**无人机身份认证方案**

# 简介及需求

身份认证（Authentication）又称“验证”、“鉴权”，是指通过一定的手段，完成对用户身份的确认。

身份认证的目的是确认当前所声称为某种身份的用户，确实是所声称的用户，从而确定该用户是否具有对某种资源的访问和使用权限，进而使计算机和网络系统的访问策略能够可靠有效地执行，防止攻击者假冒合法用户获得资源的访问权限，保证系统和数据的安全，以及授权访问者的合法权益。

身份认证的方法有很多，基本上可分为：基于[共享密钥](https://zh.wikipedia.org/w/index.php?title=%E5%85%B1%E4%BA%AB%E5%AF%86%E9%92%A5&action=edit&redlink=1)的身份认证、基于[生物学](https://zh.wikipedia.org/wiki/%E7%94%9F%E7%89%A9%E5%AD%A6)[特征](https://zh.wikipedia.org/wiki/%E7%89%B9%E5%BE%B5)的身份认证和基于[公开密钥加密算法](https://zh.wikipedia.org/wiki/%E5%85%AC%E5%BC%80%E5%AF%86%E9%92%A5%E5%8A%A0%E5%AF%86%E7%AE%97%E6%B3%95)的身份认证。不同的身份认证方法，安全性也各有高低。

1. 基于[共享密钥](https://zh.wikipedia.org/w/index.php?title=%E5%85%B1%E4%BA%AB%E5%AF%86%E9%92%A5&action=edit&redlink=1)的身份认证：基于共享密钥的身份验证是指[服务器](https://zh.wikipedia.org/wiki/%E6%9C%8D%E5%8A%A1%E5%99%A8)端和用户共同拥有一个或一组[密码](https://zh.wikipedia.org/wiki/%E5%AF%86%E7%A0%81)。当用户需要进行身份验证时，用户通过输入或通过保管有密码的设备提交由用户和服务器共同拥有的密码。服务器在收到用户提交的密码后，检查用户所提交的密码是否与服务器端保存的密码一致，如果一致，就判断用户为合法用户。如果用户提交的密码与服务器端所保存的密码不一致时，则判定身份验证失败。使用基于共享密钥的身份验证的服务有很多，如：绝大多数的[网络接入服务](https://zh.wikipedia.org/w/index.php?title=%E7%BD%91%E7%BB%9C%E6%8E%A5%E5%85%A5%E6%9C%8D%E5%8A%A1&action=edit&redlink=1)、绝大多数的[BBS](https://zh.wikipedia.org/wiki/BBS)以及[维基百科](https://zh.wikipedia.org/wiki/%E7%BB%B4%E5%9F%BA%E7%99%BE%E7%A7%91)等等。
2. 基于[生物学](https://zh.wikipedia.org/wiki/%E7%94%9F%E7%89%A9%E5%AD%A6)[特征](https://zh.wikipedia.org/wiki/%E7%89%B9%E5%BE%B5)的身份认证：基于生物学特征的身份验证是指基于每个人身体上独一无二的特征，如[指纹](https://zh.wikipedia.org/wiki/%E6%8C%87%E7%B4%8B)、[虹膜](https://zh.wikipedia.org/wiki/%E8%99%B9%E8%86%9C)等等。
3. 基于[公开密钥加密算法](https://zh.wikipedia.org/wiki/%E5%85%AC%E5%BC%80%E5%AF%86%E9%92%A5%E5%8A%A0%E5%AF%86%E7%AE%97%E6%B3%95)的身份认证：基于公开密钥加密算法的身份验证是指通信中的双方分别持有公开密钥和私有密钥，由其中的一方采用私有密钥对特定数据进行加密，而对方采用公开密钥对数据进行解密，如果解密成功，就认为用户是合法用户，否则就认为是身份验证失败。使用基于公开密钥加密算法的身份验证的服务有：[SSL](https://zh.wikipedia.org/wiki/SSL)、[数字签名](https://zh.wikipedia.org/wiki/%E6%95%B0%E5%AD%97%E7%AD%BE%E5%90%8D)等等。

## 无人机认证需求

近年来，民用无人机的生产和应用在国内外蓬勃发展，特别是低空、慢速、轻微小型无人机数量快速增加，随之而来的无人机事故也时有发生，对无人机进行监管就成了迫在眉睫的需求。

* 可靠的身份认证是对无人机行为监管的前提条件，飞行可追溯，责任可认定，防抵赖栽赃
* 无人机与云监管平台之间必须是安全通信，需要保证保密性，认证性，完整性，不可抵赖性
  + 对于无人机上报数据进行认证，防止篡改，伪造，重放
  + 对云监管平台进行认证，保证数据上报有效到达

