|  |
| --- |
| 3GPP TR 33.898 V0.4.0 (2023-01) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on Security and Privacy of AI/ML-based Services and Applications in 5G;(Release 18) |
|   |
|  | 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.© 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 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 3

1 Scope 6

2 References 6

3 Definitions of terms, symbols and abbreviations 6

3.1 Terms 6

3.2 Symbols 7

3.3 Abbreviations 7

4 Key issues 7

4.1 KI #1: Privacy and authorization for 5GC assistance information exposure to AF 7

4.1.1 Key issue details 7

4.1.2 Security threats 7

4.1.3 Potential security requirements 7

5 Solutions 7

5.1 Solution #1: Reusing existing mechanism for authorization of 5GC assistance information exposure to AF 8

5.1.1 Introduction 8

5.1.2 Solution details 8

5.1.3 Evaluation 8

5.2 Solution #2: UE profile based 5GC assistance information exposure authorization 8

5.2.1 Introduction 8

5.2.2 Solution details 8

5.2.3 Evaluation 9

5.3 Solution #3: Reusing existing authorization mechanism for internal or external AF 9

5.3.1 Introduction 9

5.3.2 Solution details 9

5.3.3 Evaluation 10

5.4 Solution #4: Authorization for 5GC assistance information exposure to external AF 10

5.4.1 Introduction 10

5.4.2 Solution details 10

5.4.3 Evaluation 11

5.5 Solution #5: Authorization for 5GC assistance information exposure to internal AF 11

5.5.1 Introduction 11

5.5.2 Solution details 11

5.5.3 Evaluation 12

5.6 Solution #6: New solution to privacy protection for 5GC assistance information exposure to AF 12

5.6.1 Solution overview 12

5.6.2 Solution details 12

5.6.3 Evaluation 14

5.Y Solution #Y: <Solution Name> 14

5.Y.1 Introduction 14

5.Y.2 Solution details 14

5.Y.3 Evaluation 14

6 Conclusions 14

**Annex A:** **Classification and protection of AI/ML data transmitted between 5GC and AF** 14

A.1 General 14

Annex B (informative): Change history 18

# 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

This Technical Report will study, based on requirements as specified in clauses 6.40 and 7.10 of TS 22.261 [2] and architecture and key issues captured in TR 23.700-80 [3], 5GS assistance to support Artificial Intelligence (AI) / Machine Learning (ML) model distribution, transfer, training for various applications, e.g. video/speech recognition, robot control, automotive, etc.

The scope of this study is on how to provide security and privacy to the AI/ML-based service and applications in 5G based on the following objectives of identifying key issues, potential threats, requirements, and solutions to enable:

1. 5G system assistance for the security management which requires data transmission support for application layer AI/ML operation over the 5G system

2. The authentication and authorization involving data collection and sharing among UE, AF and the network to take part in application layer AI/ML operation, i.e., UE and network privacy protections to support application AI/ML services over 5G system.

3. UE and 5G system to secure AI/ML based services and operations.

4. Secure provisioning of the external parameter required for AI/ML (e.g., expected UE activity behaviors, expected UE mobility, etc.)

# 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 22.261: "Service requirements for the 5G system; Stage 1".

[3] 3GPP TR 23.700-80: “Study on 5G System Support for AI/ML-based Services”.

[4] 3GPP TS 33.501 "Security architecture and procedures for 5G system".

…

[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 Key issues

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

## 4.1 KI #1: Privacy and authorization for 5GC assistance information exposure to AF

### 4.1.1 Key issue details

As per KI#3 in SA2 AIML TR 23-700-80[3]studies the exposure of different types of assistance information such as traffic rate, packet delay, packet loss rate, network condition changes, candidate FL members, geographical distribution information etc.. to AF for AI / ML operations. Some of assistance information could be user privacy sensitive, such as candidate FL members, geographical distribution information etc. In some cases a single piece of information alone would not be considered as privacy-sensitive, but the combination of that piece of information along with other seeming unrelated privacy data could potentially reveal user privacy There is a need to study how to protect such privacy-related assistance information. In addition, 5GC needs to determine which assistance information is required by AF to complete AI/ML operation and to avoid exposing information that is unnecessary for AI/ML operations.

