|  |
| --- |
| 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>.

[8] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[9] 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].

AF Application Function

DoS Denial of Service

DDoS Distributed Denial of Service

eNA enablers for Network Automation

MDAS Management Data Analytics Service

MitM Man in the Middle

ML Machine Learning

NWDAF Network Data Analytics Function

OAM Operation, Administration and Maintenance

# 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:Integrity protection of data transferred between AF and NWDAF

### 5.1.1.1 Key issue details

The 5GS supports the collection and utilisation of the UE data and provide it to the NWDAF as an input to generate the analytic information (to be consumed by other NF).

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 AF and NWDAF is not secured, it may lead to following issue;

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 interface between AF and NWDAF for the UE data collection.

### 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 [9]) 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

A 5GS analytics function shall be protected from processing unsanitized or tampered data.

### 5.1.3 Key Issue #1.3: Authorization of NF Service Consumers for data access via DCCF

#### 5.1.3.1 Key issue details

A Data Collection Coordination Function (DCCF) is used to coordinate collection of data from one or more NF(s) based on data collection requests from one or more Consumer NF(s). DCCF and Data Repository Function (DRF) can be standalone NFs, possibly co-located with NWDAF, or can be hosted by NWDAF. Data Collection notification to one or more Consumer NF(s) may be supported via a Messaging Framework. Adaptors supporting 3GPP services allow NFs to interact with the Messaging Framework. Only the interface between 3GPP entities and the adaptors is under 3GPP scope. This includes 3GPP services offered by adaptors to allow NFs to interact with the Messaging Framework.

TR 23.700-91-100 conclusion mentions that "Additional authorization for Consumers to access data from a Data Source via the DCCF and to access data from DRF (directly or via DCCF) needs to be coordinated with SA3". According to SA2 KI#11 conclusions, if a consumer subscribes to analytics notifications to the DCCF, the DCCF can subscribe itself to the data source and notify the data source that notifications are directly to be sent to the consumer. The data source will then send notifications to the consumer via the MF or via the DCCF.

This key issue addresses the authorization aspects of the DCCF being allowed to subscribe the data on behalf of the consumer at the data source or the DRF, i.e. the security aspect on usage subscription/notification mechanisms for a consumer to receive notifications on a different path (as adapted in SA2 conclusions) will be studied.

#### 5.1.3.2 Security threats

DCCF introduces a new path for a NF Service Consumer (NFc) to access the data from data sources or a NF Service Producer (NFp). Due to the introduction of DCCF between consumer and producer, the existing security mechanism will not be sufficient, and the following threats needs to be addressed:

Based on a request from a DCCF, the Messaging Framework may provide data from a producer to a requesting data consumer, even though the consumer is not authorized to receive this data.

Based on a request from a DCCF data received from a data producer is stored in the DRF. When the data are later retrieved, the DCCF may provide the stored data to a non-authorized consumer if requested.

The data producer may be unable to correctly verify the identity of the data consumer since the data request is coming from DCCF on behalf of the consumer.

#### 5.1.3.3 Potential security requirements

TBD

### 5.1.4 Key Issue #1.4: Security protection of data via Messaging Framework

#### 5.1.4.1 Key issue details

In [1], in the conclusions for the Key Issue #11 ‘Increasing efficiency of data collection’, DCCF (Data Collection Coordination Function) is defined for efficient data collection in 5GS. The DCCF is a control-plane function that coordinates data collection and triggers data delivery to Data Consumers.

TR 23.700-91 [1] lists several agreed principles for normative work, some of which are as follows:

- "When a Data Collection Coordination Functionality (DCCF) is deployed, it is used to coordinate collection of data from one or more NF(s) based on data collection requests from one or more Consumer NF(s)."

- "Data Collection notification to one or more Consumer NF(s) may be supported via a Messaging Framework. Adaptors supporting 3GPP services allow NFs to interact with the Messaging Framework.

NOTE 2: The Messaging Framework is outside the scope of 3GPP. Adaptors are not expected to be standardized by 3GPP, only the interface between 3GPP entities and the adaptors is under 3GPP scope. This includes 3GPP services offered by adaptors to allow NFs to interact with the Messaging Framework."

- "The DCCF coordinates data collection so the same data is not requested multiple times from the same data source."

The Messaging Framework is not expected to be standardized by 3GPP. It contains Messaging Infrastructure that propagates event information and data (e.g.: streaming and notifications) from data sources to data consumers.

In TR 23.700-91 [1], the Figure 6.9.3-1: "Data Collection & Distribution for Event Notifications (Subscribe/Notify)" shows how the data can be transferred via Messaging Framework from data sources to data consumer.

Since the Messaging Framework is not expected to be standardized by 3GPP, it may not be trusted.

As concluded in clause 8 in TR 23.900-71[1], Data Collection Coordination Function (DCCF) and Data Repository Function (DRF) and the related interfaces (interfaces between 3GPP entities and the adaptors) are to be standardized.

