IAR Embedded Trust - Secure Boot Manager

Enabling product security adoption as well as secure, encrypted software to inhibit IP theft, malware injection, and unauthorized over-production.

With the Secure Boot Manager (SBM), IAR offers solutions for the most common security use cases: security management and software updates.

Benefits of the Secure Boot Manager include:

- Performs the security integrity checks of the system running on the device and launches a valid OEM application
- Provides an API to the application to enable security functions to be performed
- Supports source code utilizing silicon vendor ports, driver and functionality can be optimized by the OEM
- Arm® TrustZone® is supported to provide secure memory
- NXP PUF and Renesas TSIP are supported to protect the firmware, keys, certificates and sensitive data
- Supports external memory to run applications that offload the required memory
- Works in conjunction with Secure Deploy to prevent supply chain compromises through secure provisioning
- Expedites time-to-market and lowers development cost

With IAR's comprehensive end-to-end security solutions, customers can confidently develop and deploy secure embedded products. Our solutions seamlessly integrate key security features, ensuring authenticity and integrity using robust keys and certificates from development to secure production. With IAR's expertise and commitment to embedded security, customers can navigate the complexities of product development with ease, safeguarding against potential threats and vulnerabilities throughout the entire lifecycle.

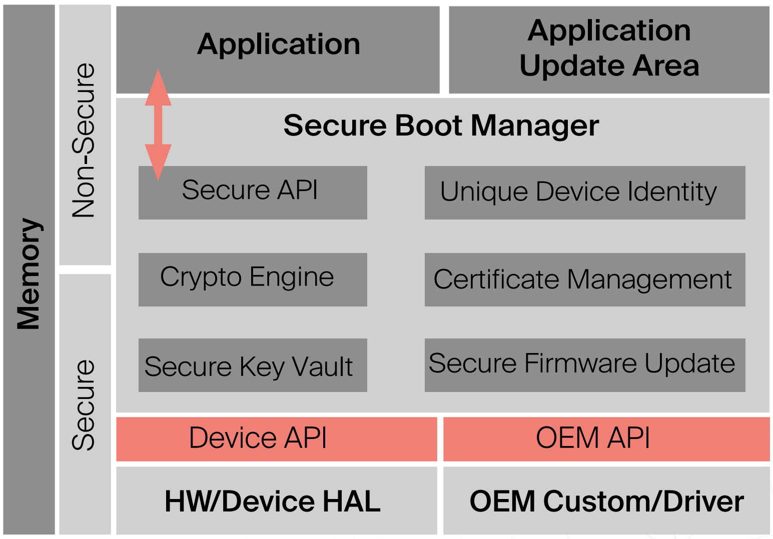


Figure 1. Secure Boot Manager Overview

Features:

- **Immutable Boot Process:**
  Immutable sequence and integrity check ensure secure system initialization.
- **Intuitive User-Friendly Configuration Wizard:**
  Allows for easy configuration of security settings based on the required assurance class of the product
- **Full Source Code:**
  Delivered in C code which allows for extensive customization in implementing security measures tailored to specific needs
- **Expedite Time-to-Market and Approval:**
  Helps facilitate FDA approval by complying with the secure software framework requirement
- **Certified to SESIP[1] Level 1:**
  Complies with the security requirements and implmentation
- **Authenticity:**
  Verifies authorized software code and application installation, safeguarding your intellectual property from the root and swiftly establishing a Root of Trust
- **Anti-Rollback and Secure Firmware Update:**
  Manages your software update processes to provide protection against roll-back attacks and versioning threats
- **Anti-Cloning:**
  Supports unique identification for software applications and device hardware, preventing counterfeits and encrypting your manufacturing
- **Active IP Protection:**
  Ensure critical key management to lock your applications onto authorized devices, providing secure application and device access right from the boot process

[1] SESIP: Security Evaluation Standard for IoT Platforms

Enhancing Security with Secure Provisioning

The immutable boot process is vital for ensuring the integrity and security of a device's software during the boot sequence. It relies on secure provisioned data to validate unique device information.

