GigaDevice Semiconductor Inc.

GD32H7 系列安全启动概述

应用手册

AN130

1.0 版本

（2023 年 10 月）

目录

图索引

表索引

1. 简介

根据ARM®的平台安全架构（Platform Security Architecture，PSA），可信启动过程的安全要求是在执行前验证下一阶段固件的完整性和真实性。安全启动流程总是从 ROM 开始启动，然后检查安全引导代码的完整性。启动ROM中的代码和安全引导代码都是不可修改的，也称为不可变引导加载程序（Immutable Bootloader，IBL）。

安全引导代码在执行用户引导代码之前验证其数字签名。如果验证失败，则MCU处于等待复位的循环状态。用户引导代码必须部署在内部闪存的安全区域，可以使用预授权固件安装（Licensed firmware install，LFI）流程进行安装。类似的，用户引导代码必须在执行下一阶段的固件前先验证合法性，下一阶段的固件可以是安全区域代码或普通区域代码。

有关安全存储管理的更多信息，请参阅***AN113 GD32H7安全存储管理***。

有关LFI的更多信息，请参阅***AN118 GD32H7系列MCU授权固件安装（LFI）概述***。

本文档是安全启动的概述，更多信息请联系GigaDevice获取***AN120 GD32H7系列MCU安全启动用户指南***。

2. 特性

- 安全引导代码被固化在专用的内部安全存储区域中，该区域用户无法访问；
- 系统复位后从ROM启动，唯一启动入口；
- 支持验证数字签名；
- 公钥哈希值存储在 EFUSE 中；
- 安全引导代码尽可能简单、可靠和通用；
- 确保安全区域中的用户引导代码是完整的和真实的。

3. 功能简介

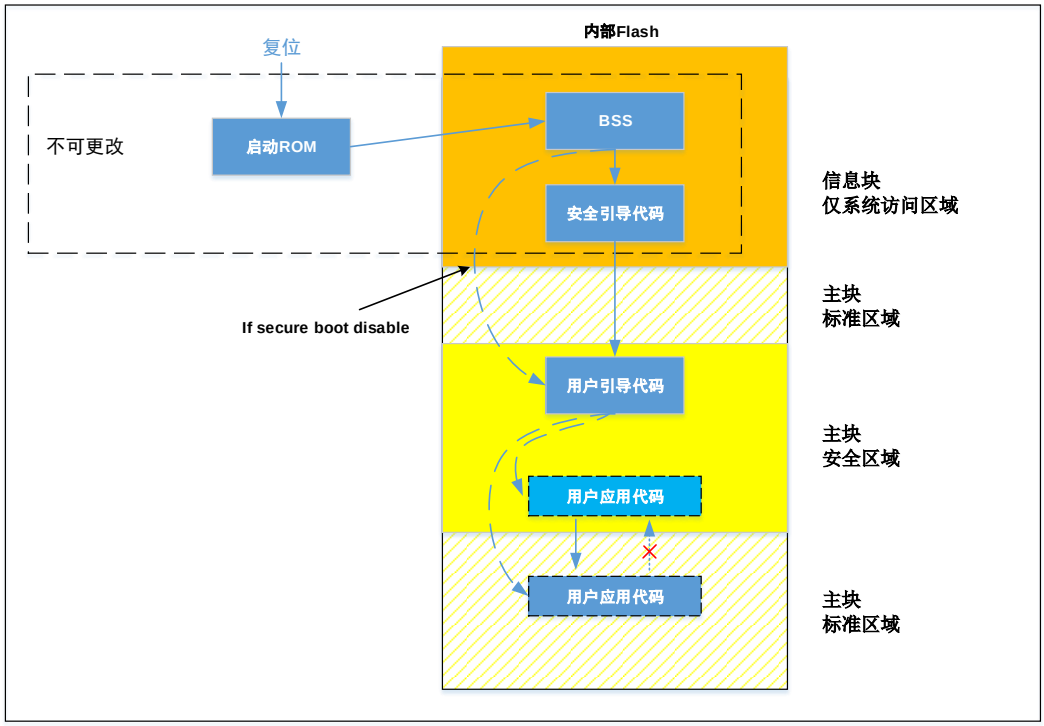
3.1. 安全启动流程

GD32H7安全启动流程如***图3-1. 安全启动流程***所示。安全启动流程默认是关闭的，要使能安全启动流程，用户必须先置位选项字节或EFUSE中的SCR位来使能安全模式，然后设置安全区域并烧录用户引导代码到该区域。必须置位EFUSE_MCU_RSV寄存器的VFIMG位来验证用户镜像。若通过EFUSE使能安全模式则无法禁用安全启动。