## 加解密基础

* 对称加密算法：加密和解密使用同样密钥的加密算法。特点是算法公开，计算量小，加密速度快，解密效率高。缺点是相同密钥安全性得不到保证，并且每对通信双方必须使用不同的密钥，密钥数量随用户数几何级数增长。
* 非对称加密算法：加密和解密使用不用的密钥。非对称加密算法需要两个密钥：公开密钥（publickey）和私有密钥（privatekey）。公开密钥和私有密钥是一对，如果用公开密钥对数据加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据加密，只有对应的公开密钥才能解密。特点是算法复杂，安全性依赖于算法和密钥。缺点是加解密速度慢。
* 安全HASH函数：HASH函数可将变长的数据块输入，产生固定长度的HASH值。密码学上的HASH函数需要以下两种情况计算上不可行：对预先指定的HASH值找到对应数据（单向性）；找到两个不同的数据块对应相同的HASH值（抗碰撞性）。使用在消息认证，数字签名和其它应用（比如产生单项口令文件）
* 消息认证码：用来验证所收到的消息确认来自真正的发送方，且是未被修改的消息，它也可验证消息的顺序和及时性
* X.509证书：X.509是基于公钥密码体制和数字签名的服务，其核心是于每个用户相关的公钥证书，这些证书是由可信任的签证机构（CA）创建并被CA或者用户放入目录服务器。

在无人机身份认证中，无人机身份和飞行授权使用X.509证书表示，好处是：

* + 标准接口，易于扩展
  + 可以建立可信证书链，实现跨区域飞机认证
  + 可以利用证书撤销链，收回可以飞机证书

## 无人机以及认证方式分级

无人机因为其大小，载重能力和飞行距离的不同，威胁性也不一样，这里定义低威胁（比如微型无人机等），中威胁（比如小型无人机等），高威胁（比如农用机等），对于不同威胁等级的无人机提出不同认证和需求

本文将无人机，地面站以及对应的手机APP作为无人机整体系统，系统内部安全和模块之间认证不在本文讨论范围。

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 威胁等级 | 无人机加密认证算法 | | | | 无人机网络连接途径 | | | 无人机安全存储 | | | |
| AES/国密SM1 | CMAC  国密SM3 | RSA 2048 | ECC/  国密SM2 | 无人机 | 地面站 | 手机APP | 无人机SOC内部存储 | 无人机SOC外部存储 | 地面站存储 | 手机APP存储 |
| 低威胁无人机 | 需要支持 | 需要支持 | 不需要支持 | 不需要支持 | 不需要支持 | 不需要支持 | 不需要支持 | 不需要支持 | 需要支持 | 不需要支持 | 不需要支持 |
| 中威胁无人机 | 需要支持 | 需要支持 | 需要支持 | 不需要支持 | 需要支持 | 不需要支持 | 不需要支持 | 需要支持 | 不需要支持 | 不需要支持 | 不需要支持 |
| 高威胁无人机 | 需要支持 | 需要支持 | 需要支持 | 需要支持 | 需要支持 | 不需要支持 | 不需要支持 | 需要支持 | 不需要支持 | 不需要支持 | 不需要支持 |

# 系统构架



云监管平台、第三方实名认证平台、无人机生产企业、无人机和无人机用户协同完成无人机身份认证。无人机和无人机用户是被认证对象；云监管平台是核心，其保存无人机和用户的关键数据；第三方实名认证平台提供用户的实名认证服务，保证用户是其声称的用户；无人机生产企业从云监管平台获得无人机唯一ID和认证密钥，并将ID和密钥烧录到无人机中。云监管平台和无人机身份认证相关的模块有无人机注册管理模块，用户管理模块，无人机认证模块，这些模块可以是一个服务器的不同服务也可以存在于不同的服务器，这里统称为云监管平台。无人机身份认证包含以下过程：

## 无人机云监管平台注册

该步骤是由无人机厂商在无人机出厂之前完成。无人机厂商从云监管平台申请无人机身份并烧录到无人机内部安全存储空间，同时烧录得还有云监管平台的X.509证书。无人机身份包含无人机ID和认证密钥，无人机ID和认证密钥用户不可修改。以下情况需要返还厂商重新烧录无人机ID和认证密钥：

