AN12901

DCP-How to do Key Management

Rev. 0 — June 2020

Application Note

Contents

1 Introduction

The i.MX RT10xx provides a Data Co-Processor (DCP) block, which supports Advanced Encryption Standard (AES) encryption and hashing functions. The AES block implements a 128-bit key/data encryption/decryption block. The key is important for encryption and must be used for protection. This application note describes how to use the AES block with different keys, and how to manage keys.

2 Abbreviations

This section provides an overview of the abbreviations used in this document.

Table 1. Abbreviations

Abbreviation	Description
OCOTP	On-chip One-Time Program
AES	Advanced Encryption Standard
ECB	Electronic Cookbook Mode
CBC	Cipher Block Chaining
SW_GP2	Software general purpose key from fuse
SNVS	Secure Non-Volatile Storage
DCP	Data Co-Processor. This module provides general encryption and hashing functions.

3 AES keys of DCP

There are various AES keys provided with the DCP block, as shown in the following figure. One AES key needs to be selected before encryption/decryption.

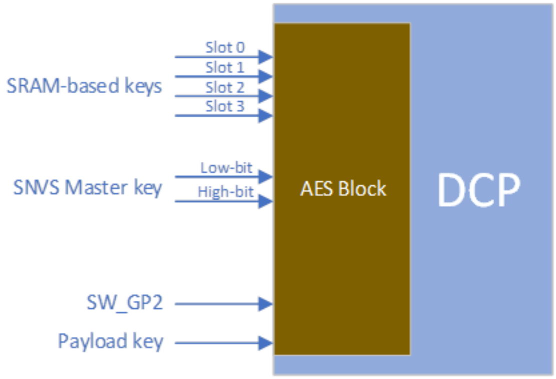


Figure 1. AES keys of DCP

3.1 SRAM-based keys

The DCP implements four SRAM-based keys that can be used by the software to securely store keys on a semi-permanent basis. You can write the keys through the programming interface by specifying a key index that specifies which key to load and a subword pointer that indicates which word to write within the key. After you write a subword, the logic automatically increments the subword pointer so that the software can program the higher-order words of the key without rewriting the key index.

NOTE

The keys written in the key storage are not readable.

3.2 SNVS Master key

eFuse is the source of the SNVS Master key. The SNVS Master key is 256-bit. A MUX is used to select the high or low 128 bits of the key for AES. SNVS can supply its Master key to DCP, given the DCP_KEY_SEL and DCPKEY_OCOTP_OR_KEYMUX bits in the IOMUXC_GPR register are configured.

3.3 SW_GP2

SW_GP2 is from eFuse which can be remapped at OCOTP Bank5. After the system reset, SW_GP2 is copied to shadow registers automatically. You can burn and lock it. When you burn and lock bits, SW_GP2 cannot be read/written by software.

3.4 Payload key

When the PAYLOAD_KEY bit of the control register is set, it indicates that the payload contains the key. The first entry in the payload is the key that is used for the operation.

3.5 Summary

When the key selection changes for DCP, do the software reset of DCP through the register to make the new key effective. The following table gives the summary for different keys.

Key	Access	Remark
SRAM-based key	W	The keys are stored in SRAM. User can set through registers, but not read it.
SNVS Master key[1]	None	Black key. It is from SNVS module.

Table continues on the next page...

Table continued from the previous page...

SW_GP2	WR[2]	It is from eFuse.
Payload key	RW	It is from payload.

1. If the device is in the Non-secure state, SNVS Master key reset to all 0.
2. Once burned lock bits, SW_GP2 cannot be read/write by software.

