**3GPP TSG-SA3 Meeting #119 draft\_S3-244683-r2**

**Orlando, US, 11 -15 November 2024** **(revision of xx-yyxxxx)**

**Source: Cisco Systems**

**Title: New WID on Automatic Certificate Management Environment (ACME) for the Service Based Architecture (SBA)**

**Document for: Approval**

**Agenda Item: 6**

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: Automatic Certificate Management Environment (ACME) for the Service Based Architecture (SBA)

Acronym: ACME\_SBA

Unique identifier:

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 …

|  |  |
| --- | --- |
|  | Study |
|  | Normative – Stage 1 |
| x | 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) |
| FS\_ACME\_SBA | SA3 | 1020040 | Study of ACME for Automated Certificate Management in SBA |

### 2.3 Other related Work Items and dependencies

|  |  |  |
| --- | --- | --- |
| Other related Work /Study Items (if any) | | |
| Unique ID | Title | Nature of relationship |
|  |  |  |

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

IETF RFC 8555: "Automatic Certificate Management Environment (ACME)".

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

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

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

IETF RFC 9447: "Automated Certificate Management Environment (ACME) Challenges Using an Authority Token".

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

IETF RFC 7519: " JSON Web Token (JWT)".

IETF RFC 9110: "HTTP Semantics".

IETF RFC 7515: "JSON Web Signature (JWS)".

IETF RFC 4122: "Universally Unique IDentifier (UUID) URN Namespace".

IETF RFC 5280: “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”.

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

# 3 Justification

The TR 33.776: "Study on Automatic Certificate Management Environment (ACME) for the Service Based Architecture (SBA)" is concluding. It is proposed to start the normative work as described in this WID. Additional objectives will be added as the conclusions are agreed within the study.

# 4 Objective

The objective of this work item is normative work according to the conclusions from TR 33.776: "Study on Automatic Certificate Management Environment (ACME) for the Service Based Architecture (SBA)", as described in clause 7. This includes the following:

* Describe initial trust framework for asserting the certificate requesting client’s identity before issuing security credential when using ACME.
* Describe how ACME messaging is integrity protected, confidentiality protected, replay protected, and mutually authenticated.
* Describe suitable ACME challenge types for use within the 5GC SBA.
* Describe certificate enrolment, renewal, and revocation procedures when using ACME for 5GC SBA.
* Describe how to use ACME for all 5GC SBA certificates.

The following are general principles applicable to all KIs in TR.776:

* ACME as an alternative protocol to CMPv2 is applicable only to 5G SBA and not applicable for RAN.
* ACME as a protocol to be specified as optional to support and optional to use.
* In normative phase, details can be captured for ACME in the informative Annex of TS 33.310 [3].
* Separate clause can be used for ACME in the TS 33.310 [3].

The following are conclusions for individual KIs.

* KI#3: In the normative phase, solution #1, #2, #3 can be considered as basis for aspects for challenge validation.
* KI#6: It is proposed to adopt Solution #6 on ACME automated revocation of certificates during normative phase. Guidance towards implementation of ACME client-based certificate revocation procedures as part of the certificate lifecycle management will be developed in the form of informative text during the normative phase of this study.

# 5 Expected Output and Time scale

***{If this WID covers both stage 2 and stage 3, clearly indicate the different completion dates.}***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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 |
|  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Impacted existing TS/TR {One line per specification. Create/delete lines as needed} | | | |
| TS/TR No. | Description of change | Target completion plenary# | Remarks |
| TS 33.310 | Enable use of ACME as an option for Automated Certificate Management (ACME) for 5GC Service Based Architecture (SBA) | SA #108 |  |

# 6 Work item Rapporteur(s)

{Mandatory: <FamilyName>, <GivenName>, <Company>, <email address>}

{Optional: <FamilyName>, <GivenName>, <Company>, <email address>: Secondary task(s)}

{The first listed Rapporteur is the work item primary Rapporteur. The role of a Rapporteur is further described in [www.3gpp.org/specifications-groups/delegates-corner/writing-a-new-spec](http://www.3gpp.org/specifications-groups/delegates-corner/writing-a-new-spec). By default, the primary Rapporteur shall ensure the production of the post-completion summary.   
Secondary Rapporteur(s) are possible for specific secondary task(s), such as: "Write the post-completion summary"; "In charge of a specific aspect of the work item (specify which)"; "Rapporteur for a secondary responsible WG (specify which)"}

# 7 Work item leadership

SA WG3

# 8 Aspects that involve other WGs

To be defined according to further conclusions. If any, CT4 for stage 3 work.

# 9 Supporting Individual Members

|  |
| --- |
| Supporting IM name |
| Cisco Systems |
| Johns Hopkins University APL |
| US National Security Agency |
| Charter Communications |
| Google |
| NCSC |
| CableLabs |
| AT&T |
| BT |
| Deutsche Telekom |