This Key Issue is related to objective #2, and aims at studying what assistance information is related to user privacy, how 5GC protects these privacy-sensitive information, and how 5GC authorizes AF to access such assistance information.

### 4.1.2 Security threats

Without proper privacy protection mechanism, UE’s privacy information may be leaked resulting in loss of user privacy.

Unauthorized access of 5GC assistance information by AF can lead to misuse and user privacy leakage.

### 4.1.3 Potential security requirements

5GC shall support the protection of user privacy sensitive assistance information being exposed to AF.

5GC shall support authorization of AF for accessing assistance information.

# 5 Solutions

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

## 5.1 Solution #1: Reusing existing mechanism for authorization of 5GC assistance information exposure to AF

### 5.1.1 Introduction

This solution addresses key issue#1 on authorization for 5GC assistance information exposure to AF. It is proposed to reuse existing mechanism for authorization of 5GC assistance information exposure to AF.

### 5.1.2 Solution details

5GC assistance information exposure to external AF in the data network is authorized by reusing the OAuth-based authorization mechanism as depicted in clause 12.4 in TS 33.501 [4]. If CAPIF is used, authorization method for 5GC assistance information exposure to AF defined in clause12.5 in TS 33.501 [4] is reused.

### 5.1.3 Evaluation

TBA

## 5.2 Solution #2: UE profile based 5GC assistance information exposure authorization

### 5.2.1 Introduction

This solution addresses KI #1.

In this solution, UE privacy profile/local policies are employed to authorize UE-related 5GC assistance information exposure.

UE privacy profile/local policies may also contain protection policies that indicate how 5GC assistance information should be protected (e.g., encryption, integrity protection, etc).

### 5.2.2 Solution details



Figure 5.2.2-1: UE profile based 5GC assistance information exposure authorization.

0. The UE privacy profile is stored in the UDM/UDR. For each UE, the UE privacy profile determines whether the specific AF can request or modify specific information of a specific UE. UE profile includes UE identity (e.g., SUPI, SUCI, IMPI, Application layer ID of UE, GPSI), expected service identifier, data type of target 5GC assistance information (e.g., location information), granularity of target 5GC assistance information type (e.g., TAI for location information), expiration time (expiration), authorization policies (e.g., specific UE related 5GC assistance information can be handled by a specific service.), protection policies (e.g., a specific UE related 5GC assistance information needs to be encrypted before sharing to AFs).

1. AF sends 5GC assistance information request to the NEF/NWDAF. The request includes the AF identity (e.g., AF\_ID, Application layer ID, FQDN), expected service identifier, data type of target 5GC assistance information (e.g., location information), details of target 5GC assistance information (e.g., TAI), target UE identity (e.g., IMPI, Application layer ID of UE, GPSI).

2. Upon receiving the request, NEF/NWDAF identifies the UE privacy profile according to the target UE identity. If NEF/NWDAF does not contain the UE privacy profile, NEF/NWDAF obtain the profile from UDM/UDR.

NEF/NWDAF leverages the local policies/UE profile to check if the UE authorizes the AF to access the UE-related 5GC assistance information.

3. NEF/NWDAF sends the UE-related 5GC assistance information to AF when the local policies/UE privacy profile authorize the AF to access the information. According to the local policies/UE privacy profiles, NEF/NWDAF may need to protect the 5GC assistance information with security mechanisms.

### 5.2.3 Evaluation

Editor’s Note: Each solution should motivate how the potential security requirements of the key issues being addressed are fulfilled.

TBA

## 5.3 Solution #3: Reusing existing authorization mechanism for internal or external AF

### 5.3.1 Introduction

This solution addresses the Key issue #1 “Privacy and authorization for 5GC assistance information exposure to AF”. It is proposed to reuse the existing authorization mechanism for internal AF or external AF requesting 5G assistance information.

