|  |
| --- |
| 3GPP TR 33.891 V0.1.0 (2022-07) |
| Technical Report |
| 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects;Study on Security of Phase 2 for UAS, UAV and UAM(Release 18) |
|   |
|  |  |
|  |
| 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.© 2022, 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 Overview 7

5 Key Issues 7

5.1 Key issue #1: Direct C2 Security 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 of DAA unicast connection 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.X Solution #X: Title of solution 8

6.X.1 Introduction 8

6.X.2 Solution details 8

6.X.3 Evaluation 8

7 Conclusions 8

Annex <A>: <Informative annex title for a Technical Report> 9

Annex <X> (informative): Change history 10

**Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.Error! Bookmark not defined.**Error! Bookmark not defined.Error! Bookmark not defined.

# 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 and privacy threats and corresponding security requirements for Uncrewed Aerial Vehicles (UAVs) and Urban Air Mobility (UAM) that derive from the architecture and system level enhancements studied in TR 23.700-58 [2]. Furthermore, the present document considers solutions and analyses these to make recommendations for possible normative work taking into consideration the conclusions of TR 23.700-58 [2].

# 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 23.570-58: " Study of further architecture enhancements for uncrewed aerial systems and urban air mobility".

[3] 3GPP TS 22.125: "Uncrewed Aerial System (UAS) support in 3GPP".

[4] 3GPP TS 23.256: "Support of Uncrewed Aerial Systems (UAS) connectivity, identification and tracking".

[5] 3GPP TS 33.256: "Security aspects of Uncrewed Aerial Systems (UAS)".

# 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].

C2 Command and Control

DAA Detect And Avoid

UAS Uncrewed Aerial System

UAM Urban Air Mobility

UAV Uncrewed Aerial Vehicle

# 4 Overview

Editor’s Note: Will include some simple background for the TR

Requirements for UAS (Uncrewed Aerial System) are defined in TS 22.125 [3] with some specification done to address those requirements done in TS 23.256 [4] and TS 33.256 [5]. The present document will study the security issue arising from the study in TS 23.700-58 [2], which covers:

 - a mechanism to transport Broadcast Remote Identification and Command and Control (C2) communications via the 3GPP system; and

- a mechanism to support aviation applications such as Detect And Avoid (DAA).

# 5 Key Issues

## 5.1 Key issue #1: Direct C2 Security

### 5.1.1 Key issue details

In TR 23.700-58 [2], key issue #1 focuses on the transport of C2 communications over PC5 in the 3GPP system, while considering the following aspects:

"- how is the C2 communication over PC5 between a UAV and UAV controller established;

- how is the UAV authorized for setting up direct C2 communication over PC5 with a UAV controller, both for in-coverage and out of coverage scenarios, and how is the authorization revoked;

- whether the UAV needs to discover the UAV controller, or vice versa and if so, how?"

### 5.1.2 Security threats

The lack of security for the PC5 unicast link between UAV and UAV-C used for C2 communication may let the attackers to eavesdrop and control the UAV operations thereby leading to UAV hijack and misoperations.

### 5.1.3 Potential security requirements

The 3GPP system shall provide means for UAV and UAV-C to establish secure PC5 link used for C2 communication.

## 5.2 Key issue #2: Security of DAA unicast connection

### 5.2.1 Key issue details

Some solutions for transport of DAA traffic discuss using a unicast connection . In such cases, signalling might be needed to establish the connection between the appropriate entities and hence would need protection which could also be applied to the user plane.

### 5.2.2 Security threats

Signalling messages and data sent using a unicast connection for DAA can be modified or eavesdropped by an attacker.

### 5.2.3 Potential security requirements

The 5GS shall support the ability to confidentiality, integrity and replay protect any 3GPP signalling traffic used to establish and manage the unicast connection for DAA and any user plane of such a connection.

# 6 Solutions

## 6.X Solution #X: Title of solution

### 6.X.1 Introduction

### 6.X.2 Solution details

### 6.X.3 Evaluation

# 7 Conclusions

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

Editor’s Note: Delete Annex if not used.

Annex <X> (informative):
Change history

|  |
| --- |
| **Change history** |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2022-07 | SA3#107e Adhoc | S3-221607 |  |  |  | Approved skeleton (S3-221512) plus S3-221604, S3-221605 and S3-221610 | 0.1.0 |