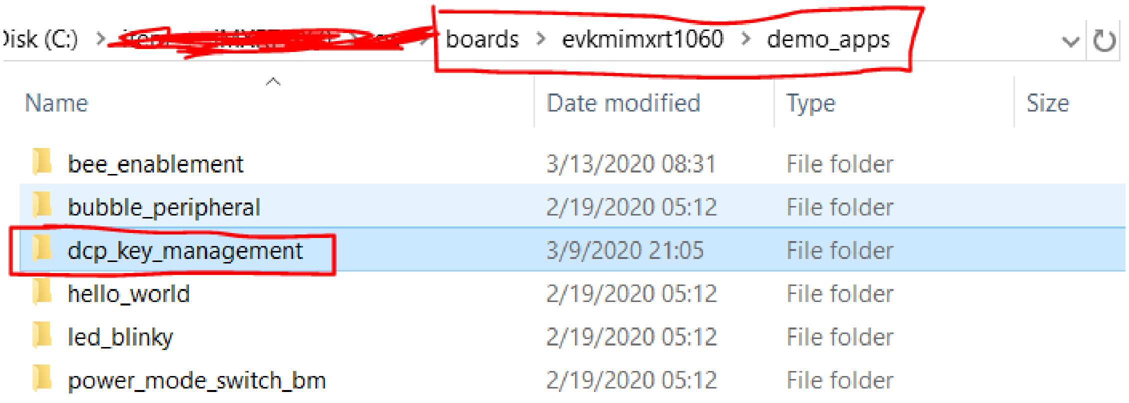
NOTE

- W: Write
- None: Cannot read and write
- RW: Read and write

4 Application example

The application example describes how to use different keys for DCP. In the example code, all keys are used to encrypt/decrypt data in AES, ECB, and CBC mode.

The example code is based on SDK_2.7.0_EVK-MIMXRT1060. Download the example code from the attached file and then unzip it in the SDK project folder: .\boards\evkmimxrt1060\demo_apps, as shown in the following figure.



Disk (C:) > [redacted] > boards > evkmimxrt1060 > demo_apps

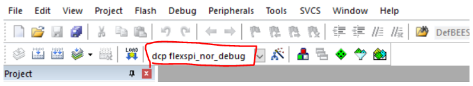
Name	Date modified	Type	Size
bee_enablement	3/13/2020 08:31	File folder	
bubble_peripheral	2/19/2020 05:12	File folder	
dcp_key_management	3/9/2020 21:05	File folder	
hello_world	2/19/2020 05:12	File folder	
led_blinky	2/19/2020 05:12	File folder	
power_mode_switch_bm	2/19/2020 05:12	File folder	

Figure 2. Example code folder

The example project can only be opened by MDK IDE.

To run the example project, follow these steps:

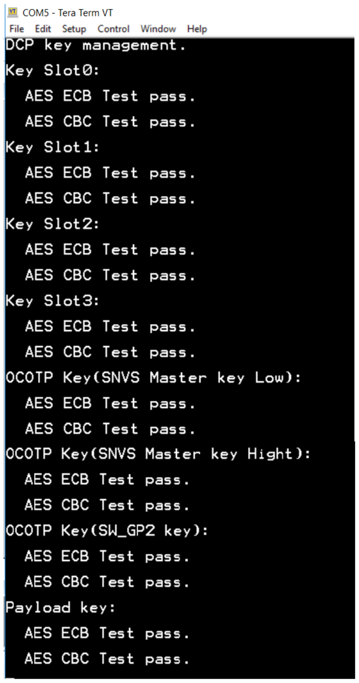
1. Connect a USB cable between the host PC and the Open SDA USB port (J14) on MIMXRT1060-EVK board.
2. Open a serial terminal with the setting: 115200 baud rate, 8 data bits, no parity, one stop bit, and no flow control.
3. Open the example project with MDK IDE, and select "dcp_flexspi_nor_debug" mode to compile and download.



dcp flexspi_nor_debug

Figure 3. "dcp_flexspi_nor_debug" mode for project

4. Press SW9 button on the board and the serial terminal shows the text, as shown in the following figure.



```
DCP key management.
Key Slot0:
  AES ECB Test pass.
  AES CBC Test pass.
Key Slot1:
  AES ECB Test pass.
  AES CBC Test pass.
Key Slot2:
  AES ECB Test pass.
  AES CBC Test pass.
Key Slot3:
  AES ECB Test pass.
  AES CBC Test pass.
OCOTP Key(SNVS Master key Low):
  AES ECB Test pass.
  AES CBC Test pass.
OCOTP Key(SNVS Master key Hight):
  AES ECB Test pass.
  AES CBC Test pass.
OCOTP Key(SW_GP2 key):
  AES ECB Test pass.
  AES CBC Test pass.
Payload key:
  AES ECB Test pass.
  AES CBC Test pass.
```

Figure 4. Printed information on terminal

5 Conclusion

This application note introduces DCP key management, and give an example project to use different keys. The application explains how all keys can be used by DCP and the user can select different keys based on application.

