|  |
| --- |
| 3GPP TR 33.xxx V0.1.0 (2025-09) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on Security and Privacy Aspects of Integrated Sensing and Communication(Release 20) |
|   |
|  | 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.© 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 7

4 Architecture and security assumptions 7

5 Key issues 7

5.1 Key Issue #1: Security of authorization for sensing service invocation and revocation 7

5.1.1 Key issue details 7

5.1.2 Security threats 7

5.1.3 Potential security requirements 7

5.2 Key Issue #2: Security protection for sensing service operations 8

5.2.1 Key issue details 8

5.2.2 Security threats 8

5.2.3 Potential security requirements 8

6 Solutions 8

6.0 Mapping of solutions to key issues 8

6.X Solutions to KI#X 9

6.X.Y Solution #X.Y: <Solution Title> 9

6.X.Y.1 Introduction 9

6.X.Y.2 Solution details 9

6.X.Y.3 Evaluation 9

7 Conclusions 9

Annex X: Change history 10

# 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 investigates and identifies the security threats, requirements and potential solution for Integrated Sensing and Communication (ISAC). Based on the architecture and system level enhancements studied in TR 23.700-14 [2], the work in this document focuses on the security aspects of gNB-based mono-static sensing mode for UAV sensing target use cases.

The UAV sensing target uses cases defined by TS 22.137 [3] and TR 22.837 [4] serve either the purpose of public safety, or as requested by the management entity (UAV management department, USS or UTM), without the necessity to identify the object.

Specifically, the present document covers the following:

- The identified key issues, threats, potential requirements and solutions for security protection during the service operations and procedures supporting Sensing services;

- The identified key issues, threats, potential requirements and solutions for protecting privacy for sensing data collection, sensing data processing, and sensing data exposure.

# 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 23.700-14: "Study on Integrated Sensing and Communication; Stage 2".[3] 3GPP TS 22.137: "Service requirements for Integrated Sensing and Communication; Stage 1".

[4] 3GPP TR 22.837: "Feasibility Study on Integrated Sensing and Communication".

[5] 3GPP TR 33.501: "Security architecture and procedures for 5G system".

# 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 Architecture and security assumptions

The following architecture and security assumptions are applied to the study:

- The architecture assumptions and principles for Integrated Sensing and Communication as defined in TR 23.700-14 [2] are used as architecture assumptions in this study.

- The security architecture, procedures, and security requirements for 5GS as defined in TS 33.501 [5] are used as a baseline.

# 5 Key issues

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

## 5.1 Key Issue #1: Security of authorization for sensing service invocation and revocation

### 5.1.1 Key issue details

In TR 23.700-14 [2], architecture for sensing services is studied to enable the 3GPP network to support sensing service invocation and revocation from the service consumer.

Solutions addressing the KI#2 in TR 23.700-14 [2] of authorization and revocation for particular sensing services are developed, which focus on service request authorization or revocation based on the information of the service level agreement. Security aspects need to be discussed about for the above mentioned procedures.

NOTE: Security aspects of sensing service revocation triggered by sensing service consumer is addressed in this key issue.

This key issue is related to KI#2 of TR 23.700-14 [2] and addresses the security aspects for sensing service invocation and revocation procedures between the network and sensing service consumer.

### 5.1.2 Security threats

Without proper authentication and authorization for sensing service, unauthorized party may be able to access to sensing service.

If the connection between sensing service consumer and NEF/SF is not protected, the attacker can tamper, inject, sniff or replay messages related to sensing service invocation and revocation.

### 5.1.3 Potential security requirements

The 5G system shall be able to support mutual authentication between sensing service consumer and NEF/SF.

The 5G system shall be able to support integrity protection, confidentiality protection and replay protection for the communication between sensing service consumer and NEF/SF.

The 5G system shall be able to authorize sensing service request from a sensing service consumer.

## 5.2 Key Issue #2: Security protection for sensing service operations

### 5.2.1 Key issue details

According to TR 23.700-14 [2], after the sensing service request from the service consumer is authorized by the network, sensing service operations will be triggered and performed by the relevant network functions, which communicate with each other to obtain the sensing result.

In TR 23.700-14 [2], there are multiple solutions proposing sensing service operation procedures supported by sensing entities and different sensing related network functions (e.g. NEF, SF, sensing management function, sensing control function, sensing processing function). The NEF needs to discover and select the SF to trigger sensing service operation. The SF needs to select proper sensing entity to collect sensing data in a specific sensing mode. When any of the service conditions of a sensing service is no longer met, an ongoing sensing service can be revoked by the network. The security aspects of all these sensing operations and procedures are to be addressed in this key issue.

NOTE 1: Security aspects of service operation revocation triggered by sensing functions is addressed in this key issue, as it can be viewed as one type of sensing service operations.

### 5.2.2 Security threats

As the sensing service operations are performed among sensing function(s) and sensing entities, if the 5GC does not support sensing service operation authorization, the sensing service operation can be abused.

If the connection between sensing functions is not securely established, an attacker is able to tamper or inject or replay sensing operation messages and the sensing result to be exposed, or sniff the sensing result.

If the connection between sensing entity and sensing function is not securely established, an attacker is able to tamper or inject or replay sensing control messages and sensing data, or sniff the collected sensing data.

### 5.2.3 Potential security requirements

The 5G system shall be able to support mutual authentication between SFs.

The 5G system shall be able to support authorization for sensing service operations.

The 5G system shall be able to support integrity protection, confidentiality protection and replay protection for the connection between sensing entity and SF.

The 5G system shall be able to support integrity protection, confidentiality protection and replay protection for the connection between SFs.

NOTE 2: If there is no interaction between SFs based on architecture defined in SA2, the security requirements between SFs are not needed.

Editor’s Note: More security requirements will be added depends on SA2 progress.

# 6 Solutions

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

## 6.0 Mapping of solutions to key issues

Editor's Note: This clause contains a table mapping between key issues and solutions.

Table 6.1-1: Mapping of solutions to key issues

|  |  |  |  |
| --- | --- | --- | --- |
| Solutions | KI#1 | KI#2 | KI#Z |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## 6.X Solutions to KI#X

### 6.X.Y Solution #X.Y: <Solution Title>

#### 6.X.Y.1 Introduction

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

#### 6.X.Y.2 Solution details

#### 6.X.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:
Change history

|  |
| --- |
| Change history |
| Date | Meeting | TDoc | CR | Rev | Cat | Subject/Comment | New version |
| 2025-08 | SA3#123 | S3-252869 |  |  |  | Skeleton for ISAC Security TR | 0.0.0 |
| 2025-09 | SA3#123 | S3-253011 |  |  |  | Implemented S3-252693, S3-253012, S3-253013 and S3-253014 | 0.1.0 |