|  |
| --- |
| 3GPP TR 33.759 V0.5.0 (2024-11) |
| 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 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.© 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 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 and Security Assumptions 8

5 Key issues 8

5.1 Key Issue #1: security enhancements to NEF services in support of multiple USSs 8

5.1.1 Key issue details 8

5.1.2 Threats 8

5.1.3 Potential security requirements 8

5.X Key Issue #X: <Key Issue Name> 9

5.X.1 Key issue details 9

5.X.2 Threats 9

5.X.3 Potential security requirements 9

6 Solutions 9

6.0 Mapping of solutions to key issues 9

6.1 Solution #1: UAV Authentication and Authorization for Multiple USS 9

6.1.1 Introduction 9

6.1.2 Solution details 10

6.1.3 Evaluation 10

6.2 Solution # 2: UUAA supporting multiple USS 10

6.2.1 Introduction 10

6.2.2 Solution details 11

6.2.3 Evaluation 11

6.3 Solution # 3: Pairing authorization supporting multiple USS 11

6.3.1 Introduction 11

6.3.2 Solution details 11

6.3.3 Evaluation 12

6.4 Solution # 4: revocation supporting multiple USS 12

6.4.1 Introduction 12

6.4.2 Solution details 12

6.4.3 Evaluation 12

6.5 Solution #5: UUAA and authorization of target USS for the multiple USS case 13

6.5.1 Introduction 13

6.5.2 Solution details 13

6.5.2.1 Identification of USS-level changeover need 13

6.5.2.2 Enhancement for UUAA 13

6.5.2.3 Enhancement for authorization of target USS to use exposure services for the UAV 13

6.5.3 Evaluation 14

6.6 Solution #6: UUAA and authorization of target USS using token for the multiple USS case 14

6.6.1 Introduction 14

6.6.2 Solution details 14

6.6.2.1 Identification of USS-level changeover need 14

6.6.2.3 Enhancement for UUAA 14

6.6.2.5 Enhancement for authorization of target USS to use exposure services for the UAV 14

6.6.3 Evaluation 15

6.7 Solution #7: UUAA for USS changeover 15

6.7.1 Introduction 15

6.7.2 Solution details 15

6.7.3 Evaluation 16

6.8 Solution #8: UAV triggered UUAA for USS changeover 16

6.8.1 Introduction 16

6.8.2 Solution details 16

6.8.3 Evaluation 16

6.9 Solution #9: Serving USS triggered UUAA for target USS 16

6.9.1 Introduction 16

6.9.2 Solution details 17

6.9.3 Evaluation 17

6.Y Solution #Y: <Solution Name> 17

6.Y.1 Introduction 17

6.Y.2 Solution details 17

6.Y.3 Evaluation 17

7 Conclusions 18

7.1 Conclusion on KI #1 18

Annex A (informative): Change history 19

# 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].

## 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].

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

## 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.

###

# 6 Solutions

## 6.0 Mapping of solutions to key issues

Table 6.0-1: Mapping of Solutions to Key Issues

| Solutions | Key Issues |
| --- | --- |
| KI#1 |
| Solution #1: UAV Authentication and Authorization for Multiple USS | X |
| Solution #2: UUAA supporting multiple USS | X |
| Solution #3: Pairing authorization supporting multiple USS | X |
| Solution #4: revocation supporting multiple USS | X |
| Solution #5: UUAA and authorization of target USS for the multiple USS case | X |
| Solution #6: UUAA and authorization of target USS using token for the multiple USS case | X |
| Solution #7: UUAA for USS changeover | X |
| Solution #8: UAV triggered UUAA for USS changeover | X |
| Solution #9: Serving USS triggered UUAA for target USS | X |

## 6.1 Solution #1: UAV Authentication and Authorization for Multiple USS

### 6.1.1 Introduction

This solution addresses *"Key Issue #1: security enhancements to NEF services in support of multiple USSs".*

Enhancements are proposed to UUAA procedure to enable the exchange of a list of authorized serving USSs between the UAS NF and the USS that performs the UUAA procedure based on existing UUAA procedure (3GPP TS 33.256 [4], clause 5.2).

Enhancement are proposed to enable the change of serving USS during UAV flight, based on the USS initiated re-authorization (3GPP TS 23.256 [3], clause 5.2.4.3).

