|  |
| --- |
| 3GPP TR 33.abc V0.0.0 (2025-08) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects; Study on Security for Core Network Enhanced Support for Artificial Intelligence (AI) / Machine Learning (ML) Phase 2;(Release 20) |
|   |
|  |  |
|  |
| 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 16Internethttps://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.© 2025, 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 6

3.1 Terms 6

3.2 Symbols 6

3.3 Abbreviations 6

4 Overview 6

5 Key issues 7

5.1 Key Issue #1: Security of UE connection setup with Data Collection NF 7

5.1.1 Key issue details 7

5.1.2 Security threats 7

5.1.3 Potential security requirements 7

6 Solutions 8

6.1 Mapping of solutions to key issues 8

6.Y Solution #Y: <Solution Name> 8

6.Y.1 Introduction 8

6.Y.2 Solution details 8

6.Y.3 Evaluation 8

7 Conclusions 8

Annex A: Change history 9

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In the present document, modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

# Scope

Editor’s Note: This clause is going to capture the scope of this study.

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 23.700-04: “ Study on Core Network Enhanced Support for Artificial Intelligence (AI)/Machine Learning (ML);”.

…

[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 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 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 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 TR 21.905 [1].

<ABBREVIATION> <Expansion>

# 4 Overview

TR 23.700-04 [2] studies transfer of standardized data over UP for UE data collection to meet requirements for AI/ML for NR air interface operation with UE-side model training, all the architecture assumptions and architecture requirements defined in TR 23.700-04 [2] are also applicable to the present document, and any security impact is documented in the present document.

# 5 Key issues

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

## 5.1 Key Issue #1: Security of UE connection setup with Data Collection NF

### 5.1.1 Key issue details

The architecture requirement in clause 4.2 of TS 23.700-04 [2] is that MNO has full controllability and visibility for standardized data. That means the training data between UE and the 5G core will be standardized and it is visible to 5G core and MNO will be data controller.

The key issue aims to address the security issues, such as authentication and authorization for the UE during the connection setup with the data collection network function (Naming and role of data collection function is TBD and subject to progress of TR 23.700-04 [2]). This will ensure only legit and authorized UE are able to share its data towards the Data collection NF.

Another aspect is to address the security issues, ensuring integrity and confidentiality of the UE related data between UE towards the 5GC Data collection NF as studied in KI#1 of TR 23.700-04 [2] to meet requirements for AI/ML for NR air interface operation with UE-side model training.

So, the focus is to identify the means to authenticate and authorize the connection setup between UE and NF before the data transmission take place and to study security of the communication between UE and data collection NF during data transmission.

Editor’s Note: UE to 5GC interaction is ffs depending on progress by SA2.

### 5.1.2 Security threats

Lack of authentication and authorization may lead to unauthorized access to network services.

Lack of confidentiality, integrity protection in collecting UE related data can lead to disclosure and tampering of UE related information.

Tampering of UE related data in transit can also impact the quality of training data towards 5GC data collection NF and subsequently to external OTT servers.

Lack of user consent may lead to inadvertent UE data disclosure.

### 5.1.3 Potential security requirements

The 5GS should support authentication and authorization between UE and data collection NF before data transmission takes place.

Editor’s Note: Authentication and authorization between UE and data collection NF is ffs depending on progress on the architecture aspects by SA2.

The 5GS should support confidentiality, integrity and replay protection for data in transit between UE and data collection NF.

The 5GS should support user consent mechanism for data collection by the network depending on the local regulations and operator policies.

Editor’s note: whether user consent is applicable or not will be decided by SA3 based on SA2 progress.

# 6 Solutions

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

## 6.1 Mapping of solutions to key issues

Editor’s Note: This clause captures mapping between key issues and solutions.

Table 6.1-1: Mapping of solutions to key issues

|  |  |
| --- | --- |
|  | **Key Issues** |
| **Solutions** |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## 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 captures the conclusions of this study.

Annex A:
Change history

|  |
| --- |
| Change history |
| Date | Meeting | TDoc | CR | Rev | Cat | Subject/Comment | New version |
| 2025-08 | SA3#123 | S3-253064 |  |  |  | S3-252564, S3-252988, S3-252990 for endorsed TR skeleton, overview and new key issue | 0.0.0 |