* 认证密钥泄露
* 无人机ID被盗用
* 因无人机损坏而更新主要部件

无人机注册流程如下，需要注意：

* 无人机企业服务器和云监管平台服务器之间采用SSL链接，传输数据加密
* 认证密钥可以是对称加密算法密钥也可以是非对称加密算法密钥，但是对于低威胁以外的无人机，必须采用非对称加密算法。
  + 对称认证密钥由云监管平台生成发送到无人机企业，可以不同设备之间密钥的不相关性
  + 非对称认证密钥由无人机企业生成，并把公钥作为无人机特性的一部分发送给云监管平台
* 无人机ID，认证密钥必须安全存储于无人机内部，对于中高威胁无人机，安全存储必须防止板级物理攻击





### 无人机ID和认证密钥

* 采用OID表示无人机ID。OID是ISO/IECI，ITU国际组织共同提出的标识机制，用于对任何对象，概念或者事物进行全球无歧义唯一的命名。我国也组建了“OID注册中心”，管理国际规范下的中国OID分支，负责国内OID的注册，管理，维护以及国际备案。无人机ID采用OID管理的好处是国际通用，可以追踪。无人机ID格式定义如下：1.2.156.M.N.O.P。
  + M：云监管平台标识。云监管平台标识是云监管平台的身份标识，由监管部门维护
  + N：厂商标识。厂商标识是厂商向云监管平台注册时分配的标识，在云监管平台内部唯一
  + O：无人机型号标识。无人机型号由无人机厂商在向云监管平台申请的型号标识，用以区分一类无人机
  + P：无人机身份。无人机身份由云监管平台维护分配，带有一定的随机性，攻击者不能预测/推断下一个无人机的身份号码
* 认证密钥可以是对称密钥或者非对称密钥，分别用于对称加密算法和非对称加密算法。对称加密算法是AES 128/国密SM1；非对称加密算法是RSA 2048/ECC/国密SM3
* 无人机ID和密钥是生产过程，为了生产过程方便，厂商可以在云监管平台协助下搭建代理服务器，可以一次从云监管平台获得一批无人机ID和授权密钥，然后在产线内部分配无人机ID和认证密钥的使用，以解决产线没有网络连接问题



## 用户注册及实名认证

### 用户实名认证方法

* 可用于认证的因素
  + 生物特征：
    - 人脸：便于采集，一般需要人工确认，较难实现无人干预的认证
    - 指纹：受限于指纹数据库，以及认证时的采集设备，无法实现无人工干预的认证
    - 语音：受限于目前的技术，无法实现自动化
  + 身份证：可能被盗用
* 借助第三方认证平台
  + 第三方认证平台：身份认证中心、国政通、深圳鹏元、APIX（北京黑格）等
  + 第三方支付系统：银联、支付宝（已实名认证）、微信（已实名认证）
  + 手机：移动公司没有完全解决认证的问题，可信度不够

### 用户注册和实名认证过程



用户需要提供用户名，PIN码，联系方法和其它实名认证所需要的信息给运监管平台进行注册和实名认证，通过用户状态查询实名认证结果。只有通过实名认证的用户，才可以进行以下的操作：

* 认证绑定飞机
* 操作飞机，否则在用户认证时将不予通过

云监管平台通过第三方平台进行实名认证,其数据结构不在本文详述。

## 无人机身份认证

### 无人机身份认证的基本方法

无人机身份认证是基于不可复制的ID和认证密钥，认证密钥可以是对称密钥或者公私钥对，认证方法是基于challenge/response，认证结果是得到会话密钥。会话密钥用来加密无人机和云监管平台之间的通信，会话密钥有一定的有效期（比如一个月），失效之后需要无人机重新认证。

### 无人机与云监管平台的双向认证过程



### 无人机身份认证数据结构

* 无人机发送到云监管平台的challenge1数据，开始监管平台认证（u2c\_challenge1）

|  |  |  |
| --- | --- | --- |
| 数据项 | 数据项描述 | 名称 |
| challenge1 | 无人机发出的challenge，用以认证云监管平台 | Challenge1 |

* 云监管平台发送到无人机的response1以及用以认证无人机的challenge2数据（c2u\_challenge2）

|  |  |  |
| --- | --- | --- |
| 数据项 | 数据项描述 | 名称 |
| response1 | 云监管平台用私钥加密challenge1，作为response1，返回给无人机 | Response1 |
| challenge2 | 云监管平台生成的challenge，用以验证无人机 | challenge2 |

* 无人机发送到云监管平台的response2，无人机ID和nonce（u2c\_response2）

|  |  |  |
| --- | --- | --- |
| 数据项 | 数据项描述 | 名称 |
| 无人机ID | 无人机唯一ID，由监管平台分配，在无人机生产阶段烧录到无人机 | drone\_id |
| response2 | 无人机用认证密钥加密challenge2，作为response2，返回给云监管平台 | response2 |
| nonce | 随机数，以防止重放攻击 | nonce |

