MT793X IoT SDK for AES User Guide

Version: 1.0

Release date: 2021-07-29

Version History

Version	Date	Description
1.0	2021-07-29	Official release

Table of Contents

1 Getting Started

This chapter introduces the AES (Advanced Encryption Standard) feature and gives you an idea of what you need to prepare to get started.

1.1 Overview

Support AES CBC (Cipher Block Chaining), ECB (Electronic Codebook) and GCM (Galois/Counter Mode).

1.2 Code Layout

driver\chip\mt7933\src\hal_aes.c
driver\chip\inc\hal_aes.h
driver\chip\mt7933\inc\hal_gcpu_internal.h

1.3 AES APIs

hal_aes_cbc_decrypt()
hal_aes_cbc_decrypt_iteration()
hal_aes_cbc_encrypt()
hal_aes_cbc_encrypt_iteration()
hal_aes_ecb_decrypt()
hal_aes_ecb_encrypt()
hal_aes_gcm_decrypt()
hal_aes_gcm_encrypt()

2 AES Sample Use Cases

Use the AES in CBC mode to perfrom encryption and decryption.

Step 1. Call hal_aes_cbc_encrypt() to encrypt.
Step 2. Call hal_aes_cbc_decrypt() to decrypt.

Sample code:

```
uint8_t aes_cbc_iv[HAL_AES_CBC_IV_LENGTH] = {

0x61, 0x33, 0x46, 0x68, 0x55, 0x38, 0x31, 0x43,

0x77, 0x68, 0x36, 0x33, 0x50, 0x76, 0x33, 0x46

};

uint8_t plain[] = {

0, 11, 22, 33, 44, 55, 66, 77, 88, 99, 0, 11, 22, 33, 44, 55,

66, 77, 88, 99, 0, 11, 22, 33, 44, 55, 66, 77, 88, 99

};

hal_aes_buffer_t plain_text = {

.buffer = plain,

.length = sizeof(plain)

};

hal_aes_buffer_t key = {

.buffer = hardware_id,

.length = sizeof(hardware_id)

};

uint8_t encrypted_buffer[32] = {0};

hal_aes_buffer_t encrypted_text = {
```

```
.buffer = encrypted_buffer,

.length = sizeof(encrypted_buffer)

};

hal_aes_cbc_encrypt(&encrypted_text, &plain_text, &key, aes_cbc_iv);

uint8_t decrypted_buffer[32] = {0};

hal_aes_buffer_t decrypted_text = {

.buffer = decrypted_buffer,

.length = sizeof(decrypted_buffer)

};

hal_aes_cbc_decrypt(&decrypted_text, &encrypted_text, &key, aes_cbc_iv);
```

Exhibit 1 Terms and Conditions

Your access to and use of this document and the information contained herein (collectively this "Document") is subject to your (including the corporation or other legal entity you represent, collectively "You") acceptance of the terms and conditions set forth below ("T&C"). By using, accessing or downloading this Document, You are accepting the T&C and agree to be bound by the T&C. If You don't agree to the T&C, You may not use this Document and shall immediately destroy any copy thereof.

This Document contains information that is confidential and proprietary to MediaTek Inc. and/or its affiliates (collectively "MediaTek") or its licensors and is provided solely for Your internal use with MediaTek's chipset(s) described in this Document and shall not be used for any other purposes (including but not limited to identifying or providing evidence to support any potential patent infringement claim against MediaTek or any of MediaTek's suppliers and/or direct or indirect customers). Unauthorized use or disclosure of the information contained herein is prohibited. You agree to indemnify MediaTek for any loss or damages suffered by MediaTek for Your unauthorized use or disclosure of this Document, in whole or in part.

MediaTek and its licensors retain titles and all ownership rights in and to this Document and no license (express or implied, by estoppels or otherwise) to any intellectual propriety rights is granted hereunder. This Document is subject to change without further notification. MediaTek does not assume any responsibility arising out of or in connection with any use of, or reliance on, this Document, and specifically disclaims any and all liability, including, without limitation, consequential or incidental damages.

THIS DOCUMENT AND ANY OTHER MATERIALS OR TECHNICAL SUPPORT PROVIDED BY MEDIATEK IN CONNECTION WITH THIS DOCUMENT, IF ANY, ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE. MEDIATEK SPECIFICALLY DISCLAIMS ALL WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, FITNESS FOR A PARTICULAR PURPOSE, COMPLETENESS OR ACCURACY AND ALL WARRANTIES ARISING OUT OF TRADE USAGE OR OUT OF A COURSE OF DEALING OR COURSE OF PERFORMANCE. MEDIATEK SHALL NOT BE RESPONSIBLE FOR ANY MEDIATEK DELIVERABLES MADE TO MEET YOUR SPECIFICATIONS OR TO CONFORM TO A PARTICULAR STANDARD OR OPEN FORUM.

Without limiting the generality of the foregoing, MediaTek makes no warranty, representation or guarantee regarding the suitability of its products for any particular purpose, nor does MediaTek assume any liability arising out of the application or use of any product, circuit or software. You agree that You are solely responsible for the designing, validating and testing Your product incorporating MediaTek's product and ensure such product meets applicable standards and any safety, security or other requirements.

The above T&C and all acts in connection with the T&C or this Document shall be governed, construed and interpreted in accordance with the laws of Taiwan, without giving effect to the principles of conflicts of law.