

# **RTL8762E Security Mechanism User Guide**

**V1.0**

**2022/05/17**

## 修订历史

日期	版本	修改	作者	审阅
2022/05/17	V1.0	Release Version	Serval Li	Lory

Realtek  
Confidential

# 目 录

1 概述 .....	1
2 安全机制 .....	2
2.1 加密 Image .....	2
2.2 Flash Key .....	2
2.3 SWD 接口控制 .....	2
3 安全级别 .....	3
4 使用示例 .....	4
4.1 配置加密 key .....	4
4.2 生成加密 APP image .....	4
4.3 烧录 eFuse .....	5

## 表目录

表 3-1 Security Level 配置项设定.....	3
---------------------------------	---

Realtek  
Confidential

## 图目录

图 4-1 APP 编译为加密 Code .....	4
图 4-2 生成用于烧录的 eFuse 文件.....	5
图 4-3 选择 eFuse 烧录文件.....	5

Realtek  
Confidential

# 1 概述

本文介绍 RTL8762E 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，以及控制调试接口关闭等功能。

Realtek  
Confidential

## 2 安全机制

安全机制主要包括加密 Image、Flash key、SWD 接口控制这三部分。

### 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 Flash 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 Flash Key

加密和解密用的是同一个 key，长度为 128bit，所以需要特殊的机制来保护加密 key 不被泄露。加密 key 经过加密 Tool 加密一次得到 key'，key'再发布给工厂烧录到 IC Flash 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，对调试程序有着很大的作用。但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关闭 SWD 接口的方法。通过配置并烧录 Security Level 可以关闭 SWD 接口。

### 3 安全级别

RTL8762E 提供 4 种安全级别：0，1，2 和 3。数字越高安全级别越高，越高的安全级别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 或 3 级。

表 3-1 Security Level 配置项设定

Security Level	SWD Control	eFuse Read	eFuse Write
0	Enable	Enable	Enable
1	Disable	Enable	Enable
2	Disable	Enable	Disable
3	Disable	Disable	Disable

Realtek  
Confidential



## 4 使用示例

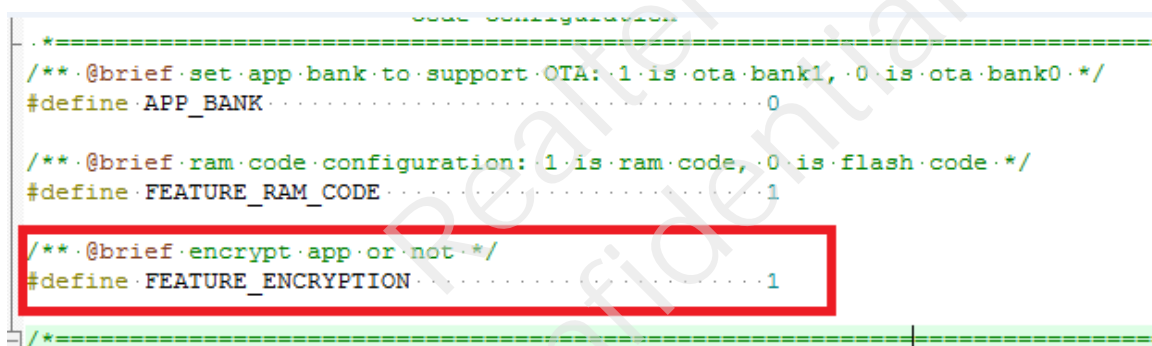
### 4.1 配置加密 key

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

```
1.  {
2.    "OCEK": "a1a2a3a4a5a6a7a8a9aaabacadaeafb0"
3.  }
```

### 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。如图 4-1 所示。



```

===== Code Configuration =====
/** @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

注意事项：eFuse 烧录时必须供 2.5V（±10%）电压。RTL8762E 内置宽压 Flash，可以在 2.5V 电压工作。这样 Flash 和 eFuse 烧录可以在一站完成。

### 1. RD 端配置生成用于烧录的 eFuse 文件

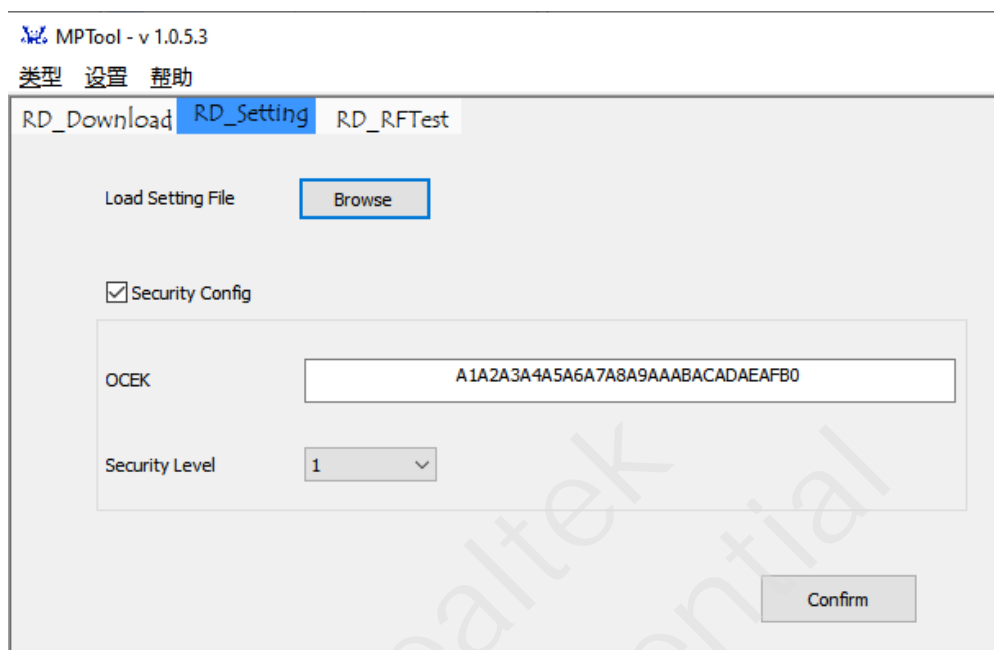


图 4-2 生成用于烧录的 eFuse 文件

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) 选中 “Security Config”，选择想使用的 Security Level；
- 3) 点击 “Confirm” 按钮，生成 EfuseWrite.json，该文件可以提供给工厂烧录。

### 2. 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。

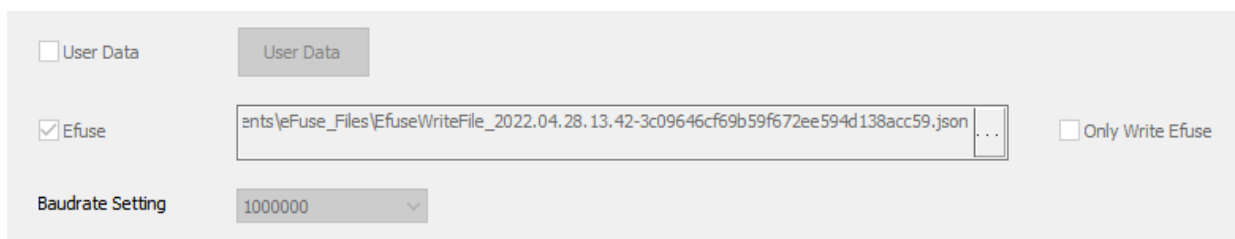


图 4-3 选择 eFuse 烧录文件

- 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。