The DCCF and the Messaging Framework decouple the data collection between the data consumer and the data source; however, this may induce a security problem because the data consumer cannot verify that the data from the data source is not modified by the Messaging Framework and the confidentiality of the data cannot be guaranteed by the Messaging Framework.

#### 5.1.4.2 Threats

An attacker may eavesdrop or manipulate or replay the communication or initiate the MitM attacks on the interface.

If the integrity of the data collected from the data source is not protected, then the Messaging Framework may modify the data, which results in producing wrong analytics.

If the confidentiality of the data collected from the data source is not protected, then the Messaging Framework may access the sensitive data, which may cause privacy leakage.

Replay attacks may lead to usage of same data more than once, and therefore, it may cause wrong analytic results.

#### 5.1.4.3 Potential security requirements

The transfer of the data between data source and data consumer via the messaging framework shall be confidentiality, integrity and replay protected end-to-end between data source and data consumer.

Confidentiality protection, integrity protection and replay-protection shall be supported on the new interfaces between 3GPP entities and the adaptors.

## 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

The 5GC supports different NF deployments that could be in distributed or redundant fashion so that the NF provides the services from several locations and several execution instances. When these NFs are distributed across multiple cloud infrastructures, it is possible that the NFs may behave in an undefined manner. The undefined behaviour of the NF may be caused by internal errors such as configuration mistakes or internal data corruption. This misbehaviour may impact one or more UE services based on the type of NF. Thus, the correlation of which NF is handling which UE data is an important aspect, such that NWDF is enabled to conclude from UE related data reported, which NF may have anomalous behaviour.

In all such instances, it is imperative that an analytics function such as NWDAF monitors the behaviour of all the NFs and ensures that the NFs behave as defined. If the NFs behave erroneously, it should be possible to detect the anomaly so that appropriate steps can be taken, e.g. by an operator, to control the potentially damaging behaviour.

Note, it is up to the operator to define the details of what NFs should report if such monitoring and detection by NWDAF is wished. However, there is a need to enable NWDAFs to receive or request reports by NFs which serve the detection of anomalous NF behaviour.

#### 5.2.2.2 Security threats

Different NFs may behave in an undefined manner. Anomalous or malicious NF behaviour could be, for instance, to try to access NF/NF service which was not authorized to a NF as NF/NF service consumer, to consume lots of resource for NF as either NF/NF service consumer or producer, to trigger DoS attack on NF service producer by continuously sending some malicious message, e.g. ill http request, etc., to try to exhaust connections of http server.

This can be either due to internal data corruption, configuration errors, or due to cross communication between NFs from different vendors. Based on the NF type, such NFs could cause damage to either one or multiple UEs. For example, in case of an AMF or SMF dedicated to a network slice, the service for all UEs within the whole network slice could be affected. Even the whole network slice could get out of service.

An erroneous NF may succeed in knocking the whole network out of service by sending wrong messages to other NFs, causing other NFs to get out of service.

The NFs within the 5GC are already authenticated and communicate with each other based on the authentication and authorization. If the NF is misconfigured or has internal data corruption, etc, the assumption of trust becomes invalid and causes potential threats.

#### 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.

NOTE: By this requirement it is only assured that specific data can be collected by and/or reported to an analytics function. Which AI/ML is used is implementation specific and out of scope in 3GPP.

## 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.

### 5.3.2 Key Issue #3.2: Protection of UE data in transit

#### 5.3.2.1 Key issue details

The UE is providing the core network functions with data, which are reported to or requested by analytics functions. The transfer of any data between core network functions needs to be protected.

According to TS 23.288 [y] the NWDAF collects data from various data sources and provides Analytics Output to different NWDAF data consumers. In addition, according to the solutions for KI#2 "Multiple NWDAF Instances" proposed in TR 23.700-91 [x] the analytics data or the analytics output can be transferred from one NWDAF instance to another NWDAF instance.

Data in transit needs to be protected while in transfer between NWDAFs, NF to NWDAFs and NWDAF to another entity, e.g. DCCF.

This key issue addresses security for data in transit involving an analytics function.

#### 5.3.2.2 Security Threats

If data is transferred between NFs or different NWDAF Instances, a MitM (for instance a malicious SCP) can compromise data by eavesdropping or modification.

A rogue NWDAF Instance can send wrong or modified data to another NWDAF instance.

#### 5.3.2.3 Potential security requirements

Data transferred between core network functions shall be integrity, confidentiality and replay protected.

# 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 | 1.3 | 1.4 | 1.X | 2.1 | 2.2 | 2.Y | 3.1 | 3.2 | 3.Z |
| #1: UE data collection protection |  |  |  |  | X |  |  |  |  |  |  |
| #2: Network Analysis Framework for DDoS Attack |  |  |  |  |  | X |  |  |  |  |  |
| #3: Usage of current SBA mechanisms to protect data in transit |  |  |  |  |  |  |  |  |  | X |  |
| #X: <Solution name> |  |  |  |  |  |  |  |  |  |  |  |

## 6.1 Solution #1: UE data collection protection

### 6.1.1 Introduction

This solution addresses KI#1.X on UE data collection protection at NF/NWDAF

### 6.1.2 Solution details

For enhancing the 5GS to support 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) the communication between UE and NF/NWDAF needs to be secured.