* 云监管平台发送到无人机的nonce，会话密钥以及MAC（c2u\_sessionkey）

|  |  |  |
| --- | --- | --- |
| 数据项 | 数据项描述 | 名称 |
| nonce | 随机数，以防止重放攻击 | nonce |
| 会话加密密钥 | 加密密钥，用以加密通信数据，用无人机认证密钥加密 | session\_enc\_key |
| 会话认证密钥 | 认证密钥，用以生成消息认证码，用无人机认证密钥加密 | session\_auth\_key |
| 消息认证码 | 包含nonce的CMAC/SM3，用无人机认证密钥 | mac |

## 用户认证及绑定

### 用户认证及绑定过程



* 用户认证通过无人机完成
* 此处无人机会话密钥在无人机-云平台双向认证过程中生成
* Token用于进一步数据上报时保护无人机以及用户信息。
* Token随用户密码修改以及无人机重新认证而失效。需要重新认证用户
* 每次无人机重新开机时，将对用户PIN码进行验证，以保证用户信息真实

### 用户认证及绑定数据结构

* 用户认证申请（u2c\_user\_authentication）

|  |  |  |
| --- | --- | --- |
| 数据项 | 数据项描述 | 名称 |
| 无人机ID | 无人机唯一ID，由监管平台分配，在无人机注册阶段烧录到无人机 | drone\_id |
| nonce | 随机数，以防止重放攻击 | nonce |
| 用户名 | 用会话加密密钥加密的用户名 | user |
| PIN码哈希值 | 用会话加密密钥加密的用户PIN码HASH | pin\_hash |
| 消息认证码 | 包含无人机ID，nonce和加密的用户名PIN码哈希值的CMAC/SM3，用无人机认证密钥 | mac |

* 用户认证申请应答（c2u\_user\_authentication\_reply）

|  |  |  |
| --- | --- | --- |
| 数据项 | 数据项描述 | 名称 |
| nonce | 随机数，用以标识本次数据发送，应答也带有nonce ，用以匹配数据发送 | nonce |
| token | 令牌，标识同一用户在同一无人机上的一次会话。无人机ID，用户ID，会话密钥任一个要素改变会使令牌失效，令牌失效时候可以认证用户重新获得。如果用户认证失败，返回的token为无效值（0） | token |
| 消息认证码 | 包含nonce，token的CMAC/SM3，用无人机认证密钥 | Mac |

# 无人机应用数据

## 无人机飞行记录安全上报

飞行记录上报是无人机在飞行过程中向云监管平台上报飞行信息，根据这些飞行记录，云监管平台可以：

* 查询一个地区飞行架次
* 无人机违规飞行情况

### 飞行记录上报流程

* 所有的飞行记录都是加密并且计算MAC后上传，返回的结果也是加密和有MAC，达到保护隐私和双向认证的目的
* 只有安全上传的记录才会从飞机删除
* 如果飞机有过多记录没有上传，将强制要求联网上传，否则禁止飞行



### 飞行记录上报数据定义

* 飞行记录上报数据定义（u2c\_upload\_record）

|  |  |  |
| --- | --- | --- |
| 数据项 | 数据项描述 | 名称 |
| token | 令牌，标识同一用户在同一无人机上的一次会话。无人机ID，用户ID，会话密钥任一个要素改变会使令牌失效，令牌失效时候可以认证用户重新获得 | token |
| nonce | 随机数，用以标识本次数据发送，应答也带有nonce ，用以匹配数据发送 | nonce |
| 时间 | ms | datetime |
| 经度 | 当前位置经度，精度1e-7度 | longitude |
| 纬度 | 当前位置纬度，精度1e-7度 | latitude |
| 离地高度 | 1. GPS高度是WGS84椭球上的大地高（非海拔高）；一般GPS的误差可能较大。 2. 离地高低可以由超声、TOF、视觉等获取   精度0.01m | altitude |
| 航向角 | 航向角，精度0.01度 | yaw |
| 俯仰角 | 俯仰角，精度0.01度 | pitch |
| 横滚角 | 横滚角，精度0.01度 | roll |
| 水平速率 | 机头方向水平速率，精度0.01m/s | horizontal\_speed |
| 垂直速率 | 机头方向垂直速度,精度0.01m/s | vertical\_speed |
| 消息认证码 | 包含前述所有数据的消息认证码，用无人机认证密钥 | mac |