### 5.3.2 Solution details

For the AI/ML AF that is internal to the operator’s network, the OAuth 2.0 based authorization of NF service access as specified in clause 13.4 of TS 33.501[4] can be reused for 5G assistance information exposure.

For the AI/ML AF that is external to the operator’s network, the NEF authorizes the external AF’s service request using OAuth-based authorization mechanism as specified in clause 12.4 of TS 33.501 [4]. If NEF supports CAPIF for external exposure, the CAPIF authorization mechanism specified in clause 6.5 of TS 33.122 [y] can be reused.

### 5.3.3 Evaluation

TBD.

## 5.4 Solution #4: Authorization for 5GC assistance information exposure to external AF

### 5.4.1 Introduction

This solution addresses the Key issue #1 “Privacy and authorization for 5GC assistance information exposure to AF”. It is proposed to reuse the existing service authorization mechanism for AF that is external to the operator’s network.

### 5.4.2 Solution details



**Figure 5.4.2-1:** **Authorization for 5GC assistance information exposure to external AF**

Step 1. The AF discovers and selects its serving NEF that supports its target AI/ML Service.

Step 2. A PDU Session between the UE and the AF may have been established.

Step 3. AF requests the AI/ML service by sending NEF service request.

Step 4. The NEF authorizes the service request using OAuth-based authorization mechanism as specified in clause 12.4 of TS 33.501 [4]. If NEF supports CAPIF for external exposure, the CAPIF authorization mechanism specified in clause 6.5 of TS 33.122 [y] can be reused.

The NEF determines whether the user consent check is needed based on the service request and operator's local policy, e.g., whether the requested service is to process user's personal information, whether regulation is required, etc. If there is no need to check user consent, steps 5-7 can be skipped.

Step 5. If there is no user consent parameter in the NEF's UE context, the NEF sends the Nudm\_SDM\_Get Request message to the UDM, including the UE ID, and may include purpose of data processing, data processor ID.

Step 6. The UDM returns requested user consent parameters.

Step 7. The NEF is deemed an enforcement point for user consent and checks the user consent reusing the user consent framework defined in Annex V in TS 33.501 [4].

Step 8. Based on the outcome of the AI/ML service procedures, NEF replies to AF with the service response.

### 5.4.3 Evaluation

TBD.

## 5.5 Solution #5: Authorization for 5GC assistance information exposure to internal AF

### 5.5.1 Introduction

This solution addresses the Key issue #1 “Privacy and authorization for 5GC assistance information exposure to AF”. It is proposed to reuse the existing OAuth 2.0 based authorization of NF service access for the AF that is internal to the operator’s network.

### 5.5.2 Solution details



**Figure 5.5.2-1:** **Authorization for 5GC assistance information exposure to internal AF**

Step 1. A PDU Session between the UE and the AF may have been established.

Step 2. The AF requests the AI/ML service by sending Nnrf\_AccessToken\_Get Request to the NRF with the access required parameters, expected NF Service name(s), NF type, AF ID.

Step 3. The NRF authorizes the internal AF service access using OAuth 2.0 based authorization mechanism as specified in clause 13.4 of TS 33.501[4].

Step 4. The AF sends Nnwdaf\_<Service-X> or Nnef\_<Service-Y> Request to the requested NWDAF or NEF with the access token.

Step 5. If there is need to check user consent, the NWDAF/NEF is deemed as an enforcement point. Otherwise, steps 6-8 can be skipped.

Step 6. If there is no user consent parameter in the UE context stored in NWDAF/NEF, the NWDAF/NEF sends the Nudm\_SDM\_Get Request message to the UDM, including the UE ID, and may include purpose of data processing, data processor ID.

Step 7. The UDM returns requested user consent parameters.

Step 8. The NWDAF/NEF checks the user consent reusing the user consent framework defined in Annex V in TS 33.501 [4].

Step 9. The NWDAF/NEF replies to AF with the service response, based on the outcome of the AI/ML service procedures.

