|  |
| --- |
| 3GPP TR 33.794 V0.0.1 (2024-02) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on enablers for Zero Trust Security(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 6

3.1 Terms 6

3.2 Symbols 6

3.3 Abbreviations 6

4 Security Assumptions 6

5 Security Analysis and Considerations 7

5.1 Use cases for security evaluation and monitoring 7

5.1.X Use case #X: <Use case Name> 7

5.1.X.1 Description 7

5.1.X.2 Relevant data 7

5.2 Evaluation of the identified data 7

5.3 Security mechanism for dynamic policy enforcement 7

5.3.X Security policy enforcement Use Case #X: <Use case Name> 7

5.3.X.1 Description 7

5.3.X.2 Scope of dynamic security policy enforcement 7

6 Key issues 7

6.X Key Issue #X: <Key Issue Name> 8

6.X.1 Key issue details 8

6.X.2 Security threats 8

6.X.3 Potential security requirements 8

7 Solutions 8

7.Y Solution #Y: <Solution Name> 8

7.Y.1 Introduction 8

7.Y.2 Solution details 8

7.Y.3 Evaluation 8

8 Conclusions 8

Annex <X> (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.

# 1 Scope

Editor’s Note: This clause describes the scope for the study based on the agreed objectives in the study proposal.

The present document …

# 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 Security Assumptions

Editor’s Note: This clause contains security assumptions to be considered for the study (e.g., per work task).

# 5 Security Analysis and Considerations

This clause contains security analysis and considerations as applicable for each of the work tasks.

## 5.1 Use cases for security evaluation and monitoring

Editor’s Note: [For WT1] This clause covers the security analysis to identify potential threat(s) and attack(s) on 5G SBA layer intended to identify which data may be relevant for threats and attack detection.

### 5.1.X Use case #X: <Use case Name>

#### 5.1.X.1 Description

Editor’s Note: This clause covers the details on the potential threat/attack traces on the SBA layer, along with the impacts. The impacts are the risk if security evaluation and monitoring is not performed in the above scenario.

#### 5.1.X.2 Relevant data

Editor’s Note: This clause identifies and lists the relevant data and parameters that could aid in security evaluation and monitoring for this particular scenario.

## 5.2 Evaluation of the identified data

Editor's Note: This clause describes the necessary actions on such data (exposure, notification, logging, etc.) identified in Clause 5.1 and an analysis of the security implications if any.

## 5.3 Security mechanism for dynamic policy enforcement

Editor’s Note: [For WT2] This clause covers the security analysis to identify use cases/scenarios in SBA, where a potential threat/attack can be controlled with dynamic security policy enforcement.

### 5.3.X Security policy enforcement Use Case #X: <Use case Name>

#### 5.3.X.1 Description

Editor’s Note: This clause describes the details about the threat scenario in Core network SBA that can benefit with results from operator’s security function (e.g., in case of attack identification (or) based on nature of the results) specific to the scenario identified in clause 5.1

#### 5.3.X.2 Scope of dynamic security policy enforcement

Editor’s Note: This clause provides the details on how dynamic security policy enforcement can control the potential attack/threat and it’s impacts in the identified scenario.

# 6 Key issues

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

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

### 6.X.1 Key issue details

### 6.X.2 Security threats

### 6.X.3 Potential security requirements

# 7 Solutions

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

## 7.Y Solution #Y: <Solution Name>

### 7.Y.1 Introduction

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

### 7.Y.2 Solution details

### 7.Y.3 Evaluation

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

# 8 Conclusions

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

Annex <X> (informative):
Change history

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