Enhancement are proposed to enable authorization for location tracking by an alternate authorized USS obtained during enhanced UUAA procedure above, based on Location tracking authorization procedures.

### 6.1.2 Solution details

The following enhancements are proposed based on the UUAA procedure described in 3GPP TS 33.256 [4], clause 5.2:

- the UAV indicates its support for multiple USSs which is forwarded to UAS NF by AMF or SMF, which forwards it to USS. Based on that indication, the UAS NF may receive information about other authorized (target) USSes (next bullet) and allow changeover of USS for the UAV (described below).

- the UAS NF receives from the serving USS that performs the UUAA a list of authorized serving USSs info which the UAS NF stores in the UUAA context of the UAV and forwards to the UAV via AMF or SMF.

NOTE 1: The serving USS is assumed to be aware of the other USSs info based on UAV flight planning information. How the serving USS obtains information about other USSes is out of 3GPP scope.

To enable a change of serving USS during flight, enhancement to the USS initiated re-authorization procedure described in 3GPP TS 23.256 [3], clause 5.2.4.3 is proposed as follows:

- the UAS NF is informed about the new serving USS info during a USS initiated re-authorization. The authorization payload forwarded to the UAV includes the new serving USS info that the UAV is authorized to communicate with. The UAS NF verifies that the new USS is authorized to request UAV re-authorization based on list of authorized serving USSs info in the UAV UUAA context and above indication for support of changeover of USS.

NOTE 2: It is assumed that a change of USS can be initiated by the USS based on its knowledge of the other USSes serving areas associated with the UAV flight plan and ability to invoke existing UAV location tracking procedures. How the USSs communicate with each other the information related to the change of USS for the UAV is out of 3GPP scope.

The following enhancements are proposed based on the Location tracking authorization procedures described in 3GPP TS 33.256 [4], clause 5.3:

- for location reporting and presence monitoring, the UAS NF checks that the USS requesting location info is in the list of authorized serving USS info in the UUAA context.

- for the list of arieal UEs in an area, the UAS NF performs a filtering based on the list of authorized serving USS info in the UUAA context.

### 6.1.3 Evaluation

The solution adresses the requirement of Key Issue #1. Namely:

* UUAA is reused and enhanced to allow the UAS NF to store authorized target USS related information received from serving USS during UUAA.
* UAV Re-authentication/authorization is reused and enhanced to allow an authorized target USS to perform a changeover of USS, including updating the serving USS in the UUAA context and informing the UAV about the changeover to the target USS.
* Location tracking authorization related procedures are reused and enhanced to allow an authorized target USS to request UAV location information before or after changeover of USS.

## 6.2 Solution # 2: UUAA supporting multiple USS

### 6.2.1 Introduction

This solution addresses the key issue #1.

The solution adapts the UUAA procedure in TS 33.256 [4] to support multiple USS. By and large, there are two changes: the UAV’s request and the UAS NF’s authentication requests/results are revised to support more than one USS.

### 6.2.2 Solution details

With reference to the clause 5.2.1.2/5.2.1.3 in TS 33.256 [4], the amended UUAA steps at registration/PDU session establishment respectively are shown below to support multiple USS:

1. The AMF/SMF triggers UUAA based on the CAA-Level UAV ID(s) provided by the UAV. The UAV may provide more than one USS addresses to indicate more than one USS is involved in the UUAA.

The UAV may have one unique CAA-Level UAV ID shared amongst multiple USS. In this case, one CAA-Level UAV ID is provided by the UAV. Alternatively, the UAV may also have one CAA-Level UAV ID assigned per USS. In this case, more than one CAA-Level UAV IDs are provided by the UAV.

NOTE 1: it is also allowed for UAV to provide single USS address in a UUAA procedure. This implies one UUAA procedures per USS identified by the USS address.

2. The AMF/SMF sends a message to UAS-NF as in TS 33.256 [4].

3-4. The UAS NF resolves the USS address based on CAA-Level UAV ID or uses the provided USS address. If more than one USS addresses are resolved, the UAS NF sends an Authentication Request to each of the USS. The procedures of sending each of the Authentication Requests and the follow-up steps can follow the steps described in TS 33.256 [4].

5. The UAS NF can store multiple UUAA results (one for each USS) for each UAV.

6-8. The UAS NF sends USS-specific UUAA results (one for each USS) together with the USS Identifier to the UAV.

