further complemented by the speed at which the certificate life cycle is completed, i.e., speed at which certificates are issued, revoked, renewed.

The adoption of the Automated Certificate Management Environment (ACME) [1] for the SBA can significantly enhance the 5GS. ACME and 5G SBA can be integrated to leverage root certificates in the trust store as trust anchors during the certificate validation process. The trust anchor ensures the integrity of all certificates issued by a Certificate Authority (CA) and/or supports the inclusion of multiple CAs as trust anchors providing a robust foundation for the secure operation of the 5GS system.

# 4 Detailed proposal

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

## 5.X Key issue #X: Initial Trust and Trust Anchors

### 5.X.1 Key issue details

For automated certificate management in SBA, ACME requires mechanisms for establishing initial trust of a Certificate Authority (CA) [1]. There are 3 practical models for trust anchor establishment that 5GC can leverage. They are described as follows:

1. Use the WebPKI's Common CA Database (CCADB) (cccadb.org) as the basis for inclusion and sync with it at least every 6 months.

2. Use private hierarchies and federation among members of the ecosystem to securely establish trustworthy certificates.

3. A hybrid system that allows both public and private hierarchies.

3GPP may highly benefit from private hierarchies to run a private CA infrastructure for signing issuing intermediates for validated ecosystem participants or to designate an entity to fulfill that role.

As defined in [2], the protection of the NF certificate enrolment procedure has the prerequisite to build initial trust between the 5GC NF and the operator CA/RA. There are three options for OAM to facilitate the initial trust establishment between NF and operator CA/RA . The initial trust can be implemented by 1) OAM issued certificates, 2) an Initial Authentication Key (IAK), or 3) OAM issued signature of certain NF profile parameters, at least including the NF instance ID.

Trust stores need to be actively maintained to remain useful. An outdated trust store will contain expired anchors and miss new ones which may cause chain validation failures for trustworthy certificates or worse, fail to prevent the use of revoked CAs due to distrusted anchors not being removed in a timely fashion.

### 5.X.2 Security Threats

Various security threats can emerge in the absence of a trust anchor in a 5G SBA and ACME that may compromise integrity, confidentiality, and reliability of the network. Malicious entities may attempt to obtain certificates through fraudulent means, leading to unauthorized access and potential exploitation of the infrastructure. There is an increased security risk such as certificate tampering and forgery, insecure certificate renewals, identity spoofing and unauthorized certificate issuance in the absence of a trust anchor.

### 5.X.3 Potential security requirements

To support ACME in the 5GC SBA, security procedures and mechanisms for establishing initial trust of a CA is required for the following use case models:

1. WebPKI’s CCADB as the basis for inclusion and sync
2. Private CA hierarchies and federation
3. Hybrid public and private CA hierarchies
4. OAM trust establishment options

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