**OneNET平台DTLS加密用户使用说明**

Version: 1.0

中移物联网有限公司开放平台部

2019年1月

**目录**

1、 概述 2

1.1DTLS加密介绍 2

1.2平台psk介绍 2

2、 使用说明 3

2.1使用流程 3

2.2页面注册设备 3

2.3查看与重置 5

2.4 API 5

## 概述

### 1.1DTLS加密介绍

DTLS(Datagram Transport Layer Security)即数据包传输层安全性协议，是基于TLS协议架构上提出的扩展，用于保证UDP连接的传输安全。

平台支持基于PSK（pre-shared key，预共享密钥）的DTLS协议，在用户设备和OneNET平台之间建立安全通道，用于认证和数据安全传输。DTLS协议运行在UDP之上，保证了传输数据的加密性。

### 1.2平台psk介绍

设备可通过连接引导机和直接连接接入机两种方式注册到平台，因此分为bs\_psk和acc\_psk两种。bs\_psk为连接引导机时握手所需psk，acc\_psk为连接接入机时握手所需psk。使用引导机接入的地址为183.230.40.39，接入机地址为183.230.40.40，加密端口为5864。

## 使用说明

### 2.1使用流程

1. 情况一：先烧录后注册

用户选择引导机或接入机接入 — 选择对应psk烧录于终端设备 — 通过OneNET平台注册设备 — 注册时输入预置psk — 连接端口5864进行加密传输

1. 情况二：先注册后烧录

用户通过OneNET平台注册设备获得随机psk — 将psk烧录于设备中 — 连接5864端口进行加密传输

### 2.2页面注册设备

点击添加设备，在DTLS加密选项中，下拉菜单，可对PSK进行配置



其中，默认为系统自动生成psk，支持手动输入，若不填写，则由平台自动随机生成；

点击确定后，页面会展示一次PSK



### 2.3查看与重置

在详情界面中，可以查看与重置psk码。



用户进行此操作需要通过短信验证后才可以查看与重置。重置仅支持平台随机生成psk码，若需要手动更改，请使用API进行变更。详情可在开发文档-应用开发指南-API-LwM2M中查看

### 2.4 API

用户可通过API接口查看、更新psk，详情可在开发文档-应用开发指南-API-LwM2M中查看