GigaDevice Semiconductor Inc.

GD32H7 series MCU Secure boot overview

User Manual
AN130

Revision 1.0

(Oct. 2023)

Table of Contents

List of Figures

List of Tables

1. Overview

According to ARM®'s Platform Security Architecture (PSA), the security requirements of a Trusted Boot process is to verify the integrity and authentication of the next stage firmware before execution. Secure boot process is always start from boot ROM, then boot ROM code will verify the integrity of the BSS and the secure boot code, all of them are immutable (Immutable Boot Loader, IBL).

The secure boot code will verify the digital signature of the user's boot code before executing it. If the verification fails, the MCU is in a loop waiting state for a reset. The user's boot code must be deployed in secure area of internal flash, which is installed with Licensed Firmware Install (LFI) flow. Then the user's boot code can verify the next stage of firmware before executing, which can be secure or non-secure code.

For more information about secure memory management, please refer to the ***AN113 GD32H7 Secure Memory Management***.

For more information about LFI, please refer to ***AN118 GD32H7 series MCU Licensed Firmware Install (LFI) overview***.

This document is an overview for secure boot, for more information, please contact with GigaDevice to get the ***AN120 GD32H7 series MCU Secure boot user guide***.

2. Characteristics

- Secure boot code is solidfied in a dedicated, system-access-only secure area in internal flash.
- Boot from ROM after system reset, which is unique boot entry.
- Support for verifying digital signature.
- Hash value is stored in the EFUSE.
- Secure boot code is as simple, reliable and generic as possible.
- Ensure the integrity and authenticity of the user's boot code in secure area.

3. Function overview

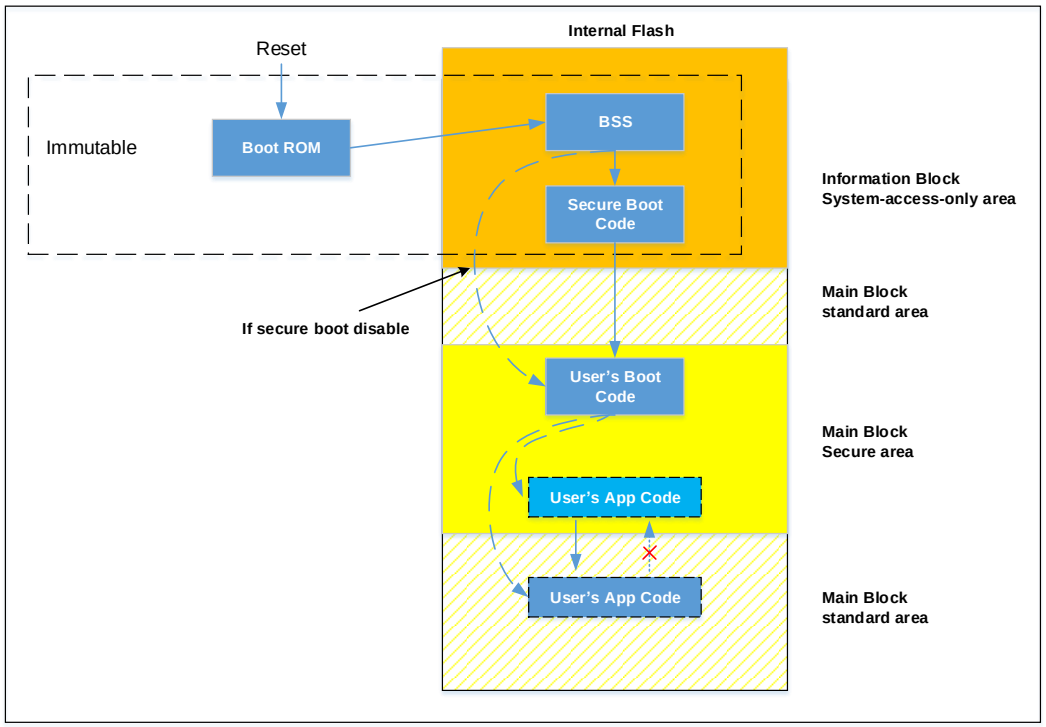
3.1. Secure Boot Process

GD32H7 secure boot flow diagram is shown in ***Figure 3-1. Secure boot process***. To enable the secure boot process, user need enable secure mode first by setting SCR bit in option bytes or EFUSE, and then split a secure area and program the user's boot image to secure area. VFIMG bit in the EFUSE_MCU_RSV register must be set to verify user's image. Secure boot mode cannot disable if secure mode is enabled by EFUSE.

Those operations have integrated in LFI flow, GigaDevice has provided some tools to help users to simplify the process.