NOTE 2: It is possible to have different authorization results for different USS. The UAS NF treats UUAA results for different USS independently. For example, if UUAA is successful for USS-A but failed for USS-B, the UAV is only allowed to perform further UAS procedure with USS-A, but not allowed with USS-B.

NOTE 3: After successfully completing multiple UUAA, the UAS NF may instruct the UAV which USS to communicate first. Alternatively, the UAV determines the USS to communicate with based on the authorized route.

### 6.2.3 Evaluation

This solution addresses the key issue #1. It amends the UUAA procedures in TS 33.256 [4] in order to support multiple USSs. It has the following impacts:

- UAV: provides more than one USS addresses to the AMF/SMF. If the CAA-Level UAV ID is assigned per USS, the UAV provides multiple CAA-Level UAV IDs, one per USS.

- UAS NF: sends authentication requests to more than one USS and stores results for more than one USS.

NOTE: the specified mechanisms to support multiple USS and USS changeover are not aligned with procedures defined in TS 23.256 [3].

## 6.3 Solution # 3: Pairing authorization supporting multiple USS

### 6.3.1 Introduction

This solution addresses the key issue #1. The solution adapts the pairing authorization procedure in TS 33.256 [4] to support multiple USS.

Pairing authorization can occur during the UUAA-SM procedure or after a successful UUAA. For the former, it is assumed that UUAA has been amended to support multiple USS and no further change is needed. This solution is to address the latter scenario.

### 6.3.2 Solution details

With reference to the clause 5.4.2 in TS 33.256 [4], the amended UUAA procedure at PDU session establishment/modification is shown below to support multiple USS:

1.The UAV includes the USS address(es) of the UAV-C to pair in the PDU session establishment/modification request, in addition to other information as specified in TS 33.256 [4].

NOTE 1: Although the pairing information may contain USS information, it is transparent to the UAS NF. The UAS NF may send to a different USS for pairing authorization.

2. The SMF invokes the pairing authorization procedure and the UAS NF exchanges authorization messages with and receives results with the USS identifier from the USS identified by the USS address(es) in step 1. The rest are the same as in the step 2 in the clause 5.4.2 of TS 33.256 [4].

3. The SMF informs the UE the paring authorization result which may include USS identifier in addition to information specified in the step 3 in the clause 5.4.2 of TS 33.256 [4].

NOTE 2: Different USS may have different pairing authorization results. The UAS NF treats pairing authorization results for different USS independently, i.e., USS-specific paring result. If paring authorization is only successful for some USSs, it implies the UAV can not fly with a route involves multiple USSs. The UAV is only allowed to be operated by the UAV-C with successful pairing authorization.

### 6.3.3 Evaluation

This solution addresses the key issue #1. It amends the pairing authorization procedures in TS 33.256 [4] in order to support multiple USSs. It has the following impacts:

- UAV: provides more than one USS addresses to the SMF and stores USS-specific results, one per USS.

- UAS NF: stores results, one per USS.

NOTE: the specified mechanisms to support multiple USS and USS changeover are not aligned with procedures defined in TS 23.256 [3].

## 6.4 Solution # 4: revocation supporting multiple USS

### 6.4.1 Introduction

This solution addresses the key issue #1. The solution adapts the revocation procedure in TS 33.256 [4] to support multiple USS.

### 6.4.2 Solution details

With reference to the clause 5.2.1.5 in TS 33.256 [4], the steps are amended as follows to support multiple USS:

1-2. no change to the corresponding steps in the clauses 5.2.1.4 in TS 33.256 [4].

3a or 3b. The UUAA revocation message that the UAS NF sent to the target AMF or SMF also includes the USS identifier.

NOTE 1: As stated in 5.2.1.6 in TS 33.256 [4], the USS identifier is based on the security link on the interface between UAS NF and USS (e.g., the identity mapped during link establishment or the identity in certificate).

3c-4. no change.

4a or 4b. The UUAA revocation indication message that the target AMF or the SMF sent to the UE contains also the USS identifier.

5. The UE on receiving the revocation indication only delete authorization data corresponding to the USS identifier.

### 6.4.3 Evaluation

This solution addresses the key issue #1. It amends the revocation procedures in the TS 33.256 [4] in order to support multiple USSs. It has the following impacts:

- UAS NF: sends the USS identifier to the UAV since the UAV needs to delete authorization data specific to the USS, not all authorization data.

