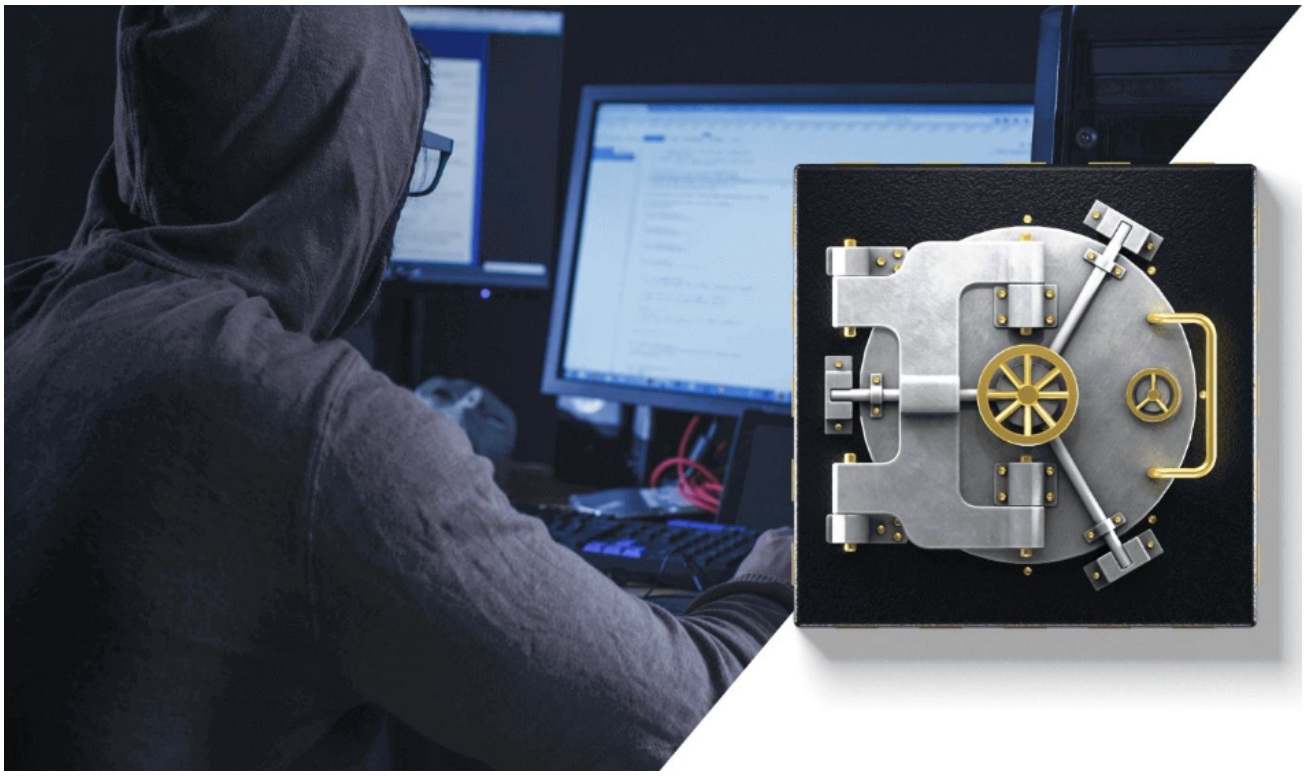
IoT Security

- Using IoT Security Features
- Getting Started
- IoT Security Fundamentals (PDF)
- Developer's Guide
  - Overview
  - Series 2 Secure Debug (PDF)
  - Series 2 TrustZone (PDF)
  - Production Programming of Series 2 Devices (PDF)
  - Anti-Tamper Protection Configuration and Use (PDF)
  - Authenticating Silicon Labs Devices using Device Certificates (PDF)
  - Secure Key Storage (PDF)
  - Programming Series 2 Devices Using the DCI and SWD (PDF)
  - Integrating Crypto Functionality with PSA Crypto vs. Mbed TLS (PDF)
  - Protocol-Specific Information

Using IoT Security Features

Using Silicon Labs IoT Security Features

Silicon Labs offers a range of security features depending on the part you are using and your application and production needs.



The content on these pages is intended for those who want to implement security features as part of your IoT device management. If you are looking for an introduction to Silicon Labs Security features and to security issues that confront those implementing IoT systems, see the Silabs.com Security page.

For details about this release: Links to release notes are available on the silabs.com Gecko SDK page as part of the Gecko Platform release notes.

For background on security issues in general: IoT Security Fundamentals explains some security basics.

To get started with implementing security: See the Getting Started page for help determining what features you want to implement based on the series 2 part you are working with. Series 2 devices are the preferred choice for secure system implementation.

