RTL8762D Security Mechanism User Guide

V0.1

2020/06/04

修订历史（Revision History）

日期	版本	修改	作者	Reviewer
2020/06/04	Draft v0.1	初稿	Serval	

目 录

表目录

图目录

1 概述

本文介绍 RTL8762D 的安全机制以及使用方法。安全机制是通过加密数据来保护 flash 上的 image，同时也包括烧录解密 key 以及控制调试接口的开关等功能。

2 安全机制

安全机制主要包括加密 image、eFuse key、SWD 接口控制和 Password 调试这四部分。

2.1 加密 image

Patch image 是加密的，APP image 可以根据需求选择加密与否。加密使用的是 AES 对称加密算法，加密 key 长度为 128 bit。在 IC 启动时，会通过读取 eFuse 中的 key 来解密 image，如果 key 没有烧录或者烧录的 key 和加密的 key 不匹配，都会导致启动失败。

2.2 eFuse Key

加密和解密用的 key 是同一个，长度 128 bit，所以需要特殊的机制来保护加密 key 不被泄露。加密 key 会经过加密 Tool 加密一次得到 key’, key’再发布给工厂烧录到 IC eFuse 中。烧录的过程中，烧录 Tool 会对 Key’解密得到原始的 key，同时会读取 IC 的 UUID 和 key 计算后写入，以保证每块 IC 中烧录的 key 值都是不同的。

2.3 SWD 接口控制

SWD 接口作为重要的调试接口，对调试程序起了很大的作用。但是同样也会增加暴露程序数据和代码的风险。所以安全机制提供了控制 SWD 接口的方法。有 3 种控制方式：开，关和 Password 控制。其中 Password 控制表示需要通过 HCI UART 输入正确的 Password 才能打开，否则是关闭状态。

2.4 Password 调试

Password 和加密 key 类似，也是烧录在 IC 的 eFuse 中。如果某个功能是设定成 Password 控制，就需要通过 HCI UART 输入正确的 Password，然后 IC 会自动重启并检查 Password 是否正确，如果正确则打开该功能。每次 IC 重启都需要重新输入 Password 才能打开该功能。

3 安全级别

RTL8762D 提供 3 种安全级别：0，1 和 2。数字越高安全级别越高，安全级别越高可能会对调试或者重烧 eFuse 有影响。表 3-1 是不同的安全级别下各个模块的功能开关控制。建议在少量试产时设定成 1 级，正式量产时设定成 2 级。

表 3-1 Security Level 配置项设定

Security Level	SWD Control	eFuse Read	eFuse Write	HCI Download	HCI BT Test
0	Enable	Enable	Enable	Enable	Enable
1	Enable by password	Enable by password	Enable	Enable	Enable
2	Enable by password	Disable	Enable by password	Enable	Enable

4 使用示例

4.1 配置加密 key

编辑 sdk\tool\key. json，配置 OCEK 和 PASSWORD。该文件里的 OCEK 和 PASSWORD 是明文，需要注意保护该文件。

```
{
    "OCEK":    "a1a2a3a4a5a6a7a8a9aaabacadaeafb0",
    "PASSWORD":  "00112233445566778899aabbccddeeff"
}
```

4.2 生成加密 APP image

要加密的函数前使用 APP_ENCRYPTION_TEXT_SECTION 修饰。SDK 的 mem_config. h 中通过宏 FEATURE_ENCRYPTION 来控制是否编译成加密 APP。默认设定是 0，表示非加密。

```
/**·@brief·set·app·bank·to·support·OTA:·1·is·ota·bank1,·0·is·ota·bank0·*/
#define·APP_BANK·····0

/**·@brief·ram·code·configuration:·1·is·ram·code,·0·is·flash·code·*/
#define·FEATURE_RAM_CODE·····1

/**·@brief·encrypt·app·or·not·*/
#define·FEATURE_ENCRYPTION·····1
```

图 4-1 APP 编译为加密 Code

4.3 烧录 eFuse

注意：

eFuse 烧录时必须供给 2. 5V（±10%）电压，本文档的烧录步骤适用于采用宽压 Flash，并且 2. 5V（±10%）供电。这样烧录 Flash 和 eFuse 可以在一站完成。