Note: only the user's boot image in the secure area is verified.

Figure 3-1. Secure boot process



The Secure boot process is set to be executed once after reset and never call external API, which always start from ROM. The following table ***Table 3-1. Secure boot hardware features*** lists the hardware features of the MCU. With characteristics of immutability and priority to ensure the security and reliability of the first instruction. The secure boot code supports signature verification by ECDSA algorithm. Thus, user can customize their own boot code to verify the application code before running used the same way.

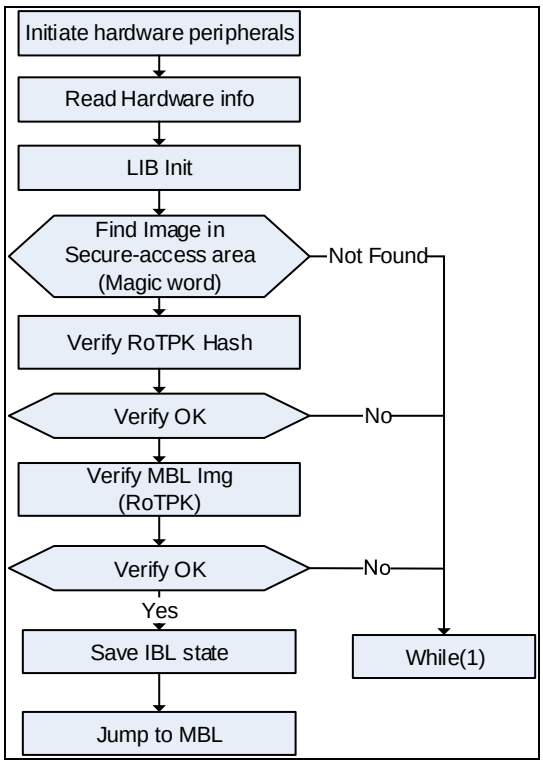
Table 3-1. Secure boot hardware features

Item	Requirement
EFUSE	1. EFUSE is write once 2. Secure boot is enabled by a bit in EFUSE.
ROM	1. Close the ROM before jumping to MBL. Close the ROM is that Secure boot code can be executed again only after the system is reset. 2. The Secure boot code can access SRAM and secure-access area, while debug is turned off.
SRAM	1. After the system is reset, the SRAM area used by the Secure boot code is automatically cleared.
Peripheral	1. TRNG, CAU, HASH engine data registers are cleared automatically after system reset.

3.2. Secure Boot Code

Figure 3-2. Secure Boot Code Flow shows the secure boot code process. The Secure boot code configures peripherals for the subsequent signature authentication process. If the verification passes, MCU jumps to MBL, otherwise, it goes into an infinite loop and waits for the next reset.

Figure 3-2. Secure Boot Code Flow

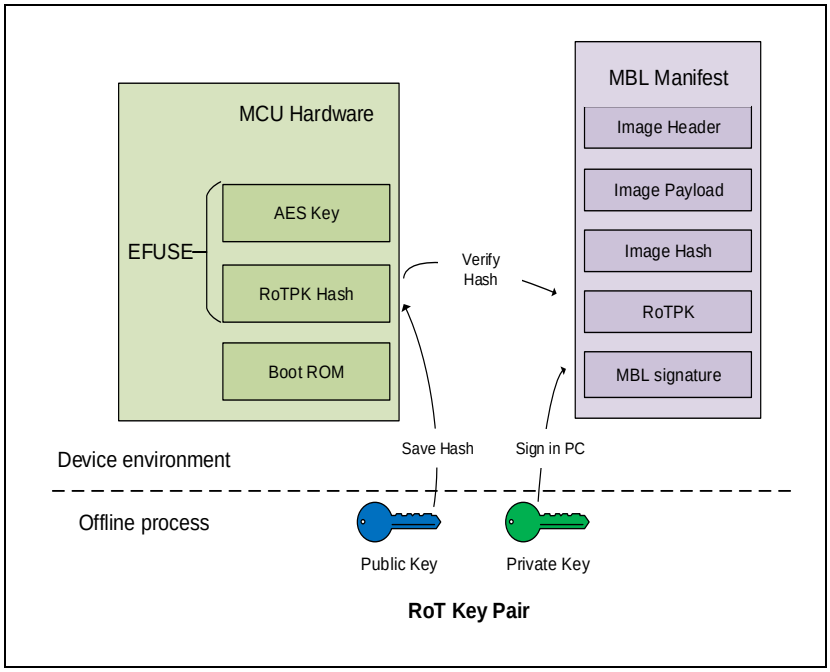


3.3. Signature Verification Process

The user's boot image needs including digital signature, it is generated by tool from GigaDevice. User also can develop owner tool for signature, where the code format is open. The digital signature uses an asymmetric encryption algorithm (ECDSA). The tool helps developer to generate a RoT (Root of Trust) key pair. The private key is used to sign the user's boot code. The public key will be delivered to and stored in MCU when install, it will be used by the MCU to verify the integrity and authentication of the user's boot image. The hash value of the public key will be stored in EFUSE on the same time.

