RTL8762E Security Mechanism User Guide

V1.0

2022/05/17

Revision History

Date	Version	Comments	Author	Reviewer
2022/05/17	V1.0	Release Version	Serval Li	Lory

Contents

Table List

Figure List

1 Introduction

This paper introduces security mechanism of RTL8762E as well as its usage. Security mechanism protects images in Flash by encrypting data, and it also includes debug port control.

2 Security Mechanism

Security mechanism includes image encryption, Flash key and SWD interface.

2.1 Image Encryption

Encryption is mandatory to Patch image and optional to APP image. AES symmetric encryption algorithm is used to encrypt the images and the encryption key has the length of 128 bits. When IC is booting, image will be decrypted by reading the key in Flash. If key is not programmed or the key programmed doesn’t match the encryption key, the boot process will fail.

2.2 Flash Key

It is necessary to find out a special mechanism to protect encryption key from leakage for the reason that Encryption and decryption use the same 128-bit key. A new key will be generated when passing Encryption key to Encryption Tool, which will also be published and downloaded into Flash Config of IC. During the download process, Download Tool will decrypt the new key to obtain original key and read UUID of IC at the same time. These information will be combined together to generate a new key to ensure that each IC has a unique key.

2.3 SWD Interface Control

SWD interface is an important debug port that plays a vital role in debugging program. However, it also increases the risk of exposing data and code. We can close the SWD interface by programming Security Level.

3 Security Level

RTL8762E provides 4 security levels: 0, 1, 2 and 3. Larger number indicates higher security level, which will affect debug and re-program of eFuse. Function control of each module under different security level is listed in Table 3-1. It is suggested to configure security level to level 1 during minor trial-production and level 2 or 3 in mass production.

Table 3-1 Security Level Configuration

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

4 Usage Example

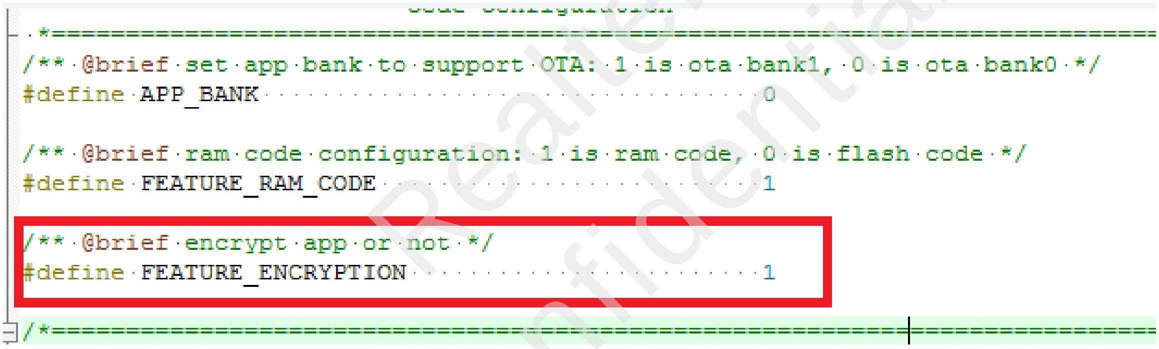
4.1 Configure Encryption Key

Edit JSON file located at sdk\tool\key.json to configure OCEK, where OCEK is plaintext that needs protection.

```
{
    "OCEK": "a1a2a3a4a5a6a7a8a9aaabacadaeafb0"
}
```

4.2 Generate Encrypted APP Image

Attach APP_ENCRYPTION_TEXT_SECTION to the function to be encrypted. In mem_config.h of SDK, Macro FEATURE_ENCRYPTION determines if the APP requires encryption. It is assigned to 0 by default, which indicates not encrypted.



