|  |  |
| --- | --- |
| 3GPP TR 33.896 V0.3.0 (2022-10) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study of Security Aspects on User Consent for 3GPP Services Phase 2;  (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 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

1 Scope 5

2 References 5

3 Definitions of terms, symbols and abbreviations 5

3.1 Terms 5

3.2 Symbols 6

3.3 Abbreviations 6

4 Overview 6

5 Key issues 6

5.1 Key Issue #1: User consent for roaming case in eNA 6

5.1.1 Key issue details 6

5.1.2 Security threats 6

5.1.3 Potential security requirements 6

5.2 Key Issue #2: User consent for NTN 7

5.2.1 Key issue details 7

5.2.2 Security threats 7

5.2.3 Potential security requirements 7

5.X Key Issue #X: <Key Issue Name> 8

5.X.1 Key issue details 8

5.X.2 Security threats 8

5.X.3 Potential security requirements 8

6 Solutions 8

6.1 Mapping of solutions to key issues 8

6.1 Solution #1: User consent obtained by the NTN-RAN in non-mobility use case 8

6.1.1 Introduction 8

6.1.2 Solution details 8

6.2 Solution #2: User consent revocation obtained by the NTN-RAN 10

6.2.1 Introduction 10

6.2.2 Solution details 10

6.Y Solution #Y: <Solution Name> 12

6.Y.1 Introduction 12

6.Y.2 Solution details 12

6.Y.3 Evaluation 12

7 Conclusions 12

Annex X (informative): Change history 12

# 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 is to investigate potential enhancements of 5GS that would enable broader use cases in relation with user consent.

The following aspects are in the scope of the study:

1. Investigating the potential issues and solutions with user consent for:

- eNA in case of roaming.

- MEC in case of roaming.

- NTN.

- AI/ML for NG-RAN.

2. Investigating the potential generic security requirements, services and guidance for user consent derived from objective 1.

NOTE 1: This scope can be updated to reflect additional use cases.

NOTE 2: 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 3: Even where solutions exist to obtain user consent, collection and exposure of user sensitive data should be minimized and identification of the users should only be allowed where critical to the operation of the related feature.

# 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 23.700-81: “Study of Enablers for Network Automation for 5G System (5GS); Phase 3”.

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

[4] 3GPP TS 23.501: "System architecture for the 5G System (5GS)".

[5] 3GPP TS 38.300: "NR; NR and NG-RAN Overall Description".

# 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

Editor's note: This clause includes the overview applicable for the study.

# 5 Key issues

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

## 5.1 Key Issue #1: User consent for roaming case in eNA

### 5.1.1 Key issue details

As depicted in key issue #3 in 3GPP TR 23.700-81 [2], "In roaming scenario, the HPLMN/VPLMN may need to collect data or consume analytics from the VPLMN/HPLMN." In this case, the user data may be exchanged between different entity, i.e. VPLMN and HPLMN, that may be subject to different regulations with respect to user consent.

When it somes to the actions performed on the user data, the following cases need to be considered:

* HPLMN collects user data and exposes the data to VPLMN, VPLMN performs analytics and ML training.
* VPLMN collects user data and exposes the data to HPLMN, HPLMN performs analytics and ML training.

In order to cover these scenarios, it is important to assess the current user consent framework in Annex V in 3GPP TS 33.501 [3], and decides who will perform the role of enforcement point.

### 5.1.2 Security threats

If the HPLMN/VPLMN is not aware to check user consent for roaming case for eNA, e.g. data analysis or ML tranning, the HPLMN/VPLMN may expose user privacy information to VPLMN/HPLMN which could lead to a compromise of the user privacy.

If the HPLMN/VPLMN is not aware to revoke user consent for roaming case for eNA, the HPLMN/VPLMN may continue to process user privacy information which could lead to a compromise of user privacy.

### 5.1.3 Potential security requirements

The 5GS shall provide the means for a HPLMN/VPLMN to check of user consent for the roaming scenario in eNA.

The 5GS shall provide the means for HPLMN/VPLMN to revoke of user consent for the roaming scenario in eNA.

NOTE: Cross-PLMN data sharing among different countries is FFS.

## 5.2 Key Issue #2: User consent for NTN

### 5.2.1 Key issue details

NTN features are specified in clause 5.4.11 of 3GPP TS 23.501 [4] and clause 16.14 of 3GPP TS 38.300 [5]. In such features, the NG-RAN in NTN may require UE’s location information for selecting the AMF.

The way it works now is that after AS security is activated, the NG-RAN in NTN can request the UE to report its accurate location or coarse location. However, both types of location reports may require user consent depending on local regulations.

This key issue is intended to study whether there is any need to enhance the current user consent framework specified in Annex V in 3GPP TS 33.501 [3].

### 5.2.2 Security threats

If the NG-RAN in NTN is not aware of user consent status, then the NG-RAN in NTN may collect user’s location information without consent which could lead to a compromise of the user privacy.

If the NG-RAN in NTN is not aware that user consent for NTN use case has been revoked, then the NG-RAN in NTN may continue to collect user’s location information which could lead to a compromise of user privacy.

