3GPP TR 33.776 V0.0.0 (2024-02)

Technical Report

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Study of ACME for Automated Certificate Management in SBA
(Release 19)

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

Contents

Foreword

This clause is mandatory; do not alter the text in any way other than to choose between "Specification" and "Report".

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 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.

1 Scope

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

[3] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[4] IETF RFC 7540: "Hypertext Transfer Protocol Version 2 (HTTP/2)".

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

[6] IETF RFC 4210: "Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)".

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].

Intra-SBA: communication between network functions within the SBA.

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].

ACME	Automatic Certificate Management Environment
CA	Certification Authority
NPN	Non Public Network
NRF	Network Repository Function
SBA	Service-Based Architecture
SEPP	Security Edge Protection Proxy
SNPN	Standalone Non Public Network
TLS	Transport Layer Security

4 Assumptions

Editor's Note: This clause contains assumptions for the study.

4.1 Assumption #1: Protection of intra-SBA communication

All network functions (NFs) support mutually authenticated TLS [3] and HTTPS [4]. The identities in the end entity certificates are used for authentication and policy checks. NFs support both server-side and client-side certificates that are compliant with the SBA certificate profile specified in clause 6.1.3c of TS 33.310 [2].

5 Key Issues

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

5.1 Key Issue #1: Initial trust

5.1.1 Key issue details

If ACME [5] is to be used for automated certificate management in SBA, it needs to support mechanisms for establishing initial trust of a Certificate Authority (CA).

5.1.2 Security threats

5.1.3 Potential security requirements

5.2 Key Issue #2: Secure transport of messages

5.2.1 Key issue details

If ACME [5] is to be used for automated certificate management in SBA, ACME messages need to be integrity protected, confidentiality protected, replay protected, and mutually authenticated.

5.2.2 Security threats

5.2.3 Potential security requirements

5.3 Key Issue #3: Certificate enrolment

5.3.1 Key issue details

If ACME [5] is to be used for automated certificate management in SBA, it needs to support procedures for certificate enrolment in SBA (i.e., to be used by operator CAs and all 5GC NFs including NRF, SCP, SEPP, etc.).

5.3.2 Security threats

5.3.3 Potential security requirements

5.4 Key Issue #4: Certificate renewal

5.4.1 Key issue details

If ACME [5] is to be used for automated certificate management in SBA, it needs to support procedures for certificate renewal in SBA (i.e., to be used by operator CAs and all 5GC NFs including NRF, SCP, SEPP, etc.).

5.4.2 Security threats

5.4.3 Potential security requirements

5.5 Key Issue #5: Certificate revocation

5.5.1 Key issue details

If ACME [5] is to be used for automated certificate management in SBA, it needs to support procedures for certificate revocation in SBA (i.e., to be used by operator CAs and all 5GC NFs including NRF, SCP, SEPP, etc.).

5.5.2 Security threats

5.5.3 Potential security requirements

5.6 Key Issue #6: Message profiling

5.6.1 Key issue details

If ACME [5] is to be used for automated certificate management in SBA, ACME requests and response messages need to be profiled.

5.6.2 Security threats

5.6.3 Potential security requirements

5.7 Key Issue #7: Certificate profiling

5.7.1 Key issue details

If ACME [5] is to be used for automated certificate management in SBA, certificates for use with ACME need to be profiled. Ideally, the same certificates can be used independent of the certificate management protocol.

5.7.2 Security threats

5.7.3 Potential security requirements

5.8 Key Issue #8: Challenge types

5.8.1 Key issue details

ACME [5] supports multiple challenge types. These need to be investigated for suitability for SBA use cases, with one or more existing challenge types being identified as being sufficient, or new challenge types being defined.

5.8.2 Security threats

5.8.3 Potential security requirements

5.9 Key Issue #9: Challenge validation

5.9.1 Key issue details

Automated validation of authority to represent an identifier (i.e., to be authoritative for the resource for which the certificate is issued) is an important aspect of ACME. Challenge validation mechanisms need to be defined for challenge types identified for use in SBA.

5.9.2 Security threats

5.9.3 Potential security requirements

5.10 Key Issue #10: Protocol selection

5.10.1 Key issue details

Standardizing support for ACME as an option for certificate management in SBA would introduce the need for CAs and NFs to determine which of the standard protocols to use. There needs to be a mechanism for making this selection.

5.10.2 Security threats

A mismatch in support or use of certificate management protocol may result in an inability of NFs to obtain and use valid certificates as necessary to secure intra-SBA communications.

5.10.3 Potential security requirements

NF instances needs a way to determine an appropriate certificate management protocol to use to obtain and use valid certificates within a given deployment.

5.11 Key Issue #11: Mechanisms for SNPNs

5.11.1 Key issue details

SNPNs, and NPNs in general, may not include all the components or support all the mechanisms typically included in a 5GS. If ACME [5] is to be used for automated certificate management in SBA, it needs to be determined if the mechanisms it provides are sufficient in the presence of SNPNs.

5.11.2 Security threats

5.11.3 Potential security requirements

6 Solutions

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

6.Y Solution #Y: <Solution Name>

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> (informative): Change history

Use style "Heading 8" in TSs and "Heading 9" in TRs. Do not use "informative" in the title in TRs.

This is the last annex for TS/TSs which details the change history using the following table.
This table is to be used for recording progress during the WG drafting process till TSG approval of this TS/TR.
For TRs under change control, use one line per approved Change Request
Date: use format YYYY-MM
CR: four digits, leading zeros as necessary
Rev: blank, or number (max two digits)
Cat: use one of the letters A, B, C, D, F
Subject/Comment: for TSs under change control, include full text of the subject field of the Change Request cover
New vers: use format [n]n.[n]n.[n]n

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**