GigaDevice Semiconductor Inc.

Execution Environment of OSPI Flash of GD32H7 MCU User Guide

Application Notes

AN122

Version 1.0

(April 2023)

Table of Contents

List of Figures

List of Tables

1 Introduction

OSPI can be used to connect external memories, including single, dual, quad, and octal SPI memories. It can work in three modes: indirect mode, status polling mode, and memory-ma pped mode.

This document introduces ways of using OSPI, related tools and software, and precautions.

2 Hardware resources

2.1 OSPI

GD32H7xx MCU provides two OSPI interfaces at most, namely OSPI0 and OSPI1.

When OSPI is working in the indirect mode, OSPI register is used to perform all operations. In the status polling mode, MCU reads and detects the status register value of the external memory periodically.

In the memory-mapped mode, where the external memory is mapped to the address space of MCU (OSPI0 is mapped to 0x9000 0000, while OSPI1 is mapped to0x7000 0000.), MCU can access SPI memory just like accessing an internal memory.

2.2 Real-time decryption (RTDEC) module

GD32H7xx MCU provides two RTDECs at most, namely RTDEC0 and RTDEC1. Each RTDEC can be configured with four different independent encrypted areas. Each OSPI can correspond to one RTDEC. In the memory-mapped mode of OSPI, when reading OSPI Flash data, it can be decrypted in real time in AES-128 CTR mode.

3 Algorithm download through IDE

Gigadevice official package provides the algorithm for downloading data to OSPI Flash through keil and IAR. After the package is installed, users can download data to OSPI Flash through keil and IAR.

4 BootLoader support

The built-in Bootloader of GD32H7xx MCU is able to burn data to OSPI Flash. For details, please refer to ***Precautions for AN126 GD32H7xx BootLoader Operation.***

5. Boot from OSPI Flash

5.1. Supported modes of OSPI Flash

OSPI can operate in two modes, namely single data rate (SDR) and double transfer rate (DTR).

5.1.1 SDR mode

Single mode: SPI flash of GD series, like GD25Q127C, GD25Q16E, GD25Q32E, GD25Q64F, and GD25F64F can operate in such mode.

Quad mode: SPI flash of GD series, like GD25Q127C, GD25Q16E, GD25Q32E, GD25Q64F, and GD25F64F can operate in such mode.

Octal mode: OSPI flash of GD series, like GD25X and GD25LX, can operate in such mode.

5.1.2 DTR mode

Octal mode: OSPI flash of GD series, like GD25X and GD25LX, can operate in such mode.

5.2. OSPI boot configuration

5.2.1. OSPI boot mode selection

GD32 MCU provides different boot sources which can be selected through the level of BOOT pin and BOOT_ADDR0/1[15:0] of FMC_BTADDR_MDF register. For details, please see ***Table 5-1. Boot mode*** selection and ***Table*** 5-2. . The level of BOOT pin will be latched at the rising edge of the fourth reset CK_SYS (system clock). Users can select the boot source by setting the level of BOOT pin after power-on and system resetting. Once the level of the pin is sampled, it can be released for other purposes.

When the level of the BOOT pin is confirmed and OSPI boots, it is required to configure BOOT_ADDRx[15:0] as 0x7000 or 0x9000.

Table 5-1. Boot mode selection

Boot source address	Pin selection for boot mode
	BOOT
MSB of the boot address: defined by BOOT_ADDR0[15:0] LSB of the boot address: 0x0000	0
MSB of the boot address: defined by BOOT_ADDR1[15:0] LSB of the boot address: 0x0000	1