### 5.2.3 Potential security requirements

TBA.

Editor's Note: whether access to NTN service implies consent to NTN requesting location is ffs.

Editor's Note: requirements is ffs.

## 5.3 Key Issue #3: Unified framework for user consent related data retrieval, notification, and revocation

### 5.3.1 Key issue details

User consent is stored in the UDM/UDR. All NFs/AFs must retrieve the consent flag from the UDM and accordingly collect the data from a UE or UE related data from other NFs. However, not all NFs/AFs do contact UDM before collecting data.

For example, AF does not interact with UDM before collecting the data related to a UE. Even if AF interacts with UDM for the user consent, then AF collects data via AMF, therefore AMF also needs to coordinate with UDM before collecting data from a UE or UE related data from other NFs. This means, that the same consent checking is necessary at multiple places/NFs. Furthermore, keeping track of revocation and which NF has received which UE-related user consent details seems to become tedious. Rel-17 TS 33.501 clause V.2 states that user consent revocation service is not provided by UDM.

This key issue looks into the benefits of a unified framework such as a central function or a service for coordinating and keeping track of user consent retrieval, notification, and revocation.

### 5.3.2 Security threats

When user consent needs to get revoked, all NFs/AFs that have asked for user data beforehand need to revoke them. Otherwise, there is the danger that some NFs/AFs are not tracked and thus not informed about the revocation demand. This can result in accessing user-related data by NFs/AFs even after revocation by the user.

### 5.3.3 Potential security requirements

In addition to the requirements listed in TS 33.501 clauses V.1 and V.4:

The 5GS shall ensure that all NFs/AFs that collected user consent related data are notified.

Editor’s Note: Further security requirement is FFS.

## 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

## 6.1 Mapping of solutions to key issues

Table 6.1-1: Mapping of solutions to key issues

|  |  |  |  |
| --- | --- | --- | --- |
| Solutions | KI#1 | KI#2 | KI#3 |
| **Solution#1: User consent obtained by the NTN-RAN in non-mobility use case** |  | X |  |
| **Solution #2: User consent revocation obtained by the NTN-RAN** |  | X |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

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

## 6.1 Solution #1: User consent obtained by the NTN-RAN in non-mobility use case

### 6.1.1 Introduction

This solution addresses the Key Issue #2 on NTN specific user consent. Specifically, it addresses the first requirement in KI#2.

In NTN use case, the network function requiring user consent is the NTN-RAN, which needs to obtain user consent for configuring the UE to report its GNSS-based information and processing the UE location information. By referring to TS 33.501 [3] Annex V, the NTN-RAN is the enforcement point for user consent which shall not perform the related operation unless user consent is granted.

According to TS 33.501 [3] Annex V.2, the parameters indicating user consent preference are stored in the UDM as subscription data, which can be retrieved via UDM service for network function to check whether user consent is granted for the requested operation or not. Specifically for NTN use case, it is proposed that user consent preference for a UE can be stored in a UE NTN privacy profile as part of UE subscription data in the UDM/UDR. The user consent preference within the UE NTN privacy profile can be used to indicate whether the configuration on the UE performed by the NTN-RAN is allowed or disallowed.

### 6.1.2 Solution details

Given that the use of user consent information at the NTN-RAN in NTN could allow its enforcement at the earliest RAN convenience as indicated by RAN WG3, it is proposed that the user consent information shall be provisioned by the UDM at the earliest possibility to the AMF, i.e. during Registration procedure, which could be “initial registration”, “periodic registration update” or “mobility registration update” procedure, etc. The AMF can store the received user consent preference in the UE context, which further provisions the user consent preference to the NTN-RAN.



Figure 6.1.2-1: NTN Specific User Consent in Non-mobility Case

1. The UE sends the Registration Request to the NTN-RAN (gNB or NTN-GW) including its SUCI or 5G-GUTI.

2. The NTN-RAN selects an AMF for the UE and sends to the AMF a N2 message (e.g. Initial UE Message) containing N2 parameters in addition to the Registration Request. The N2 message also includes a UE Context Request indicating that the user consent preference on UE location information for NTN access is needed or to be updated.

3. Based on the N2 message from the NTN-RAN, the AMF determines that the RAT type is NTN access. If the received N2 message contains a UE Context Request requesting the user consent preference, the AMF checks whether its stored UE context already contains the user consent preference of the UE for NTN access by checking against the SUCI or 5G-GUTI. If the user consent preference of the UE is not available in the UE context or the validity timer for user consent preference has expired, the AMF proceeds to step 4. Otherwise, the AMF proceeds to step 8.

4. The AMF sends a Nudm\_SDM\_Get request to the UDM for retrieving the user consent preference on UE location information for NTN access from the UE’s subscription data.

5. After receiving the Nudm\_SDM\_Get request, the UDM checks with the UDR for the user consent preference on location information for NTN access, probably within the NTN privacy profile of the UE’s subscription data, against the SUPI of the UE.

6. The UDM sends a Nudm\_SDM\_Get response to the AMF containing the user consent preference on UE location information for NTN access.

