

**GigaDevice Semiconductor Inc.**

**GD32H7 系列预授权固件安装概述**

**应用笔记**

**AN118**

1.0 版本

(2023 年 9 月)

## 目录

目录.....	2
图索引.....	3
表索引.....	4
1. 前言.....	5
2. 硬件资源.....	7
3. 软件资源.....	8
3.1. GD licensed Data Creator.....	8
3.2. GD licensed Data Programmer.....	9
4. 授权固件安装流程.....	10
4.1. OEM 工作流程.....	10
4.2. 代工制造商工作流程.....	10
5. 版本历史.....	11

## 图索引

图 1-1 GD LFI 流程示意图.....	5
图 3-1 GD licensed Data Creator .....	8
图 3-2 GD licensed Data Programmer .....	9

## 表索引

表 5-1 版本历史 .....	11
------------------	----

## 1. 前言

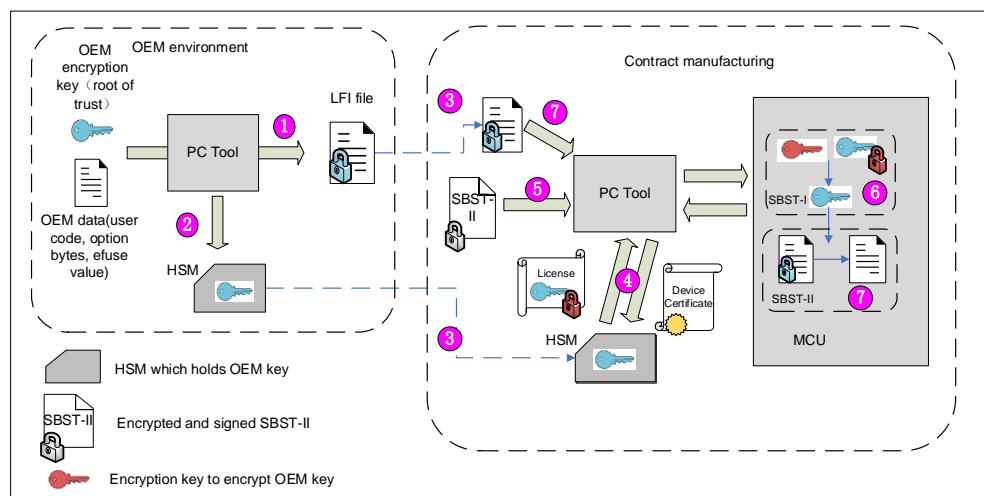
产品制造外包使原始设备制造商（OEM）能够降低直接成本，并专注于高附加值的活动，如研发、销售和营销。然而，代工制造商将 OEM 的专有资产置于风险之中，并且由于代工制造商（CM）可能会向其他客户披露 OEM 知识产权，或导致 OEM 知识产权被挪用。为了满足新的市场安全要求并保护客户免受任何 IP 泄漏风险，Gigadevice 引入了一个新的安全概念：预授权固件安装（LFI），预授权固件安装（LFI）允许 OEM 固件以安全的方式编程到 GD32 MCU 内部闪存(具有机密性，身份验证和完整性检查)。GD32 系列设备支持保护机制，可以保护关键操作（如加密算法）和关键数据（如密钥）免受意外访问。

Gigadevice 的预授权固件安装（Licensed firmware install, LFI）的概念，允许代工制造商以安全的方式安装固件。当固件在非可信环境中安装时，LFI 保证 OEM 固件的完整性、可靠性和保密性。LFI 提供了生产总量控制，并且支持 USB 和 USART 通讯协议。

在本文档中，以 USART 协议为例，简要介绍 LFI 流程，如果需要了解详细信息，请参考 [AN131 GD32H7 系列预授权固件安装用户手册](#)，此文档需要联系 Gigadevice 获得。

LFI 整体流程需要 OEM 以及代工制造商参与，借助于 Gigadevice 提供的相关软件，OEM 生成加密的 LFI 文件，同时配置 HSM，交给代工制造商用于生产，LFI 详细流程如下 [图 1-1 GD LFI 流程示意图](#)。

图 1-1 GD LFI 流程示意图



其中 OEM 主要负责：

1. 用 OEM 密钥加密 OEM 文件；
2. 使用 Gigadevice 提供的工具软件将 OEM 密钥，最大生产数量，存储到 HSM(硬件安全模块)专用设备中；
3. 发送 LFI 文件，HSM 给代工制造商；

