|  |
| --- |
| 3GPP TR 33.891 V0.5.0 (2023-01) |
| 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.© 2023, 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 5

1 Scope 7

2 References 7

3 Definitions of terms, symbols and abbreviations 7

3.1 Terms 7

3.2 Symbols 7

3.3 Abbreviations 8

4 Overview 8

5 Key Issues 8

5.1 Key issue #1: Direct C2 Security 8

5.1.1 Key issue details 8

5.1.2 Security threats 8

5.1.3 Potential security requirements 9

5.2 Key issue #2: Security of DAA unicast connection 9

5.2.1 Key issue details 9

5.2.2 Security threats 9

5.2.3 Potential security requirements 9

5.3 Key issue #3: Direct C2 Authorization 9

5.3.1 Key issue details 9

5.3.2 Security threats 9

5.3.3 Potential security requirement 10

5.4 Key issue #4: UAV/UAV-C Privacy over PC5 link for C2 10

5.4.1 Key issue details 10

5.4.2 Security threats 10

5.4.3 Potential security requirement 10

5.5 Key issue #5: Privacy protection over PC5 for DAA unicast messages 10

5.5.1 Key issue details 10

5.5.2 Security threats 11

5.5.3 Potential security requirements 11

5.6 Key issue #6: Privacy and security aspects of broadcast DAA traffic 11

5.6.1 Key Issue Details 11

5.6.2 Security Threats 11

5.6.3 Potential Security Requirements 11

5.7 Key issue #7: Privacy and security aspects of Broadcast Remote ID 11

5.7.1 Key Issue Details 11

5.7.2 Security Threats 11

5.7.3 Potential Security Requirements 11

6 Solutions 12

6.1 Solution #1: Security establishment and link security protection of unicast PC5 communication 12

6.1.1 Introduction 12

6.1.2 Solution details 12

6.1.3 Evaluation 13

6.2 Solution #2: Solution to secure direct C2 and DAA connection 13

6.2.1 Introduction 13

6.2.2 Solution details 13

6.2.3 Evaluation 15

6.3 Solution #3: C2 and DAA unicast security using V2X unicast solution 16

6.3.1 Introduction 16

6.3.2 Solution details 16

6.3.3 Evaluation 16

6.4 Solution #4: Direct C2 communication over PC5 security 17

6.4.1 Introduction 17

6.4.2 Solution details 17

6.4.3 Evaluation 18

6.5 Solution #5: Restricted Discovery for Direct C2 18

6.5.1 Introduction 18

6.5.2 Solution details 18

6.5.3 Evaluation 19

6.6 Solution #6: Privacy for 3GPP identifiers used to transport DAA traffic 19

6.6.1 Introduction 19

6.6.2 Solution details 19

6.6.3 Evaluation 19

6.7 Solution #7: Privacy for 3GPP identifiers used to transport Broadcast Remote ID 20

6.7.1 Introduction 20

6.7.2 Solution details 20

6.7.3 Evaluation 20

7 Conclusions 20

7.1 Conclusion for Key issue #1 20

7.2 Conclusion for Key issue #2 20

7.3 Conclusion for Key issue #3 21

7.4 Conclusion for Key issue #4 21

7.5 Conclusion for Key Issue #5 21

7.6 Conclusion for Key Issue #6 21

7.7 Conclusion for Key Issue #7 21

Annex A (informative): Change history 22

# 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 23.700-58: "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)".

[6] 3GPP TS 33.536: "Security aspects of 3GPP support for advanced Vehicle-to-Everything (V2X) services".

[7] 3GPP TS 33.503: "Security Aspects of Proximity based Services (ProSe) in the 5G System (5GS)".

[8] 3GPP TS 23.287: "Architecture enhancements for 5G System (5GS) to support Vehicle-to-Everything (V2X) services".

# 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].

## 3.2 Symbols

Void.

## 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

Some requirements for UAS (Uncrewed Aerial System) defined in TS 22.125 [3] are not addressed in TS 23.256 [4] and TS 33.256 [5], which includes:

- Direct C2 communication: the UAV controller and UAV establish a direct C2 link to communicate with each other and both are registered to the 5G network using the radio resource configured and scheduled provided by the 5G network.

- Broadcast UAS Remote Identification (Remote ID) services. UAS Remote ID refers to a UAS in flight provides identification and tracking information that can be received by regulatory agencies.

- Collision avoidance: UAV can navigate safely from one place to its goal without colliding with other UAVs or obstacles.

The requirements above are studied in TS 23.700-58 [2] for architecture aspects and this present document for security aspects, which covers:

 - a mechanism for Command and Control (C2) communications over PC5 interface in3GPP system;

- a mechanism to transport Broadcast Remote Identification; 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.