7. After receiving the Nudm\_SDM\_Get response, the AMF stores the user consent preference in the UE context, or replaces its stored user consent preference with the one received from the UDM. The AMF forwards the user consent preference to the NTN-RAN.

8. The AMF sends a N2 message (e.g. Initial Context Setup Request) to the NTN-RAN, which includes user consent result or user consent preference for NTN access in addition to the Registration Accept.

9. After receiving the N2 message, the NTN-RAN stores the user consent result or user consent preference in its UE context. Based on the received user consent result/preference, the NTN-RAN determines how to enforce the user consent with proper configuration on the UE.

10. The NTN-RAN sends the RRCReconfiguration message (including Registration Accept and location configuration info) to the UE. If the user consent is granted for location reporting, the NTN-RAN sends the configuration for the UE to report its location (e.g. via *includeCommonLocationInfo* in the *reportConfig*); if the use consent is not granted for location reporting, the NTN-RAN does not send such configuration.

11. The UE sends the RRCReconfigurationComplete message to the NTN-RAN.

12. The NTN-RAN sends a N2 message (e.g. Initial Context Setup Response) to the AMF.

13. The UE sends the Registration Complete message to the NTN-RAN.

NOTE: The granularity of user consent preference could be detailed in the UE privacy profile for NTN in the UE subscription.

## 6.2 Solution #2: User consent revocation obtained by the NTN-RAN

### 6.2.1 Introduction

This solution addresses the Key Issue #2 on NTN specific user consent. Specifically, it addresses the second requirement in KI#2.

As per TS 33.501 [3] Annex V, besides the retrieval of user consent parameters, the notification of user consent parameters change or user consent revocation shall also be supported for user consent mechanism. Any 5GC consumer NFs (processing the data pertaining to user consent) shall subscribe to the UDM for user consent parameter change notification, except if the consent enforcement NF that is deemed an enforcement point is tracking of those NFs and is actively informing those consumer NFs in case of user consent revocation.

The solution is introduced for NTN-RAN to obtain user consent parameters change or user consent revocation in NTN use case, so as to protect the user privacy while user consent is updated or revoked.

### 6.2.2 Solution details

In NTN use case, the enforcement point of user consent is not a 5GC NF but the NTN-RAN, which is informed of the user consent status by the 5GC NF, i.e. the AMF in this case. As the AMF is able to track multiple NTN-RANs within the tracking area it covers, this solution proposes that the AMF subscribes to the UDM for user consent parameter change notification or revocation notification, which then informs the NTN-RAN at which the UE is camped.



Figure 6.2.2-1: NTN Specific User Consent Revocation Procedure

1. The AMF subscribes to the UDM for the service of user consent update and/or revocation notification via Nudm\_SDM\_Subscribe service operation. The service could be subscribed for a specific UE or it could be a generic service subscription for all UEs.

2. The user consent parameters are updated or revoked in the subscription data during the related procedure between a specific UE and the UDM.

3. The UDM retrieves the AMF ID serving the UE and notifies the AMF about the user consent parameter change via Nudm\_SDM\_Notification service operation. The user consent parameter change is associated with the UE by indicating the UE ID, i.e. SUPI. The user consent parameter change may also contain the NTN-RAN ID which is effected by the change, e.g. the NTN-RAN which was allowed to obtain UE location before it is no longer allowed.

4. Upon receiving the notification from the UDM, the AMF updates the user consent parameters in its locally stored UE context associated with the SUPI.

5. The AMF sends a N2 message to the NTN-RAN including, e.g. UE Context Modification Request, which contains the user consent parameter change. The AMF associates the user consent parameter change with a temporary UE ID, e.g. 5G GUTI.

6. Upon receiving the N2 message from the AMF, the NTN-RAN updates the user consent parameters in its locally stored UE context associated with a temporary UE ID, e.g. I-RNTI.

7. Based on the updated user consent parameters, the NG-RAN determines the configuration and sends the RRCReconfiguration message to the UE. If the user consent is revoked, the NG-RAN does NOT send the configuration (e.g. includeCommonLocationInfo in the reportConfig) so as to prevent the UE from reporting its location.

8. Upon receiving the RRCReconfiguration message without the configuration for location reporting, the UE stops reporting its location.

9. The UE sends the RRCReconfigurationComplete message to the NTN-RAN.

10. The NTN-RAN sends a N2 message to the AMF including e.g. UE Context Modification Response.2. The NTN-RAN selects an AMF for the UE and sends to the AMF a N2 message (e.g. Initial UE Message) containing N2 parameters in addition to the Registration Request. The N2 message also includes a UE Context Request indicating that the user consent preference on UE location information for NTN access is needed or to be updated.

## 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 X (informative):  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2022-06 | SA3#107Adhoc-e | S3-221680 |  |  |  | S3-221400, S3-221401, S3-221668, S3-221669 | 0.1.0 |
| 2022-08 | SA3#108-e | S3- 222342 |  |  |  | S3-222350, S3-222351 | 0.2.0 |
| 2022-10 | SA3#108Adhoc-e | S3-223130 |  |  |  | S3-223039, S3-222819r3 | 0.3.0 |