### 5.5.3 Evaluation

TBD.

Editor’s Note: The user consent checking for internal AI/ML AF is FFS.

## 5.6 Solution #6: New solution to privacy protection for 5GC assistance information exposure to AF

## 5.6.1 Solution overview

This solution addresses key issue#1 on privacy protection for 5GC assistance information exposure to AF, that is, authorization of sensitive data processing and authorization of AF for accessing assistance information in AI/ML.

### 5.6.2 Solution details

Dual user consent checking in AI/ML scenarios

 

Figure 5.6.2-1: Dual user consent checking procedure

0) The UDM maintains user consent parameters and complies with operator's policy or local regulation for the subscriber. User consent parameters are associated with the user's SUPI and stored in the UDM as subscription data.

 1) The AF sends subscribes assistance information requests to the serving NF. The message may include Application ID.

 NOTE 1: The enforcement point can be located in the same entity with the serving NF, which will be NWDAF if AF is in operator’s trust domain or will be NEF if AF is a 3rd party entity.

 NOTE 2: Application ID, the running instance of the specific AI/ML service. This is because the existing general-purpose servers usually run multiple services at the same time and use the same storage space. For sensitive user privacy data, it should be ensured that only specific services are authorized to use it.

 2) After receiving request for specific assistance information, the enforcement point checks whether user consent is needed for sharing the assistance information and data collection according to local policy, e.g., whether regulation is required, whether it is related to sensitive information of user privacy, etc. If there is no need to check user consent, steps 3-7 can be skipped.

 3) If there is no related user consent parameter in UE context, the enforcement point invokes Nudm\_SDM\_Get Request service to retrieve related user consent parameters. Otherwise, steps 4-5 can be skipped.

 4) The enforcement point sends Nudm\_SDM\_Get Request message to the UDM, the message includes UE ID, and may include purpose of data processing and Application ID.

 5) The UDM returns requested user consent parameters, which includes user consent result.

6) The enforcement point stores the user consent parameters in the UE context and determines whether to authorize the sharing the assistance information and data collection request or not according to the user consent parameters. If the user consent result is authorized, go to step 8, if it is not authorised, go to step 7.

7) If the user consent result of sharing the assistance information and data collection is not allowed, the enforcement point rejects the AF's request with specific cause.

8) Provider NFs start to collect the requested data based on the authorized consent.

9) The NWDAF returns the assistance information to AF.

### 5.6.3 Evaluation

TBA

Editor's Note: The enforcement point and procedures for user consent check is FFS.

Editor's Note: Avoiding multiple enforcement point is FFS.

NOTE 3: The user consent checking needs to be coordinated with the R18 SID of user consent.

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

### 5.Y.1 Introduction

Editor’s Note: Each solution should list the key issues being addressed.

### 5.Y.2 Solution details

### 5.Y.3 Evaluation

Editor’s Note: Each solution should motivate how the potential security requirements of the key issues being addressed are fulfilled.

# 6 Conclusions

Editor’s Note: This clause contains the agreed conclusions that will form the basis for any normative work.

# **Annex A:** **Classification and protection of AI/ML data transmitted between 5GC and AF**

## A.1 General

According to TR23700-80, different AI/ML data needs to be transmitted among 5GC and AF to facilitate various application AI/ML operations. Exposing this data may cause different impact on network or user depending on the nature and purpose of the data. Some may be considered user privacy-sensitive, such as data analytics (e.g., QoS sustainable analytics) may help to determine sensitive information such as subscription location and exposing these data analytics to an unauthorized AF will cause serious privacy breach issue. Some of the data (e.g., NF load analytics) is related to the state of network, and attackers may use it to perform serious attacks, such as DoS attack or lead legitimate UE to believe the incorrect state of the network (e.g., network is busy when in fact it is not) on the network side. Some of the other data (e.g., RSRP) may not be related to security and privacy and exposing them may have little or no impact to the security of the network. Since the data exchanged among 5GC and AF are essential for 5GC to provide the necessary assistance for the application AI/ML operations and not all data requires the same type of protection, it is beneficial to categorize the different type of data so that the appropriate protection scheme can be applied.