* 飞行记录上报应答数据定义（c2u\_upload\_record\_result）

|  |  |  |
| --- | --- | --- |
| 数据项 | 数据项描述 | 名称 |
| token | 令牌，标识同一用户在同一无人机上的一次会话。无人机ID，用户ID，会话密钥任一个要素改变会使令牌失效，令牌失效时候可以认证用户重新获得 | token |
| nonce | 随机数，用以标识本次数据发送，应答也带有nonce ，用以匹配数据发送 | nonce |
| 上报结果 | 成功、错误码（无效ID等） | result |
| 消息认证码 | 包含token，nonce和上报结果的CMAC/SM3，用无人机认证密钥 | mac |

## 无人机飞行计划申报

飞行申报主要针对需要预先申报的无人机类型，进行提前作业申报，批准后的结果是一个X.509描述的飞行证书，由监管云平台签发。证书用于授予对应操作员和无人机在相应时间、地点进行

### 无人机飞行申报流程



### 飞行计划申报数据结构

* 飞行计划申报数据结构（u2c\_upload\_plan）

|  |  |  |
| --- | --- | --- |
| 数据项 | 数据项描述 | 名称 |
| token | 令牌，标识同一用户在同一无人机上的一次会话。无人机ID，用户ID，会话密钥任一个要素改变会使令牌失效，令牌失效时候可以认证用户重新获得 | token |
| nonce | 随机数，用以标识本次数据发送，应答也带有nonce ，用以匹配数据发送 | nonce |
| 起始时间 | UTC时间，秒，从2010年1月1日0时开始 | start\_time |
| 结束时间 | UTC时间，秒，从2010年1月1日0时开始 | end\_time |
| 中心经度 | 飞行区域中心点经度，1e-5度 | longitude |
| 中心纬度 | 飞行区域中心点纬度，1e-5度 | latitude |
| 水平半径 | 飞行区域水平半径，1米 | radius |
| 离地高度 | 飞行最大离地高度，1米 | altitude |
| 飞行目的类型 | 飞行目的定义：（待细化，字符串）  航拍：1  运输：2  地形勘测：3  农田作业：4  电力检修：5  火情勘察：6 | purpose |
| 飞行目的详述 |  | detail |
| 消息认证码 | 包含前述所有数据的CMAC/SM3，用无人机认证密钥 | mac |

* 飞行计划申报应答数据结构（c2u\_upload\_plan\_result）

|  |  |  |
| --- | --- | --- |
| 数据项 | 数据项描述 | 名称 |
| token | 令牌，标识同一用户在同一无人机上的一次会话。无人机ID，用户ID，会话密钥任一个要素改变会使令牌失效，令牌失效时候可以认证用户重新获得 | token |
| nonce | 随机数，用以标识本次数据发送，应答也带有nonce ，用以匹配数据发送 | nonce |
| 结果 | 错误码或飞行证书 | certificate |
| 飞行证书 |  |  |
| 消息认证码 | 包含前述所有数据的CMAC/SM3，用无人机认证密钥 | mac |

### 飞行授权证书

飞行授权需要包含以下数据内容

|  |  |  |
| --- | --- | --- |
| 数据项 | 数据项描述 | 名称 |
| 批准单位 | 云监管平台名称和ID | authorizer |
| 无人机ID | 无人机ID | drone\_id |
| 用户ID | 用户ID | user\_id |
| 起始时间 | UTC时间，单位秒 | start\_time |
| 结束时间 | UTC时间，单位秒 | end\_time |
| 中心经度 | 飞行区域中心点经度，精度1e-5度 | longitude |
| 中心纬度 | 飞行区域中心点纬度，精度1e-5度 | latitude |
| 水平半径 | 飞行区域水平半径，精度1米 | radius |
| 离地高度 | 飞行最大离地高度，精度1米 | altitude |
| 飞行目的类型 | 飞行目的定义：（待细化，字符串）  航拍：1  运输：2  地形勘测：3  农田作业：4  电力检修：5  火情勘察：6 | purpose |

用X.509格式描述飞行授权，证书中主体对应无人机ID加用户ID，发行者对应飞行授权批准单位，飞行特定数据放入证书扩展域，飞行相关特性放在扩展域中，如下如所示。



# 通信接口数据说明

## 数据类型定义

|  |  |  |  |
| --- | --- | --- | --- |
| **类型** | **名称** | **字节数** | **说明** |
| UINT8 | 8位无符号整数 | 1 | 小端模式，高位在后 |
| UINT16 | 16位无符号整数 | 2 | 小端模式，高位在后 |
| INT16 | 16位无符号整数 | 2 | 小端模式，高位在后 |
| UINT32 | 32位无符号整数 | 4 | 小端模式，高位在后 |
| INT32 | 32位有符号整数 | 4 | 小端模式，高位在后 |
| UINT64 | 64位无符号整数 | 8 | 小端模式，高位在后 |
| UUID | 128位 | 16 |  |
| STRING | 字符串类型 | / |  |