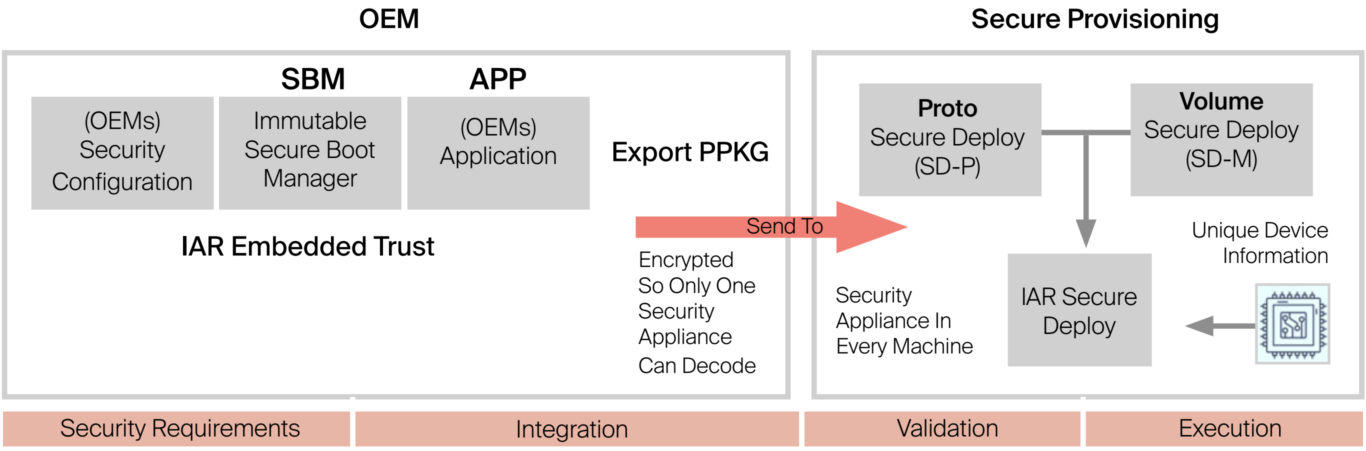
Secure provisioning plays a crucial role in the boot process by programming essential data, such as keys and certificates, into the device's memory. This provisioned device key is unique to each device and serves as a form of validation, confirming that the device is genuine and free from tampering. To achieve a higher level of security, secure provisioning is performed using a hardware security module, which includes a Trusted Platform Module (TPM) that is FIPS certified. This certification ensures that the security appliance has undergone rigorous testing and meets specific cryptographic standards, making it resistant to various attacks. The security appliance provides a secure environment for generating and storing cryptographic keys, certificates and other sensitive credentials.

By incorporating secure provisioning into the immutable boot process, the device can verify its identity and integrity every step of the boot process. This prevents unauthorized modifications or tampering attempts, ensuring that the device only boots with trusted and validated components.

The importance of the immutable boot process together with secure provisioning lies in the enhanced security it provides. It safeguards against various threats, such as application firmware attacks, rootkits, and boot-time malware. The approach protects the device from potential compromises during the boot process.

Furthermore, secure provisioning helps maintain the confidentiality of sensitive information stored on the device. By validating unique device information, it ensures that only authorized users or entities can access the device and its data.

In conclusion, secure provisioning is a vital aspect of the immutable boot process. It enables the validation of unique device information, enhancing embedded security and protecting against unauthorized modifications or tampering. By incorporating the immutable boot process and secure provisioning, devices can establish their identity and ensure a trusted and secure boot process.



OEM
Secure Provisioning
SBM
APP
(OEMs) Security Configuration
Immutable Secure Boot Manager
(OEMs) Application
Export PPKG
IAR Embedded Trust
Send To
Encrypted So Only One Security Appliance Can Decode
Proto Secure Deploy (SD-P)
Volume Secure Deploy (SD-M)
Unique Device Information
Security Appliance In Every Machine
IAR Secure Deploy
Security Requirements
Integration
Validation
Execution

Figure 2. The End-to-End Security Flow

Enhancing Security with Secure Provisioning

Technical Specifications

The secure boot manager is designed to optimize the boot process and minimize the time it takes for the device to start up and become operational. By implementing efficient and streamlined boot procedures, the secure boot manager helps reduce boot time, enabling faster system initialization and improving overall device responsiveness.

Additionally, the secure boot manager's code size is optimized to minimize the memory footprint required for its implementation. This is particularly advantageous in resource-constrained embedded systems where memory usage is critical. By minimizing the code size, the secure boot manager allows for efficient utilization of the available memory, freeing up space for other essential functionalities and applications within the device.

SBM Boot Time
Boot Time[1] ~100 ms

SBM Flash Memory
Code Size 8-10 KB[2]

SBM Security Lifecycle:

- **Debug Port Control:**
  Enable / Delayed Disabled / Fully Disabled
- **Permanent SBM Lock Down:**
  Device-dependent
- **Chain of Trust:**
  Have the device / intermediate / root cert public keys
- **Protect Provisioned Data:**
  Disabled / Hash per device /Encrypt and Authenticate (Device-dependent)
- **Software Update Mechnism from an Authentic Source:**
  Full encryption / Basic signature checking
- **Version Number Check:**
  No checking / Greater or equal to current / Greater than current

[1] The boot time of the SBM is measured using STM32F407 NUCLEO and ECC signature verification

[2] The code size of the SBM does not include any hardware drivers and cryptographic libraries