Table 5-2. Details of Boot mode

SCR	SPC[7:0]	BOOT_ADDRESS (configured at BOOT_ADDRx(x = 0,1))	BOOT_MODE	Boot address
1	x	XXXX	SECURITY BOOT	ROM
0	Protection level high	0x9000_0000	USER BOOT	OSPI0
		0x7000_0000	USER BOOT	OSPI1
		0x0800_0000~max user flash	USER BOOT	BOOT_ADDRESS
		Other addresses	USER BOOT	0x0800_0000
	No protection / Protection level low	0x9000_0000	USER BOOT	OSPI0
		0x7000_0000	USER BOOT	OSPI1
		0x2408_000 max RAM shared (ITCM/DTCM/AXI)	SRAM BOOT (RAM shared)	BOOT_ADDRESS
		0x2400_0000~ max AXI SRAM	SRAM BOOT (AXI SRAM)	BOOT_ADDRESS
		0x2000_0000	SRAM BOOT (DTCM)	0x2000_0000
		0x0800_0000~max user flash	USER BOOT	BOOT_ADDRESS
		0x0000_0000	SRAM BOOT (ITCM)	0x0000_0000
		0x1FF0_0000	SYSTEM BOOT	BootLoader
		Other	USER BOOT	0X0800_0000 (BOOT Pin = 0)
			SYSTEM BOOT	BootLoader (BOOT Pin = 1)

5.2.2. GPIO mapping when OSPI boots

OSPI Flash GPIO used when OSPI boots is as shown in ***Table 5-3. OSPI GPIO*** pins and other pins are not supported for the time being.

Table 5-3. OSPI GPIO pins

OSPI0	GPIO pins	OSPI1	GPIO
OSPI0_IO0	PD11	OSPI1_IO0	PF0
OSPI0_IO1	PD12	OSPI1_IO1	PF1
OSPI0_IO2	PA3	OSPI1_IO2	PF2

OSPI0	GPIO pins	OSPI1	GPIO
OSPI0_IO3	PD13	OSPI1_IO3	PF3
OSPI0_IO4	PD4	OSPI1_IO4	PG0
OSPI0_IO5	PD5	OSPI1_IO5	PG1
OSPI0_IO6	PD6	OSPI1_IO6	PG10
OSPI0_IO7	PD7	OSPI1_IO7	PG11
OSPI0_CLK	PB2	OSPI1_CLK	PF4
OSPI0_NCS	PB6	OSPI1_NCS	PG12

5.2.3. OSPI boot parameters

When OSPI Flash boots, related parameters can be read from OSPI.

1. Selection of OSPI communication mode: single, dual, quad, or octal OSPI;
2. Communication rate;
3. STR or DTR mode used by OSPI;
4. Configuration of RTDEC corresponding to OSPI;
5. Whether cache is enabled;
6. Configuration of option bytes.

5.3. Security support in OSPI boot mode

For data security, when OSPI boots, files in OSPI Flash are protected and MCU can be bound with OSPI Flash.

5.3.1. Protection of files in OSPI Flash

Documents in OSPI Flash consist of system area and data area. The original user files are generated with software supported by Gigadevice.

System area

System area is a 4K byte space and programmed in the first sector of OSPI flash memory. The area is always encrypted in two modes, namely public mode and user mode.

- Public mode: OSPI boot system area is encrypted by using AES-256 method in such mode. Gigadevice own encryption mode and key are adopted for access by all users.
- User mode: OSPI boot system files are encrypted by using AES-128 method in such mode. KEY/IV is defined by users. KEY is set in EFUSE_AES_KEYX. IV is set in FMC_AESIVX_MDF.

Data area

Data area is a free space which can be encrypted or not at the user's discretion. It is a combination of some encrypted areas and non-encrypted areas.

A RTDEC module corresponding to each OSPI is used to encrypt data in up to four areas, and KEY and IV defined by users can be used in each area.

5.3.2. Binding of OSPI Flash with MCU

GD32H7xx MCU is allowed to be bound with OSPI Flash to avoid the user' products from being plagiarized and programs from being tampered with. If this function is enabled, MCU will be automatically bound at first boot. Subsequently, MCU ID will be identified at each boot and the function will not work if it doesn't match. Therefore, even for the same type of products, OSPI Flash can't work in any other products and encrypted area can't be tampered with. To replace MCU but keep using the chip where OSPI Flash is installed, users need to initialize files in OSPI Flash.

