RTL8762C Security Mechanism
User Guide

V1.2
2023/06/07

Realtek Semiconductor Corp.
No.2, Innovation Road II, Hsinchu Science Park, Hsinchu 300, Taiwan
Tel.: +886-3-578-0211. Fax: +886-3-577-6047
www.realtek.com

COPYRIGHT

DISCLAIMER

Realtek provides this document 'as is', without warranty of any kind. Realtek may make improvements and/or changes in this document or in the product described in this document at any time. This document could include technical inaccuracies or typographical errors.

TRADEMARKS

Realtek is a trademark of Realtek Semiconductor Corporation. Other names mentioned in this document are trademarks/registered trademarks of their respective owners.

USING THIS DOCUMENT

This document is intended for the software engineer's reference and provides detailed programming information. Though every effort has been made to ensure that this document is current and accurate, more information may have become available subsequent to the production of this guide.

ELECTROSTATIC DISCHARGE (ESD) WARNING

This product can be damaged by Electrostatic Discharge (ESD). When handling, care must be taken. Damage due to inappropriate handling is not covered by warranty.

Do not open the protective conductive packaging until you have read the following, and are at an approved anti-static workstation.

- Use an approved anti-static mat to cover your work surface
- Use a conductive wrist strap attached to a good earth ground
- Always discharge yourself by touching a grounded bare metal surface or approved anti-static mat before picking up an ESD-sensitive electronic component
- If working on a prototyping board, use a soldering iron or station that is marked as ESD-safe
- Always disconnect the microcontroller from the prototyping board when it is being worked on

Revision History

Date	Version	Comments	Author	Reviewer
2018/09/05	Draft V0.1	First edition	Astor	Rui
2022/03/08	Draft V0.2	Support more security levels	Serval	Rui
2022/10/24	V1.0	Revise Format	Serval	David
2023/04/03	V1.1	Grammar Check	Lory	
2023/06/07	V1.2	Add Disclairm	Lory	

Contents

1 Introduction 1

2 Security Mechanism 2

2.1 Image Encryption 2

2.2 Flash Key 2

2.3 SWD Interface Control 2

2.4 Password Debug 2

3 Security Level 3

4 Usage Example 4

4.1 Configure Encryption Key 4

4.2 Generate Encrypted APP Image 4

4.3 Program eFuse 4

4.4 Password Debug 6

Table List

Table 3-1 Security Level Configuration 3

Figure List

Figure 4-1 Encrypt APP Code 4
Figure 4-2 Generate the File to Program eFuse 5
Figure 4-3 Select the File to be Programmed in eFuse 5
Figure 4-4 Use PASSWORD to unlock SWD 6

1 Introduction

This paper introduces security mechanism of RTL8762C as well as its usage. Security mechanism protects images in Flash by encrypting data, and it also includes downloading decryption key and controlling debug port.

2 Security Mechanism

Security mechanism includes image encryption, eFuse key, SWD interface control and Password debug.

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 the encryption key from leakage because Encryption and decryption use the same 128-bit key. A new key will be generated when passing the 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. This information will be combined 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 a program. However, it also increases the risk of exposing data and code. Security mechanism provides 3 methods to control SWD interface: Open, Close and Password Control, among which Password Control denotes the SWD interfaces is always closed unless the correct password is received through HCI UART.

2.4 Password Debug

Similar to encryption key, password is also programmed in the eFuse of the IC. When password is received through HCI UART, IC will reboot automatically to check if the password is correct. The function configured as Password control is always closed unless the password is correct. Each time IC reboots, password need be retyped to active the function.

3 Security Level

RTL8762C provides 6 security levels: 0 to 5. The security levels can be divided into two groups: 0 to 2 and 3 to 5. The only one difference of them is the HCI Download feature. A 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 the security level to level 1 during trial-production and level 2 in mass production. If you want to prevent an unauthorized user from cracking your board by reprogramming, please configure the security level to level 4 or 5. Please update the MP Tool to version 1.0.4.7 or newer before configure security level to level 3, 4 or 5.

Table 3-1 Security Level Configuration

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
3	Enable	Enable	Enable	Enable by password	Enable
4	Enable by password	Enable by password	Enable	Enable by password	Enable
5	Enable by password	Disable	Enable by password	Enable by password	Enable

4 Usage Example

4.1 Configure Encryption Key

Edit JSON file located at sdk\tool\key.json to configure OCEK (for APP Image Encryption) and PASSWORD (for SWD Debug), where OCEK and PASSWORD are plaintext that needs protection.

