|  |  |
| --- | --- |
| Document information | |
| Info | Content |
| Keywords | DCP |
| Abstract | <Abstract text> |

| Revision history | | |
| --- | --- | --- |
| Rev | Date | Description |
| <M.m> | <yyyymmdd> | <revision description (delete row if not required)> |
| <M.m> | <yyyymmdd> | <revision description, including important changes re. previous version; no author name(s); latest information in top row> |

# Introduction

i.MX RT10xx provides a data co-processor(DCP) block, which supports AES encryption and hashing functions. The AES block implements a 128-bit key/data encryption/decryption block. It is generally known that the key is a key point for encryption. The key should be used and protected reasonably to avoid to get by hacker. This application note explains how to use the AES block with different keys, and how to manage keys.

# Abbreviations

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

|  |  |
| --- | --- |
| **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 |

# AES keys of DCP

There are many keys provided to AES of DCP to use, see Figure 1. . One key needs to be selected for AES, before encryption/decryption.



1. AES Keys of DCP

## 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. The keys may be written via the programming interface by specifying a key index(to specify which key to load) and a subword pointer that indicates which word to write within the key. After a subword is written, 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. **The keys written into the key storage are not readable**.

## SNVS Master key

eFuse is the source of the SNVS Master key. The SNVS Master key is 256-bit and 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 IOMUXC\_GPR register are configured.

## SW\_GP2

SW\_GP2 is from eFuse which can remapped at OCOTP Bank5. After system reset, SW\_GP2 is copied to shadow registers automatically. User can burn and lock it. Once burned lock bits, SW\_GP2 cannot be read/written by software.

## Payload key

If PAYLOAD\_KEY bit of control register is set, it indicates the payload contains the key. the first entry in the payload is the key to be used for the operation.

## Summary

Note that when key selection changes for DCP, should do software reset of DCP via register to make the new key effective. The following table gives a summary for different keys.

|  |  |  |
| --- | --- | --- |
| Key | Access | Remark |
| SRAM-based key | W | The keys are stored in SRAM. User can set via registers, but not read them |
| SNVS Master key\* | None | Black key. It is from SNVS module. |
| SW\_GP2 | WR\*\* | it is from eFuse. |
| Payload key | RW | It is from payload. |

Note: W -- Writable, None -- cannot read and write, RW – readable and writable.

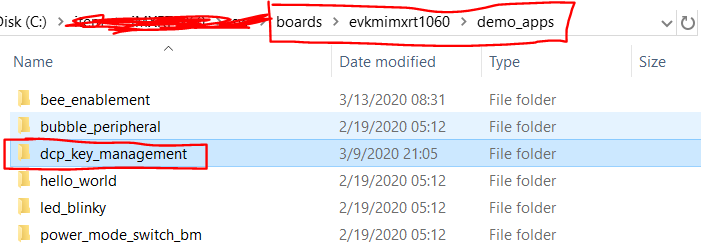
\*If device is in the Non-secure state, SNVS Master key is reset to all 0.

\*\*Once burned lock bits, SW\_GP2 cannot be read/written by software.

# Application example

The application example shows 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 can be downloaded on <https://mcuxpresso.nxp.com/>. Download the example code on xxx and then unzip it in the SDK project folder .\boards\evkmimxrt1060\demo\_apps. See Figure 2. .

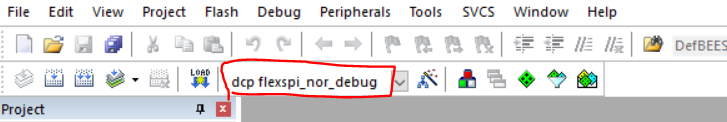


1. Example code folder

The example project can only be opened by MDK IDE.

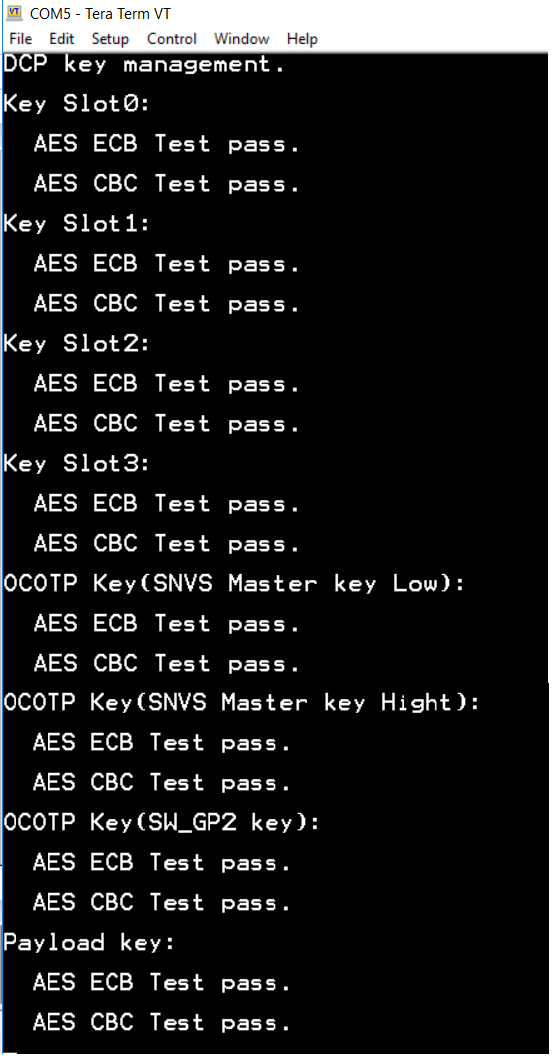
For running the example project, do it as following steps.

