|  |
| --- |
| 3GPP TS 33.502 V0.1.0 (2025-08) |
| Technical Specification |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Security related Events Handling(Release 20) |
|   |
|  |  |
|  |
| 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 16Internethttps://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.© 2025, 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

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 Overview of Security related Events handling 6

5 Security related events requirements 7

5.1 General Requirements 7

5.2 Requirements on events storage 7

5.3 Requirements on configuration for events detection and delivery 7

5.4 Requirements on delivery of detected events 8

6 Security related Events 8

7 Protection of Security related events 8

Annex <A> (normative): <Normative annex for a Technical Specification> 9

Annex <B> (informative): <Informative annex for a Technical Specification> 10

Annex <C> (informative): Change history 11

# Foreword

This Technical Specification 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.

# 1 Scope

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".

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms given in 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 TR 21.905 [1].

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

## 3.2 Symbols

Void.

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 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 TR 21.905 [1].

# 4 Overview of Security related Events handling

Editor’s Note: This clause addresses the architectural view of the feature

The Service Based Architecture (SBA) is the dominant method for control plane as well as the Service Based Management Architecture (SBMA) is for management communications. In addition to the many benefits of using SBA, e.g. agility to increase and decrease the number of service instances in coordination with demand, potential attacks may still appear for network, service and/or APIs.

The 5G system includes heterogeneous and varied Network Functions (NF) deployments, where each and every Network Function has a specified behaviour according to 3GPP specifications. If any NF runs into errors, e.g. a violation of the normal behaviour, or abnormal access or unauthorised request, then the NF needs to be evaluated from security perspective. Collection of data related to abnormal events needs to be performed for the evaluation of the NF behaviour, with related data being transmitted towards a security entity that will execute the evaluation.

The following figure shows an example of trust domains in the overall architecture for the collection and transmission of the Security related Events detected by NFs.



Figure 4-1 Example of trust domains in the Security related Events Handling architecture

Editor’s Note: this figure is for information purposes to illustrate the requirement work. It will be revisited further once the requirements get agreed.

NOTE 1: The definition of the trust domains is to be established by the PLMN-operator.

NOTE 2: The Security related Events Collecting entity is under operator control (e.g. through business agreements, policy, managed service, directly managed, etc) and it is out of the scope of 3GPP.

NOTE 3: Whether the security collecting entity is the same as the management entity is an operator decision.

# 5 Security related events requirements

Editor’s Note: This clause addresses the general requirements to secure the procedures to configure, collect and deliver security related events.

## 5.1 General Requirements

The NFs in the 5G system shall support the generation of security related events.

## 5.2 Requirements on events storage

Security related events data shall be securely stored with confidentiality and integrity protection.

Access to security related events data shall be authorized.

## 5.3 Requirements on configuration for events detection and delivery

The 5G system shall support the capability to configure the NFs.

Editor’s Note: The detailed set of information elements and reporting type to include for configuration is for further discussion.

The 5G system shall support mutual authentication between the 5GC NF (for configuration/activation of the functionality) and the Management Entity in charge of the configuration/activation of the events.

The 5G system shall support authorization to the Management Entity in charge of the configuration/activation of the events.

The 5G system shall support integrity protection, replay protection and confidentiality protection for communication between the 5GC NF and the Management Entity in charge of the configuration/activation of the events.

Editor’s Note: Separation of the configuration for security related events from other management related configurations is for further discussion.

Editor’s Note: These requirements and whether additional requirements are needed is FFS.

## 5.4 Requirements on delivery of detected events

The delivery of security related events shall be protected against unauthorized parties. Mutual authentication shall be supported between the end entities of such a delivery.

The delivery of security related events shall be confidentiality, integrity and replay protected.

The delivery of the security related events should be separate from other 5G system traffic.

Editor’s Note: How this separation is done is for FFS.

Editor’s Note: How to deliver the security events is to be defined by SA5 and/or CT groups.

# 6 Security related Events

Editor’s Note: This clause addresses the list and description of the events as well as naming convention for the events.

# 7 Protection of Security related events

Editor’s Note: This clause addresses the protection for the configuration, collection and delivery of events.

Annex <A> (normative):
<Normative annex for a Technical Specification>

Annex <B> (informative):
<Informative annex for a Technical Specification>

Annex <C> (informative):
Change history

|  |
| --- |
| Change history |
| Date | Meeting | TDoc | CR | Rev | Cat | Subject/Comment | New version |
| 08/2025 | SA3#123 | S3-252547 |  |  |  | Initial draft | 0.0.1 |
| 08/2025 | SA3#123 | S3-252991 |  |  |  | Includes agreed tdocs S3-252547, S3-252992, S3-252993, S3-252994 and S3-252995 | 0.1.0 |