In line with 5GS generic security requirements it is therefore proposed that the transfer of data between UE and NF/NWDAF related to UE data collection re-uses existing 5GS security mechanisms.

For UE data collection by NFs and NWDAF, the current NAS and AS security mechanisms for authentication, confidentiality, integrity and replay protection as described in 3GPP TS 33.501 are used.

NOTE: Whether user consent is necessary is subject of the user consent study FS\_UC3S.

For transfer of UE data to NF/NWDAF privacy requirements could apply.

### 6.1.3 Evaluation

TBD

## 6.2 Solution #2: Network Analysis Framework for DDoS Attack

### 6.2.1 Introduction

The solution addresses key issue #2.1: Cyber-attacks Detection supported by NWDAF.

### 6.2.2 Solution details

#### 6.2.2.1 Introduction

As depicted in clause 6.7.5 in TS 23.288 [4], the NWDAF could collect the following input data:

* Exceptions information from AF, including: IP address 5-tuple, exception ID, exception level, and exception trend.
* UE mobility information from OAM is UE location carried in MDT data.
* Network data related to UE mobility from AMF, including: UE ID, UE location, Timestamp, TAC, frequent mobility registration update.
* Service data related to UE mobility provided by AF, including: UE ID, Application ID, UE location, Timestamp.
* Service data related to UE communication provided by SMF, AF, UPF, including: UE ID, group ID, S-NSSAI, DNN, Application ID, Expected UE behaviour parameters, communication description per application (e.g. communication start, communication stop, UL data rate, DL data rate, traffic volume), TAC.

The NWDAF could output the following: Exception ID, Exception Level, Exception trend, UE characteristics, SUPI list (1..SUPImax), Ratio, Amount, Additional measurement, Confidence.

Specifically, exception ID can be “Suspicion of DDoS attack” means that the UE may trigger a DDoS attack. In this case, Additional measurement is “Victim's address (target IP address list)”. And the mitigation can be “PCF may request SMF to release the PDU session. SMF may release the PDU session and apply SM back-off timer.”

However, the analysis is just for DDoS attack to external AF.

DDoS attack to internal NF, e.g. RAN, Core Network should also be investigated. In order to make it more clear to capture the DDoS analysis, it is proposed a network analysis framework for DDoS attack.

#### 6.2.2.2 Network Analysis Framework for DDoS attack

The framework is depicted in table 6.2.2.2-1. In column DDoS attack, target network entity and attack method shall be clarified. In column analysis, input, output and mitigation are listed as the same way as TS 23.288 [4]. With the framework, it will be more clear how to capture attack and how to detect the DDoS attack.

Table 6.2.2.2-1 Network Analysis Framework for DDoS attack.

|  |  |
| --- | --- |
| DDoS Attack | Analysis |
| Target | Method | Input | Output | Mitigation |
| AF | DDoS using heavy UP traffic | AF: GPSI, external group ID, Exception information (IP address 5-tuple, exception ID, exception level, and exception trend), Application ID, communication description per application (communication start, communication stop, UL data rate, DL data rate, traffic volume), Expected UE Behaviour parametersSMF: SUPI, internal group ID, Application IDUPF: UE communication description per application (communication start, communication stop, UL data rate, DL data rate, traffic volume)AMF: TAC | DDoS to AF | PCF may request SMF to release the PDU session.SMF may release the PDU session and apply SM back-off timer. |
| TBA | TBA | TBA | TBA | TBA |

### 6.2.3 Evaluation

TBA

## 6.3 Solution #3: Usage of current SBA mechanisms to protect data in transit

### 6.3.1 Introduction

This solution addresses KI#3.2 on protection of data in transfer.

### 6.3.2 Solution details

Any data transferred between core network functions is protected by SBA mechanisms as described in clause 13.3 and clause 13.4 of 3GPP TS 33.501 [8] for authentication and authorization of NF Service Consumer and NF Service Producer.

According to 3GPP TS 33.501 [8], clause 13.3.0, all network functions shall support mutually authenticated TLS and HTTPS. TLS shall be used for transport protection within a PLMN unless network security is provided by other means. Thus, communication between NFs is integrity, confidentiality and replay protected.

By using an access token issued by NRF, NFs are authorized for requesting analytics from an analytics function or providing analytics data to the analytics function.

Editor's Note: End-to-end integrity and confidentiality protection is FSS.

Editor's Note: Whether the user consent of data sharing between NFs is mandatory is FFS.

### 6.3.3 Evaluation

TBD

# 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 |
| 2021-01 | SA3#102-e | S3-210681 |  |  |  | S3-210569, S3-210570, S3-210581, S3-210115, S3-210571, S3-210446, S3-210109, S3-210110, S3-210572, S3-210229, S3-210573, S3-210574,S3-210679 | 0.3.0 |