|  |  |
| --- | --- |
| 3GPP TR 33.759 V0.1.0 (2024-04) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on security enhancements of Uncrewed Aerial Systems (UAS) Phase 3  (Release 19) | |
|  | |
|  |  |
| 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.  © 2024, 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

1 Scope 6

2 References 6

3 Definitions of terms, symbols and abbreviations 6

3.1 Terms 6

3.2 Symbols 7

3.3 Abbreviations 7

4 Overview and Security Assumptions 7

5 Key issues 7

5.1 Key Issue #1: security enhancements to NEF services in support of multiple USSs 7

5.1.1 Key issue details 7

5.1.2 Threats 7

5.1.3 Potential security requirements 8

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

5.X.1 Key issue details 8

5.X.2 Threats 8

5.X.3 Potential security requirements 8

6 Solutions 8

6.0 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 (informative): 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.

# 1 Scope

The present document identifies potential security and privacy issues and provides potential security solutions to support additional scenarios and requirements for UAV (Uncrewed Aerial Vehicle) and UAM (Urban Air Mobility) including:

- identify potential security issues and provide solutions for the enhanced NEF services to support service exposure and interactions between MNOs and UTM functions, e.g. security impact of supporting multiple USS.

- identify potential security and privacy issues related to network-assisted/ground-based mechanism for DAA (Detect And Avoid).

- identify potential security and privacy issues related to no-transmit zones for UAVs

Furthermore, the present document makes potential recommendations for possible normative work taking into consideration the conclusions of TR 23.700-59 [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 23.700-59: "Study on architecture enhancements of UAS, UAV and UAM; Phase 3"

[3] 3GPP TS 23.256: " Support of Uncrewed Aerial Systems (UAS) connectivity, identification and tracking; Stage 2"

[4] 3GPP TS 33.256: "Security aspects of Uncrewed Aerial Systems"

[5] 3GPP TS 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].

DAA Detect and Avoid

NTZ No-Transmit Zone

UAM Urban Air Mobility

UAV Uncrewed Aerial Vehicle

UTM Unmanned Aerial System Traffic Management

# 4 Overview and Security Assumptions

The TR 23.700-59 [2] describes the enhancements to the architecture and features defined in TS 23.256 [3] for supporting enhanced NEF service exposure, network-assisted/ground-based mechanism for Detect And Avoid (DAA) and no-transmit zones (NTZ) for UAVs. The TS 33.256 [4] specifies the security procedures and features in support of the system architecture and features defined in TS 23.256 [3].

The security assumptions are as follows:

- The existing security mechanisms and procedures specified in TS 33.256 [4] and TS 33.501 [5] should be reused as much as possible for solutions.

# 5 Key issues

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

## 5.1 Key Issue #1: security enhancements to NEF services in support of multiple USSs

### 5.1.1 Key issue details

In the TR 23.700-59 [2], a key issue has been included to enhance NEF services to support service exposure and interactions between MNOs and UTM functions, e.g. pre-mission flight planning and in-mission flight monitoring for UAVs and supporting multiple USSs serving different geographical areas corresponding to the UAV flight path. The UTM, taking the role of AF and interacting with the MNO, can be a third-party entity. The enhancements to the security procedures to support multiple USSs need to be studied to ensure security of UUAA and pairing authorization etc, since UAV is currently allowed to be served by single USS (see TS 33.256 [4], clause 5.2).

### 5.1.2 Threats

If security procedures, e.g. UUAA and paring authorization etc, are not adapted to support multiple USSs, the security procedures may fail in the multiple USS scenarios. For example, if a UAV is only authenticated and authorized by one USS, the UAV will be rejected by a second USS when the UAV flies into a different geographical areaserved by the second USS as the UAV was not authenticated or authorized by the second USS. In addition, the second USS can not perform flight monitoring of the entering UAV if the second USS is not authorized beforehand (since only the one USS is authenticated and authorized). This may become a risk for other UAVs and for public safety.

### 5.1.3 Potential security requirements

The 5G system shall ensure the security procedures support multiple USS scenarios.

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

### 5.X.1 Key issue details

### 5.X.2 Threats

### 5.X.3 Potential security requirements

# 6 Solutions

## 6.0 Mapping of solutions to key issues

Table 6.0-1: Mapping of Solutions to Key Issues

| Solutions | Key Issues |
| --- | --- |
| X |

## 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 A (informative):  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2024-04-08 | SA3#115Adhoc-e | S3-241224 |  |  |  | TR skeleton | 0.0.0 |
| 2024-04-22 | SA3#115Adhoc-e | S3-241503 |  |  |  | Approved skeleton (S3-241224) plus S3-241540, S3-241502 and S3-241551 | 0.1.0 |