This solution is in line with the conclusions in TR 23.700-59 [2].

## 6.5 Solution #5: UUAA and authorization of target USS for the multiple USS case

### 6.5.1 Introduction

This solution addresses key issue #1 (security enhancements to NEF services in support of multiple USSs) by providing enhancements to the UUAA and authorization of target USS in invoking exposure services for the UAV.

### 6.5.2 Solution details

#### 6.5.2.1 Identification of USS-level changeover need

For identification of changeover need, USS-A can use a planned flight path of the UAV, some data analytics to predict the location of the UAV, use the information of intersection of geographical areas served by both USSes, or can rely on notifications from the UAS NF.

The changeover procedure includes the authentication and authorization (A&A) procedure executed between the UAV and the target USS, so changeover can be completed successfully after the successful A&A procedure.

NOTE: It is not addressed in the present document how to ensure AA with USS-B is in time before changeover.

#### 6.5.2.2 Enhancement for UUAA

When the serving USS (USS-A) that has performed the UUAA procedure with the UAV identifies that USS-level changeover with a target USS (USS-B) is necessary, then

- USS-A informs USS-B about the changeover and sends information about the UAV. The interface between USS-A and USS-B is out of 3GPP scope.

- USS-A informs the UAV and sends information about USS-B e.g address of USS-B and security credentials.

- The UAV and USS-B uses the information provided by USS-A for authentication and authorization purpose.

- USS-B informs the network about the authentication and authorization result.

#### 6.5.2.3 Enhancement for authorization of target USS to use exposure services for the UAV

When the serving USS (USS-A) that has performed the UUAA procedure with the UAV identifies that USS-level changeover with a target USS (USS-B) is necessary, then

- USS-A informs USS-B about the changeover and sends information about the UAV. The interface between USS-A and USS-B is out of 3GPP scope.

- USS-A informs the UAS NF and sends information about USS-B and UAV.

- The UAS NF stores the information that USS-B is authorized to consume the exposure services for the UAV. Note that from the CN side there is no increase in the threat level because USS-B will not be able to access resources which are not accessible by the USS-A, i.e., there will be no additional resources accessible by USS-B but not by USS-A.

- When the UAS NF receives a request from USS-B about UAV, the UAS NF authorizes USS-B by using the stored information and checks whether the location of the UE is inside the geographical area served by USS-B.

NOTE 1: Interface between USSs is out of scope of the present document. It is not addressed in the present document whether it is in scope that USS-A obtains credential for USS-B.

NOTE 2: Can UAS NF trust info sent by USS-A that USS-B is trustworthy is not addressed in the present document. Any threat introduced to CN is not addressed in the present document.

### 6.5.3 Evaluation

This solution addresses the key issue #1. It has the following impacts:

- USS-A informs USS-B about the changeover and sends information about the UAV.

- USS-A informs the UAV and sends information about USS-B.

- USS-A informs the UAS NF and sends information about USS-B and UAV.

- The UAS NF stores the information that USS-B is authorized to consume the exposure services for the UAV.

## 6.6 Solution #6: UUAA and authorization of target USS using token for the multiple USS case

### 6.6.1 Introduction

This solution addresses key issue #1 (security enhancements to NEF services in support of multiple USSs) by providing enhancements to the UUAA and authorization of target USS in invoking exposure services for the UAV.

### 6.6.2 Solution details

#### 6.6.2.1 Identification of USS-level changeover need

For identification of changeover need, USS-A can use a planned flight path of the UAV, some data analytics to predict the location of the UAV, use the information of intersection of geographical areas served by both USSes, or can rely on notifications from the UAS NF.

The changeover procedure includes the authentication and authorization (A&A) procedure executed between the UAV and the target USS, so changeover can be completed successfully after the successful A&A procedure.

NOTE: How to ensure AA with USS-B is in time before changeover is not addressed in the present document.

#### 6.6.2.3 Enhancement for UUAA

When the serving USS (USS-A) that has performed the UUAA procedure with the UAV identifies that USS-level changeover with a target USS (USS-B) is necessary, then

- USS-A informs the UAV, sends information about USS-B and provides a token to be used towards USS-B. The token content is out of 3GPP scope. The token, sent from USS-A to the UAV in the application layer, is transparent to the 3GPP system.