6. Introduction to GD32H7xx LFIx

Resources related to LFIx (Licensed Firmware Install X) are used to help install OSPI Flash firmware of GD32H7xx series in public encryption mode and user encryption mode. In either mode, except for areas designated by users, data in OSPI Flash are always encrypted.

Public encryption mode is concise and efficient, where Gigadevice own encryption mode and key are adopted for access by all users.

Under the support of HSM (Hardware Secure Module), passwords and parameters defined by users are used for encryption throughout the process in the user encryption mode.

To support development and massive production of users, Gigadevice has prepared related tools for online and offline massive production. For detailed software operation, please refer to ***User Manual of AN133_GD32H7 MCU Security Firmware Generator.***

6.1. File structure in OSPI Flash

OSPI Flash is divided into system area and data area. Data area is divided into nine optional user areas in sizes defined by users in compliance with matching requirements as shown in ***Table 6-1. File structure in OSPI*** Flash.

Table 6-1. File structure in OSPI Flash

S/N	Name	Description
0	System area	4 KB, fixed to 0x90000000 (OSPI0) or 0x70000000 (OSPI1)
1	User area 1	Optional, non-encrypted data area
2	User area 2	Optional, encrypted data area Encrypted based on AES-128 CTR mode and decrypted by sector y in RTDECx in real time
3	User area 3	Optional, non-encrypted data area
4	User area 4	Optional, encrypted data area Encrypted based on AES-128 CTR mode and decrypted by sector y in RTDECx in real time
5	User area 5	Optional, non-encrypted data area
6	User area 6	Optional, encrypted data area Encrypted based on AES-128 CTR mode and decrypted by sector y in RTDECx in real time
7	User area 7	Optional, non-encrypted data area
8	User area 8	Optional, encrypted data area Encrypted based on AES-128 CTR mode and decrypted by sector y in RTDECx in real time
9	User area 9	Optional, non-encrypted data area

6.2. Public encryption mode

In public encryption mode, all products that use GD32H7xx are of Gigadevice's private encryption solutions. By using Gigadevice's private encryption solutions, encryption is made based on AES 256/128, user programs and data use separate encryption parameters according to different phrases of LFIx and encrypted after adding salt, and significant parameters are encrypted in multiple layers for secure rapid development and low-cost production.

6.2.1. Program file structure in public encryption mode

In public encryption mode, file structure is as shown in ***Table 6-2 Program file structure in public encryption*** mode.

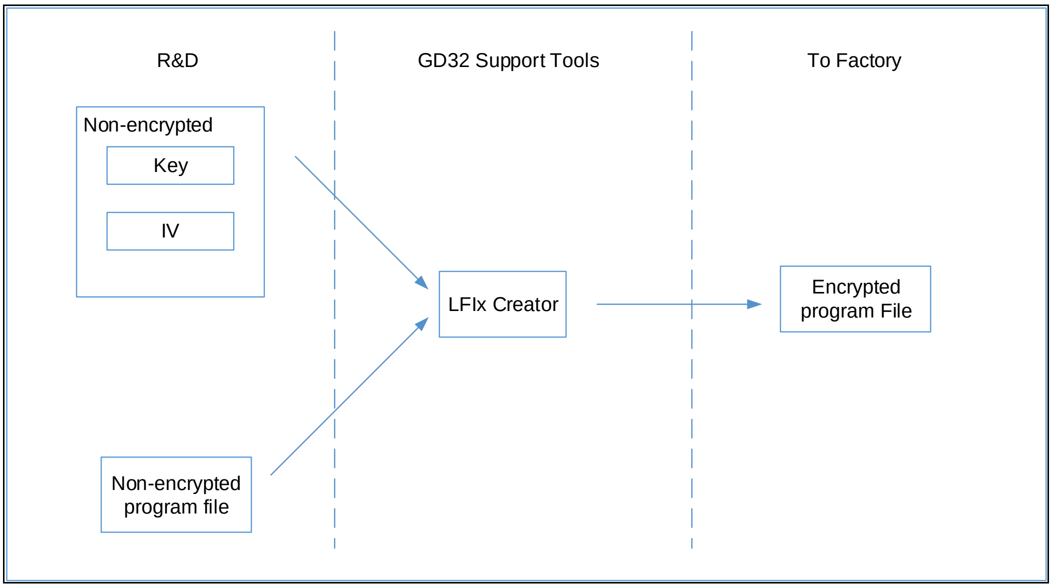
Table 6-2 Program file structure in public encryption mode

