|  |  |
| --- | --- |
| 3GPP TR 33.738 V0.1.0 (2022-05) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on security aspects of enablers for Network Automation for 5G - phase 3;  (Release 18) | |
|  | |
| *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.  © 2021, 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 3

Introduction 4

1 Scope 5

2 References 5

3 Definitions of terms, symbols and abbreviations 5

3.1 Terms 5

3.2 Symbols 5

3.3 Abbreviations 5

4 Architectural assumptions 5

5 Key issues 6

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

5.X.1 Key issue details 6

5.X.2 Security threats 6

5.X.3 Potential security requirements 6

6 Solutions 6

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

6.Y.1 Introduction 6

6.Y.2 Solution details 6

6.Y.3 Evaluation 6

7 Conclusions 6

Annex A (informative): Change history 7

# 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 studies the security aspects of enablers for network automation for the 5G system based on the outcome of TR 23.700-81 [6]. More specifically, this document will identify security issues and requirements and provide corresponding security solutions related to the following scenarios:

- Security aspects of potential architecture enhancement: roaming, supporting federated learning, interaction between NWDAF and MDAS/MDAF, etc.

- Handling of sensitive information inherent to application detection, roaming and location information.

- KIs from R17 which don’t have enough time to proceed, e.g. NWDAF detection related issues.

- Any further security enhancements which need to be studied based upon the ongoing SA2 eNA Phase 3 work

# 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 TS 23.501: "System Architecture for the 5G System; Stage 2".

[3] 3GPP TS 23.502: "Procedures for the 5G system, Stage 2".

[4] 3GPP TS 23.503: "Policy and Charging Control Framework for the 5G System".

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

[6] 3GPP TR 23.700-81: " Study of Enablers for Network Automation for 5G System (5GS); Phase 3".

[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 Overview

The architecture for the present study shall be based on the existing NWDAF framework as specified in TS 23.288 [5], TS 23.501 [2], TS 23.502 [3] and TS 23.503 [4].

Solutions shall comply with the 5G System architectural principles in TS 23.501 [2], and network data analytics principles in TS 23.288 [5].

TR 23.700-81 [6] is an enhanced study on eNA Phase 3, for which any security impact will be documented in the present document.

# 5 Key issues

## 5.1 Key Issue #1: Protection of data and analytics exchange in roaming case

### 5.1.1 Key issue details

As per Key Issue #3 in TR 23.700-81 [6], the HPLMN/VPLMN may need to collect data or consume analytics from the VPLMN/HPLMN in roaming scenario. The data or analytics may relate to particular UEs or contain information about all UEs or groups of UEs. Both PLMNs (VPLMN, HPLMN) need the ability to control the amount of data exposed and to abstract or hide network-internal aspects based on operator policy, regulatory constraints and/or roaming agreements.

As there might be possible architecture enhancements to support this exchange in roaming scenarios and of any necessary enhancements to related NFs in HPLMN and VPLMN. This key issue studies the security aspects of data and analytics exchange in roaming case should be considered.

### 5.1.2 Security threats

If the communication between PLMNs is not confidentiality protected, then sensitive information may be leaked to unauthorized entities.

If the integrity of the data exchanged between PLMNs is not protected, the data may be modified.

If the PLMNs don’t have the ability to control the amount of data exposed and to abstract or hide network-internal aspects, the sensitive data may be leaked to other entities.

If exchanged data has not been adequately protected before it is shared between PLMNs, it may be subject to be leaked and abused.

### 5.1.3 Potential security requirements

5GS shall support confidentiality, integrity, and replay protection for data and analytics exchange between PLMNs.

5GS shall be able to control the amount of exposed data and to abstract or hide internal network aspects based on operator policy, regulatory constraints and/or roaming agreements.

Based on the sensitivity of the data, 5GS shall provide confidentiality protection while at rest to certain data based on policies.

NOTE: The user consent for UE data collection is not addressed in the present document.

## 5.2 Key Issue #2: Authorization of selection of participant NWDAF instances in the Federated Learning group

### 5.2.1 Key issue details

3GPP SA2 studies the architecture enhancement to support Federated Learning which allows the cooperation of multiple NWDAFs containing MTLF to train an ML model in 3GPP network. As per KI#8 in TR 23.700-81[6], it will involve selection of participant NWDAF instances in the Federated Learning group.

This key issue studies the authorization aspect of including participant NWDAF instances in the Federated Learning group.

### 5.2.2 Security threats

If a Federated Learning group can include a NWDAF without being authorized by the NWDAF, it may lead to the following issues:

- NWDAF(MTLF)’s resource may be used up by being included into many unauthorizd Federated Learning groups.