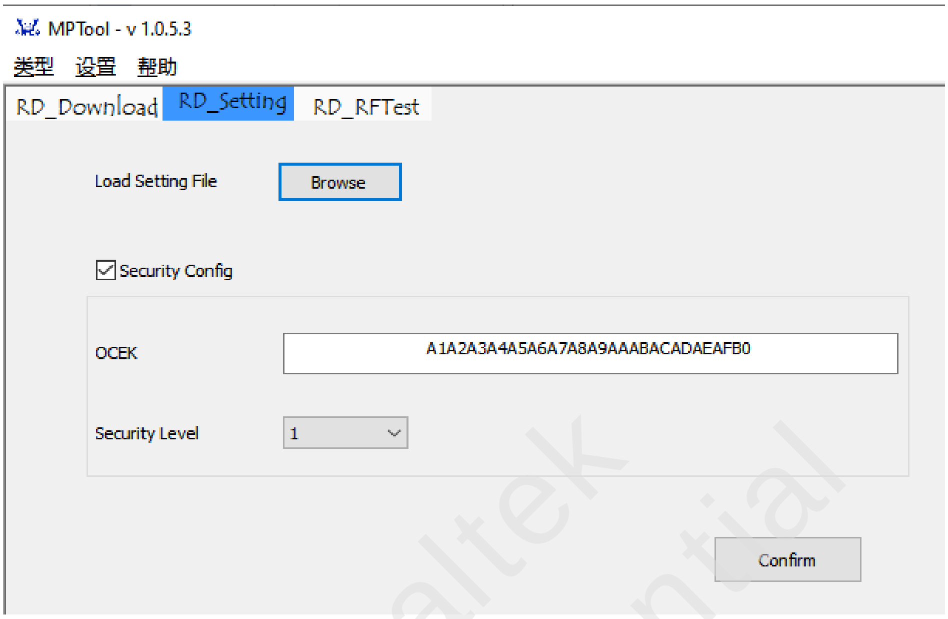
```
 *============================================================================
/** @brief set app bank to support OTA: 1 is ota bank1, 0 is ota bank0 */
#define APP_BANK                                  0

/** @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

/*============================================================================
```

Figure 4-1 Encrypt APP Code

4.3 Program eFuse

Note: 2.5V (±10%) power supply must be applied when programming eFuse. RTL8762E has an embedded wide range Flash which can work at 2.5V, Flash and eFuse can be programmed in the same station.

1. **Program eFuse in RD end**



Load Setting File

☑ Security Config

OCEK: A1A2A3A4A5A6A7A8A9AAABACADAEAFB0

Security Level: 1

Figure 4-2 Generate the File to Program eFuse

Above all, confirm that MP Tool is in debug mode: Click ‘Type’ button on tool bar and tick ‘Debug’.

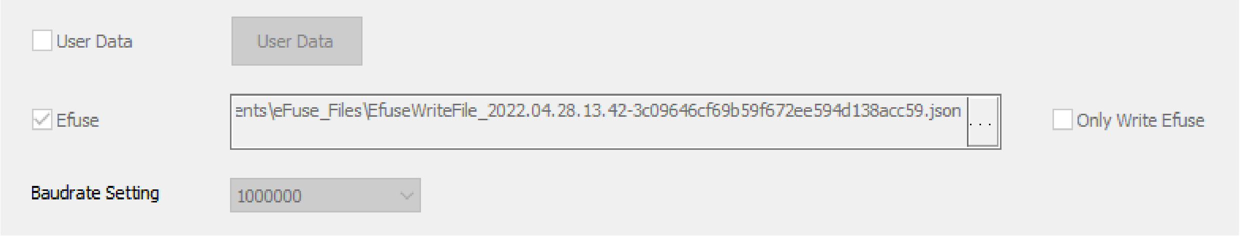
1) Click ‘Browse’ button to import key.json file in ‘RD Setting’ UI.

2) Click ‘Security Config’, select appropriate Security Level for project.

3) Click ‘Confirm’ button to generate EfuseWrite.json file, which can be released to factory for programming eFuse.

2. **Program eFuse in factory**

Above all, confirm that MP Tool is in mass production mode: Click ‘Type’ button on tool bar and tick ‘MP’.



□ User Data

☑ Efuse: ents\eFuse_Files\EfuseWriteFile_2022.04.28.13.42-3c09646cf69b59f672ee594d138acc59.json

□ Only Write Efuse

Baudrate Setting: 1000000

Figure 4-3 Select the File to be Programmed in eFuse

1) Tick ‘Efuse’ in ‘MP Setting’ UI and select the eFuse file to be downloaded.

2) Click ‘Download’ button in ‘MP Download’ UI to program eFuse.