这些操作已经集成在LFI解决方案中，GigaDevice提供了一些工具来帮助用户简化流程。

注意：安全启动代码仅验证安全区域中的用户引导代码。

图 3-1. 安全启动流程



安全启动流程复位后仅执行一次，无需调用外部API且仅能从ROM启动。*表3-1. 安全启动相关硬件特性*列出了MCU的硬件特性。这些不可改变和唯一特性保证了首条指令的安全性和可靠性。安全引导代码支持ECDSA算法进行签名验证。因此用户可以定义自己的引导代码，用户定义引导代码被称为主引导加载程序（Main Bootloader，MBL）。

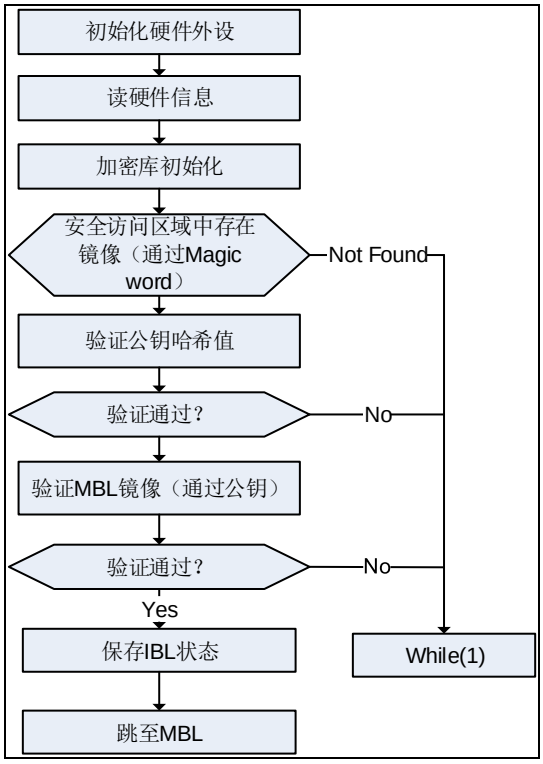
表 3-1. 安全启动相关硬件特性

项	硬件特性
熔丝	1. EFUSE 仅可写一次。 2. EFUSE 中的位可开启安全启动。
ROM	1. 在将跳转到 MBL 之前，通过写入特定位来关闭 ROM。保证安全引导代码只能在系统复位后才能再次执行。 2. 当代码在安全引导代码区域时，安全引导代码可以访问 SRAM 和安全访问区域，此时调试被关闭。
SRAM	1. 系统复位后，安全引导代码使用的 SRAM 区域会自动清除。
外设	1. TRNG、CAU、HASH 引擎的数据寄存器在系统复位后自动清除。

3.2. 安全引导代码流程

*图3-2. 安全引导代码流程*显示了安全启动过程。系统复位后，安全引导代码将配置相应的外设用于后续的签名认证流程。如果验证通过，则MCU跳转到MBL，否则，它将进入死循环等待下一次复位。