代工制造商主要负责：

1. 获取 LFI 文件以及 HSM；
2. 借助于 Gigadevice 提供的相关软件，使用协商的密钥加密密钥（KEK）加密 OEM 密钥，然后发送持有加密的 OEM 密钥的许可证。PC 机将许可证和 SBSTII 写入单片机，然后复

位单片机；

3. 使用 GigaDevice 提供的相关软件，用 KEK 检索 OEM 密钥；
4. 使用 OEM 密钥检索 OEM 固件，然后编程固件数据。

另外，为满足安全要求，代工制造商需要对加密的 OEM 固件进行解密。因此 OEM 密钥转移是一个关键点，SBSTI/SBSTII 用于安全地将 OEM 密钥传输到 MCU 中。代工制造场景下的 SBSTI（引导加载程序阶段 1）/SBSTII（引导加载程序阶段 2）为 GD32 安全引导加载程序，它保证了在非可信环境下下载 OEM 固件时的完整性、可靠性以及整个生产过程中数据的保密性。

SBSTI 主要功能如下：

1. 验证包含 OEM 密钥的许可证并协商 KEK；
2. 检索 OEM 密钥；
3. 验证 SBSTII 代码。然后跳转到运行 SBSTII；

其次，SBSTII 主要功能为从 PC 接收 LFI 文件，解密出 OEM 固件和配置数据并安装在指定区域。SBSTII 支持不同接口，如 USART、DFU 等。

## 2. 硬件资源

LFI 允许 OEM 固件代码和配置数据以加密文件的形式交付和编程，然后在安全时在 MCU 内部解密并安装，从而降低固件泄露的风险。LFI 是一种由有关软硬件资源组成的一套完整的安全机制，允许在非可信的生产环境（如 OEM 代工制造商）中安全且计数地安装 OEM 固件。

LFI 流程要求 OEM 以及代工制造商准备合适的硬件资源，同时配合 GigaDevice 提供的 HSM 完成该流程。关于各部分的硬件的介绍如下：

### 硬件安全模块(HSM)负责：

1. 安全存储 OEM AES 密钥；
2. GD32 设备证书验签，用于对 GD32 设备安装进行授权，生成并提供许可证给安全引导程序，以便在 GD32 设备上安全地安装加密固件；
3. 控制 GD32 设备的生产数量；

其中 GigaDevice 提供的 HSM 解决方案，使用 HSM 与 GD32 MCU 一起持有 OEM 密钥以生成许可证。HSM 以 GD32 单片机为核心，实现了 OEM 密钥的安全存储、证书管理、硬件加解密加速、生产数量控制等功能。关于 HSM 的更多细节请参考 [AN116 GD32 MCU 硬件安全模块概览](#)；

### OEM 硬件：

1. 准备 GigaDevice HSM；
2. 准备上位机等相关工具，准备进行文件加密；
3. HSM 连接到上位机，并正确安装驱动；

### 代工制造商硬件：

1. 获取 GigaDevice HSM；
2. GD32H7 MCU 下载平台；
3. USB/USART 连接 GD32H7 MCU 下载平台与上位机；
4. HSM 连接上位机。

