|  |  |
| --- | --- |
| 3GPP TR 33.867 V0.3.0 (2021-1) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on User Consent for 3GPP services  (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 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.  © 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 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 4

Introduction 5

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 User consent background, analysis 7

4.1 Background 7

4.2 Analysis 7

5A Use Cases 8

5A.1 Use Cases #1: UE Related Analytics of NWDAF 8

5A.1.1 Use Case details 8

5A.1.2 Individual Architecture 8

5A.X Use case #X 9

5A.X.1 Use Case details 9

5A.X.2 Individual architecture 9

5B Common architecture 9

6 Key issues 9

6.X Key issue #X: <Key issue name> 10

6.X.0 Use case mapping 10

6.X.1 Key issue details 10

6.X.2 Security threats 10

6.X.3 Potential security requirements 10

7 Potential solutions 10

7.0 Mapping of solutions to key issues 10

7.Y Solution #Y: <Solution name> 11

7.Y.1 Solution overview 11

7.Y.2 Solution details 11

7.Y.3 Solution evaluation 11

8 Conclusions 11

Annex A (Informative): Observations related to regulations 11

Annex <A>: <Informative annex title for a Technical Report> 13

Annex <X> (informative): Change history 14

# 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.

# Introduction

Editor’s Note: Content is FFS

# 1 Scope

The scope of present document is to identify and evaluate the requirements and solutions to support user consent for 3GPP services while complying with user privacy considerations.

The details are as follows:

* Review TR 33.849 [xx] with regards to the concept of user consent for 3GPP users, and identify what types of data collection and conditions under which the support of the user consent is required; then update them if needed;
* Identify target usage scenarios and trust domains;
* Analyse potential security threats and requirements for conditions under which user sensitive data are collected without user consent, and when user consent indication is not protected;
* Identify potential solutions to address the above security requirements.

NOTE 1: Principles, regulations, and definitions related to privacy, which are recognized differently in each different country or area, are taken into account when deriving the concept of user consent for 3GPP users.

NOTE 2: Even where solutions exist to obtain user consent, collection and exposure of user sensitive data should be minimized and only be allowed where critical to the operation of the related feature.

Editor's Note: The structure of the TR needs to be updated to reflect the objectives.

Editor's Note: Scope may need to be updated to reflect the result of the analysis of TR33.849 to differentiate the scope of the present document and of TR33.849.

# 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 23.558: "Architecture for enabling Edge Applications (EA) ".

[3] 3GPP TR 33.849: “Study on subscriber privacy impact in 3GPP”.

[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 (5GS)”

# 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].

**Data subject:** As defined in TR 33.849 [3].

**Data controller:** As defined in TR 33.849 [3].

**Data processor:** As defined in TR 33.849 [3].

**Personal data**: As defined in TR 33.849 [3].

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

<symbol> <Explanation>

Editor’s Note: Example needs to be deleted

## 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>

Editor’s Note: Example needs to be deleted

# 4 User consent background, analysis

Editor’s Note: This clause will look at various aspects around user consent, e.g., how it is interpreted, its need for type/purpose of data processing, example of use cases, etc..

## 4.1 Background

Editor’s Note: This clause will introduce concept of user consent and why we study user consent in SA3.

## 4.2 Analysis

Editor’s Note: This clause will capture the relevant information of user consent, and comparison to the existing solutions or studies, such as comparison to TR 33.849.

# 5A Use Cases

Editor’s Note: This clause will present the system architecture on user consent for 3GPP services, i.e. which part of 5G and connected systems are considered, what a data is expected to be processed, and for what purpose.

## 5A.1 Use Cases #1: UE Related Analytics of NWDAF

### 5A.1.1 Use Case details

NWDAF can provide UE related analytics services. The NWDAF collects UE related data, e.g. from UE, NFs, 3rd party, and outputs related analytics result, e.g. UE mobility analytics, UE mobility analytics, expected UE behavioural parameters related network data analytics and abnormal behaviour related network data analytics as depicted in clause 6.7 in 3GPP TS 23.288 [4].

