**智慧工地数据中心接口之**

**认证鉴权接口v3.0**

|  |  |  |
| --- | --- | --- |
| 版本 | 时间 | 变更内容 |
| V3.0 | 2019-07-19 | 3．0版本 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

## 接口说明

智慧工地信息管理平台所有接口的权限认证都采用密钥签名的认证方式，工作原理为：在系统内生成唯一的密钥，颁发给数据采集设备或其他外部系统。外部系统获取密钥对之后妥善保存密钥，在调用接口上传数据时，外部系统使用密钥当前请求进行签名，将签名后的结果放在http请求头部与数据一起发送至监管端的数据采集接口。数据采集接口根据请求头部包含的签名信息查找对应的密钥信息，验证当前请求是否合法。

## 签名方法

## 生成密钥

### 供应商密钥

智慧工地信息管理平台中可以为获得建委授权的设备供应商或软件供应商创建密钥对，密钥主要包括以下信息：

|  |  |  |
| --- | --- | --- |
| 字段名称 | 数据类型 | 描述 |
| keyId | String | 授权id，全局唯一 |
| keySecret | String | 密钥值，用于请求签名，不在请求中传输，需要妥善保管 |

### 项目密钥

项目的密钥对由项目管理人员掌握，在项目需要上传数据时将密钥对告知供应商，密钥主要包括以下信息：

|  |  |  |
| --- | --- | --- |
| 字段名称 | 数据类型 | 描述 |
| keyId | String | 授权id，全局唯一 |
| keySecret | String | 密钥的值，用于请求签名，不在请求中传输，需要妥善保管 |

## 为密钥授权

供应商拥有了合法的密钥对，在帮助项目上传数据时需要取得项目的密钥对，同时拥有两个密钥对时方可上传数据。

## 为请求签名

在调用数据接口发送数据时，需要使用密钥对请求进行签名，具体签名方式如下所示:

本次示例所用密钥对：

|  |  |  |
| --- | --- | --- |
|  | 字段名 | 字段值 |
| 供应商 | keyId | e6fe9dd5-58af-11e8-857d-00163e32d704 |
| keySecret | Ny35o694RgXURrNQ7hCBbI4wyearCWxx7H4n |
| 项目 | keyId | 1b0f28a4-a5a8-4ea8-ae1a-3b80d6e72397 |
| keySecret | RMSRvZBhviBiWlddbXil5EqVQhkHJ0WJUbH7 |

1. 取发送请求时取服务器的UNIX时间戳（服务器时间需要提前与标准时间进行校对），例如：1526438202

2. 生成一个随机字符串，长度至少10位，由英文字符与数字组成，如：jUY9ybWcM3DH，注意随机字符串每次请求都要不同，不要在不同请求中使用相同随机字符串。

3. 使用下划线将随机字符串，时间戳与密钥(供应商密钥在前项目密钥在后)拼接为预处理字符串：

jUY9ybWcM3DH\_1526438202\_Ny35o694RgXURrNQ7hCBbI4wyearCWxx7H4n\_ RMSRvZBhviBiWlddbXil5EqVQhkHJ0WJUbH7

4. 使用sha1 Hash算法对预处理字符串进行加密，得到的结果即为签名后的字符串：e914fed7db86318b6d8ce01a6f7cfe463c929f3d

5. 将密钥的keyId，随机字符串（rCode），计算签名时的UNIX时间戳以及签名放入http请求的头部,格式为：[供应商keyId]\_[项目keyId]，与数据一起发送给重庆市两江新区智慧工地信息管理平台数据接口。此时HTTP请求头中包含的签名信息如下：

keyId=e6fe9dd5-58af-11e8-857d-00163e32d704\_1b0f28a4-a5a8-4ea8-ae1a-3b80d6e72397（授权id,以下划线连接，供应商的在前，项目的在后）

ts=1526438202（时间戳）

rCode= jUY9ybWcM3DH (随机字符串)

signature= e914fed7db86318b6d8ce01a6f7cfe463c929f3d（密钥签名）

## 校验签名

接上述例子，平台收到请求后，从请求头部获取到密钥的keyId，随机串，时间戳与签名。平台鉴权计算过程如下：

1. 检查时间戳，如果时间戳小于当前时间60秒（这个值可以根据具体情况设置），则判定请求已过期，丢弃本次请求。
2. 通过密钥的keyId找到对应的密钥，按照2.3所述的方法计算签名。
3. 将计算结果与接种中的签名进行比较，如果相等则说明请求合法。
4. 记录请求日志。

5. 处理请求中上传的数据。

## 算法特点

密钥签名方式进行接口权限认证主要有以下特点：

* 在整个请求的鉴权过程中，密钥不会随数据一起通过网络进行传输，只有监管端与数据采集与提供方知晓密钥的具体内容，只要不泄露密钥，就能保证数据传输过程的安全。
* 密钥与具体的数据结构无关，即使意外泄露，也只需要双方更新对应的密钥secret值，对已有的数据与接口无任何影响。
* 整个鉴权过程由算法控制，无需保持客户端连接与会话上下文，所有请求都是无状态的，在客户端较多的情况下能够大幅减少服务器的资源消耗，提高系统运行的效率与稳定性。