When secure booting, the secure boot code first calculates the hash value of the public key and compares it with the hash value in EFUSE to verify the correctness of the public key. After the verification is passed, the public key is used to decrypt the file information of user's boot image.

Figure 3-3. Signature Verification Scheme



3.4. The User's Boot Image Verification Process

Figure 3-4. The User's Boot Image Verification Flow

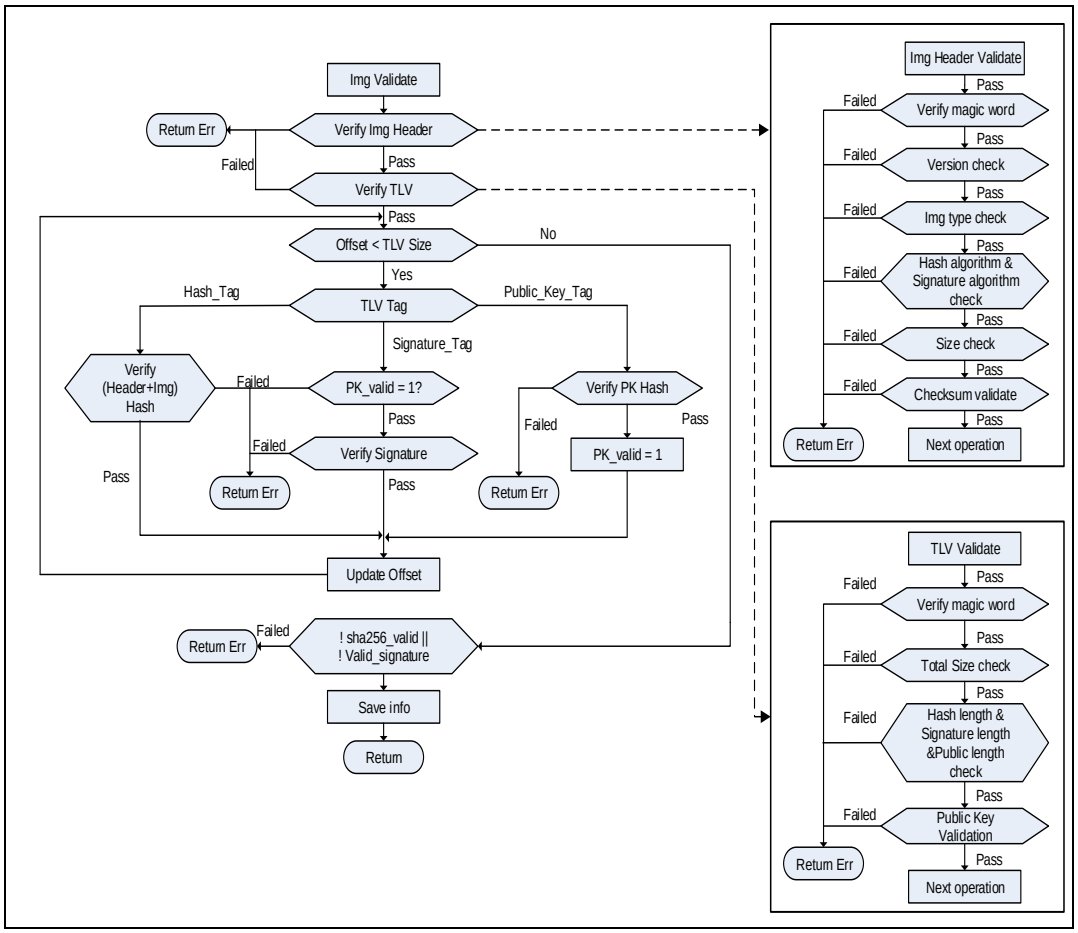


Figure 3-4. The User's Boot Image Verification Flow shows the user's boot image verification process.

First verify that the Image header is correct, respectively checking the Magic word, version number, type, hash value of the Image, Size, Checksum. Then TLV verification, respectively check Magic word, Total Size, hash/signature/public key length, public key. Check whether the verification is complete based on the offset value set by the system. After the verification is passed, save the information and go to run the user's boot code.

4. Revision history

Table 4-1. Revision history

Revision No.	Description	Date
1.0	Initial Release	Oct. 23, 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 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.