图 3-2. 安全引导代码流程

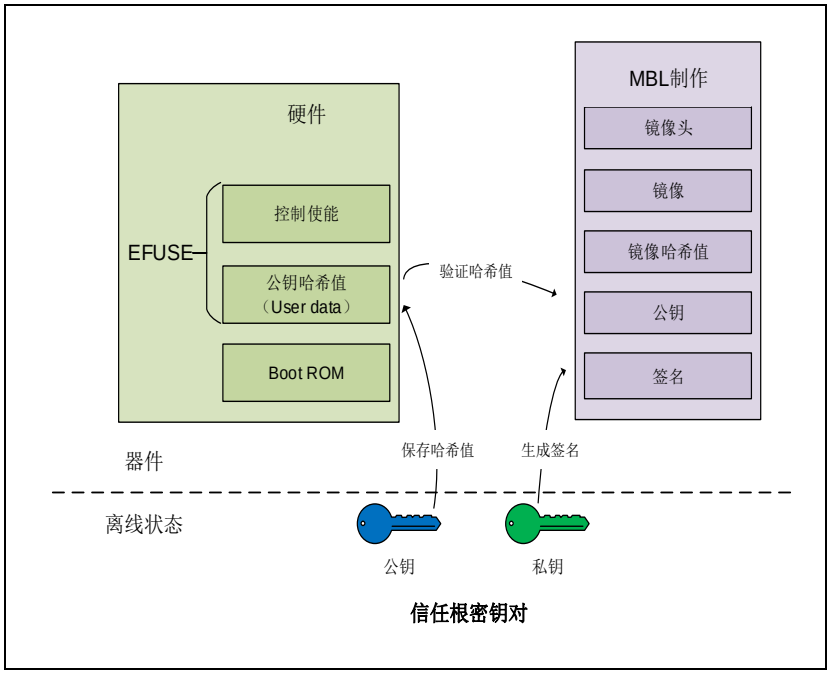


3.3. 签名验证

用户引导代码（MBL）需要包含数字签名，数字签名可通过GigaDevice工具生成。用户也可根据开放的代码格式开发自己的签名工具。数字签名使用非对称加密算法（ECDSA）。开发人员可使用GigaDevice工具生成信任根（RoT，Root of Trust）密钥对。密钥对中的私钥用于对用户引导代码进行签名。密钥对中的公钥会传递并保存在MCU中，用于MCU验证用户引导代码的完整性和真实性。同时，公钥的哈希值也会保存在EFUSE中。

安全启动时，安全引导代码首先计算公钥的哈希值，并与EFUSE中的哈希值进行比较，验证公钥正确性。验证通过后，使用该公钥来解密用户引导固件的文件信息。

图 3-3. 签名验证流程



3.4. 用户引导镜像验证流程

图 3-4. 用户引导镜像验证流程

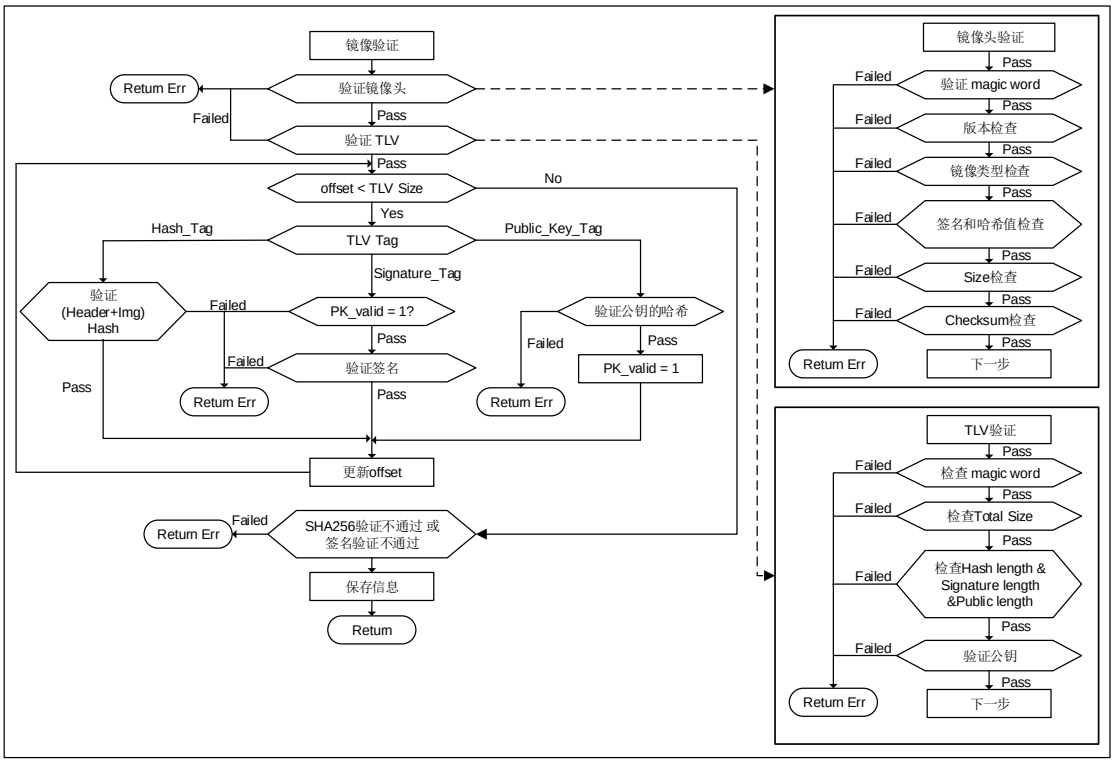


*图3-4. 用户引导镜像验证流程*显示了用户引导镜像验证流程。首先验证镜像头是否正确，分别检查Magic word、版本号、类型、镜像的哈希值、Size、Checksum。然后进行TLV验证，分别

检查Magic word、Total Size、哈希/签名/公钥长度、公钥。根据系统设置的偏移值判断各部分是否校验完成，当验证通过后，保存信息并开始执行用户引导代码。

4. 版本历史

表 4-1. 版本历史

版本号.	说明	日期
1.0	首次发布	2023 年 10 月 23 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 it’s 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 it’s 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.