|  |
| --- |
| 3GPP TR 33.866 V0.3.0 (2021-01) |
| 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 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.© 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 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 7

3.1 Terms 7

3.2 Symbols 7

3.3 Abbreviations 7

4 Overview of eNA 7

5 Key issues 7

5.1 Key issues related to securing the data provided to any type of analytics function 8

5.1.1 Key Issue #1.1: Key issue on integrity protection of data transferred between AF and NWDAF 8

5.1.1.1 Key issue details 8

5.1.1.2 Security Threats 8

5.1.1.3 Potential Requirements 8

5.1.2 Key Issue #1.2: Processing of tampered data 8

5.1.2.1 Key issue details 8

5.1.2.2 Security threats 8

5.1.2.3 Potential security requirements 9

5.2 Key issues related to detection of cyber-attacks and anomaly events by analytics function 9

5.2.1 Key Issue #2.1: Cyber-attacks detection supported by NWDAF 9

5.2.1.1 Key issue details 9

5.2.1.2 Security threats 10

5.2.1.3 Potential security requirements 10

5.2.2 Key Issue #2.2: Anomalous NF behaviour detection by NWDAF 10

5.2.2.1 Key issue details 10

5.2.2.2 Security threats 10

5.2.2.3 Potential security requirements 10

5.3 Key issues related to data transfer protection 10

5.3.1 Key Issue #3.1: Privacy preservation for transmitted data between multiple NWDAF instances 10

5.3.1.1 Key issue details 10

5.3.1.2 Security threats 10

5.3.1.3 Potential security requirements 10

6 Solutions 11

6.0 Mapping of Solutions to Key Issues 11

6.Y Solution #Y: <Solution Name> 11

6.Y.1 Introduction 11

6.Y.2 Solution details 11

6.Y.3 Evaluation 11

7 Conclusions 11

Annex A (informative): Change history 11

# 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 will study the security aspects of enablers for network automation for the 5G system based on the outcome of TR 23.700-91 [1]. More specifically, this study will identify security issues, requirements and corresponding potential security solutions related to the following objectives:

- UE data collection protection to fulfil the NWDAF functionalities including privacy consideration, data authenticity, data integrity, and accessibility aspects requirements.

- 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;

- Protection of data transferring (e.g. privacy consideration) in the inter-NWDAF/NWDAF instances.

NOTE: The user consent for UE data collection is not addressed in the present document, it will be discussed in TR 33.867 [2].

Editor's Note: This study is not complete until the user consent aspects in TR 33.867 that are applicable to eNA are finalized. How TR 33.867 conducts the user consent study (in a general way applicable to eNA or including specific aspects of eNA) will be discussed and addressed in the FS\_UC3S.

# 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 23.700-91: "Study on enablers for network automation for the 5G System (5GS); Phase 2".

[2] 3GPP TS 33.867: "Study on user consent for 3GPP services".

[3] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[4] 3GPP TS 23.288: "Architecture enhancements for 5G System (5GS) to support network data analytics services ".

[5] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

[6] Draft NISTIR 8269: "A Taxonomy and Terminology of Adversarial Machine Learning"; <https://doi.org/10.6028/NIST.IR.8269-draft>

[7] ETSI SAI: "AI Threat Ontology"; <https://docbox.etsi.org/ISG/SAI/70-DRAFT/001/SAI-001v008.docx>.

[x] 3GPP TR 28.809: "Study on enhancement of management data analytics".

# 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 [3] 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 [3].

**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 [3] 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 [3].

eNA enablers for Network Automation

NWDAF Network Data Analytics Function

# 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.

3GPP TS 23.288 [4] provides the Stage 2 architecture enhancements for 5G System (5GS) to support network data analytics services in 5G Core network, which forms the baseline for the present study on security aspects of enablers for Network Automation (eNA) for the 5G system (5GS).

The Network Data Analytics Function (NWDAF) as specified in 3GPP TS 23.501 [5] interacts with different entities within 5GS for data collection based on subscription to events, retrieval of information from data repositories, retrieval of information about NFs (e.g. from NRF for NF-related information) and on demand provision of analytics to consumers. The NWDAF provides analytics to 5GC NFs and OAM. Analytics information are either statistical information of the past events, or predictive information.

3GPP TR 23.700-91 [1] is an architectural study on enhancements for analytics and NWDAF, for which any security impact will be documented in the present document. This is in particular security impact for UE data collection protection, detection of cyber-attacks and anomaly events supported by NWDAF and its related functions, on protection of data transferring in the inter-NWDAF/NWDAF instances.