## 无人机与云监管平台通信接口

### 接口数据包头数据包格式

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 字段 | 数据类型 | 描述 | 字节数 |
| 1 | 同步字 | UINT32 | 0x55415643 | 4 |
| 2 | 版本 | UINT32 |  | 4 |
| 3 | 本次传输标记 | UINT32 | 用于响应匹配对应的请求，要求不重复（比如可以使用起始时间秒数每次加1） | 4 |
| 4 | 接口ID | UINT32 | 接口标识 | 4 |
| 5 | 数据长度 | UINT32 | 消息长度，包含消息头 | 4 |
| 6 | date | UINT32 | UTC时间，BCD码表示，格式：YYYYMMDD | 4 |
| 7 | time | UINT32 | UTC时间，BCD码表示，格式：hhmmss.ss | 4 |

### 接口ID汇总

|  |  |  |
| --- | --- | --- |
| 接口ID（16进制） | 接口名称 | 功能说明 |
| 0x00000010 | u2c\_challenge1 |  |
| 0x00000011 | c2u\_challenge2 |  |
| 0x00000012 | u2c\_response2 |  |
| 0x00000013 | c2u\_sessionkey |  |
| 0x00000020 | u2c\_user\_authentication |  |
| 0x00000021 | c2u\_user\_authentication\_reply |  |
| 0x00001000 | u2c\_upload\_record |  |
| 0x00001100 | c2u\_upload\_record\_result |  |
| 0x00002000 | u2c\_upload\_plan |  |
| 0x00002100 | c2u\_upload\_plan\_result |  |
| 0x00003000 | u2c\_upload\_takeoff |  |
| 0x00003100 | c2u\_upload\_takeoff\_result |  |
| 0x00004000 | u2c\_upload\_land |  |
| 0x00004100 | c2u\_upload\_land\_result |  |

### 无人机与云监管平台的双向认证接口定义

#### 无人机发送到云监管平台的challenge1数据，开始监管平台认证（u2c\_challenge1）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 字段 | 数据类型 | 描述 | 字节数 |
| 1 | drone\_id | STRING | 无人机唯一ID，由监管平台分配，在无人机注册阶段烧录到无人机 | 32 |
| 2 | algorithm | UINT32 | 无人机所支持的云监管平台认证算法 | 4 |
| 3 | challenge1 | UINT32 | 无人机发出的challenge，用以认证云监管平台 | 4 |
| 4 | mac 或 signature | UINT8 | 所有数据的mac或者signature，取决于algorithm |  |

#### 云监管平台发送到无人机的response1以及用以认证无人机的challenge2数据（c2u\_challenge2）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 字段 | 数据类型 | 描述 | 字节数 |
| 1 | drone\_id | STRING | 无人机唯一ID，由监管平台分配，在无人机注册阶段烧录到无人机 | 32 |
| 2 | algorithm | UINT32 | 云监管所使用的认证算法 | 4 |
| 3 | challenge1 | UINT32 | 无人机发送过来的challenge1 | 4 |
| 4 | challenge2 | UINT32 | 云监管平台生成的challenge，用以验证无人机 | 4 |
| 5 | mac 或 signature | UINT8 | 所有数据的mac或者signature，取决于algorithm |  |

#### 无人机发送到云监管平台的response2，无人机ID和nonce（u2c\_response2）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 字段 | 数据类型 | 描述 | 字节数 |
| 1 | drone\_id | STRING | 无人机唯一ID，由监管平台分配，在无人机注册阶段烧录到无人机 | 32 |
| 2 | challenge2 | UINT32 | 无人机返回的监管平台的challenge2 | 4 |
| 3 | algorithm | UINT32 | 无人机所使用的认证算法 | 4 |
| 4 | enc\_algorithm | UINT32 | 会话密钥加密算法 | 4 |
| 5 | auth\_algorithm | UINT32 | 会话密钥认证算法 | 4 |
| 6 | mac 或 signature |  | 所有数据的mac或者signature，取决于algorithm |  |

