|  |
| --- |
| 3GPP TR 33.776 V0.1.0 (2024-02) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study of Automatic Certificate Management Environment (ACME) for the Service Based Architecture (SBA) (Release 19) |
|   |
|  |  |
|  |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. |

|  |
| --- |
|  |
| ***3GPP***Postal address3GPP support office address650 Route des Lucioles - Sophia AntipolisValbonne - FRANCETel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16Internethttp://www.3gpp.org |
| ***Copyright Notification***No part may be reproduced except as authorized by written permission.The copyright and the foregoing restriction extend to reproduction in all media.© 2024, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).All rights reserved.UMTS™ is a Trade Mark of ETSI registered for the benefit of its members3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersLTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational PartnersGSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 4

Introduction 5

1 Scope 6

2 References 6

3 Definitions of terms, symbols and abbreviations 7

3.1 Terms 7

3.2 Symbols 7

3.3 Abbreviations 7

4 Assumptions 7

5 Key issues 7

5.1 Key issue #1: ACME initial trust framework 7

5.1.1 Key issue details 7

5.1.2 Security threats 8

5.1.3 Potential security requirements 8

5.2 Key issue #2: Secure transport of messages 8

5.2.1 Key issue details 8

5.2.2 Security threats 8

5.2.3 Potential security requirements 8

5.3 Key issue #3: Aspects of challenge validation 8

5.3.1 Key issue details 8

5.3.2 Security threats 8

5.3.3 Potential security requirements 8

5.4 Key issue #4: Certificate enrolment 9

5.4.1 Key issue details 9

5.4.2 Security threats 9

5.4.3 Potential security requirements 9

5.5 Key issue #5: Certificate renewal 9

5.5.1 Key issue details 9

5.5.2 Security threats 9

5.5.3 Potential security requirements 9

6 Solutions 9

6.1 Mapping of solutions to key issues 10

6.Y Solution #Y: <Title> 10

6.Y.1 Introduction 10

6.Y.2 Solution details 10

6.Y.3 Evaluation 10

7 Conclusions 10

Annex <X> : Change history 11

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

# Introduction

5G Service Based Architecture (SBA) is secured using X.509 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.

Automated Certificate Management Environment (ACME) [2] was defined specifically for automated certificate management and is particularly well suited for some scenarios. Infrastructure deployment such as NFs deployed on cloud native platforms often have built-in support for ACME, so it is a natural fit. 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 and in cross-carrier scenarios.

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

# 1 Scope

The scope of this document is to identify key issues and study 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.), including the following:

- ACME transport and request/response messages for 5G SBA use cases

- ACME certificate profiles for all 5G SBA entities

- 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:

- Creation, deletion, rotation, revocation and storage of the certificates

- Ability to automate ACME challenge validation

- Suitability of existing mechanisms when 5G SBA is for standalone NPN (SNPN)

- Call flow of the messages exchanged between different entities in the chain of trust.

NOTE: Certificate management for the external interface of the SEPP is out of scope.

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

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

[3] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF) ".

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

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

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

[7] SP-231787: "New Study of ACME for Automated Certificate Management in SBA".

# 3 Definitions of terms, symbols and abbreviations

This clause and its three subclauses are mandatory. The contents shall be shown as "void" if the TS/TR does not define any terms, symbols, or abbreviations.

## 3.1 Terms

For the purposes of the present document, the terms given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

Definition format (Normal)

**<defined term>:** <definition>.

**example:** text used to clarify abstract rules by applying them literally.

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

<symbol> <Explanation>

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

CA Certificate Authority

NPN Non-Public Network

NRF Network Repository Function

SCP Service Communication Proxy

SEPP Security Edge Protection Proxy

SNPN Stand-Alone Non-Public Network

# 4 Assumptions

This clause contains assumptions for the study. If there are no assumptions at the end of the study, the clause will be removed before sending for approval.

# 5 Key issues

Editor’s Note: This clause contains all the key issues identified during the study.

## 5.1 Key issue #1: ACME initial trust framework

### 5.1.1 Key issue details

For automated certificate management in SBA, ACME requires the operator root certificates to be pre-installed and trusted. Solutions should take this into account.

ACME’s initial trust framework for asserting the certificate requesting client’s identity before issuing security credential is to be studied in this key issue.

### 5.1.2 Security threats

Not applicable.

### 5.1.3 Potential security requirements

Not applicable.