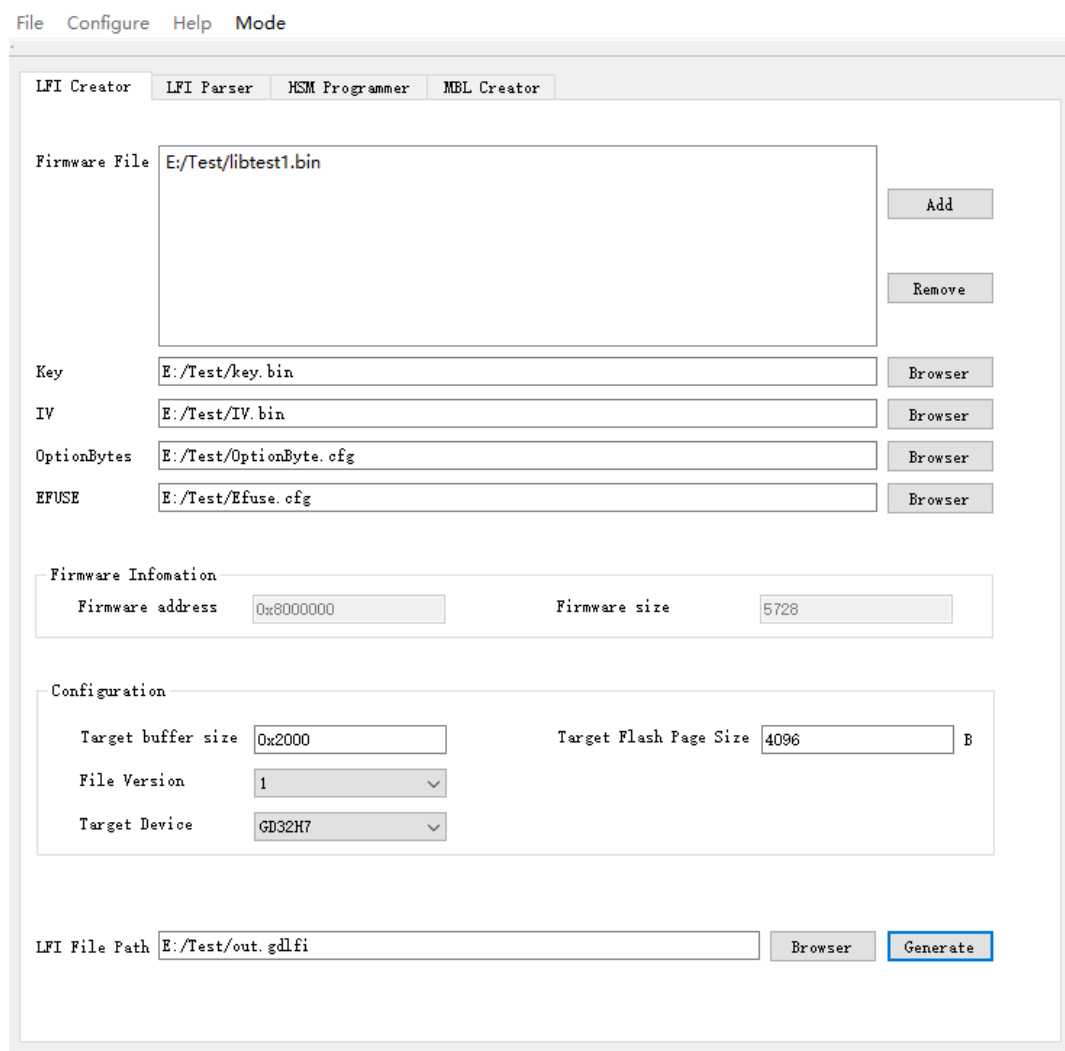
### 3. 软件资源

LFI 流程要求 OEM 以及代工制造商依据 GigaDevice 提供的 LFI User guide 和软件工具手册正确执行软件操作，其中 GigaDevice 提供了 GD licensed Data Creator 和 GD licensed Data Programmer 两款软件用于 LFI 文件加解密以及 LFI 文件安全安装。

#### 3.1. GD licensed Data Creator

LFI 文件格式是由 GigaDevice 创建的加密格式。在 LFI 过程中可以通过 GD licensed Data Creator 生成授权的 LFI 文件，软件界面如 [图 3-1 GD licensed Data Creator](#)。

