

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>

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.

© 2023, 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 members
3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners
LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners
GSM® 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	6
3.1 Terms	6
3.2 Symbols	7
3.3 Abbreviations	7
4 Assumptions	7
5 Key issues	7
5.X Key issue #X: <Title>	7
5.X.1 Key issue details	7
5.X.2 Security threats	7
5.X.3 Potential security requirements	7
6 Solutions	7
6.1 Mapping of solutions to key issues	8
6.Y Solution #Y: <Title>	8
6.Y.1 Introduction	8
6.Y.2 Solution details	8
6.Y.3 Evaluation	8
7 Conclusions	8
Annex <X>: Change history	9

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".

...

[x] <doctype> <#>[([up to and including]{yyyy[-mm]}V<a[.b[.c]]>[onwards])]: "<Title>".

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].

Abbreviation format (EW)

<ABBREVIATION> <Expansion>

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.X Key issue #X: <Title>

5.X.1 Key issue details

5.X.2 Security threats

5.X.3 Potential security requirements

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

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

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