**3GPP TSG-SA3 Meeting #112 *S3-234346***

**Goteburg, Sweden, 14 – 18 August 2023** *revision of S3-233864*

|  |
| --- |
| *CR-Form-v12.1* |
| **DRAFT CHANGE REQUEST** |
|  |
|  |  | **CR** |  | **rev** |  | **Current version:** |  |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME | **X** | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | security aspects of Rel-18 UAS features |
|  |  |
| ***Source to WG:*** | Qualcomm Incorporated |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | UAS\_Ph2 |  | ***Date:*** | 2022-02-01 |
|  |  |  |  |  |
| ***Category:*** |  |  | ***Release:*** | Rel-18 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)…Rel-15 (Release 15)Rel-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)* |
|  |  |
| ***Reason for change:*** | New UAS features are being added to Rel-18. Some of these features require security enhancements. |
|  |  |
| ***Summary of change:*** | Add the security aspects of the added Rel-18 UAS features |
|  |  |
| ***Consequences if not approved:*** | No security for these UAS features |
|  |  |
| ***Clauses affected:*** | 2, 3.1, 3.3, 4, 5.X (new), 5.Y (new), 5.W (new), 5.Z (new) |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **x** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **x** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **x** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** | NOTE: Coversheet detail will need revising to align with final CR |
|  |  |
| ***This CR's revision history:*** | S3-232100: Base version agreed in SA3#110-ad-hoc.S3-232552: Submission of above to SA3#111.S3-233425: Incorporating S3-232925, S3-233282, S3-233284, S3-233285, S3-233286 and S3-233289.S3-233864: Submission of above to SA3#112.S3-234346: Incorporating S3-234208, S3-234209, S3-234210 and S3-234211. |

**\*\*\*\* START OF CHANGES \*\*\*\***

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 TS 33.501: "Security architecture and procedures for 5G system".

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

[4] 3GPP TS 23.273: "5G System (5GS) Location Services (LCS); Stage 2".

[5] 3GPP TS 23.502: "Procedures for the 5G System (5GS)".

[6] 3GPP TS 22.125: "Uncrewed Aerial System (UAS) support in 3GPP".

[7] 3GPP TS 33.536: "Security aspects of 3GPP support for advanced Vehicle-to-Everything (V2X) services".

**\*\*\*\* NEXT CHANGE \*\*\*\***

3.1 Terms

For the purposes of the present document, the terms given in 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 TR 21.905 [1].

**3GPP UAV ID:** as defined in TS 23.256 [3].

**A2X:** as defined in TS 23.256 [3].

**BRID**: as defined in TS 23.256 [3].

**CAA (Civil Aviation Administration)-Level UAV Identity:** as defined in TS 23.256 [3].

**Command and Control (C2) Communication:** as defined in TS 23.256 [3].

**DAA**: as defined in TS 23.256 [3].

**UAS NF:** as defined in TS 23.256 [3].

**UAS Service Supplier (USS):** as defined in TS 23.256 [3].

**UAS Traffic Management (UTM):** as defined in TS 23.256 [3].

**UAS Services:** as defined in TS 23.256 [3].

**Uncrewed Aerial System (UAS):** as defined in TS 23.256 [3].

**UUAA:** as defined in TS 23.256 [3].

**UUAA-MM:** as defined in TS 23.256 [3].

**UUAA-SM:** as defined in TS 23.256 [3].

**\*\*\*\* NEXT CHANGE \*\*\*\***

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 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 TR 21.905 [1].

A2X Aircraft-to-anything

BRID Broadcast Remote Identification

DAA Detect And Avoid

UAS Uncrewed Aerial System

UAV Uncrewed Aerial Vehicle

USS UAS Service Supplier

UTM UAS Traffic Management

**\*\*\*\* NEXT CHANGE \*\*\*\***

4 Overview

 TS 23.256 [3] describes the architecture enhancements for supporting Uncrewed Aerial Systems (UAS).TS 23.256 [3] contains the reference architecture and message flows to support this new functionality for UAVs. The present document describes the security of these new features including:

- Authentication and authorization of a Uncrewed Aerial Vehicle (UAV) with the UAS Service Supplier (USS) during 5GS registration;

- Authentication and authorization of a PDU session establishment and PDN connection establishment with the USS;

- Support re-authentication, re-authorisation and revocation of the above;

- Support for USS authorization of pairing of UAVs and UAV-Cs;

- Support for authorisation of providing location information and providing network based location to mitigate against UAVs reporting false location data;

- Support for security and privacy of Command and Control (C2) communications over PC5 interface in 3GPP system;

- Support for security and privacy of transporting Broadcast Remote Identification; and

- Support for security and privacy for Detect And Avoid (DAA) traffic.

**\*\*\*\* NEXT CHANGE \*\*\*\***

## 5.X A2X Direct Communication

### 5.X.1 General

This clause describes the security support of an Aircraft-to-everything (A2X) mechanism based on PC5 reference point. A2X services such as C2 Communication, BRID and DAA are detailed in TS 23.256 [3].

A2X service authorization and provisioning to UE may be initiated by the PCF, by the UE, or by the AF.

A2X Direct Communication supports both unicast and broadcast modes.

### 5.X.2 Unicast mode A2X Direct Communication

#### 5.X.2.1 General

The unicast mode A2X Direct Communication procedures are described in TS 23.256 [3]. Unicast mode A2X Direct Communication is used by two UEs that directly exchange traffic for the A2X applications running between the peer UEs.

