|  |  |
| --- | --- |
| 3GPP TR 33.866 V0.1.0 (2020-10) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on security aspects of enablers for Network Automation (eNA) for the 5G system (5GS) Phase 2;  (Release 17) | |
|  | |
| *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 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.  © 2020, 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

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 eNA 6

5 Key issues 7

5.1 Key issues related to securing the data provided to any type of analytics function 7

5.1.1 Key Issue #1.1: Cyber-attacks Detection supported by NWDAF 7

5.1.1.1 Key issue details 7

5.1.1.2 Security threats 7

5.1.1.3 Potential security requirements 7

5.2 Key issues related to detection of cyber-attacks and anomaly events by analytics function 7

5.2.X Key Issue #2.X: <Key Issue Name> 8

5.2.X.1 Key issue details 8

5.2.X.2 Security threats 8

5.2.X.3 Potential security requirements 8

5.3 Key issues related to data transfer protection 8

5.3.1 Key Issue #3.1: Privacy preservation for transmitted data between multiple NWDAF instances 8

5.3.1.1 Key issue details 8

5.3.1.2 Security threats 8

5.3.1.3 Potential security requirements 8

6 Solutions 8

6.0 Mapping of Solutions to Key Issues 8

6.Y Solution #Y: <Solution Name> 9

6.Y.1 Introduction 9

6.Y.2 Solution details 9

6.Y.3 Evaluation 9

7 Conclusions 9

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.

# 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".

[2] 3GPP TR 23.700-91: " Study on enablers for network automation for the 5G System (5GS); Phase 2".

# 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 Overview of eNA

Editor’s Note: This clause will contain a brief overview on eNA based on SA2’s study (TR 23.700-91), including architectural assumptions, etc.

# 5 Key issues

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

## 5.1 Key issues related to securing the data provided to any type of analytics function

Editor’s Note: This clause is for key issues on UE data collection protection to fulfil the NWDAF functionalities including privacy consideration, data authenticity, data integrity, accessibility aspects requirements, according to the first objective of the SID.

## 5.1.X Key Issue #1.X: <Key Issue Name>

### 5.1.X.1 Key issue details

### 5.1.X.2 Security threats

### 5.1.X.3 Potential security requirements

## 5.2 Key issues related to detection of cyber-attacks and anomaly events by analytics function

Editor’s Note: This clause is for key issues on detection of cyber-attacks and anomaly events supported by NWDAF and its related functions, specifically to define parameters provided by UE to help detect attacks and abnormal behaviours, according to the second objective of the SID.

## 5.2.1 Key Issue #2.1: Cyber-attacks Detection supported by NWDAF

### 5.2.1.1 Key issue details

NWDAF has been defined to offer automatic network analytics and alarming, with possible capabilities of artificial intelligence and machine learning to help proactively manage the 5G network. TR 23.700-91[2] has identified the use case of NWDAF detecting cyber-attacks by monitoring events and data packets in the UE and the network, with support of machine-learning algorithms. To achieve cyber-attacks detection, the NWDAF can collaborate with UE and any other NFs to collect related data as inputs, afterwards providing alerts of anomaly events as outputs to OAM and other NFs which have subscribed to them so that they could take proper actions.

This key issue describes what kind of cyber-attacks can be detected by NWDAF. In order to mitigate the identified cyber attacks, the data/parameters collected by NWDAF need to be studied.

The specific cyber attacks include but are not limited to the following examples:

**(1) MitM attacks on the radio interface:** MitM attacks or fraudent relay nodes may modify or change messages between the UE and the RAN, resulting in failures of higher layer protocols such as NAS or the primary authentication. The NWDAF may detect MitM attacks.

**(2) DoS attacks:** 5G has high performance requirements for system capacity and data rate, improved capacity and higher data rate may lead to much higher processing capability cost for network entities, which may make some network entities (e.g. RAN, Core Network Entities) to suffer from DDoS attack. The NWDAF may also enable the detection of DDoS attacks.

### 5.2.1.2 Security threats

Cyber attacks or anomaly events may not be detected by the 5G network, thus further attacks could be conducted.

### 5.2.1.3 Potential security requirements

TBD

## 5.3 Key issues related to data transfer protection

Editor’s Note: This clause is for key issues on protection of data transferring (e.g. privacy consideration) in the inter-NWDAF/NWDAF instances, according to the third objective of the SID.

## 5.3.1 Key Issue #3.1: Privacy preservation for transmitted data between multiple NWDAF instances

### 5.3.1.1 Key issue details

In the case of Multiple NWDAF Instances, during the transfer of data/metadata/analytics output, it needs to be ensured that the privacy of the user is preserved.

It needs to be ensured that appropriate measures are taken by the sender NWDAF to protect any information which can hamper the privacy of the user, such as positioning information, user profile information, etc, before sending it to the other NWDAF instance.

### 5.3.1.2 Security threats

Information that can reveal the identity of the user can compromise privacy when transmitted unprotected.

If personal identifiable information related data is transferred without adequate mesaures, it provides a threat against user privacy and possibly against regulations on data protection.

Editor's note: Description of the attacker model is FFS.

### 5.3.1.3 Potential security requirements

TBD

# 6 Solutions

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

## 6.0 Mapping of Solutions to Key Issues

Table 6.0-1: Mapping of Solutions to Key Issues

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Solutions | Key Issues | | | | | | | | |
| 1 Key issues related to securing the data provided to any type of analytics function | | | 2 Key issues related to detection of cyber-attacks and anomaly events by analytics function | | | 3 Key issues related to data transfer protection | | |
|  | 1.1 | 1.2 | 1.X | 2.1 | 2.2 | 2.Y | 3.1 | 3.2 | 3.Z |
| #1: <Solution name> | X |  |  |  |  |  |  |  |  |
| #X: <Solution name> | X |  |  |  |  |  |  |  |  |

## 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** |
| 2020-10 | SA3#100bis-e | S3-202767 |  |  |  | S3-202674, S3-202766，S3-202425 | 0.1.0 |