6 References

- i.MX RT1050 Processor Reference Manual
- Security Reference Manual for the i.MX RT1050 Processor

7 Revision history

Table 2. Revision history

Revision number	Date	Substantive changes
0	06/2020	Initial release

How To Reach Us

Home Page:

nxp.com

Web Support:

nxp.com/support

Information in this document is provided solely to enable system and software implementers to use NXP products. There are no express or implied copyright licenses granted hereunder to design or fabricate any integrated circuits based on the information in this document. NXP reserves the right to make changes without further notice to any products herein.

NXP makes no warranty, representation, or guarantee regarding the suitability of its products for any particular purpose, nor does NXP assume any liability arising out of the application or use of any product or circuit, and specifically disclaims any and all liability, including without limitation consequential or incidental damages. “Typical” parameters that may be provided in NXP data sheets and/or specifications can and do vary in different applications, and actual performance may vary over time. All operating parameters, including “typicals,” must be validated for each customer application by customer's technical experts. NXP does not convey any license under its patent rights nor the rights of others. NXP sells products pursuant to standard terms and conditions of sale, which can be found at the following address: nxp.com/SalesTermsandConditions.

While NXP has implemented advanced security features, all products may be subject to unidentified vulnerabilities. Customers are responsible for the design and operation of their applications and products to reduce the effect of these vulnerabilities on customer’s applications and products, and NXP accepts no liability for any vulnerability that is discovered. Customers should implement appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP, the NXP logo, NXP SECURE CONNECTIONS FOR A SMARTER WORLD, COOLFLUX, EMBRACE, GREENCHIP, HITAG, ICODE, JCOP, LIFE VIBES, MIFARE, MIFARE CLASSIC, MIFARE DESFire, MIFARE PLUS, MIFARE FLEX, MANTIS, MIFARE ULTRALIGHT, MIFARE4MOBILE, MIGLO, NTAG, ROADLINK, SMARTLX, SMARTMX, STARPLUG, TOPFET, TRENCHMOS, UCODE, Freescale, the Freescale logo, AltiVec, CodeWarrior, ColdFire, ColdFire+, the Energy Efficient Solutions logo, Kinetis, Layerscape, MagniV, mobileGT, PEG, PowerQUICC, Processor Expert, QorIQ, QorIQ Qonverge, SafeAssure, the SafeAssure logo, StarCore, Symphony, VortiQa, Vybrid, Airfast, BeeKit, BeeStack, CoreNet, Flexis, MXC, Platform in a Package, QUICC Engine, Tower, TurboLink, EdgeScale, EdgeLock, eIQ, and Immersive3D are trademarks of NXP B.V. All other product or service names are the property of their respective owners. AMBA, Arm, Arm7, Arm7TDMI, Arm9, Arm11, Artisan, big.LITTLE, Cordio, CoreLink, CoreSight, Cortex, DesignStart, DynamIQ, Jazelle, Keil, Mali, Mbed, Mbed Enabled, NEON, POP, RealView, SecurCore, Socrates, Thumb, TrustZone, ULINK, ULINK2, ULINK-ME, ULINK-PLUS, ULINKpro, μVision, Versatile are trademarks or registered trademarks of Arm Limited (or its subsidiaries) in the US and/or elsewhere. The related technology may be protected by any or all of patents, copyrights, designs and trade secrets. All rights reserved. Oracle and Java are registered trademarks of Oracle and/or its affiliates. The Power Architecture and Power.org word marks and the Power and Power.org logos and related marks are trademarks and service marks licensed by Power.org.

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: June 2020
Document identifier: AN12901