RD 端配置生成用于烧录的 eFuse 文件

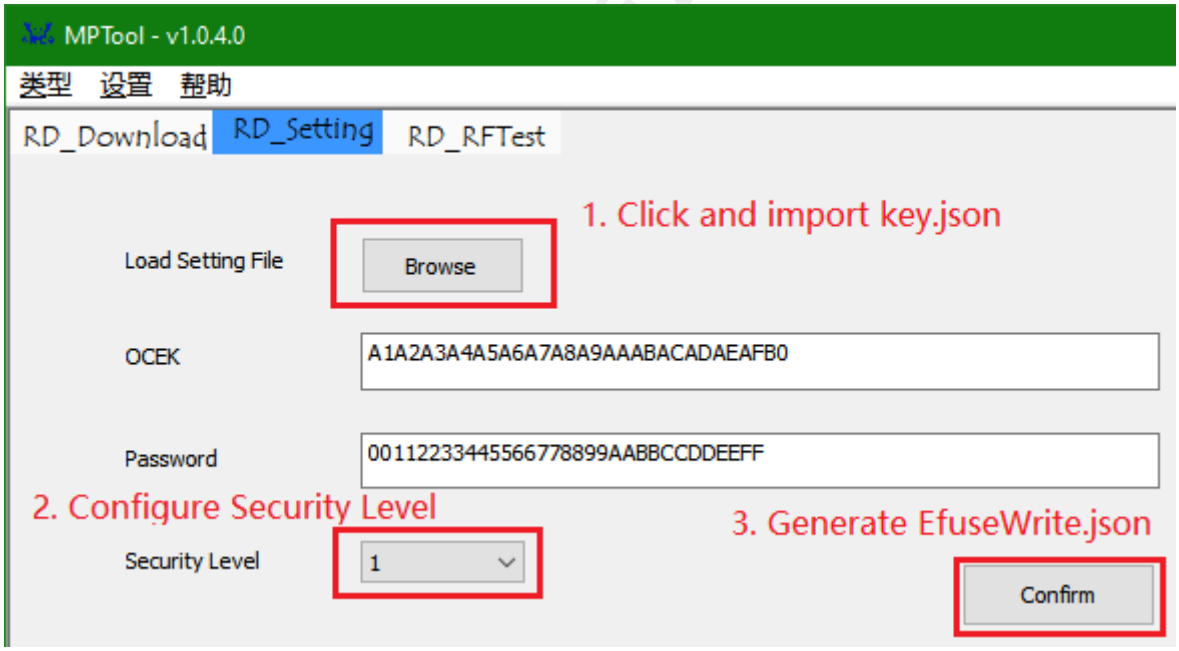

图 4-2 生成用于烧录的 eFuse 文件

首先确保 MP Tool 处于调试模式：可通过 MP Tool“类型”选择“调试”进入。

1. 在“RD Setting”页面，点击“Browse”按钮导入 key.json 文件；
2. 选择项使用的 Security Level；
3. 点击“Confirm”按钮，生成 EfuseWrite.json，该文件可以提供给工厂烧录。

工厂端烧录 eFuse

首先确保 MP Tool 处于量产模式：可通过 MP Tool“类型”选择“量产”进入。

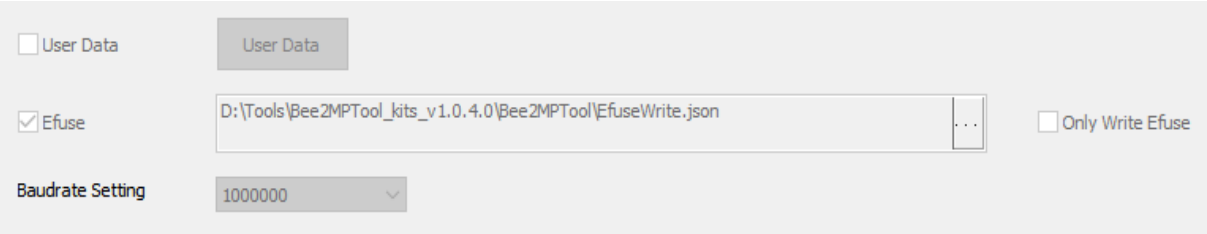

图 4-3 选择 eFuse 烧录文件

1. 在“MP Setting”页面勾选“Efuse”，并选择待烧录的 eFuse 文件。
2. 点击“MP Download”页面的“下载”按钮进行烧录。

4.4 通过 Password 调试

当 Security Level 烧录为 1 或 2 时，SWD 被禁掉，RD 端可以通过 PASSWORD 重新打开 SWD。

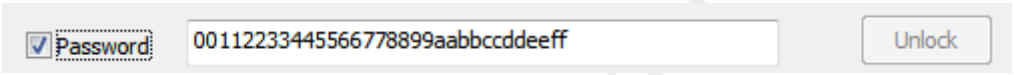

图 4-4 使用 PASSWORD 解锁 SWD

步骤如下：

在调试模式“RD Download”界面打开串口，选择“Password”，输入 key. json 中的原始明文 PASSWORD，点击“Unlock”按钮。之后 IC 会重启，重启之后 SWD 便被打开。