The NWDAF can process UE related data as the following:

* Collect UE related data to provide UE related analytics for the user, e.g. UE mobility analytics.
* Share analytics result to NF consumers, e.g. internal NF or 3rd AF.

The PLMN NFs or AFs can process UE related data as the following:

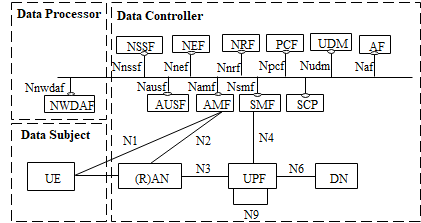
* Collect and store UE related data.
* Share UE related data to NWDAF.

Since the UE related data may contain personally identifiable information, thus, processing of those data should consider user consent aspects.

### 5A.1.2 Individual Architecture

For this use case, the architecture and framework as specified in TS 23.288 [4], TS 23.501 [5] are regarded as the baseline. The solutions shall build on the 5G System architectural principles as in TS 23.501 [5], including flexibility and modularity for newly introduced functionalities.

Moreover, the individual architecture is shown in figure 5A.1.2-1.



5A.1.2-1 Individual Architecture for data analytics

The UE related data is derived from the UE.

The NFs, for example, AMF, SMF, OAM, AF, etc., collect and store UE related data derived from the UE. Thus, the legal entity of those network entities is data controller. In case that the AF is outside of 3GPP network, the legal entity of the AF is another data controller.

The NWDAF collects UE related data from the NFs, and processes data for UE related analytics to provide UE related analytics services. Thus, the legal entity of the NWDAF is data processor. In case that the NWDAF is NF of data controller, the legal entity of the NWDAF is also data controller.

NOTE: Roaming architecture for NWDAF is not considered in R17.

## 5A.X Use case #X

### 5A.X.1 Use Case details

Editor’s Note: This clause will capture the use case when the user consent is needed.

### 5A.X.2 Individual architecture

Editor’s Note: This clause is used to show the individual architecture of each use case. The architecture may show the legal entities that is relevant to user consent. Different individual architectures will be used together to generate a common architecture for user consent in 5G system..

# 5B Common architecture

Editor’s Note: This clause will capture the common architecture for user consent in 5G system. Common architecture could be derived from different individual architectures for user consent in 5G system.

# 6 Key issues

Editor’s Note: This clause will contain the agreed key issues.

NOTE: Key issues should align with the background/analysis done in clause 4 and 5 above.

Editor’s Note: The clear split between user consent aspects studied in eNA study and UC3S study need to be clarified.

Editor’s Note: Below a generic template of headings for a key issue is provided and need to be deleted before the TR goes for approval. The subclauses may not necessarily be needed as part of a KI

6.1 Key Issue #1: User's consent for exposure of information to Edge Applications

6.1.1 Key issue details

EES exposes UE Identifier API to the EAS in order to provide an identifier uniquely identifying a UE. Further, the Edge Enabler Server exposes the UE location API to the Edge Application Server in order to support tracking or checking the valid location of the UE. In order to expose such user related private information to the Edge Application servers, consent from the user is needed.

EES capability exposure to EAS as defined in TS 23.558 [2], mandates the end user's consent for reporting UE's information, particularly for UE Identifier API and UE location API. Also as suggested in TS 23.558 [2], whether and how user's consent is obtained to share the UE identifier with a particular EAS is covered in this key issue.

6.1.2 Security threats

Use of user’s information to identify and track the user or user’s behavior without the permission or knowledge of the user, poses huge threat to user’s privacy.

6.1.3 Potential security requirements

Architecture for enabling edge applications shall support a mechanism for Edge Application Servers to obtain user's authorization, in order to access to and/or to expose the user's sensitive information (e.g. user's location).

Editor’s Note: the security requirements are TBA.

