**3GPP TSG-SA3 Meeting #113 draft\_S3-23xxxx-r1**

**Chicago, US, 6 – 10 November 2023** **(revision of S3ah-230004)**

**Source: Cisco Systems, Google, Mavenir, CableLabs,**

**Charter Communications, AT&T, Microsoft, TELUS, DISH Network, Deutsche Telekom, Johns Hopkins University APL**

**Title: Study of ACME for Automated Certificate Management in SBA**

**Document for: Approval**

**Agenda Item: 6.1**

3GPP™ Work Item Description

Information on Work Items can be found at <http://www.3gpp.org/Work-Items>   
See also the [3GPP Working Procedures](http://www.3gpp.org/specifications-groups/working-procedures), article 39 and the TSG Working Methods in [3GPP TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm)

Title: Study of ACME for Automated Certificate Management in SBA

Acronym: FS\_ACME\_SBA

Unique identifier: xxx

{A number to be provided by MCC at the plenary}

Potential target Release: Rel-19

# 1 Impacts

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Affects: | UICC apps | ME | AN | CN | Others (specify) |
| Yes |  |  |  | x |  |
| No | x | x | x |  |  |
| Don't know |  |  |  |  |  |

# 2 Classification of the Work Item and linked work items

## 2.1 Primary classification

### This work item is a …

|  |  |
| --- | --- |
| x | Study |
|  | Normative – Stage 1 |
|  | Normative – Stage 2 |
|  | Normative – Stage 3 |
|  | Normative – Other\* |

**\* Other = e.g. testing**

## 2.2 Parent Work Item

For a brand-new topic, use “N/A” in the table below. Otherwise indicate the parent Work Item.

|  |  |  |  |
| --- | --- | --- | --- |
| Parent Work / Study Items | | | |
| Acronym | Working Group | Unique ID | Title (as in 3GPP Work Plan) |
| N/A | N/A | N/A | N/A |

### 2.3 Other related Work Items and dependencies

|  |  |  |
| --- | --- | --- |
| Other related Work /Study Items (if any) | | |
| Unique ID | Title | Nature of relationship |
|  |  | {optional free text} |

**Dependency on non-3GPP (draft) specification:**

IETF [RFC 8555](https://www.rfc-editor.org/info/rfc8555): “Automatic Certificate Management Environment (ACME)”

IETF [RFC 8259](https://www.rfc-editor.org/rfc/rfc8259): “The JavaScript Object Notation (JSON) Data Interchange Format”

IETF [RFC 9110](https://www.rfc-editor.org/rfc/rfc9110): “HTTP Semantics”

IETF [RFC 8738](https://www.rfc-editor.org/rfc/rfc8738): “Automated Certificate Management Environment (ACME) IP Identifier Validation Extension”

# 3 Justification

5G Service Based Architecture (SBA) is secured using certificates across the large number of SBA components and corresponding Network Functions (NFs). Virtualization and increased modularity of NFs has resulted in multi-vendor environments becoming more prevalent. It is now common for NFs to come from different vendors and for the cloud native environment in which they run to come from yet another vendor and for all of these to be independent of the Certificate Authority that is authoritative for the certificates used to secure communications. In such deployments, it is impractical to manage certificates manually.

Release 18 work in SA3 defined the use of CMPv2 for automated certificate management for SBA. ACME was defined specifically for automated certificate management may be particularly well suited for some scenarios, especially when considering infrastructure deployment specifics such as NFs deployed on cloud native platforms (e.g., Kubernetes) that have built-in support for ACME. Another important benefit of ACME is automated validation of authority to represent an identifier (i.e., to be authoritative for the resource for which the certificate is issued). This is particularly helpful for multi-vendor environments.

Additional work is required to determine the feasibility and confirm the benefits of the use of ACME in 5G SBA.

# 4 Objective

Identify key issues and define solutions addressed using ACME for automated certificate management in SBA.

Areas of study include:

* Automated certificate management protocol and procedures for certificate life cycle events (i.e., enrolment, renewal, and revocation) within 5G SBA (i.e., to be used by operator CAs and all 5GC NFs including NRF, SCP, SEPP, etc.) and for northbound interfaces for 5G SBA (i.e., to be used by all 5GC NFs comprising northbound interfaces, including NEF N33 and SCEF T8), including the following:
  + ACME transport and request/response messages for 5G SBA use cases
  + ACME certificate profiles for all 5G SBA entities
  + Considerations for 5GC NFs that have dual homing, e.g.,
    - AMF with RAN domain N2 & SBA domain SB
    - VNF with SBI and OA&M plane interfaces
* Mechanisms for establishing initial trust and chain of trust of Certificate Authority hierarchies, including the following:
  + Existing ACME challenge types and if any new challenge types are needed for 3GPP use cases
  + Ability to automate ACME challenge validation
  + Suitability of existing mechanisms when 5G SBA is for standalone NPN (SNPN)
* Interaction of certificate management functionality with the immutability requirements of containerized network functions (CNFs)

Note, certificate management for the external interface of the SEPP is out of scope.

# 5 Expected Output and Time scale

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| New specifications {One line per specification. Create/delete lines as needed} | | | | | |
| Type | TS/TR number | Title | For info  at TSG# | For approval at TSG# | Rapporteur |
| External TR | 33.XXX | 3rd Generation Partnership Project; Technical Specification Group Service and System Aspects WG3; Study of ACME for Automated Certificate Management in SBA (Release 19) | TSG#103 | TSG#104 | TBD |
|  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Impacted existing TS/TR {One line per specification. Create/delete lines as needed} | | | |
| TS/TR No. | Description of change | Target completion plenary# | Remarks |
|  |  |  |  |
|  |  |  |  |

# 6 Work item Rapporteur(s)

TBD

# 7 Work item leadership

SA3

# 8 Aspects that involve other WGs

The result of this study can have impact to CT4 specifications.

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| Cisco Systems |
| Google |
| Mavenir |
| CableLabs |
| Charter Communications |
| AT&T |
| Microsoft |
| TELUS |
| DISH Network |
| Deutsche Telekom |
| Johns Hopkins University APL |