S/N	Name	R&D data	To factory data
0	System area	4KB	Gigadevice's private encryption solutions based on AES 256
1	User area 1	Optional, non-encrypted data area	Unprocessed
2	User area 2	Optional, encrypted data area	Unprocessed
3	User area 3	Optional, non-encrypted data area	Unprocessed
4	User area 4	Optional, encrypted data area	Unprocessed
5	User area 5	Optional, non-encrypted data area	Unprocessed
6	User area 6	Optional, encrypted data area	Unprocessed
7	User area 7	Optional, non-encrypted data area	Unprocessed
8	User area 8	Optional, encrypted data area	Unprocessed
9	User area 9	Optional, non-encrypted data area	Unprocessed

6.2.2. Preparation of massive production resources in public encryption mode

All products that use GD32H7xx use the same encryption solutions and Gigadevice-supported tools as shown in ***Figure 6-1. Structure in public encryption mode***.

Figure 6-1. Structure in public encryption mode



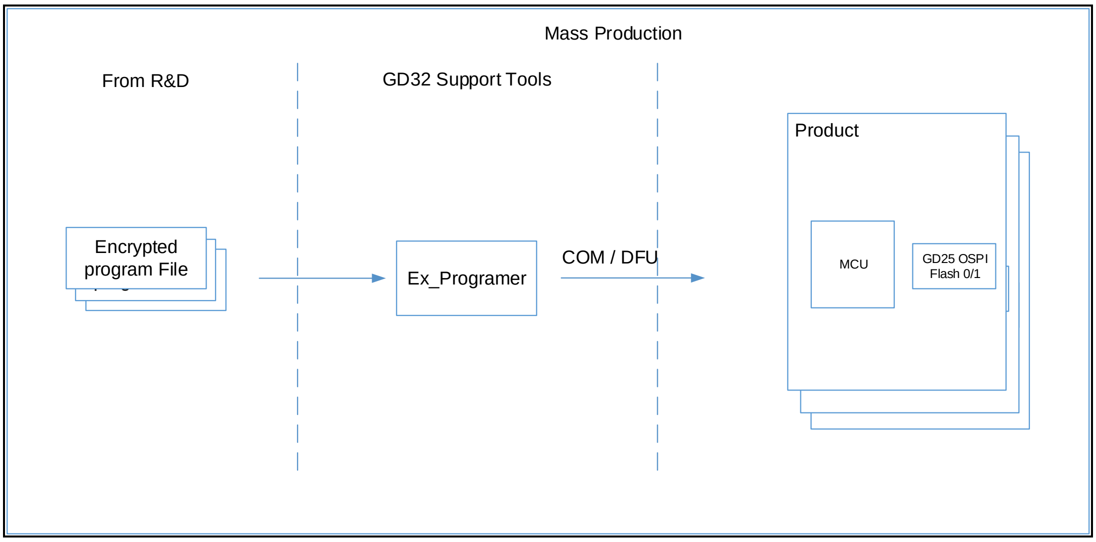
6.2.3. Support to massive production

To support development and massive production of users, related tools are prepared for online and offline massive production.

Online massive production

In public encryption mode, online massive production is as shown in ***Figure 6-2. Structure of online massive production in public encryption*** mode.