## 5.3 Key issue #3: Direct C2 Authorization

### 5.3.1 Key issue details

TS 23.256 [4] and TS 33.256 [5] describe how the UAV pairing with a UAV-C is authorized by a USS over a PDU Session for C2 communications performed over Uu.

In TR 23.700-58 [2], key issue #1 focuses on the support for transport of C2 communications over PC5 in the 3GPP system and 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;*

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

The following service requirement in TS 22.125 [3] applies to the C2/pairing authorization, independently of the communication mode used to operate the UAV i.e., over Uu or direct over PC5:

 *[R-5.1-010] The 3GPP system shall enable UTM to inform an MNO of the outcome of an authorisation to operate.*

This is further captured for direct C2 in TR 23.700-58 [2] architectural assumption:

*- A UAV shall obtain authorization from 3GPP system and USS to perform direct C2 communication as defined in TS 22.125 [4].*

The solutions in TR 23.700-58 [2] (e.g., solution#1, #4) propose to support Direct C2 communication between UAV and UAV-C considering that UAV and UAV-C may be pre-paired or dynamically paired.

### 5.3.2 Security threats

If pairing authorization of UAV and UAV-C is not performed securely before establishment of a direct connection between the UAV and UAV-C, an unauthorized UAV-C may be able to communicate with the UAV and perform an unauthorized flight which could cause tremendous risks to the security of UAS and public safety.

If 3GPP system is not capable to handle revocation of the direct connectivity pairing authorization from USS, then USS might not be able to take appropriate measures to deal with misbehaving UAVs which might cause accidents or become attack vectors.

### 5.3.3 Potential security requirement

3GPP system shall support enabling authentication and authorization by the USS of a UAV and UAV-C pairing before enabling a direct data connection over PC5 between the UAV and UAV-C

3GPP system shall provide means for the USS to revoke a UAV and UAV-C pairing authorization in order to close the direct connection over PC5 between the UAV and UAV-C.

## 5.4 Key issue #4: UAV/UAV-C Privacy over PC5 link for C2

### 5.4.1 Key issue details

In TR 23.700-58 [2], key issue #1 focuses on the support for transport of C2 communications over PC5 in the 3GPP system and 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?"*

3GPP system has to be able to protect the privacy of the UE (UAV or UAV-C) privacy sensitive identities when using PC5 link during direct discovery or for direct communications over the PC5 unicast link.

NOTE 1: Broadcast Remote ID (BRID) is not considered in this key issue.

### 5.4.2 Security threats

If privacy sensitive identities of the UE (i.e., UAV or UAV-C) are not protected during direct discovery or direct C2 communication over the PC5 unicast link procedures used for C2, an eavesdropper can perform privacy attacks on the UE (UAV/UAV-C).

### 5.4.3 Potential security requirement

The 5G System should provide means for mitigating trackability and linkability attacks on UAV/UAV-C during communications over the PC5 unicast link used for C2.

The 5G System should provide means for mitigating trackability and linkability attacks on UAV/UAV-C during discovery over the PC5 link used for C2.

## 5.5 Key issue #5: Privacy protection over PC5 for DAA unicast messages

### 5.5.1 Key issue details

KI#3 in TR 23.700-58 [2] addresses the support of DAA, and solutions such as #5 and#7 propose the unicast between entities over PC5 for DAA, this may introduce privacy issues for unicast messages related to long duration unicast session, e.g. source L2 ID tracking. If the same L2 ID is used by a UE for a certain period of time, it is possible that other UEs and/or attackers can track and identify the source of the message based on the PC5 parameters sent as part of the PC5 transmissions.

### 5.5.2 Security threats

An adversary that is capable of connecting and linking L2 identities to a real or a long-term Application Layer ID will be able to track and trace the endpoint in space and time. Such trackability and linkability will be an attack on U2X endpoint privacy.

### 5.5.3 Potential security requirements

The 5G System shall provide means for mitigating trackability attacks on L2 identities during U2X unicast communications over PC5 for DAA.

The 5G System shall provide means for mitigating linkability attacks on L2 identities during U2X unicast communications over PC5 for DAA.

## 5.6 Key issue #6: Privacy and security aspects of broadcast DAA traffic

### 5.6.1 Key Issue Details

The protection of the broadcast DAA traffic is left out of scope of 3GPP, e.g. similar to V2X application as the application will be defined outside 3GPP. If the 3GPP transport of broadcast DAA traffic is not privacy protected, it may lead to tracking of the UAVs.

### 5.6.2 Security Threats

If the 3GGP identities used in transporting broadcast DAA traffic are not privacy protected, then it may be possible to track the UAV.