## 5.2 Key issue #2: Secure transport of messages

### 5.2.1 Key issue details

The ACME automated certificate management protocol provides procedures and recommendations to support different aspects of the certificate lifecycle [2]. Using ACME for automated certificate management in SBA, would require messages to be integrity protected, confidentiality protected, replay protected, and mutually authenticated.

### 5.2.2 Security threats

Not applicable.

### 5.2.3 Potential security requirements

Not applicable.

## 5.3 Key issue #3: Aspects of challenge validation

### 5.3.1 Key issue details

The objective of this key issue is to identify and evaluate suitable ACME challenge types for use within the 5G SBA. This includes new challenge types to address different NF types, and when challenges are not necessary.

Challenges require the client to have an identifier. The ACME protocol supports the issuance of certificates with domain names, IP addresses, or email address as subject identifiers. More precisely, according to the current ACME protocol specifications [2][4][5][6], the protocol can be used for the following purposes: Issuance of Web PKI certificates attesting to domain name or IP addresses, issuance of Short-Term Automatically Renewed (STAR) X.509 certificates, issuance of certificates for use by email users (S/MIME), issuance of STI (Secure Telephone Identity) certificates, and issuance of end user client and code signing certificates. However, in SBA, the NF instance ID is used as the unique identifier for NF instances. In addition, based on the current provisions of TS 33.310 [3], the use of IP addresses only is not allowed.

As noted, ACME is tailored to automated certificate validation for server-side certificates. ACME challenges suitable for TLS client certificates will require study.

Editor’s note: The requirement to include ACME challenges for other certificate types is FFS

### 5.3.2 Security threats

Not applicable.

### 5.3.3 Potential security requirements

Not applicable.

## 5.4 Key issue #4: Certificate enrolment

### 5.4.1 Key issue details

The ACME automated certificate management protocol provides procedures and identifies solutions to support authentication to the enrolment server CA and secure message protocol to protect ACME message exchanges during the certificate enrolment process against replay and confidentially protection. To address the objectives of this study [7] there is a requirement to identify procedures and solutions to use ACME across the 5GC SBA for different scenarios (e.g., multi-vendor integration) and use cases (e.g., authentication of domain names, HTTPS, mutual TLS authentication). Procedures and solutions for automated certificate enrolment to consider for this key issue include:

- Support for ACME client and authentication

- Certificate signing request (CSR) – content and creation of request

- CSR submission

- Certificate issuance

This KI is to identify ACME certificate enrolment procedures and solutions for different use cases for the 5GC SBA.

### 5.4.2 Security threats

Not applicable.

### 5.4.3 Potential security requirements

Not applicable.

## 5.5 Key issue #5: Certificate renewal

### 5.5.1 Key issue details

The ACME automated certificate management protocol provides procedures and recommendations to support different aspects of the certificate lifecycle [2]. Certificate renewal is the process of issuing a new digital certificate for an existing certificate that needs to be reissued (e.g., when a certificate is about to expire or if the certificate has been compromised). Certificate renewal may be conducted for a variety of other reasons, such as if a certificate needs to be changed or updated due to changes in the NF or network domain. In addition, the certificate that was replaced is revoked to prevent the potential for unauthorized use.

This KI is to identify ACME certificate renewal procedures and solutions in the 5GC SBA. In addition, the certificate expiration period and renewal interval need to be set appropriately against potential security threats while reducing certificate management overhead and associated risk (e.g., certificates expiring prior to being renewed).

### 5.5.2 Security threats

Not applicable.

### 5.5.3 Potential security requirements

Not applicable.

# 6 Solutions

Editor’s Note: This clause contains the proposed solutions addressing the identified key issues.

## 6.1 Mapping of solutions to key issues

Table 6.1-1: Mapping of solutions to key issues

|  |  |  |  |
| --- | --- | --- | --- |
| Solution | KI#1 | KI#2 |  KI#3 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## 6.Y Solution #Y: <Title>

### 6.Y.1 Introduction

Editor’s Note: Each solution should list the key issues being addressed.

### 6.Y.2 Solution details

### 6.Y.3 Evaluation

Editor’s Note: Each solution should motivate how the potential security requirements of the key issues being addressed are fulfilled.

# 7 Conclusions

Editor’s Note: This clause contains the agreed conclusions that will form the basis for any normative work.

Annex <X> :
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2024-02 | SA3#115 | S3-240207 |  |  |  | Skeleton | 0.0.0 |
| 2024-02 | SA3#115 | S3-240982 |  |  |  | Incorporate pCRs that add introduction (S3-240983), scope (S3-240987), and five key issues (S3-240998, S3-240997, S3-240984, S3-240985, S3-240986)  | 0.1.0 |