|  |
| --- |
| 3GPP TR 33.876 V0.1.0 (2022-02) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on Automated Certificate Management in SBA;(Release 18) |
|   |
| *5G-logo_175px* | 3GPP-logo_web |
|  |
| 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.© 2021, 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 3

Introduction 4

1 Scope 6

2 References 6

3 Definitions of terms, symbols and abbreviations 6

3.1 Terms 6

3.2 Symbols 6

3.3 Abbreviations 7

4 Architectural and security assumptions 7

5 Key issues 7

5.X Key Issue #X: <Key Issue Name> 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.Y Solution #Y: <Solution Name> 7

6.Y.1 Introduction 7

6.Y.2 Solution details 7

6.Y.3 Evaluation 7

7 Conclusions 7

Annex A (informative): Change history 9

# 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

Editor’s Note: This clause contains some background information for the study.

According to TS 33.501, the use of mutual TLS for authentication of NF requires compliance to 3GPP TS33.310 section 6.1.3c for TLS client and TLS server certificate profiles, in addition to TLS profile compliance with clause 6.2 of TS 33.210 with the restriction that it shall be compliant with the profile given by HTTP/2 as defined in RFC 7540.

The use of TLS certificates in 5G SBA is ubiquitous. Also, as per section 9.9 of TS33.501, certificate based NDS/IP is to be used for protection of non-SBI interfaces. E.g., N4, N9.

However, unlike standardised model using CMPv2 in RAN, SBA does not have a standardised model and set of procedures for automated certificate management. SBA does not currently have either a standardised protocol for managing life cycle events of the certificates. e.g., bootstrap, request, issue, enrolment, revocation, renewal etc.

Lack of standardisation has resulted into number of bespoke methodologies and varying choices of certificate management protocols resulting into inconsistent model. In addition, once service slicing and NPN are introduced in service provider network, manual management or lack of standardised procedures for life cycle management of TLS certificates belonging to separate legal entities could further complicate the architecture.

All the above have potential of increasing the security risk and impact the deployment and availability of operators’ 5G SBA network.

RAN has benefitted from the standardisation of CMPv2 to be used for eNodeB/gNodeB automated certificate management. The specification defined a bootstrap procedure based on the use of vendor certificate for requesting an operator certificates for the set-up of IPSec IKE2 towards the SeGW. 5G SBA is within the operator core network domain that could benefit from a study that leads to the standardisation of an automated certificate management procedure using a standardised protocol that fits for purpose to serve the 5G Core Network.

# 1 Scope

Editor’s Note: This clause contains scope for the study.

The objectives of this study are to identify key issues, potential security and privacy requirements and solutions with respect to

* Standardise the use of a single automated certificate management protocol and procedures for certificate life cycle events within intra-PLMN 5G SBA (i.e. to be used by all 5GC NFs including NRF, SCP, SEPP etc.)
* Study which lifecycle events (e.g. enrolment, renewal, revocation) of a certificate need to be covered.
* Study to reference at minimum following principles:
1. Principle to be reusable when 5G SBA is for NPN (standalone and PNI)
2. Principles standardised to be able to support NFs doing mTLS in Slicing
3. Principles involving ‘Chain of Trust’ of Certificate Authorities
4. Principles for security of CA’s cryptographic private key

# 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

## 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].

**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> <Expansion>

# 4 Architectural and security assumptions

Editor's note: This clause includes the architectural and security assumptions applicable for the study.

# 5 Key issues

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

## 5.X Key Issue #X: <Key Issue Name>

### 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.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 A (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2022-02 | SA3#106-e |  |  |  |  | TR Skeleton | 0.0.0 |
| 2022-02 | SA3#106e | S3-220504 |  |  |  | Adding Introduction and Scope sections | 0.1.0 |