Editor’s Note: When defining any procedures obtaining user's consent, it is needed to clarify “when” user’s consent is obtained, on “what” information it is obtained and provide details on “why” user’s consent is obtained (e.g. for what purposes the user consented information will be used).

## 6.X Key issue #X: <Key issue name>

### 6.X.0 Use case mapping

Editor’s Note: If the key issue is relevant with a use case, then the clause number of the use case should be given here. Otherwise, descriptions of key issue scenario should be given here.

### 6.X.1 Key issue details

Editor’s Note: This clause provides details of the key issue

### 6.X.2 Security threats

Editor’s Note: This clause list the threats derived from the key issue details

### 6.X.3 Potential security requirements

Editor’s Note: This clause list the potential security requirements derived from the threats

# 7 Potential solutions

Editor’s Note: This clause will contain the proposed solutions

Editor’s Note: Solutions are only to be provided, when common understanding of user consent topic (clause 4) is reached and the system architecture (clause 5) clearly stated.

## 7.0 Mapping of solutions to key issues

Table 6.0-1: Mapping of Solutions to Key Issues

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Solutions | Key Issues | | | |
| 1 | X |  |  |
| #1: <Solution name> | X |  |  |  |
| #X: <Solution name> | X |  |  |  |

Editor’s Note: This clause provides the mapping of Solutions to Key Issues.

Editor’s Note: Below a generic template of headings for a new solution is provided and need to be deleted before the TR goes for approval

## 7.Y Solution #Y: <Solution name>

### 7.Y.1 Solution overview

Editor’s Note: This clause starts with the (part of) the key issue(s) addressed and is followed with a brief overview of the solution

### 7.Y.2 Solution details

Editor’s Note: This clause provides the details of the solution

### 7.Y.3 Solution evaluation

Editor’s Note: This clause provides the evaluation of the solution

# 8 Conclusions

Editor’s Note: This clause will contain the conclusion, principle and guidelines of user consent in 5G

Annex A (Informative):  
Observations related to regulations

NOTE: There are many regional privacy regulations. In this clause specific ones like GDPR are considered for guidance only.

The European General Data Protection Regulation (GDPR) can be considered one of the leading privacy regulations as other countries (such as India) are using it as a blueprint to update their own privacy regulations. It defines that consent must be freely given, specific, informed, and unambiguous. It also means that, for users in the European Union, if consent is chosen as the legal basis for processing, users have to agree actively through an affirmative action (opt in). Other legislations such as Brazil’s Lei Geral de Proteção de Dados Pessoais (LGPD) from August 2020 and the upcoming Indian privacy law both use similar guidelines for obtaining consent. Jurisdictions such as California and their Consumer Privacy Act (CCPA), while not having limitations on the initial collection of personal data, do have updated consent controls regarding the selling and onward transfer of personal data. Thus, there could be different views around the world how user consent should be handled as there are different laws and principles around privacy in the different countries/regions.

Under the GDPR, while most of the interest revolves around the legal basis of consent for processing personal data, it forms only one of six legal bases. The other five (contract, legal obligations, vital interests of the data subject, public interest, and legitimate interest) are all used as well. Thus, there could be other legal bases for processing personal data than consent.

Consent can be obtained through a variety of methods and techniques, as long as the action is an affirmative one by the data subject and matches the GDPR requirements of being freely given, specific, informed, and unambiguous. This can be from ticking a box on a website to writing a letter confirming everything. Thus, how consent can be given depends on the concrete use case and also on the laws of the jurisdictions which govern the use case.

Annex <A>:  
<Informative annex title for a Technical Report>

Annex <X> (informative):  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2020.10 | SA3#100bis-e | S3- 202785 |  |  |  | S3-202622,S3-202338, S3-202589r2, | 0.1.0 |
| 2020.11 | SA3#101-e | S3-203458 |  |  |  | S3-203451 | 0.2.0 |
| 2021.1 | SA3#102-e | S3-210671 |  |  |  | S3-210227, S3-210275, S3-210324r3 | 0.3.0 |