#### 5.X.2.2 Security requirements

The initiating UE shall establish a different security context for each peer UE during the PC5 unicast establishment if the security is activated. It shall be possible to establish security context also when either one or both the A2X-enabled UEs are out of coverage.

The mutual authentication between two A2X-enabled UEs during PC5 unicast shall be supported.

The PC5 unicast signalling shall support confidentiality protection, integrity protection and anti-replay protection.

The PC5 unicast user plane shall support confidentiality protection, integrity protection and anti-replay protection.

The PCF shall be able to provision the A2X security policies to the UE per A2X application during service authorization and information provisioning procedure as defined in TS 23.256 [3].

The 5G system shall support means for a secure refresh of the UE security context.

NOTE 1: The security context refresh may be triggered based on various options (e.g. validity time etc.).

The 5G System should provide means for mitigating trackability attacks on a UE during PC5 unicast communications.

The 5G System should provide means for mitigating link ability attacks on a UE during PC5 unicast communications.

NOTE 2: The 5G system provides means for mitigating trackability and link ability if security of the connection is activated.

#### 5.X.2.3 Security procedures

The unicast mode security mechanism defined in clause 5.3 of TS 33.536 [7] is reused in A2X to provide unicast mode A2X Direct Communication security (i.e., the signalling and user plane confidentiality and integrity protection) based on the A2X security policies.

#### 5.X.2.4 Identity privacy for the PC5 unicast link

The privacy protection procedures defined in clause 5.3.3.2 of TS 33.536 [7] are reused in A2X to provide unicast mode A2X Direct Communication security.

NOTE: For the privacy of the UAV and UAV-C Application Layer ID in the DCR (as Source User Info and Target User Info), the USS can decide whether it is acceptable to use the UAV’s and UAV-C’s permanent identities or whether some other privacy-preserving identities are provided for use instead. The use of privacy-preserving identities is left to the application layer and according to local regulations.

### 5.X.3 Broadcast mode A2X Direct Communication

#### 5.X.3.1 General

This clause specifies the security requirements and the procedures of the broadcast mode A2X Direct Communication (see TS 23.256 [3]).

#### 5.X.3.2 Security requirements

There are no requirements for securing the broadcast mode A2X Direct Communication.

The 5G System should protect against linkability and trackability attacks on Layer-2 ID and IP address for broadcast mode.

#### 5.X.3.3 Security procedures

There are no particular procedures defined for securing the broadcast mode A2X Direct Communication.

The broadcast mode security mechanism to randomise the UE’s source Layer-2 ID and source IP address including IP prefix (if used), as defined in clause 5.5 of TS 33.536 [7], is reused in A2X to provide broadcast mode a A2X Direct Communication security.

## 5.Y A2X Direct C2 Communication

### 5.Y.1 General

The unicast mode Direct C2 Communication procedures are described in TS 23.256 [3]. Unicast mode Direct C2 Communication is used by two UEs that directly exchange traffic for the A2X applications running between the peer UEs.

Before taking part in Direct C2 Communication, the UAV needs to be authorised as described in TS 23.256 [3] (see also the present document for more details of C2 authorisation over the network). If the UE is authorised over the 3GPP network, the USS may send a C2 session security information as part of the C2 authorization payload as described in clause 5.4. The content of C2 session security information (e.g., key material to help establish security between the UAV and UAV-C) is not in 3GPP scope.

### 5.Y.2 Unicast mode Direct C2 Communication

Unicast mode Direct C2 Communication has the same requirements and procedures as unicast mode A2X Direct Communication (see clause 5.X.2 of the present specification) with the following exception:

- The A2X Policy Provisioning is done based on TS 23.256 Clause 6.2.1 and the A2X Policy includes A2X security policy for each A2X services (e.g., C2 and DAA). The C2 service specific security policy available as part of A2X security policy is used for the security establishment (i.e. included in the direct communication request and is further replayed in the Direct security mode command to provide protection against bidding down attacks as described in TS 33.536 [7]), where the signalling and user plane confidentiality and integrity are set as required based on local policy.

## 5.W Broadcast Remote ID

### 5.W.1 General

This clause specifies the security requirements and the procedures of the Remote ID broadcast communication. Broadcast Remote ID traffic is sent using A2X broadcast mode (see TS 23.256 [3]).

### 5.W.2 Broadcast mode

The requirement and security procedures Remote ID broadcast mode follow the general A2X requirements and security procedure as given in clauses 5.X.3 of the present document.

## 5.Z Direct Detect and Avoid

### 5.Z.1 General

Direct Detect and Avoid traffic is sent using either A2X unicast mode or A2X broadcast mode (see TS 23.256 [3]).

### 5.Z.2 Unicast mode

The requirements, security procedure and privacy procedures for DAA unicast mode follow the general A2X requirements, security procedures and privacy procedures as given in clauses 5.X.2 of the present document with the following exception:

- The A2X Policy Provisioning is done based on TS 23.256 [3] Clause 6.2.1 and the A2X Policy includes A2X security policy for each A2X services (e.g., C2 and DAA services). The DAA service specific security policy available as part of A2X security policy is used for the security establishment (i.e., included in direct communication request and further replayed in the Direct security mode command to provide protection against bidding down attacks as described in TS 33.536 [7]).

### 5.Z.3 Broadcast mode

The requirement and security procedures for DAA broadcast mode follow the general A2X requirements and security procedure as given in clauses 5.X.3 of the present document.

**\*\*\*\* END OF CHANGES \*\*\*\***