图 3-1 GD licensed Data Creator

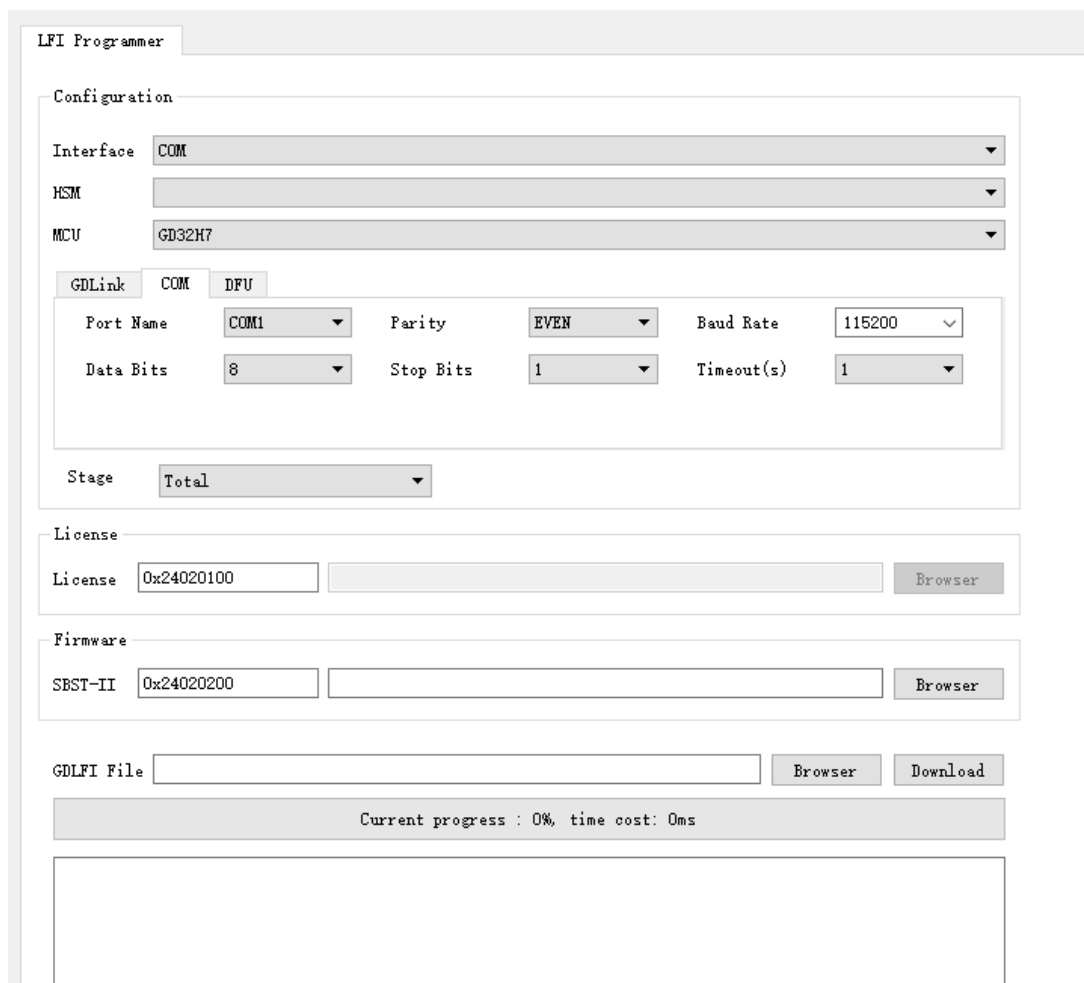




## 3.2. GD licensed Data Programmer

GD licensed Data Programmer 通过主机的 USART 端口或 USB 端口与 GD32H7 MCU 下载平台相连。在 GD licensed Data Programmer 中选择 LFI programmer,选择 GD licensed Data Creator 生成的 LFI 文件，点击 download 完成固件下载。

图 3-2 GD licensed Data Programmer



在正确连接相关硬件，配置好相关软件后，Gigadevice 还提供了一键下载功能，其功能为：

1. 配置GDM32H7从引导加载程序启动；
2. 使用BootLoader命令获取证书；
3. HSM生成安装许可证；
4. 下载许可证和加密的SBSTII bin文件到目标MCU SRAM；
5. GDM32H7:在选项字节或熔断中设置SCR位。
6. 目标 MCU 复位；
7. 连接 SBSTII。BSS 阶段不涉及任何数据传输。因此，当 BSS 阶段完成时，工具将直接连接到 SBSTII；
8. LFI 文件传输；
9. 完成所有 sections 数据传输。然后单片机将自动复位。

## 4. 授权固件安装流程

授权固件安装主要有两个方面，首先是 OEM 开发经过加密的 LFI 文件，OEM 将 LFI 文件授权给代工制造商进行加工制造，完成发布文件的加密和生产数量的控制，其次是代工制造商拿到经过授权的 LFI 文件以及 HSM 等相关工具生成安装许可证，代工制造商即可完成产品生产。

### 4.1. OEM workflow

1. OEM 自行开发 OEM 固件（bin 文件）；
2. 使用 GD licensed Data Creator 准备 LFI 文件。；
3. 配置 HSM。其中 HSM 包含最大生产数量控制信息和 LFI 文件 license 生成信息。
4. 提供 LFI 文件和 HSM 给代工制造商。

### 4.2. 代工制造商 workflow

代工制造商 workflow 如下：

1. 准备接收文件和配套的 HSM，安装 GD 的 GD licensed Data Programmer；
2. 准备合适的下载平台，连接 串口和 USB；
3. PC 上插入 HSM，GD licensed Data Programmer 识别成功，指定下载文件；
4. 循环按下载键，等待成功提示，更换芯片，只有下载成功以后，HSM 计数器才会自动减一。

## 5. 版本历史

表 5-1 版本历史

版本号.	说明	日期
1.0	首次发布	2023 年 9 月 18 日

## 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.