- Sensitive data may be used to train unauthorizd Federated Learning group’s ML model.

- Unauthorized Federated Learning group may utilize the local model received from NWDAF(MTLF) to infer sensitive training data details.

### 5.2.3 Potential security requirements

Authorization of selection of participant NWDAF instances in the Federated Learning group should be supported. A Federated Learning group should not be able to select participant NWDAF instances without NWDAF's authorization.

## 5.3 Key Issue #3: Security for AI/ML model storage and sharing

### 5.3.1 Issue details

AI/ML model is shared among NWDAFs and/or NFs (i.e., NWDAF to NWDAF, ADRF to NWDAF…). In different scenarios, the NF producer of AI/ML model can store that model in ADRF, NWDAF or other entity.

ADRF (Analytical Data Repository Function) is being enhanced to store AI/ML models to facilitate the distribution and sharing of those models amongst NFs. Since AI/ML models and their algorithms are generally proprietary (i.e., subject to intellectual property rights of the designer), it is imperative to ensure that only the NFs which have been indeed provided with access authorization to the AI/ML models can read and use those models. Moreover, the ADRF itself cannot be considered as a fully trusted entity storing the sensitive AI/ML data models. Those models are indeed exposed at rest in ADRF.

The current authorization scheme defined by 3GPP for SBA works only at service level or resource/operation-level scope. This authorization granularity may be not sufficient in the AI/ML model sharing scenario, since the ADRF (Analytical Data Repository Function) or NWDAF, or any other network function which may store the AI/ML model, cannot verify whether the NF consumer is authorized to retrieve the AI/ML model.

### 5.3.2 Security Threats

An unauthorized NFc, in principle which is not eligible to retrieve a particular model stored by a NFp, could have access to the storage entity and retrieve the model.

If there is no protection against accessing and reading an AI/ML model from the ADRF stored by NFp, a compromised ADRF may expose algorithms and sensitive data to a non-authorized entity which can easily misuse it and/or distributed further to other entities, causing a bigger data security breach.

### 5.3.3 Potential security requirements

AI/ML models shall be protected between the entity which produces the ML model or stores the ML model in ADRF (e.g., NWDAF containing MtLF, NFp) and the entity which consumes the model (NFc).

ADRF (Analytical Data Repository Function), or any other network function which may store the AI/ML model, shall be able to authorize the NFc to retrieve that AI/ML model

NF Service consumers shall be authorized to access to the AI/ML models in the ADRF (or any other NF which may store the ML model, for instance NWDAF MtLF).

## 5.4 Key Issue #4: Anomalous NF behaviour detection by NWDAF

### 5.4.1 Issue details

The 5GC supports different NF deployments that could be in distributed or redundant fashion, so that the NFs provides the services from several locations and several execution instances. When these NFs are distributed across diverse 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 the NF.

In those circumstances, it is imperative that an analytics function such as NWDAF supports the monitoring of the behaviour of all NFs and ensures that the NFs behave as defined/specified. 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.

### 5.4.2 Security Threats

Different NFs may behave in an undefined manner. Anomalous NF behaviour could include among others, failed attemps to access NF/NF services which was not authorized to a NF as NF/NF service consumer, unusual high consumption of network or compute resources by a particular NF/NF service (consumer or producer), continuous sending of compromised messages to particular NF service producer (DoS), numerous attempts to exhaust connections of a HTTP server, etc.

The above examples of anomalous behaviour can occur due to internal data corruption, configuration errors, communication between NFs from different vendors (i.e., incompatibility issues), etc. Based on the NF type, such behaviour could cause damage to one or multiple UEs. For example, in the 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 complete network slice could get out of service.

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

The NFs within the 5GC are already authenticated and allowed to communicate with each other based on successful authentication and authorization. If the NF is misconfigured or its internal data is corrupted or has other reason for anomalous behaviour, the assumption of trust on that NF becomes invalid, even if previously authenticated and authorized, and may cause potential threats and exploits.

### 5.4.3 Potential security requirements

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

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

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

### 5.X.1 Key issue details

### 5.X.2 Security threats

### 5.X.3 Potential security requirements

# 6 Solutions

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

## 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** |
| 2022-05 | SA3#107-e | S3-220771 |  |  |  | TR Skeleton | 0.0.0 |
| 2022-05 | SA3#107-e | S3-221279 |  |  |  | S3-220772, S3-220773, S3-221269, S3-221176, S3-221221, S3-221222 | 0.1.0 |