#### 云监管平台发送到无人机的nonce，会话密钥以及MAC（c2u\_sessionkey）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 字段 | 数据类型 | 描述 | 字节数 |
| 1 | drone\_id | STRING | 无人机唯一ID，由监管平台分配，在无人机注册阶段烧录到无人机 | 32 |
| 2 | enc\_algorithm | UINT32 | 会话密钥加密算法，必须与申请时一致 | 4 |
| 3 | session\_enc\_key | UINT8\*32 | 加密会话密钥，用以加密通信数据，用无人机认证密钥加密 | 32 |
| 4 | auth\_algorithm | UINT32 | 会话密钥认证算法，必须与申请时一致 | 4 |
| 3 | session\_auth\_key | UINT8\*32 | 认证会话密钥，用以生成消息认证码，用无人机认证密钥加密 | 32 |
| 4 | mac | UINT8\*16 | 用session\_auth\_key认证 | 16 |

### 用户认证以及绑定接口定义

#### 用户认证申请（u2c\_user\_authentication）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 字段 | 数据类型 | 描述 | 字节数 |
| 1 | drone\_id | STRING | 无人机唯一ID，由监管平台分配，在无人机注册阶段烧录到无人机 | 32 |
| 5 | user | UINT8\*32 | 用会话加密密钥加密的用户名 | 32 |
| 6 | pin\_hash | UINT8\*32 | 用会话加密密钥加密的用户PIN码HASH | 32 |
| 7 | mac | UINT8\*16 | 包含无人机ID，nonce和加密的用户名PIN码哈希值的CMAC/SM3，用无人机认证密钥 | 16 |

#### 用户认证申请应答（c2u\_user\_authentication\_reply）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 字段 | 数据类型 | 描述 | 字节数 |
| 1 | drone\_id | STRING | 无人机唯一ID，由监管平台分配，在无人机注册阶段烧录到无人机 | 32 |
| 5 | token | UINT8\*16 | 令牌，标识同一用户在同一无人机上的一次会话。无人机ID，用户ID，会话密钥任一个要素改变会使令牌失效，令牌失效时候可以认证用户重新获得。如果用户认证失败，返回的token为无效值（0） | 16 |
| 6 | mac | UINT8\*16 | 包含nonce，token的CMAC/SM3，用无人机认证密钥 | 16 |

### 无人机飞行记录上报接口定义

#### 飞行记录上报数据定义（u2c\_upload\_record）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 字段 | 数据类型 | 描述 | 字节数 |
| 1 | token | UINT8\*16 | 令牌，标识同一用户在同一无人机上的一次会话。无人机ID，用户ID，会话密钥任一个要素改变会使令牌失效，令牌失效时候可以认证用户重新获得 | 16 |
| 5 | date | UINT32 | UTC时间，BCD码表示，格式：YYYYMMDD | 4 |
| 6 | time | UINT32 | UTC时间，BCD码表示，格式：hhmmss.ss | 4 |
| 7 | latitude | INT32 | 当前位置纬度\*1e7，精度1e-7度 | 4 |
|  |  |  | 海拔高度 | 4 |
| 8 | altitude | INT32 | 相对于起飞点的高度。  GPS高度是WGS84椭球上的大地高（非海拔高）；一般GPS的误差可能较大。 | 4 |
| 9 | yaw | INT16 | 航向角\*100，精度0.01度 | 2 |
| 10 | pitch | INT16 | 俯仰角\*100，精度0.01度 | 2 |
| 11 | roll | INT16 | 横滚角\*100，精度0.01度 | 2 |
| 12 | horizontal\_speed | INT32 | 机头方向水平速率\*100，精度0.01m/s | 4 |
| 13 | vertical\_speed | INT32 | 机头方向垂直速度,精度0.01m/s | 4 |
| 14 | mac | UINT8\*16 | 随机数，用以标识本次数据发送，应答也带有nonce ，用以匹配数据发送 | 16 |

#### 飞行记录上报应答数据定义（c2u\_upload\_record\_result）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 字段 | 数据类型 | 描述 | 字节数 |
| 1 | token | UINT8\*16 | 令牌，标识同一用户在同一无人机上的一次会话。无人机ID，用户ID，会话密钥任一个要素改变会使令牌失效，令牌失效时候可以认证用户重新获得 | 16 |
| 5 | result | INT32 | 成功、错误码（无效ID等） | 4 |
| 6 | mac | UINT8\*16 | 包含token，nonce和上报结果的CMAC/SM3，用无人机认证密钥 | 16 |