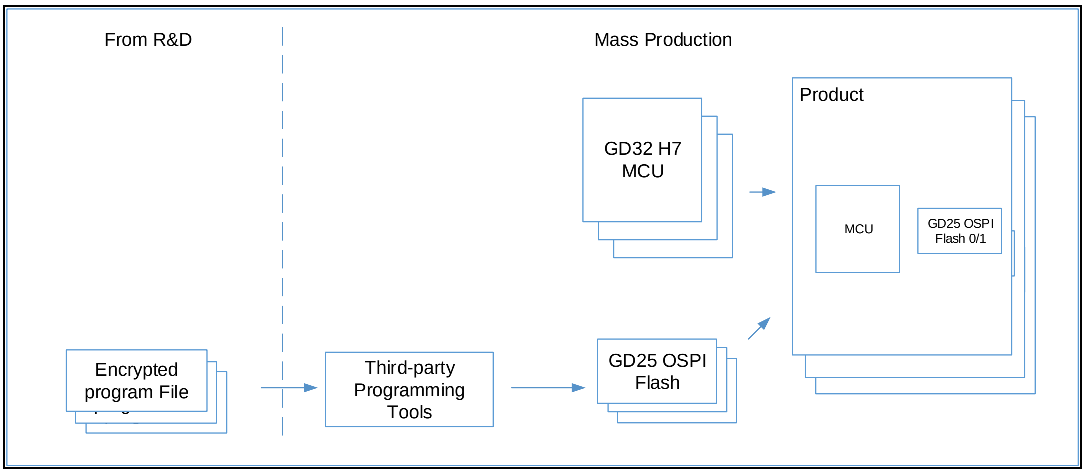
Figure 6-2. Structure of online massive production in public encryption mode



Offline massive production

In public encryption mode, offline massive production is as shown in ***Figure 6-3. Structure of offline massive production in public encryption mode***.

Figure 6-3. Structure of offline massive production in public encryption mode



6.3. User encryption mode

In this mode, all information can only be viewed after related protocols are signed. Please contact Gigadevice.

6.3.1. Program file structure in user encryption mode

In user encryption mode, document structure is as shown in ***Table 6-3 Program file structure in user encryption mode***.

Table 6-3 Program file structure in user encryption mode

S/N	Name	R&D data	To factory data
0	System area	4KB	Keys defined by users are used for encryption and programmed into Efuse of target MCU.
1	User area 1	Optional, non-encrypted data area	Unprocessed
2	User area 2	Optional, encrypted data area	Unprocessed
3	User area 3	Optional, non-encrypted data area	Unprocessed
4	User area 4	Optional, encrypted data area	Unprocessed
5	User area 5	Optional, non-encrypted data area	Unprocessed
6	User area 6	Optional, encrypted data area	Unprocessed
7	User area 7	Optional, non-encrypted data area	Unprocessed
8	User area 8	Optional, encrypted data area	Unprocessed
9	User area 9	Optional, non-encrypted data area	Unprocessed

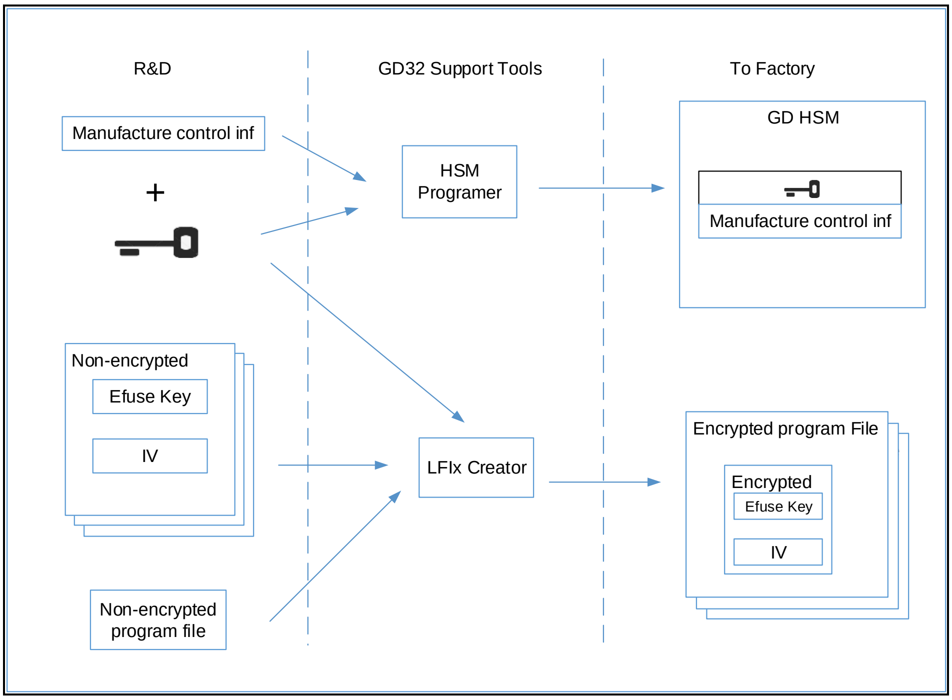
6.3.2. Preparation of massive production resources in user encryption mode

All products that use GD32H7xx use encryption solutions defined by users and HSM and LFIx Creater. In the user encryption mode, each product can use individual encryption parameter and be encrypted based on product type. Production number of products can also be controlled.

Independent encryption

In independent encryption mode, users can use different encryption parameters for each product ID as shown in ***Figure 6-4. Structure in independent encryption mode***.

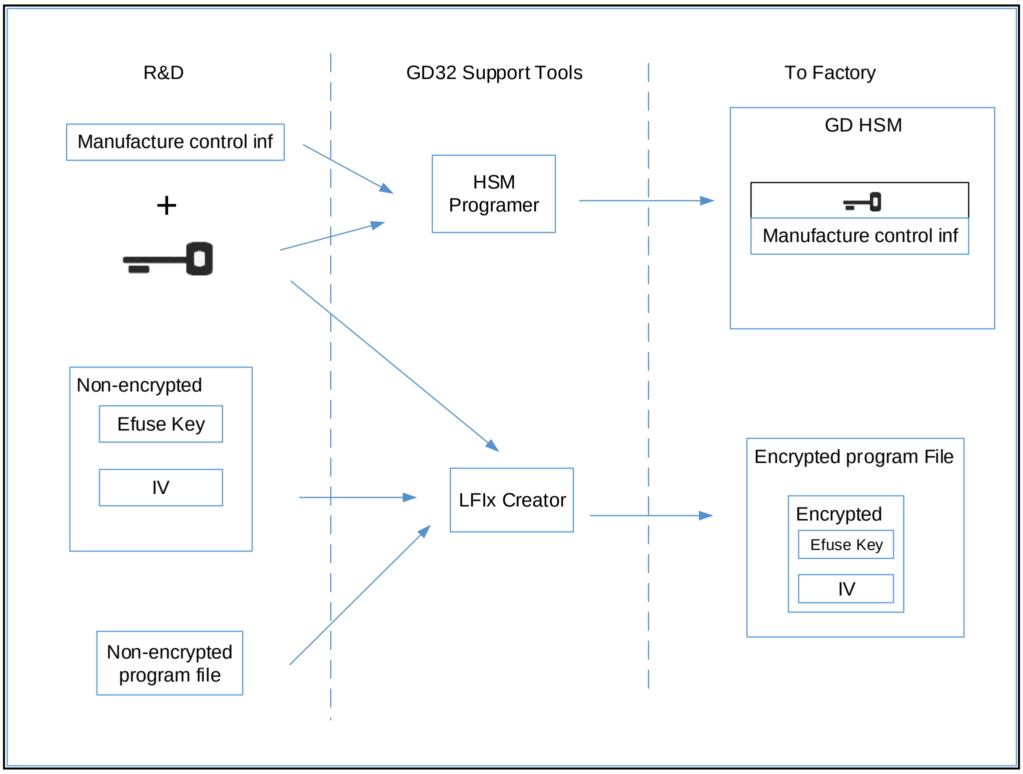
Figure 6-4. Structure in independent encryption mode



Encryption based on product type

In the encryption mode, users can use the same encryption parameters for each product type as shown in *Figure 6-5. Structure in the encryption mode based on product* type.

Figure 6-5. Structure in the encryption mode based on product type

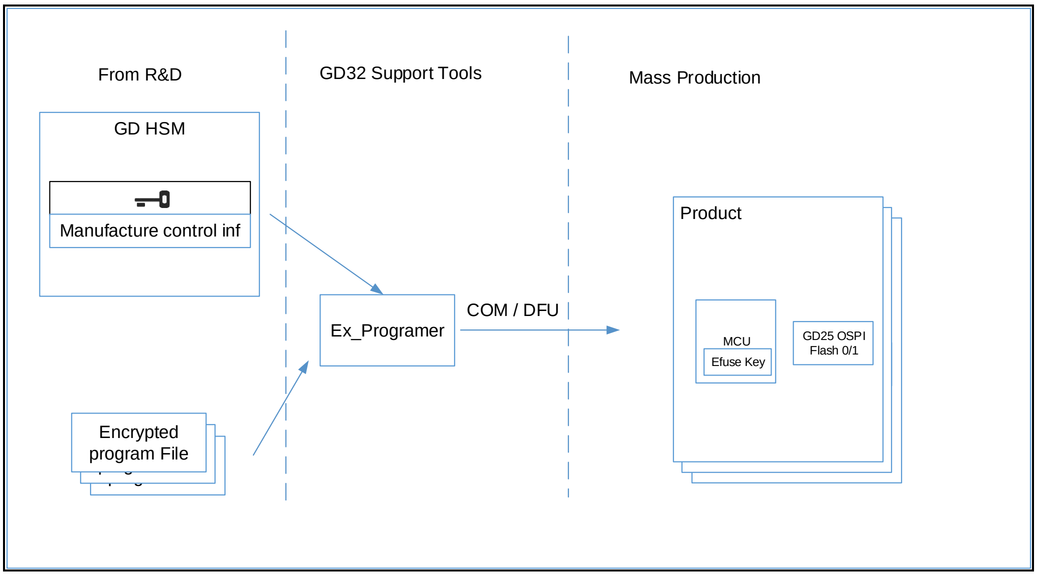


6.3.3. Support to massive production

Online massive production

In user encryption mode, online massive production is as shown in ***Figure 6-6. Structure of online massive production in user encryption mode***.

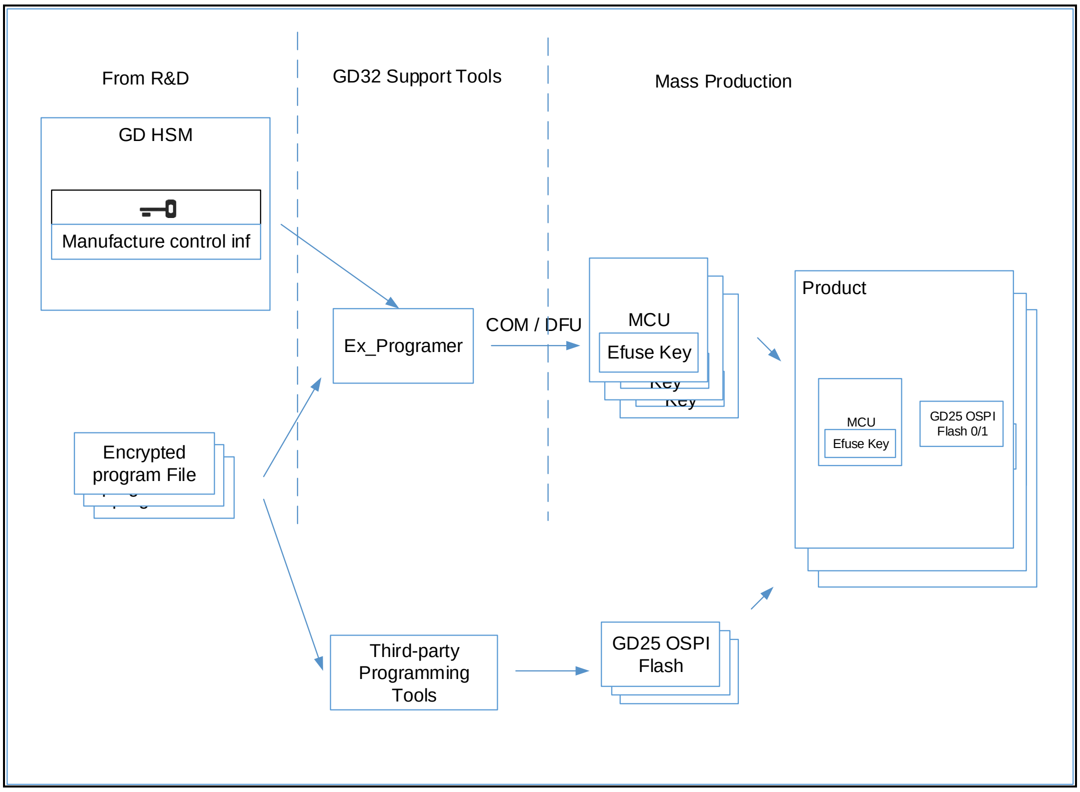
Figure 6-6. Structure of online massive production in user encryption mode



Offline massive production

In user encryption mode, offline massive production is as shown in ***Figure 6-7. Structure of offline massive production in user encryption mode***. After burning and writing, one-to-one match should be guaranteed between MCU and Flash.

Figure 6-7. Structure of offline massive production in user encryption mode



7. Revision history

Table 7-1. Revision history

Revision No.	Description	Date
1.0	Initial release	Apr.20, 2023

Important Notice

This document is the property of GigaDevice Semiconductor Inc. and its subsidiaries (the "Company"). This document, including any product of the Company described in this document (the “Product”), is owned by the Company under the intellectual property laws and treaties of the People’s Republic of China and other jurisdictions worldwide. The Company reserves all rights under such laws and treaties and does not grant any license under its patents, copyrights, trademarks, or other intellectual property rights. The names and brands of third party referred thereto (if any) are the property of their respective owner and referred to for identification purposes only.

The Company makes no warranty of any kind, express or implied, with regard to this document or any Product, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The Company does not assume any liability arising out of the application or use of any Product described in this document. Any information provided in this document is provided only for reference purposes. It is the responsibility of the user of this document to properly design, program, and test the functionality and safety of any application made of this information and any resulting product. Except for customized products which have been expressly identified in the applicable agreement, the Products are designed, developed, and/or manufactured for ordinary business, industrial, personal, and/or household applications only. The Products are not designed, intended, or authorized for use as components in systems designed or intended for the operation of weapons, weapons systems, nuclear installations, atomic energy control instruments, combustion control instruments, airplane or spaceship instruments, transportation instruments, traffic signal instruments, life-support devices or systems, other medical devices or systems (including resuscitation equipment and surgical implants), pollution control or hazardous substances management, or other uses where the failure of the device or Product could cause personal injury, death, property or environmental damage ("Unintended Uses"). Customers shall take any and all actions to ensure using and selling the Products in accordance with the applicable laws and regulations. The Company is not liable, in whole or in part, and customers shall and hereby do release the Company as well as its suppliers and/or distributors from any claim, damage, or other liability arising from or related to all Unintended Uses of the Products. Customers shall indemnify and hold the Company as well as its suppliers and/or distributors harmless from and against all claims, costs, damages, and other liabilities, including claims for personal injury or death, arising from or related to any Unintended Uses of the Products.

Information in this document is provided solely in connection with the Products. The Company reserves the right to make changes, corrections, modifications or improvements to this document and Products and services described herein at any time, without notice.