- The UAV performs authentication and authorization using the information and token.

- USS-B informs the network about the authentication and authorization result.

#### 6.6.2.5 Enhancement for authorization of target USS to use exposure services for the UAV

When the serving USS (USS-A) that has performed the UUAA procedure with the UAV identifies that USS-level changeover with a target USS (USS-B) is necessary, then

- USS-A informs USS-B about the changeover and sends token also including information about the UAV. The interface between USS-A and USS-B is out of 3GPP scope.

- USS-B sends the token to the UAS NF. The content of the token is not specified in this solution. It is left to normative work.

- The UAS NF verifies the token and stores the information that USS-B is authorized to consume the exposure services for the UAV. Note that from the CN side there is no increase in the threat level because USS-B will not be able to access resources which are not accessible by the USS-A, i.e., there will be no additional resources accessible by USS-B but not by USS-A.

- When the UAS NF receives a request from USS-B about UAV, the UAS NF authorizes USS-B by using the stored information and checks whether the location of the UE is inside the geographical area served by USS-B.

NOTE: it is not addressed in the present document if UAS NF can trust info sent by USS-A that USS-B is trustworthy. Any threat introduced to CN is not addressed in the present document.

### 6.6.3 Evaluation

 This solution addresses the key issue #1. It has the following impacts:

- USS-A informs the UAV, sends information about USS-B and provides a token to be used towards USS-B.

- USS-A informs USS-B about the changeover and sends token also including information about the UAV.

- USS-B sends the token to the UAS NF.

- The UAS NF verifies the token and stores the information that USS-B is authorized to consume the exposure services for the UAV.

## 6.7 Solution #7: UUAA for USS changeover

### 6.7.1 Introduction

This solution addresses the "Key Issue #1: security enhancements to NEF services in support of multiple USSs".

In order to accomplish the USS changeover procedure from the serving USS to the target USS specified in the clause 5.13 of 3GPP TS 23.256 [3]. The enhancements to UUAA is required, e.g., to trigger the UUAA procedure from the serving USS and determine the UUAA procedure for the candidate USS. The details are described in the following clause.

### 6.7.2 Solution details

The steps 1-21 of the procedure of USS changeover as specified in the clause 5.13.2 of the TS 23.256 [3] are amended as follows (only affected steps are described):

Step 4. The request sent from the USS to the NEF includes an indicator. This indicator indicates to the NEF to exclude some USSes for flight assistance. These USSes are not listed in the UUAA context.

Step 5 – the NEF checks whether its UUAA context contains the UUAA results for candidate USSs.

Step 6 – the NEF performs the flight assistance procedure as in the clause 5.13.2 of the TS 23.256 [3]. The NEF may skip those USSs without UUAA results in the UUAA context (step 5)

NOTE 1: Flight assistance is out of scope of the present document.

Step 8 – In the response message, the NEF includes info about whether the candidate USSs require UUAA.

Step 9 – the serving USS (e.g., USS1) may choose the target USS not requiring UUAA.

Step 20 - If the serving USS selectes a target USS (e.g., USS2) requires UUAA, the serving USS1 informs the UAV or the target USS to perform UUAA as in the clause 5.13.2 of the TS 23.256 [3].

The UAV triggers the UUAA as in TS 33.256 [4] with the target USS address received from the serving USS.

Alternatively, the selected target USS2 sends an authentication request to the NEF and the NEF sends a UUAA request to the UAV through the SMF.

NOTE 2: the USS2 needs to establish a security link between the USS2 and the NEF before performing the UUAA procedure.

The NEF stores the USS2’s UUAA results in the UUAA context as in the TS 33.256 [4] if successful.

NOTE 3: the specified mechanisms to support multiple USS and USS changeover are not aligned with procedures defined in TS 23.256 [3].

### 6.7.3 Evaluation

The solution addresses the requirement of Key Issue #1.

The USS changeover procedure defined in the TS 23.256 [3] is reused, with additional details on the amended UUAA procedures if required.

## 6.8 Solution #8: UAV triggered UUAA for USS changeover

### 6.8.1 Introduction

This solution addresses the Key Issue #1. In order to accomplish the USS changeover, the UAS NF needs to store information about authorized USS(es). In this solution, the NAS NF receives authorized USS information based on a UUAA procedure.