### 无人机飞行计划申报接口定义

#### 飞行计划申报数据结构（u2c\_upload\_plan）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 字段 | 数据类型 | 描述 | 字节数 |
| 1 | token | UINT8\*16 | 令牌，标识同一用户在同一无人机上的一次会话。无人机ID，用户ID，会话密钥任一个要素改变会使令牌失效，令牌失效时候可以认证用户重新获得 | 16 |
| 5 | start\_date | UINT32 | UTC时间，BCD码表示，格式：YYYYMMDD | 4 |
|  | start\_time | UINT32 | UTC时间，BCD码表示，格式：hhmmss.ss | 4 |
| 5 | end\_date | UINT32 | UTC时间，BCD码表示，格式：YYYYMMDD | 4 |
|  | end\_time | UINT32 | UTC时间，BCD码表示，格式：hhmmss.ss | 4 |
| 7 | longitude | INT32 | 飞行区域中心点经度\*1e7，1e-5度 | 4 |
| 8 | latitude | INT32 | 飞行区域中心点纬度\*1e7，1e-5度 | 4 |
| 9 | radius | UINT32 | 飞行区域水平半径，1米 | 4 |
| 10 | altitude | UINT32 | 飞行最大离地高度，1米 | 4 |
| 11 | purpose | UINT32 | 飞行目的定义：（待细化，字符串）  航拍：1  运输：2  地形勘测：3  农田作业：4  电力检修：5  火情勘察：6 | 4 |
| 12 | length | UINT32 | 详情字符串的长度 | 32 |
| 13 | detail | STRING | 详情字符串 |  |
| 14 | mac | UINT8\*16 | 包含前述所有数据的CMAC/SM3，用无人机认证密钥 | 16 |

#### 飞行记录上报应答数据定义（c2u\_upload\_record\_result）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 字段 | 数据类型 | 描述 | 字节数 |
| 1 | token | UINT8\*16 | 令牌，标识同一用户在同一无人机上的一次会话。无人机ID，用户ID，会话密钥任一个要素改变会使令牌失效，令牌失效时候可以认证用户重新获得 | 16 |
| 5 | result | INT32 | 成功、错误码（无效ID等） | 4 |
| 6 | length | UINT32 | 飞行证书长度 | 4 |
| 7 | certificate | UINT8 | 飞行证书（飞行证书定义见3.2.2） |  |
| 8 | mac | UINT8\*16 | 包含3~7数据的MAC，用无人机认证密钥 | 16 |

### 返回值定义

|  |  |
| --- | --- |
| 错误码 | 说明 |
| 0 | 执行成功 |
| -1 | 数据校验错误 |
| -2 | 无效的ID |
| -3 | 请求拒绝 |
| -4 | 过期TOKEN |

### 加解密算法说明

|  |  |  |
| --- | --- | --- |
| 加密算法 | 描述 | 定义 |
| 未加密 | 数据没有加密 | 0x00000000 |
| AES-128-ECB |  | 0x00000100 |
| AES-128-CBC |  | 0x00000101 |
| 国密SM1 |  | 0x00000200 |
| RSA-2048 |  | 0x00000300 |
| ECC-384 |  | 0x00000400 |
| 国密SM2-384 |  | 0x00000500 |

|  |  |  |
| --- | --- | --- |
| 认证算法 | 描述 | 定义 |
| 未认证 | 没有数据认证结果 | 0x00000000 |
| CMAC-AES128 |  | 0x00000100 |
| HMAC |  | 0x00000300 |

|  |  |  |
| --- | --- | --- |
| 散列算法 | 描述 | 定义 |
| 未认证 | 没有数据认证结果 | 0x00000000 |
| 国密SM3 |  | 0x00000100 |
| SHA-256 |  | 0x00000200 |
| MD5 |  | 0x00000300 |

# 修改记录

|  |  |  |  |
| --- | --- | --- | --- |
| **版本** | **日期** | **作者** | **修改记录** |
| 0.1 | 2016/3/1 | 陈古顺 | 初始版本，内部Review |
| 0.2 | 2016/4/1 | 陈古顺 | 1．增加国密SM1/SM2/SM3支持  2．无人机ID用OID表示 |
| 0.3 | 2016/6/1 | 陈古顺 | 1. 更新到《无人机身份认证方案v0.4.pptx》  2．增加无人机和监管平台接口 |
| 0.4 | 2016/6/5 | 陈古顺  陈永森 | 1. 更新流程图  2. 优化接口协议定义，统一认证方式为MAC或者签名  3. 增加起飞/降落数据结构 |

# 定义

无人机（UA：Unmanned Aircraft）

无人机系统（UAS：Unmanned Aircraft System）

控制站（也称遥控站、地面站）

指令与控制数据链路（C2：Command and Control data link）

无人机云系统（简称无人机云）

电子围栏（Geo-fencing）

对称加解密

非对称加解密

MAC

Challenge/response

X.509

用户实名认证

无人机身份认证

飞行记录

飞行授权证书

# 参考文献

无人机身份认证方案v0.4.pptx