### 5.6.3 Potential Security Requirements

The 3GPP system shall provide a means to mitigate privacy risks of 3GPP identities used to transport broadcast DAA traffic.

## 5.7 Key issue #7: Privacy and security aspects of Broadcast Remote ID

### 5.7.1 Key Issue Details

The protection of the Broadcast Remote ID depends on national regulation and hence is better left out of scope of 3GPP, e.g. similar to V2X application. However for the UAV communication in the 3GPP system, Broadcast Remote ID can be broadcast by the UAV using 3GPP transport. If the 3GPP transport of Broadcast Remote ID is not privacy protected, it may lead to tracking of the UAVs.

### 5.7.2 Security Threats

If the 3GGP identities used in transporting Broadcast Remote ID are not privacy protected, then it may be possible to track the UAV.

### 5.7.3 Potential Security Requirements

The 3GPP system should provide a means to mitigate privacy risks of 3GPP identities used to transport the Broadcast Remote ID.

NOTE: The 3GPP system provides means for mitigating privacy risks of 3GPP identities if Broadcast Remote ID is subject to privacy protection, based on local regulation.

# 6 Solutions

## 6.1 Solution #1: Security establishment and link security protection of unicast PC5 communication

### 6.1.1 Introduction

This solution addresses the direct PC5 communication (unicast) for both the direct C2 and unicast DAA scenarios as specified in Key Issue #1 and Key Issue #2, respectively. Generally, unicast security establishment specified in eV2X TS 33.536 [6] and 5G ProSe TS 33.503 [7] is reused as the baseline.

### 6.1.2 Solution details

The unicast PCF communication establishment starts with a Direct Communication Request (DCR) message to send the initiating UE’s security capabilities and to trigger the mutual authentication and key establishment. After mutual authentication and key establishment, the Direct Security Mode Command and the Direct Security Mode Complete messages are emitted to inform the selected security protection algorithms for the connection and the initiating UE’s user plane security policies (i.e. user plane confidentiality and integrity protection policies), respectively. Finally, the receiving UE replies a Direct Communication Accept (DCA) message to confirm the user plane protection methods and finish the unicast PC5 communication establishment procedures.

The signalling and user plane security protection are protected based on the detailed negotiation procedures:

0. UAS security-related parameter (for unicast secure communication over PC5) pre-configuration and previsioning, the signalling messages are integrity protected and the signalling ciphering protection is a configuration option.

NOTE 1: Step 0 is done only in coverage.

1. UAS discovery procedures may happen for the UAV and UAVC to find each other in direct C2 scenario.

NOTE 2: Whether or not the UAV needs to discover the UAVC or vice versa will align with the decision in SA2.

2. The initiating UE (UAV or UAVC) starts DCR message contains its security capabilities and signalling security policy. The security capabilities are the confidentiality and integrity protection algorithms that the initiating UE accepts for this connection. The security capabilities are reused as specified in TS 33.536 [6] and TS 33.503 [7]. The direct C2 or unicast DAA service use the ‘REQUIRED’ signalling security protection policies if the service needs security protection.

3. To generate the PC5 root key to protect the PC5 connection, the receiving UE may initiate the Direct authentication and key establishment procedures with the initiating UE.

4. The receiving UE uses the Chosen\_algs to indicate the selected confidentiality and integrity protection algorithms of this link and contains the Chosen\_algs in the Direct Security Mode Command message. The initiating UE’s security capabilities are sent back to the initiating UE to mitigate the bidding down attack. The receiving UE integrity protects the Direct Security Mode Command message before sending it to the initiating UE.

5. The initiating UE sends its user plane security policy to the receiving UE by using Direct Security Mode Complete message.

6. The receiving replies the DCA message to accept the DCR message and the unicast PC5 communication establishment including the user plane security indication. The user plane security protection methods (the user plane with or without confidentiality and/or integrity protection) are explicitly indicated by using the user plane security indication.

### 6.1.3 Evaluation

This solution addresses the security requirements of Key Issue #1 and #2. The solution reuses the PC5 unicast connection establishment so that the signalling/user plane of PC5 links are integrity and/or confidentiality protected based on the security policy.

## 6.2 Solution #2: Solution to secure direct C2 and DAA connection

### 6.2.1 Introduction

The solution addresses KI#1, KI#2 and KI#3.

The solution provides an overview of direct U2X connection security which describes (i) how 5GS can provide means for UAV and UAV-C to establish secure PC5 link for Command and Control (C2) communication service(s) and (ii) how 5GS can support the ability to confidentiality, integrity and replay protect any 3GPP signalling traffic used to establish and manage the unicast connection for Detect and Avoid (DAA) service(s).