### 6.8.2 Solution details

The following enhancements are proposed based on the UUAA procedure described in clause 5.2.1.2 or clause 5.2.1.3 of TS 33.256 [4]:

step 5 – If UUAA successful, the UAS NF stores (not to replace if UUAA context is available) the UAV UEs' UUAA context, including the GPSI, USS Identifier and the CAA-level UAV ID. The USSes in the UUAA context is the authorized USSes.

NOTE: the specified mechanisms to support multiple USS and USS changeover are not aligned with procedures defined in TS 23.256 [3].

### 6.8.3 Evaluation

The solution addresses the requirement of Key Issue #1. UUAA is reused and enhanced to allow the UAS NF to store multiple authorized USSes received from USSes during UUAA.

## 6.9 Solution #9: Serving USS triggered UUAA for target USS

### 6.9.1 Introduction

This solution addresses the Key Issue #1. In order to accomplish the USS changeover, the serving USS may trigger a UUAA procedure for the target USS and the UAV. In this solution, three options are presented.

### 6.9.2 Solution details

**Option 1 – serving USS triggers through PDU session**

It is assumed that the serving USS has an active PDU session with the UAV. The serving USS may send the target USS address to the UAV through the PDU session, that is transparent to the 5GC.

Upon receiving the target USS address, the UAV initiates a PDU session modification request including the target USS address for the UUAA with the target USS.

The rest procedure is the same as TS 33.256 [4]

**Option 2 – serving USS triggers UUAA through AMF/SMF**

This option is modified from the USS initiated re-authentication procedure in clause 5.2.1.4 of TS 33.256 [4].

Step 1. The serving USS sends an authentication request (instead of a re-authentication request) to the UAS NF and also includes the target USS address in the request.

Step 2. Skip the checking for re-authentication.

Step 5a/5b. The AMF/SMF initiates the UUAA with the target USS with the target USS address.

**Option 3 – target USS triggers UUAA through AMF/SMF**

This option is modified from the USS initiated re-authentication procedure in clause 5.2.1.4 of TS 33.256 [4]. The serving USS informs the target USS to trigger the UUAA with the UAV through the interface between the USSes.

Step 1. The target USS sends an authentication request (instead of a re-authentication request) and also includes the target USS address in the request.

Step 2. Skip the checking for re-authentication.

Step 5a/5b. The AMF/SMF initiates the UUAA with the target USS with the target USS address.

NOTE: the specified mechanisms to support multiple USS and USS changeover are not aligned with procedures defined in TS 23.256 [3].

### 6.9.3 Evaluation

The solution addresses the requirement of Key Issue #1.

The UUAA specified in TS 33.256 [4] is reused and enhanced with three options to trigger UUAA by a USS. Amongst them, two options are triggered by the serving USS and one option is triggered by the target USS.

# 7 Conclusions

## 7.1 Conclusion on KI #1

For Key issue #1 on the support for the multiple USS and changeover from one USS to another, the following principles apply:

- UAS NF receives and maintains info about authorized USS(es). UAS NF stores authorized USS(es) info as part of the UUAA context.

- UAS NF performs a changeover of USS with the authorized target USS. The UAS NF checks that the target USS matches one of the authorized USS(es) in the UUAA context during the procedure. The UAS NF marks the target USS as new serving USS in the UUAA context. The serving USS informs the UAV and the target USS about the changeover.

- UAS NF verifies that a USS requesting information of a UAV corresponds to an authorized USS (serving USS or target USS) in the UUAA context.

NOTE: the specified mechanisms to support multiple USS and USS changeover are to be aligned with procedures defined in TS 23.256 [3].

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 |
| 2024-05 | SA3#116 | S3-242517 |  |  |  | Incorporating S3-242516, S3-242518, S3-242519, S3-242520 | 0.2.0 |
| 2024-08 | SA3#117 | S3-243603 |  |  |  | Incorporating S3-243604, S3243668, S3-243150, S3-243605, S3-243672, S3-243673, S3-243674, S3-243675, S3-242883 | 0.3.0 |
| 2024-10 | SA3#118 | S3-243830 |  |  |  | Incorporating S3-244378, S3-244379, S3-244380, S3-244381, S3-244426, S3-244427 | 0.4.0 |
| 2024-11 | SA3#119 | S3-245194 |  |  |  | Incorporating S3-245256, S3-245257, S3-244842 | 0.5.0 |