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

4.2 Generate Encrypted APP Image

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. As shown in Figure 4-1. So If APP needs to be encrypted, set FEATURE_ENCRYPTION to 1 and add APP_ENCRYPTION_TEXT_SECTION to the function to be encrypted. Because the decryption flow in the bootloader is to decrypt code and copy them to ram, the more functions added APP_ENCRYPTION_TEXT_SECTION means more ram size is needed.

```
/**@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. The download procedure introduced in this document applies to Flash that supports wide voltage range and can be powered by 2.5V (±10%) power supply. Under such circumstances, Flash and eFuse can be programmed in one step.

1. Program eFuse in RD end

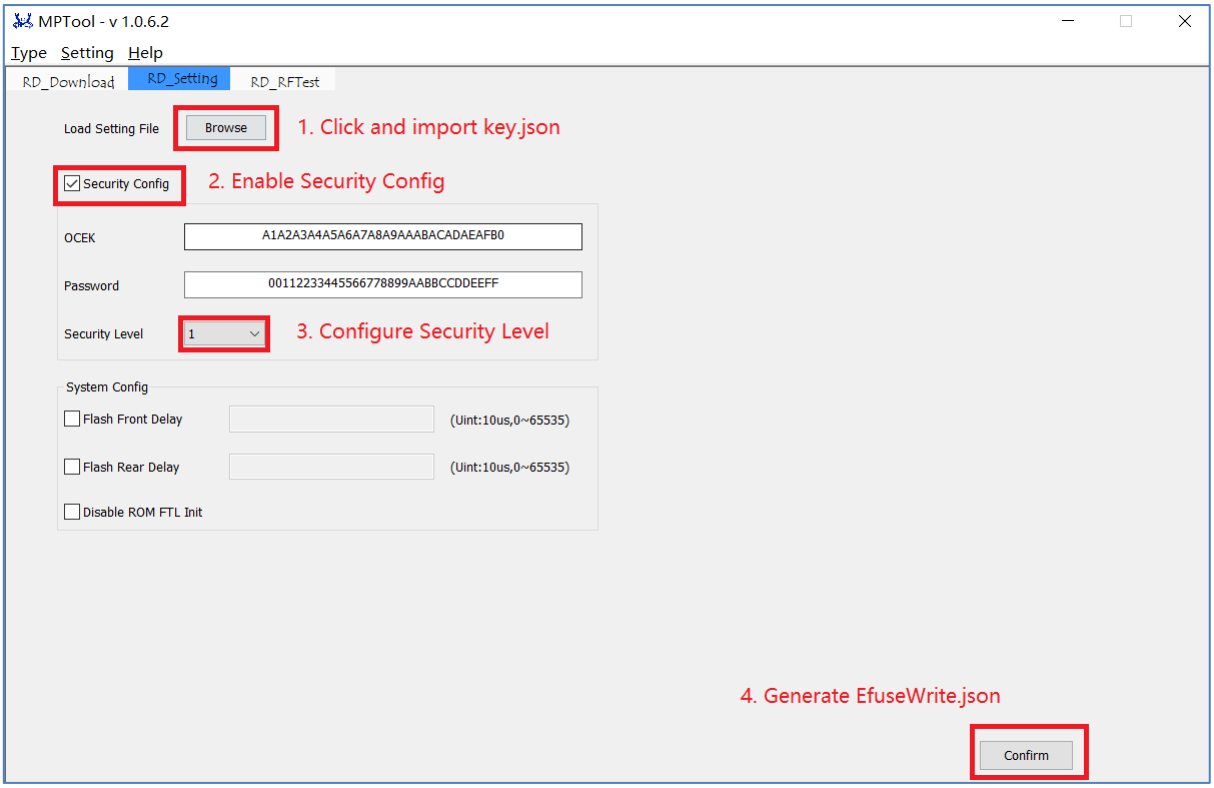

Figure 4-2 Generate the File to Program eFuse

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) 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".

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.

4.4 Password Debug

When security level is 1, 2, 4 or 5, SWD interface will be banned, and developer can reactive SWD interface by Password debug.

When security level is 3, 4 or 5, HCI Download will be banned, and developer can reactive HCI Download by Password debug.

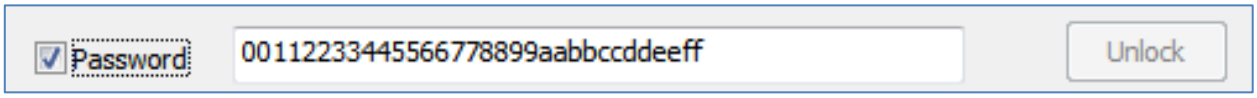

Figure 4-4 Use PASSWORD to unlock SWD

The steps are as follows:

1. Open serial port in "RD Download" interface.
2. Tick "Password".
3. Type in the plaintext of password defined in key.json.
4. Click "Unlock" button.
5. IC will reboot.
6. SWD interface will be reactivated after the reboot process.