Further the solution also describes to enable authentication and authorization by the USS of the UAV and UAV-C pairing before enabling a direct C2 connection over PC5 between UAV and UAV-C.

### 6.2.2 Solution details

UAV-to-Everything (U2X) services such as C2 and direct DAA can utilize PC5 link for establishing C2 connection (i.e., between UAV and UAV-C) and for establishing unicast connection for DAA (between UAVs) respectively as discussed in TR 23.700-58 [2].

The procedure to establish a secure U2X service direct communication is shown in the following figure 6.2.2-1.



Figure 6.2.2-1 Secure U2X service direct communication establishment

The steps shown in Figure 6.2.2-1 is described as follows:

1a-b. If the UAV is capable of Uu communication, the UAV performs UUAA procedure and C2 authorization (if required) as described in TS 23.256 [4] and TS 33.256 [5]. The UAV obtains UAV-C pairing information (if not configured already) and U2X security policy for each U2X services (i.e., C2 and DAA) along with the result of successful C2 authorization. The U2X security policy includes signalling and user plane security policy per U2X service type (i.e., for C2 and DAA, the signalling and user plane confidentiality and integrity are set as required based on local policy), pairing restrictions list, and access restriction information (i.e., UAV information which are restricted to perform DAA).

 Similarly, the UAV-C can also perform UUAA procedures and C2 authorization as described in TS 23.256 [4] and TS 33.256 [5]. The UAV-C obtains UAV pairing information (if not configured already), U2X security policy for each U2X services (i.e., C2 and DAA) along with the result of successful C2 authorization. Alternatively, these data may be configured by the USS in UAV-C which is up to USS.

NOTE 1: UUAA and C2 authorization for UAV-C is not covered in Rel-17.

2. The UAV if determines to set up C2 communication over PC5, it sends Direct Communication Request with U2X service type which indicates C2 service, UAV identifier (i.e., CAA-Level UAV ID), UAV-C identifier, U2X service security policy specific to the C2 service (i.e., confidentiality and integrity protection requirements for signalling and user plane protection), security capability and key establishment information (as described in TS 33.536 [6]) which can be related to security information for C2 security.

3. The UAV-C on receiving the direct communication request, if the U2X service type indicates C2 service, the UAV-C verifies the received U2X service security policy and UAV ID against the locally configured U2X security policy which includes the Pairing restrictions list and U2X service security policy. If the received UAV ID is same as any of the UAV ID(s) in the (authorized) pairing restrictions list and if the U2X service security policy matches with the locally stored one, then the UAV-C determines to respond with step 4.

 If the UAV ID in the direct communication request do not match with any of the UAV ID(s) in the pairing restrictions list or if the received U2X service security policy violates the locally configured U2X service security policy for the C2 service, then the UAV-C determines to reject the direct communication, where the UAV-C skip steps 4-6a and performs step 6b.

4. UAV-C performs direct authentication and key establishment (as described in TS 33.536 [6]) with the UAV.

5a. The UAV-C sends to the UAV, the Direct security mode command which includes (information as in TS 33.536 [6]) Key\_Est\_Info, MSB of Key ID (e.g., KNRP ID to indicate the C2 security key), security capability, and additional information such as those received in step 1 (i.e., U2X service type, U2X service security policy). The session key (i.e., for C2), PC5 signalling and user plane keys (for confidentiality and the integrity) as required can be derived to protect the C2 service based on the U2X service security policy.

5b. The UAV checks that the returned security capabilities, U2X service type and U2X service security policy are the same as those it sent in step 1. The UAV on receiving the Direct security mode command, if the above check is successful, based on received Key\_Est\_Info (as in TS 33.536 [6]) derives the key and choose LSB of Key ID (e.g., KNRP ID) to uniquely identify the Key and locally store the key with the identifier. Then the UAV sends to the UAV-C, the Direct security mode complete message which includes LSB of Key ID, security capabilities, U2X service type, and U2X service security policy sent in step 1. The confidentiality key and the integrity key as required can be derived to protect the C2 service based on the U2X service security policy.

6a. The UAV-C sends Direct Communication Accept over the established link. The UAV and UAV-C can start C2 communication over PC5.

6b. The UAV-C based sends a direct communication reject message (i.e., if the U2X security policy is not met, or if authentication and key establishment fails or if the direct security mode command procedure fails) with respective cause information.

**Security of DAA unicast connection:**

Direct UAV to UAV communication for the purpose of DAA can use PC5 (e.g., C-V2X) as described in TR 23.700‑58 [2] Clause 5.3. To enable confidentiality, integrity and relay protection for DAA related unicast connection, the procedure described using Figure 6.2.2-1 can be used with the following DAA specific adaptations.

2. If the UAV (e.g., UAV 1) determines to set up DAA connection over PC5, it sends Direct Communication Request with U2X service type which indicates DAA service, UAV identifier (i.e., CAA-Level UAV ID), U2X service security policy specific to the DAA service (i.e., confidentiality and integrity protection requirements for signalling and user plane protection), security capability and key establishment information (as described in TS 33.536) which can be related to security information for DAA security.

3. The UAV (e.g., UAV 2) on receiving the direct communication request, if the U2X service type indicates DAA service, the UAV-C verifies the received U2X service security policy and UAV ID against the locally configured U2X security policy which includes the access restriction information (i.e., UAV information which are restricted to perform DAA) and U2X service security policy. If the received UAV ID not part of access restriction information, and if the U2X service security policy matches with the locally stored one, then the UAV determines to respond with step 4.

 If the UAV ID in the direct communication request match with any of the UAV ID(s) in the access restriction information or if the received U2X service security policy violates the locally configured U2X service security policy for the DAA service, then the UAV-C determines to reject the direct communication, where the UAV skip steps 4-6a and performs step 6b.

4. UAV (e.g., UAV 2) performs direct authentication and key establishment (as described in TS 33.536 [6]) with the UAV (e.g., UAV 1).

5a. The UAV (e.g., UAV 2) sends to the UAV (e.g., UAV 1), the Direct security mode command which includes (information as in TS 33.536 [6]) Key\_Est\_Info, MSB of Key ID (e.g., KNRP ID to indicate the DAA security key), security capability, and additional information such as those received in step 1 (i.e., U2X service type, U2X service security policy). The session key (i.e., for DAA), PC5 signalling and user plane keys (for confidentiality and the integrity) as required can be derived to protect the DAA service based on the U2X service security policy.

5b. The UAV (e.g., UAV 1) checks that the returned security capabilities, U2X service type and U2X service security policy are the same as those it sent in step 1. The UAV on receiving the Direct security mode command, if the above check is successful, based on received Key\_Est\_Info (as in TS 33.536 [6]) derives the key and choose LSB of Key ID (e.g., KNRP ID) to uniquely identify the Key and locally store the key with the identifier. Then the UAV (e.g., UAV 1) sends to the UAV (e.g., UAV 2), the Direct security mode complete message which includes LSB of Key ID, security capabilities, U2X service type, and U2X service security policy sent in step 1. The confidentiality key and the integrity key as required can be derived to protect the DAA service based on the U2X service security policy.

6a. The UAV (e.g., UAV 2) sends Direct Communication Accept over the established link. The UAVs can start DAA communication over PC5.

6b. The UAV (e.g., UAV 2) based sends a direct communication reject message (i.e., if the U2X security policy is not met, or if authentication and key establishment fails or if the direct security mode command procedure fails) with respective cause information.

### 6.2.3 Evaluation

The solution has the following impacts:

- UE: Need to be provided with U2X security policy which includes service specific security policy (signalling and user plane security policy per U2X service type i.e., for C2 and DAA), pairing restrictions list (to allow only authorized UAV and UAV-C to be paired) and optionally may include access restriction information (to prevent any misbehaving UAVs to involve in any direct communication).

- -Need to indicate U2X service specific security policy (i.e., confidentiality and integrity protection requirements for signalling and user plane protection) in the direct connection request/responses.

 Need to indicate U2X service type in the direct communication related requests and responses to allow only related communication in the direct connection and to prevent misuse of direct connections (e.g., a UAV that sets up direct connection for DAA should not attempt C2 message exchange).

## 6.3 Solution #3: C2 and DAA unicast security using V2X unicast solution

### 6.3.1 Introduction

This solution addresses all of key issues #1, #2, #4 and #5. It re-uses the security procedures for unicast security for V2X (see TS 33.536 [6]).

### 6.3.2 Solution details

TS 33.536 [6] contains a method of establishing security for a unicast connection for V2X services. This solution proposes to re-use those procedures for establishing the security of C2 and DAA unicast connections. The relevant procedures are given in clause 5.3.3 of TS 33.356 [6].

NOTE 1: Whether discovery happens before the start of communication does not affect the set-up of the security.

NOTE 2: This solution assumes that the credentials used to protect the DAA traffic are defined outside of 3GPP specification. Hence the Key\_Est\_Info IE described in clause 5.3.3.1.3.2 of TS 33.536 [6] is used to transport the needed authentication signalling to establish PC5 keys. This IE enables authentication over PC5 using credentials and methods specified outside 3GPP.

NOTE 3: This solution is independent of the pairing method used and of the method used to establish security material at the UEs (i.e. UAV and UAV-C) to set up the security.



Figure 6.3.2-1: Message flow for the establishment of unicast security

Figure 6.3.2-1 gives an overview of the flow for (re-)establishing security for unicast connections (see TS 33.536 [6] for the details). The security policy relevant to the service (i.e. DAA or C2) will be used when establishing a connection for that service. C2 and DAA traffic will only be accepted from a peer authorised to send such traffic and be sent on different connections.

In addition to address the privacy issue of re-using identities, Link identifier update and Layer-2 release procedures are performed as described in clauses 5.3.3.2.2.1 and 5.3.3.2.2.2 of TS 33.356 [6].

### 6.3.3 Evaluation

The solution follows the V2X methods of establishing security and hence requires no new normative work. The solution works with whatever method is used to authorise the pairing for C2. It also works with all methods of providing the security material to the UEs (e.g. pre-configuration or delivery from the UAS).

## 6.4 Solution #4: Direct C2 communication over PC5 security

### 6.4.1 Introduction

This solution addresses the following key issues: Key issue #1: Direct C2 Security, Key issue #3: Direct C2 Authorization, and Key issue #4: UAV/UAV-C Privacy over PC5 link for C2.

In this solution, a UAV and a UAV-C establish a secure PC5 unicast link for C2 communication based on procedure described in TS 33.536 [6]. Both UAV and UAV-C supports PC5, with optional support for Uu connection.

The UAV that uses Uu connection is authenticated and authorized by the USS for C2 communication prior to establishing C2 communication over PC5, as per existing Rel-17 procedures. The UAV may receive security information for C2 over PC5 (e.g., key material) through these procedures, in the case of dynamic pairing with UAV-C. The UAV/UAV-c may also be preconfigured with security credentials (e.g., long term key) in the case of static pairing (i.e., pairing is pre-determined).

### 6.4.2 Solution details



Figure 6.4.2-1: PC5 unicast security establishment for C2 communication between UAV and UAV-C

1. The UAV performs UUAA procedure as described in TS 33.256 [5], clause 5.2.1. The UAV may obtain a new CAA-Level UAV ID through this procedure. The UAV uses the new CAA-Level UAV ID or a pre-configured CAA-Level UAV ID in the following steps.

2. The UAV performs Pairing Authorization procedure as described TS 33.256 [5], clause 5.4. The UAV may obtain UAV-C identifier and security information (e.g., key material) during this procedure. The UAV uses the received information or pre-configured information during the following link establishment procedure.

3. The UAV sends Direct Communication Request to initiate the PC5 unicast link establishment. The DCR includes:

- Source User Info: the UAV's Application Layer ID (e.g., CAA-Level UAV ID or any other application layer ID assigned for C2 over PC5).

- Target User Info: if the UAV-C identifier is known (e.g., received in step 2 or pre-configured), the UAV uses it as the target user info. If the UAV-C identifier is not available, Target User Info is not included in the DCR and service-oriented link established as described in TS 23.287 [8] clause 6.3.3.1 is performed.

- C2 Communication Service Identifier: this identifier is equivalent to V2X Service Type (see TS 23.287 [8]]). It may be preconfigured or derived from the UAV's CAA-Level UAV ID. It is used during the discovery of the C2 peer (UAV/UAV-C) with service-oriented method (e.g., for dynamic UAV-UAV-C pairing).

4. The UAV and UAV-C may perform a mutual authentication before next step as described in TS 33.536 [6] if the pairing is pre-determined with security credentials (e.g., long term key) pre-configured. This step is skipped if UAV/UAV-C have valid key material (e.g., KNRP and KNRP ID pair).

5. The UAV and UAV-C establishes the security for the PC5 link as described in TS 33.536 [6]. The UAV and UAV-C establish the security based on the security information (i.e., key material) received from step 2 or key material derived from a prior mutual authentication.

6. The UAV-C sends Direct Communication Accept over the established link.

7. The UAV and UAV-C engage in C2 communication over the secure PC5 unicast link.

**Privacy of identities over the PC5 unicast link:**

- To ensure the privacy of UAV/UAV-C during communication over the PC5 unicast link, the procedures for identity privacy as defined in TS 33.536 [6], clause 5.3.3.2 are reused.

### 6.4.3 Evaluation

For the security and privacy of Direct C2 communication over PC5 unicast link, this solution proposes to reuse security establishment and privacy protection mechanisms as defined in TS 33.536 [6].

This solution proposes that the authorization for Direct C2 communication over PC5 unicast link is based on C2 authorization procedure defined in TS 33.256 [5]. The UE uses pre-configured information or received from USS (e.g., CAA Level UAV ID, key material) during the PC5 unicast link establishment.