1. Connect a USB cable between the host PC and the OpenSDA 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, select “dcp\_flexspi\_nor\_debug” mode to compile and download.



1. “dcp\_flexspi\_nor\_debug” mode for project

Press the button SW9 on the board, serial terminal will show following text, see Figure 4. .



1. Printed information on terminal

# Conclusion

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

# reference

* [[i.MX RT1050 Processor Reference Manual](https://www.nxp.com/webapp/Download?colCode=IMXRT1050RM" \t "_blank)](https://www.nxp.com/webapp/Download?colCode=IMXRT1050RM)
* [Security Reference Manual for the i.MX RT1050 Processor](https://www.nxp.com/webapp/sps/download/mod_download.jsp?colCode=IMXRT1050SRM&appType=moderated" \t "_blank)

Legal information

Definitions

**Draft —**The document is a draft version only. The content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included herein and shall have no liability for the consequences of use of such information.

Disclaimers

**Limited warranty and liability —** Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors’ aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the *Terms and conditions of commercial sale* of NXP Semiconductors.

**Right to make changes —**NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

**Suitability for use —** NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer’s own risk.

**Applications —**Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer’s sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer’s applications and products planned, as well as for the planned application and use of customer’s third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer’s applications or products, or the application or use by customer’s third party customer(s). Customer is responsible for doing all necessary testing for the customer’s applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer’s third party customer(s). NXP does not accept any liability in this respect.

**Export control —**This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

**Translations —** A non-English (translated) version of a document is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Optional text for evaluation products; remove if not required.

**Evaluation products —**This product is provided on an “as is” and “with all faults” basis for evaluation purposes only. NXP Semiconductors, its affiliates and their suppliers expressly disclaim all warranties, whether express, implied or statutory, including but not limited to the implied warranties of non-infringement, merchantability and fitness for a particular purpose. The entire risk as to the quality, or arising out of the use or performance, of this product remains with customer.

In no event shall NXP Semiconductors, its affiliates or their suppliers be liable to customer for any special, indirect, consequential, punitive or incidental damages (including without limitation damages for loss of business, business interruption, loss of use, loss of data or information, and the like) arising out the use of or inability to use the product, whether or not based on tort (including negligence), strict liability, breach of contract, breach of warranty or any other theory, even if advised of the possibility of such damages.

Notwithstanding any damages that customer might incur for any reason whatsoever (including without limitation, all damages referenced above and all direct or general damages), the entire liability of NXP Semiconductors, its affiliates and their suppliers and customer’s exclusive remedy for all of the foregoing shall be limited to actual damages incurred by customer based on reasonable reliance up to the greater of the amount actually paid by customer for the product or five dollars (US$5.00). The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails of its essential purpose.

Licenses

| Purchase of NXP <xxx> components |
| --- |
| <License statement text> |

Patents

Notice is herewith given that the subject device uses one or more of the following patents and that each of these patents may have corresponding patents in other jurisdictions.

**<Patent ID> —** owned by <Company name>

Trademarks

Notice: All referenced brands, product names, service names and trademarks are property of their respective owners.

**<Name> —** is a trademark of NXP Semiconductors N.V.

# Index

D

Dummy index entry 3

# List of figures

**No table of figures entries found.**

# List of tables

**No table of figures entries found.**

# Contents

[1. Introduction 2](#_Toc252540480)

[1.1 Heading 2 2](#_Toc252540481)

[1.1.1 Heading 3 2](#_Toc252540482)

[1.1.1.1 Heading 4 2](#_Toc252540483)

[2. Legal information 2](#_Toc252540484)

[2.1 Definitions 2](#_Toc252540485)

[2.2 Disclaimers 2](#_Toc252540486)

[2.3 Licenses 2](#_Toc252540487)

[2.4 Patents 2](#_Toc252540488)

[2.5 Trademarks 2](#_Toc252540489)

[3. Index 2](#_Toc252540490)

[4. List of figures 2](#_Toc252540491)

[5. List of tables 2](#_Toc252540492)

[6. Contents 2](#_Toc252540493)