# 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.

### 5.1.1 Key Issue #1.1: Key issue on integrity protection of data transferred between AF and NWDAF

#### 5.1.1.1 Key issue details

The 5GS supports the collection and utilisation of data provided by the UE in NWDAF in order to provide input information to generate analytics information (to be consumed by other NFs).

As per KI#8 in TR 23.700-91 [1], there is no direct interface between the UE and the NWDAF. When AF is used for the communication between the NWDAF and UE for data collection, there is a need to study the security aspects for the data provided by the UE to NWDAF via AF and vice versa.

This key issue studies the integrity aspects on data collection and utilization of UE data in order to derive the analytics.

#### 5.1.1.2 Security Threats

If the data shared between new interface (i.e. between AF and NWDAF) is not secured, it may lead to following issues:

- Data can be modified and replayed by any unauthorized parties.

#### 5.1.1.3 Potential Requirements

Integrity and replay protection shall be supported on the new interface between AF and NWDAF.

### 5.1.2 Key Issue #1.2: Processing of tampered data

#### 5.1.2.1 Key issue details

5GS is using ML to an increasing extend. NWDAF (TS 23.288 [4]) in 5GC and MDAS (TR 28.809 [x]) on OAM are two centralized frameworks currently responsible for ML-based analytics, e.g. abnormal behavior analytics. Furthermore, AI/ML is decentralized used in several use cases, such as efficiency optimization in RAN. Furthermore, a new data collection framework DCCF (clause 6.9, TR 23.700-91 [1]) is proposed for Rel-17.

Network data analytics is including the following steps:

* Request of analytics by consumer
* Collection of data by analytics function
* Processing of collected data by analytics function
* Reply analytics output to consumer by analytics function

While 3GPP provides sound security on network level, the data used by AI/ML is not being subject to security controls. This key issue seeks solutions countering a number of attacks against a 5GS involving tampered data.

#### 5.1.2.2 Security threats

Editor's Note: Threats need to be revisited if in line with NIST 8269 [6] and ETSI SAI [7] terminology.

Data used by AI/ML is not being subject to security controls. This allows for a number of attacks against a 5GS with severe impact on performance up to denial of service (DoS) conditions:

* **Adversarial examples** are generated by slightly perturbating input data. The data is perturbated in a space in which AI/ML algorithms are sensitive to change, leading to severe performance degradation and misclassifications in the inference process. This attack is well-known in human-centric use cases, such as image/audio classification.
* During training, tampered training data can lead to **model skewing**. Skewed models will provide false results in inference.
* Tampered data may also lead **information disclosure** by the inference of confidential/proprietary AI/ML algorithms.
* In more **simple attacks**, perturbations may not be slight (as those generated by adversarial example methods). In non-human-centric use cases (as most are in 5GS), the perturbations may just be false data to force misinterpretation.

Unprotected analytic functions are subject to:

* Decreased efficiency, e.g. power consumption, load balancing, QoS optimization
* System failure (DoS scenario)
* Inference of confidential ML algorithms employed by 5GS
* Leakage of privacy-related data derived from AI/ML models

#### 5.1.2.3 Potential security requirements

TBD

## 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. 3GPP TR 23.700-91[1] 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 for which an analytics function may provide detection support include but are not limited to the following examples:

**(1) MitM attacks on the radio interface:** MitM attacks or fraudulent 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-attack may not be detected by the 5G network, thus further attacks could be conducted.

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

#### 5.2.1.3 Potential security requirements

The 5GS system shall support the operators in the detection of cyber-attacks by providing related inputs or collecting output analytics using an analytics function such as NWDAF.

Editor's Notes: The requirement may be updated according to SA2's feedback.

### 5.2.2 Key Issue #2.2: Anomalous NF behaviour detection by NWDAF

#### 5.2.2.1 Key issue details

TBD

#### 5.2.2.2 Security threats

TBD

#### 5.2.2.3 Potential security requirements

It should be possible for the network to detect anomalous NFs using the data collected from UE and NFs.

## 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 reveal the privacy of the user, such as positioning information, user profile information etc., before sending privacy related data to another NWDAF instance. Privacy related information that has been allowed by the User for analysis should not be transferred without sufficient protection mechanism.

#### 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 measures, 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

Any information which can reveal the identity of the user, such as positioning information, user profile information, etc, should be securely protected before data is being shared or transferred to other NWDAF Instances.

# 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 |
|  |  |  |  |  |  |  |  |  |  |
| #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 |
| 2020-11 | SA3#101-e | S3-203463 |  |  |  | S3-203450, S3-203353, S3-203367, S3-203359, S3-203449, S3-203277, S3-203370, S3-203363, S3-203473 | 0.2.0 |
|  |  |  |  |  |  |  |  |