The solution fully addresses the security requirements of Key issue #1: Direct C2 Security, Key issue #3: Direct C2 Authorization.

The solution fully addresses first requirement of Key issue #4: UAV/UAV-C Privacy over PC5 link for C2.

## 6.5 Solution #5: Restricted Discovery for Direct C2

### 6.5.1 Introduction

This solution addresses Key issue #4: UAV/UAV-C Privacy over PC5 link for C2 during discovery.

This solution proposes to reuse the security procedure for Restricted 5G ProSe Direct Discovery as defined in TS 33.503 [7], clause 6.1.3.2 as the baseline to provide confidentiality protection of the discovery messages to ensure the privacy of the UAV/UAV-C when dynamic discovery is used between UAV and UAV-C equipped with a UE.

This solution proposes that the UAS NF may play a role similar (but simplified) to the ProSe AF on behalf of the USS. It is assumed that the USS is not expected to support DIAMETER-based protocols, SBA, or ProSe specific functionality (e.g., ProSe Application Code Suffix) as per existing aviation community requirements from Rel-17.

### 6.5.2 Solution details

As part of the Direct Discovery procedure, the UAV may act as the Announcing UE or Monitoring UE (and vice-versa for the UAV-C).

The following steps are between the UE and DDNMF:

- The Announcing UE sends RPAUID corresponding to an aviation domain application User ID (e.g., CAA Level UAV ID) and its UE ID (i.e., GPSI) to the 5G DDNMF in its HPLMN and obtains a ProSe Restricted Code to announce and associated Code-Sending security parameters from the 5G DDNMF. For that, the 5G DDNMF checks for the announce authorization with the UAS NF which may check with USS and/or from locally stored information. If the UE is a UAV, the UAS NF verifies that a valid UUAA result is stored for the UE ID.

- The Monitoring UE sends its RPAUID, a target RPAUID corresponding to an aviation domain application User ID (e.g., CAA Level UAV ID) and its UE ID (i.e., GPSI) to the 5G DDNMF in its HPLMN and obtains Discovery Filter and the Code-Receiving Security Parameters from the 5G DDNMF to be allowed to monitor for the Restricted ProSe Application User IDs. For that, the 5G DDNMF checks for the monitoring authorization with the UAS NF which checks with USS if the RPAUID is allowed to discover/be paired with the target RPAUID. The 5G DDNMF of Monitoring UE may contact the 5G DDNMF of Announcing UE if they belong to different PLMNs.

The following steps are over PC5:

- The Announcing UE protects the announced discovery message using the Code-Sending security parameters as described in TS 33.503 [7], Figure 6.1.3.2.2.1-1 step 11.

- The Monitoring UE processes the security of discovery messages security that satisfies its Discovery Filter using the Code-Receiving Security Parameters as described in TS 33.503 [7], Figure 6.1.3.2.2.1-1 step 12 and 13-16 (if match reporting required).

### 6.5.3 Evaluation

The solution proposes to use reuse the security procedure for Restricted 5G ProSe Direct Discovery as defined in TS 33.503 [7], clause 6.1.3.2, as the baseline, with UAS NF providing abstraction of ProSe specific aspects from USS (solution assumes that USS will not support ProSe AF like functionality).

The solution addresses 2nd requirement of Key issue #4: UAV/UAV-C Privacy over PC5 link.

## 6.6 Solution #6: Privacy for 3GPP identifiers used to transport DAA traffic

### 6.6.1 Introduction

This solution addresses the Privacy and security aspects of DAA traffic as specified in key issue #6.

### 6.6.2 Solution details

The below privacy procedures follow the privacy mechanism defined in TS 33. 536 [6] for V2X which is intended to mitigate against the threat of tracking the UE by an attacker based on its used 3GPP identities.

The UE changes and randomizes its 3GPP identities, e.g. source Layer-2 ID and source IP address including IP prefix (if used), when the identities used in the DAA traffic is changed. The UE can change and randomize these identities at other times. The UE provides an indication to the UAS application layer whenever the 3GPP identities are changed.

### 6.6.3 Evaluation

The solution mitigates the privacy issue of the 3GPP identifiers by ensuring that the 3GPP identities are not used for longer than the identities in the application.

## 6.7 Solution #7: Privacy for 3GPP identifiers used to transport Broadcast Remote ID

### 6.7.1 Introduction

This solution addresses the Privacy and security aspects of Broadcast Remote ID as specified in key issue #7.

### 6.7.2 Solution details

The below privacy procedures follow the privacy mechanism defined in TS 33. 536 [6] for V2X which is intended to mitigate against the threat of tracking the UE by an attacker based on its used 3GPP identities.