Table 1 below lists various data based on the Solutions from TR 23.700-80 among 5GC and AF from the perspective of privacy and security

| **Data Source** | **Data Type** | **Detailed Data** | **Solution from SA2** | **Data Flow** |
| --- | --- | --- | --- | --- |
| UE-related data | * UE Status
 | * Network authorization status of the UE
 | #33 | 5GC->AF |
| * UE connectivity state（AMF）
 | #23,#39 | 5GC->AF |
| * UE reachability status(AMF)
 | #23、#39、#40 | 5GC->AF |
| * UE mobility analytics(NWDAF)
 | #8、#19、#22、#23、#25、#27、#39 | 5GC->AF |
| * UE abnormal behaviour(NWDAF)
 | #23、#27、#39 | 5GC->AF |
| * Radio link quality (RSRP)
 | #6 | 5GC collects |
| * UE location
 | * TAI(AMF)
 | #6 | 5GC collects |
| 5GC-related data | * Training assistant

Information | * Geographical distribution information for the candidate members(NWDAF)
 | #6 | 5GC->AF |
| * Expected number of iterations(NWDAF)
 | #6 | 5GC->AF |
| * Time duration: Start time and end time(NWADF)"
 | #6 | 5GC->AF |
| * Time interval for each iteration(NWADF)
 | #6 | 5GC->AF |
| * Candidate members' expected latency performance given per iteration(NWADF)
 | #6 | 5GC->AF |
| * Candidate members' expected latency performance given aggregated and local model size(NWADF)
 | #6 | 5GC->AF |
| * Prediction Information(NWADF)
 | * Packet loss rate prediction
 | #30 | 5GC->AF |
| * Packet delay prediction
 | #6,#23,#30 | 5GC->AF |
| * Network congestion prediction
 | #31 | 5GC->AF |
| * Network load predictions at UE locations
 | #6、#23 | 5GC->AF |
| * User data congestion time prediction
 | #6 | 5GC->AF |
| * Slicing Information
 | * S-NSSAI(AMF)
 | #5、#6、#13、#17 | 5GC->AF |
| AF-related data | * Expected UE Behaviour parameters
 | * Target AOI
 | #16、#18、#23 | AF->5GC |
| * UE address(es) (IP address or MAC address)
 | #16 |
| * Training time period
 | #23、#25 |
| * Target FL Coverage Area
 | #16 |
| * Target Historical nomadic period for the given target AOI
 | #18 |
| * The minimum separation distance between candidate UEs based on locations
 | #16、#25 |
| * The list of candidates UEs
 | #16、#25 |
| * The minimum/maximum number of UEs
 | #18、#23 |
| * Wireless Access technology
 | #25 |
| * QoS references
 | #9 |
| * Data sources of the local training data for the set of distributed nodes
 | #16 |
| * Data rate reporting
 | * Group Maximum Bit Rate (Group-MBR)
 | #12、#15 |
| * QoS
 | * QoS Sustainability Analytics（NWDAF）
 | #6、#7、#27, #28 | 5GC->AF |

**Table-1 Data used in AI/ML operations**

Annex B (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2022-06 | SA3#107 Adhoc-e |  |  |  |  | TR Skeleton | 0.0.0 |
| 2022-07 | SA3#107 Adhoc-e | S3-221698 |  |  |  | Incorporated S3-221508, S3-221509, S3-221510 | 0.1.0 |
| 2022-10 | SA3#108 Adhoc-e | S3-223000 |  |  |  | Incorporated S3-222996, S3-222998 | 0.2.0 |
| 2022-11 | SA3#109 | S3-223978 |  |  |  | Incorporated S3-223249, S3-223980, S3-223981 | 0.3,0 |
| 2023-01 | SA3#109Adhoc-e | S3-230494 |  |  |  | Incorporated S3-230217, S3-230373, S3-230513, S3-230514, S3-230516 | 0.4.0 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |