

Gigadevice Semiconductor Inc.

**GD32H7 series MCU Licensed Firmware
Install (LFI) overview**

Application Note

AN118

Revision 1.0

(Sep. 2023)

Table of Contents

Table of Contents	2
List of Figures	3
List of Tables	4
1. Introduction.....	5
2. Hardware resources	7
3. Software resources	8
3.1. GD licensed Data Creator.....	8
3.2. GD licensed Data Programmer	8
4. Licensed firmware installation flow	10
4.1. OEM's Licensed firmware preparing flow	10
4.2. Contract manufacturer flow	10
5. Revision history.....	11

List of Figures

Figure 1- 1 GD LFI process diagram.	5
Figure 3- 1 GD licensed Data Creator	8
Figure 3- 2 GD licensed Data Creator	9

List of Tables

Table 5-1 Revision history	11
----------------------------------	----

1. Introduction

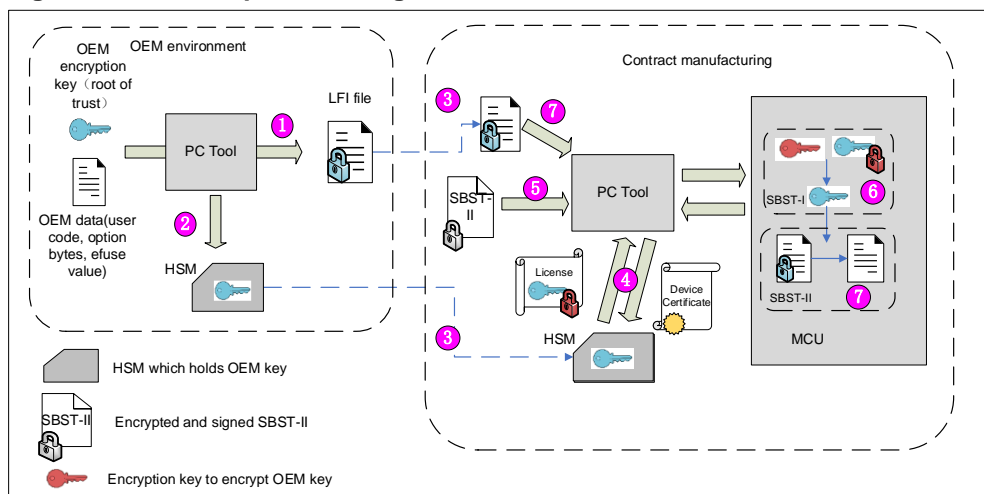
Outsourcing of product manufacturer enables original equipment manufacturer (OEM) to reduce their direct costs and concentrate on high added-value activities, such as research and development, sales and marketing. However, contract manufacturer puts the OEM's proprietary assets at risk, and since the contract manufacturer (CM) manipulates the OEM's intellectual property (IP), it might be disclosed to other customers, or appropriated. To meet the new market security requests and protect customers against any leakage of their IPs, GigaDevice introduces a new security concept, Licensed Firmware Install (LFI), permitting programming of OEM firmware into GD32 MCU internal Flash memory in a secure way (with confidentiality, authentication and integrity checks). GD32 H7 Series devices support protection mechanisms that permit the protection of critical operations (such as cryptography algorithms) and critical data (such as secret keys) against unexpected access.

To meet the requirement of property security, GigaDevice introduces the concept, secure firmware install (LFI), allowing the contract manufacturer to install the firmware in a secure way. LFI guarantees the integrity, reliability and confidentiality of OEM firmware when installing in untrusted environment. Installing number can be limited, due to total production control, On the other hand, USB and USART are supported.

In this document, the USART protocol is used as an example to briefly describe the LFI process. For details, please see the [AN131 GD32H7 series MCU Licensed Firmware Install \(LFI\) user guide](#), which can be obtained from GigaDevice.

The overall LFI process requires the participation of OEM and contract manufacturer. With the help of relevant software provided by GigaDevice, OEM generate encrypted LFI files, configure HSM at the same time, and send them to the contract manufacturer for production. The detailed LFI process is as follows [Figure 1- 1 GD LFI process diagram](#).

Figure 1- 1 GD LFI process diagram.



The OEM is mainly responsible for:

1. Encrypt OEM firmware with OEM key

2. Use the tool software provided by Gigadevice to store the OEM key, maximum production quantity, in the HSM(Hardware security module) special equipment
3. Send LFI file, HSM to to contract manufacturer

The contract manufacturer is mainly responsible for:

1. Obtain LFI files and HSM
2. Using the related software provided by gig device, encrypt the OEM key using the negotiated Key Encryption Key (KEK), and then send the license holding the encrypted OEM key.The PC writes the license and SBSTII into the microcontroller, and then reset the microcontroller
3. Use the relevant software provided by Gigadevice to retrieve the OEM key with KEK
4. Retrieve OEM firmware using OEM key, then program firmware data

To meet the security requirements, the encrypted OEM firmware is decrypted inside GD MCU. And so the OEM key transfer is a key point. SBSTI, accompanied with an HSM, is developed to securely transfer OEM key into MCU The GD32 Secure boot Loader is divided into two parts, Secure Boot Loader Stage 1 (SBSTI) and Secure Boot Loader Stage 2 (SBSTII).that guarantees integrity, reliability and confidentiality when downloading OEM firmware in untrusted environments.

SBSTI main function is as follow:

1. Verify license containing the OEM key and negotiate a KEK.
2. Retrieve OEM key.
3. Verify and install SBSTII code. And then jump to run SBSTII.

SBSTII was developed by Gigadevice to enable secure firmware installation. It is responsible for receiving LFI files from the PC, decrypting LFI files, and installing OEM firmware and configuration data. Supports different interfaces, such as USART and USB.

2. Hardware resources

LFI allows OEM firmware code and configuration data to be delivered and programmed as encrypted files, which are then decrypted and installed inside the MCU when safe, reducing the risk of firmware leaks. LFI is a complete set of security mechanisms composed of related hardware and software resources that allows secure and counted installation of OEM firmware in untrusted production environments such as OEM contract manufacturer.

The LFI process requires OEM and contract manufacturer to prepare the appropriate hardware resources and complete the process with the HSM provided by GigaDevice. The hardware of each part is described as follows.

A hardware security module (HSM) is in charge of:

1. Securely storing OEM AES secret key
2. Checking GD32 device certificate that is used to authenticate GD32 device.
3. Generating and providing the license to the secure bootloader to securely install the encrypted firmware on GD32 device.
4. Counting number of produced GD32 devices.

GigaDevice offers an HSM solution that uses an HSM to hold an OEM key along with a GD32 MCU to generate a license. With GD32 MCU as the core, HSM realizes the functions of OEM key security storage, certificate management, hardware encryption and decryption acceleration, production quantity control and so on. For more details about HSM, please refer to [AN116 GD32 MCU Hardware security module\(HSM\) overview](#).

OEM Hardware:

1. Prepare the GigaDevice HSM.
2. Prepare the host computer and other related tools to encrypt files.
3. Connect the HSM to the host computer and install the driver correctly.

Contract manufacturer Hardware:

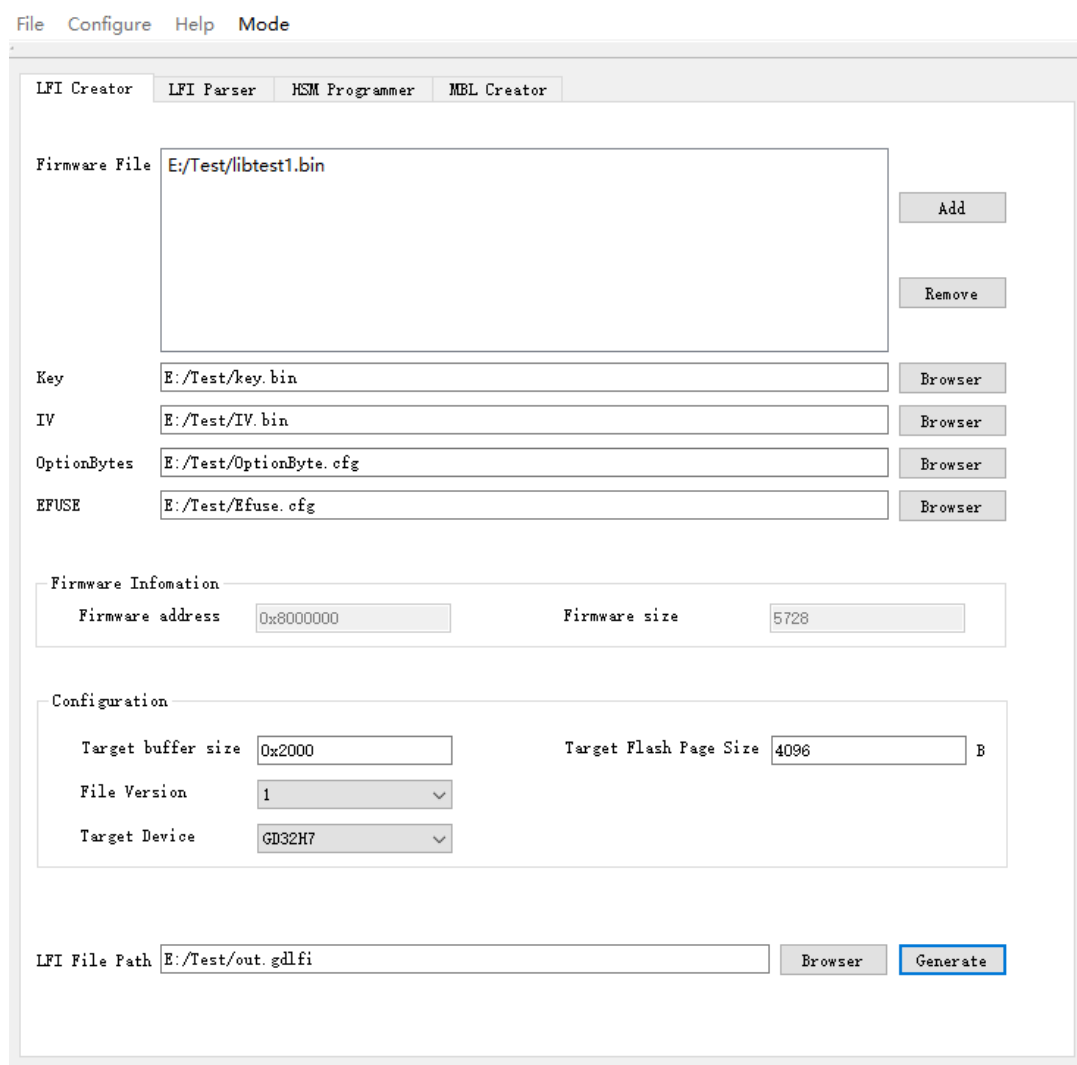
1. Obtain the GigaDevice HSM.
2. GD32H7 MCU download platform, which offers one-click download function.
3. Connect GD32H7 MCU download platform with host computer by USB/USART.
4. Connect the HSM to the host.

3. Software resources

3.1. GD licensed Data Creator

The LFI format is an encrypted format created by GigaDevice. It can generate an authorized firmware installation flow by GD licensed Data Creator. in [Figure 3- 1 GD licensed Data Creator.](#)