The UE changes and randomizes its 3GPP identities, e.g. source Layer-2 ID and source IP address including IP prefix (if used), when the identities used in the Broadcast Remote ID is changed. The UE can change and randomize these identities at other times. The UE provides an indication to the UAS application layer whenever the 3GPP identities are changed.

NOTE 1: The change of 3GPP identities is needed if Broadcast Remote ID is subject to privacy protection, based on local regulation.

### 6.7.3 Evaluation

The solution mitigates the privacy issue of the 3GPP identifiers by ensuring that the 3GPP identities are not used for longer than the identities in the application.

# 7 Conclusions

## 7.1 Conclusion for Key issue #1

To address ‘Key issue #1: Direct C2 Security’, following aspects are recommended for the normative work:

A secure PC5 unicast link for C2 service related communication can be established by re-using unicast mode security establishment procedures defined in TS 33.536 [5] as baseline with the following adaptations:

- C2 service specific security policy is used for the security establishment.

- Further C2 service specific adaptations (e.g., usage of UAV ID such as CAA-level UAV ID), or network support for transport of USS provided security materials, if any, related to unicast security establishment are up to the normative work.

## 7.2 Conclusion for Key issue #2

To address ‘Key issue #2: Security of DAA unicast connection’, following aspects are recommended for the normative work:

A secure mechanism for DAA leveraging U2X (UAV-to-everything) can be enabled, by re-using unicast mode PC5 connection security establishment procedures defined in TS 33.536 [5] as baseline with the following adaptations:

- DAA service specific security policy is used for the security establishment.

- Further DAA service specific adaptations (e.g., usage of UAV ID such as CAA-level UAV ID) if any related to security establishment are up to the normative work.

## 7.3 Conclusion for Key issue #3

Authorization for Direct C2 communication over PC5 unicast link can reuse C2 authorization procedure defined in TS 33.256 [5] as baseline. The UAV UE can perform Direct C2 communication authorization based on this procedure before initiating UAV to UAV-C Direct C2 communication over PC5.

NOTE 1: Additional details on network transport of USS provided authorization information will be determined during the normative phase.

NOTE 2: Other methods of authorisation are supported (see TR 23.700-58 [2]).

## 7.4 Conclusion for Key issue #4

Privacy of identities used over PC5 unicast link for Direct C2 communication is based on Link identifier update and Layer-2 release procedures as described in TS 33.356 [6] i.e., for KI#4 first requirement.

Privacy of identities during discovery between UAV and UAV-C is supported based on Restricted 5G ProSe Direct Discovery procedure as defined in TS 33.503 [7], clause 6.1.3.2.

NOTE: The second requirement above only applies if ProSe Discovery is specified for C2. Furthermore in such a case, additional details on the support for Restricted 5G ProSe Direct Discovery with USS will be determined during the normative phase.

## 7.5 Conclusion for Key Issue #5

The security of DAA unicast connection over PC5 is recommended for the normative work based on the PC5 link identifier privacy for PC5 unicast link procedures as specified in clause 5.3.3.2 of TS 33.536 [6].

## 7.6 Conclusion for Key Issue #6

The privacy aspects of broadcast DAA traffic is recommended for the normative work based on solution #6.

The integrity and confidentiality aspects of broadcast DAA traffic are left out of scope of 3GPP.

## 7.7 Conclusion for Key Issue #7

The privacy aspects of broadcast BRID traffic are recommended for the normative work based on solution #7.

The integrity and confidentiality aspects of broadcast BRID traffic are left out of scope of 3GPP.

Annex A (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 |
| 2022-09 | SA3#108e | S3-222323 |  |  |  | Incorporating S3-221755, S3-222087, S3-222268, S3-222361, S3-22362, S3-222427 and S3-222428. | 0.2.0 |
| 2022-09 | SA3#108e-adhoc | S3-223129 |  |  |  | Incorporating S3-222509, S3-222736, S3-222755, S3-222758, S3-222759, S3-222941, S3-222942, S3-223095 and S3-223128. | 0.3.0 |
| 2022-11 | SA3#109 | S3-224112 |  |  |  | Incorporating S3-223324, S3-223355, S3-223356, S3-223358, S3-223468, S3-223879, S3-224094, S3-224116, S3-224118 and S3-224119. | 0.4.0 |
| 2023-01 | SA3#109e-adhoc | S3-230441 |  |  |  | Incorporating S3-230277, S3-230278, S3-230279, S3-230280, S3-230284, S3-230433, S3-230434, S3-230449 and S3-230450. | 0.5.0 |