Figure 3- 1 GD licensed Data Creator

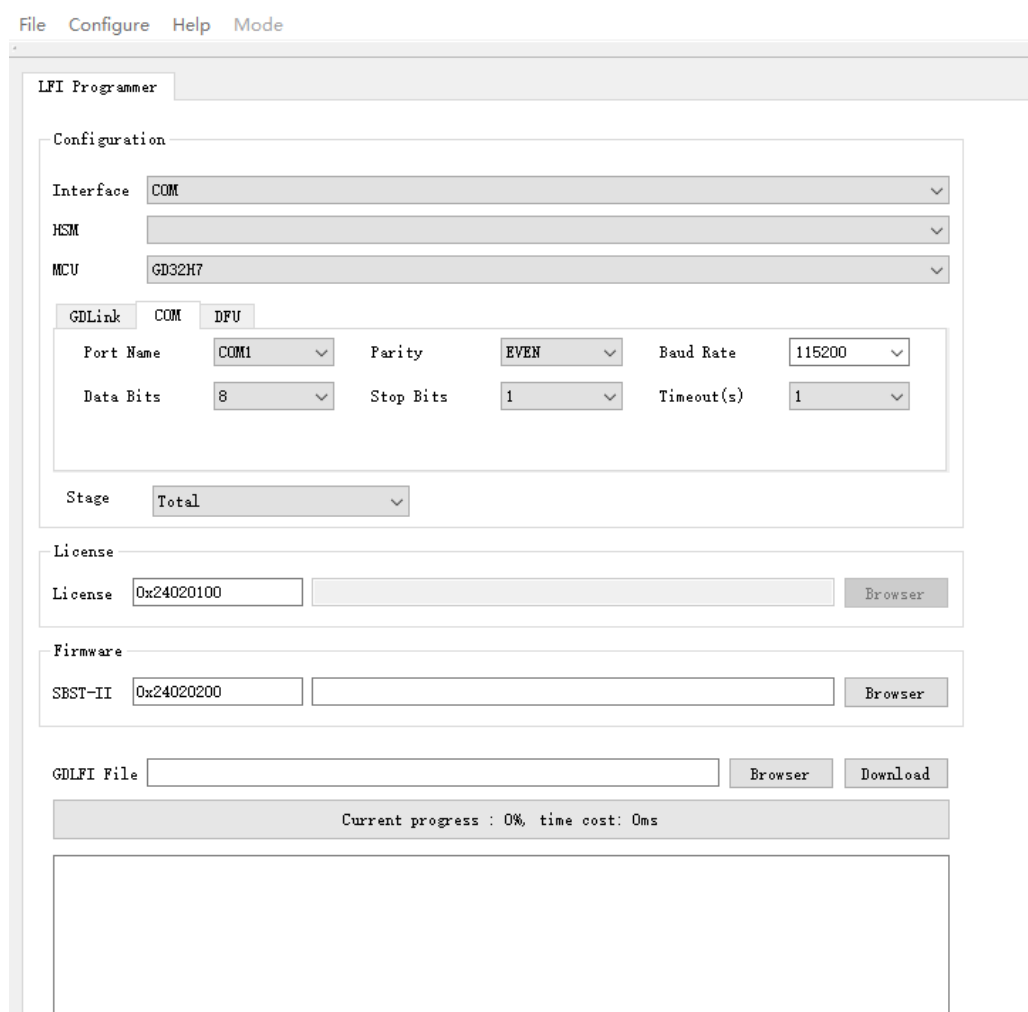


3.2. GD licensed Data Programmer

GD licensed Data Programmer was used to connect the HSM to the host computer through USART port or USB port. Select the LFI file generated by GD licensed Data Creator in GD

licensed Data Programmer such as [Figure 3-2 GD licensed Data Programmer](#).

Figure 3- 2 GD licensed Data Programmer



After the relevant hardware is properly connected and the relevant software is configured, GigaDevice also provides a one-click download function. And the process is as follows:

1. Configuring GDM32H7 to boot from bootloader.
2. Getting certificate using bootloader command.
3. Generating license by HSM.
4. Downloading license and encrypted SBSTII bin file to target MCU sram. The target address is listed below.
5. For GDM32H7: Setting SCR bit in option byte or efuse.
6. Target MCU reset.
7. Connecting to SBSTII. BSS stage will not involve any data transfer. So, tools will directly connect to SBSTII when BSS stage is finished.
8. LFI file transfer. Downloading tools transfer LFI file sections in sequence, by implementing the protocol in using USART or USB
9. Finishing all section data transfer. Then MCU will automatically reset.

4. Licensed file installation flow

There are two main aspects of licensed firmware installation, the first is the OEM development of encrypted LFI firmware, where the LFI format is an encrypted format created by GigaDevice. The OEM encrypts the original LFI through GD licensed Data Creator, at the same time, HSM is generated by HSM programmer in GD licensed Data Creator and then will authorize the encrypted LFI firmware to contract manufacturer, followed by the OEM to obtain the authorized LFI firmware and HSM and other related tools generation and installation license, the OEM can complete the encryption of published files and the control of production quantity.

4.1. OEM's Licensed firmware preparing flow

1. OEM develops its own OEM firmware(bin files).
2. Preparing LFI file using GD licensed Data Creator.
3. Configure the HSM. The HSM contains information about the maximum production quantity control and LFI file license generation.
4. Delivering LFI file and HSM to contract manufacturer.

4.2. Contract manufacturer working flow

Contract manufacturer flow is as follows:

1. Receive the files and matching HSM, and install the GD licensed Data Programmer.
2. Prepare a suitable download platform and connect USART or USB, that means Contract manufacturer should reserve communication interfaces related to LFI.
3. The HSM is inserted into the PC. The GD licensed Data Programmer identifies the HSM successfully and specifies the file to be downloaded.
4. Press the Download button repeatedly and wait for a success message to replace the chip. The counter in the HSM will automatically subtract one.

5. Revision history

Table 5-1 Revision history

Revision No.	Description	Date
1.0	Initial Release	Sep 18, 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 has 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.