If you are already in development: See the Developer's Guide for details. Security APIs are documented in the Gecko Platform API Reference.

For detailed information about implementing some security features with specific protocols: See the protocol-specific pages. An extensive body of other protocol-specific content can be accessed through the docs.silabs.com homepage.

Getting Started

Getting Started with Silicon Labs IoT Security Features on Series 2 Devices

Protecting IoT devices against security threats is central to a quality product. Silicon Labs offers several security options to help developers build secure devices, secure application software, and secure paths of communication to manage those devices. Silicon Labs' security offerings were significantly enhanced by the introduction of the Series 2 products that included a Secure Engine. The Secure Engine is a tamper-resistant component used to securely store sensitive data and keys, and to execute cryptographic functions and secure services.

On Series 1 devices, the security features are implemented by the TRNG (if available) and CRYPTO peripherals.

On Series 2 devices, the security features are implemented by the Secure Engine and CRYPTOACC (if available). The Secure Engine may be hardware-based or virtual (software-based). Here the following abbreviations are used:

- HSE - Hardware Secure Engine
- VSE - Virtual Secure Engine
- SE - Secure Engine (either HSE or VSE)

Additional security features are provided by Secure Vault. Three levels of Secure Vault feature support are available, depending on the part and SE implementation, as reflected in the following table:

Security Level (1)	SE Support	MCU	Wireless SoC (2)
Secure Vault Base (SVB)	N/A	EFM32JG1, EFM32PG1, EFM32JG12, EFM32PG12, EFM32GG11, EFM32GG12, EFM32TG11	EFR32xG1, EFR32xG12, EFR32xG13, EFR32xG14
Secure Vault Mid (SVM)	VSE (VSE-SVM)	EFM32PG22	EFR32xG22
”	HSE (HSE-SVM)	EFM32PG23A	EFR32xG21A, EFR32xG23A, EFR32xG24A
Secure Vault High (SVH)	HSE only (HSE-SVH)	EFM32PG23B	EFR32xG21B, EFR32xG23B, EFR32xG24B

Note:

1. The features of different Secure Vault levels can be found in https://www.silabs.com/security .
2. The x is a letter B, F, M, or Z.

Secure Vault Mid consists of two core security functions:

- Secure Boot: Process where the initial boot phase is executed from an immutable memory (such as ROM) and where code is authenticated before being authorized for execution.
- Secure Debug access control: The ability to lock access to the debug ports for operational security, and to securely unlock them when access is required by an authorized entity.

Secure Vault High offers additional security options:

- Secure Key Storage: Protects cryptographic keys by “wrapping” or encrypting the keys using a root key known only to the HSE-SVH.
- Anti-Tamper protection: A configurable module to protect the device against tamper attacks.
- Device authentication: Functionality that uses a secure device identity certificate along with digital signatures to verify the source or target of device communications.

A Secure Engine Manager and other tools allow users to configure and control their devices both in-house during testing and manufacturing, and after the device is in the field.

Silicon Labs strongly recommends installing the latest SE firmware on Series 2 devices to support the required security features. The latest SE firmware image (.seu and .hex) and release notes can be found in these Windows folders of the GSDK.

```
C:\Users\<UserName>\SimplicityStudio\SDKs\gecko_sdk\util\se_release\public
```

If you have not already installed the GSDK, instructions for doing so with Simplicity Studio are available in the Getting Started section of the Simplicity Studio 5 User's Guide.

Refer to *AN1222: Production Programming of Series 2 Device*s for guidance on the SE firmware upgrade procedure. The latest SE firmware shipped with Series 2 devices and modules (if available) at the time of this writing are listed in the following table:

MCU Series 2 and Wireless SoC Series 2	SE	Shipped SE Firmware Version (Device and Module)
EFR32xG21A	HSE-SVM	1.2.13
EFM32PG23A	HSE-SVM	2.1.7
EFR32xG23A	HSE-SVM	2.1.2 (Rev B), 2.1.7 (Rev C)
EFR32xG24A	HSE-SVM	2.1.7
EFR32xG21B	HSE-SVH	1.2.13
EFM32PG23B	HSE-SVH	2.1.7
EFR32xG23B	HSE-SVH	2.1.2 (Rev B), 2.1.7 (Rev C)
EFR32xG24B	HSE-SVH	2.1.7
EFM32PG22 and EFR32xG22	VSE-SVM	1.2.12

In support of these products Silicon Labs offers whitepapers, webinars, and documentation. The following table summarizes the key security documents:

Document	Summary	Applicability
AN1190: Series 2 Secure Debug	How to lock and unlock Series 2 debug access, including background information about the Secure Engine	Series 2
AN1218: Series 2 Secure Boot with RTSL	Describes the secure boot process on Series 2 devices using Secure Engine. For information on bootloading with Silicon Labs products, see *UG266/UG489*	Series 2
AN1247: Anti-Tamper Protection Configuration and Use	How to program, provision, and configure the anti-tamper module	Series 2 with SVH
AN1268: Authenticating Silicon Labs Devices using Device Certificates	How to authenticate a device using secure device certificates and signatures, at any time during the life of the product	Series 2 with SVH
AN1271: Secure Key Storage	How to securely “wrap” keys so they can be stored in non-volatile storage	Series 2 with SVH
AN1222: Production Programming of Series 2 Devices	How to program, provision, and configure security information using Secure Engine during device production	Series 2
AN1303: Programming Series 2 Devices Using the Debug Challenge Interface (DCI) and Serial Wire Debug (SWD)	How to provision and configure Series 2 devices through the DCI and how to program their internal flash memory through the SWD	Series 2
AN1311: Integrating Crypto Functionality Using PSA Crypto Compared to Mbed TLS	How to integrate crypto functionality into applications using Silicon Labs implementation of PSA Crypto compared to Mbed TLS	Series 1 and Series 2

Overview

Silicon Labs IoT Security Developer's Guide

The IoT Security Developer's Guide offers detailed information on how to implement each of the device security features. This content is applicable to any protocol that supports the feature described. Additional protocol-specific information for Bluetooth, Bluetooth Mesh, OpenThread, and Zigbee is available in the protocol-specific section.

- **Series 2 Secure Debug (PDF)** - Describes how to lock and unlock the debug access of EFR32 Gecko Series 2 devices. Many aspects of the debug access, including the secure debug unlock are described. The Debug Challenge Interface (DCI) and Secure Engine (SE) Mailbox Interface for locking and unlocking debug access are also included.
- **Series 2 TrustZone (PDF)** - Covers the basics of ARMv8-M TrustZone, describes how TrustZone is implemented on Series 2 devices, and provides application examples.
- **Production Programming of Series 2 Devices (PDF)** - Provides details on programming, provisioning, and configuring Series 2 devices in production environments. Covers Secure Engine Subsystem of Series 2 devices, which runs easily upgradeable Secure Engine (SE) or Virtual Secure Engine (VSE) firmware.
- **Anti-Tamper Protection Configuration and Use (PDF)** - Shows how to program, provision, and configure the anti-tamper module on EFR32 Series 2 devices with Secure Vault.
- **Authenticating Silicon Labs Devices using Device Certificates (PDF)** - Describes how to authenticate an EFR32 Series 2 device with Secure Vault, using secure device certificates and signatures.
- **Secure Key Storage (PDF)** - Explains how to securely "wrap" keys in EFR32 Series 2 devices with Secure Vault, so they can be stored in non-volatile storage.
- **Programming Series 2 Devices Using the Debug Challenge Interface (DCI) and Serial Wire Debug (SWD) (PDF)** - Describes how to provision and configure Series 2 devices through the DCI and SWD.
- **Integrating Crypto Functionality Using PSA Crypto Compared to Mbed TLS (PDF)** - Describes how to integrate crypto functionality into applications using PSA Crypto compared to Mbed TLS.

Protocol-Specific Information

Protocol-Specific Security References

The pages in this section offer protocol-specific information. For general content applicable to any protocol that supports the feature, see the main development section.

Bluetooth

Bluetooth Low Energy Application Security Design Considerations in SDK v3.x and Higher (PDF) - Provides details on designing Bluetooth Low Energy applications with security and privacy in mind.

Certificate-Based Bluetooth Authentication and Pairing (PDF) - Describes the theoretical background of certificate-based authentication and pairing, and demonstrates the usage of the related sample applications that can be found in Silicon Labs' Bluetooth SDK.

Bluetooth Mesh

Bluetooth Mesh Certificate-Based Provisioning (PDF) - Describes how certificates are used to establish the authenticity of devices wishing to join a mesh network.

OpenThread

Using Silicon Labs Secure Vault Features with OpenThread (PDF) - Describes how Secure Vault features are leveraged in OpenThread applications. Focuses on specific PSA features and emphasizes how these are integrated into the OpenThread stack.

Zigbee

Zigbee Security (PDF) - Introduces some basic security concepts, including network layer security, trust centers, and application support layer security features. It then discusses the types of standard security protocols available in EmberZNet PRO. Coding requirements for implementing security are reviewed in summary. Finally, information on implementing Zigbee Smart Energy security is provided.

Copyright © 2023 Silicon Laboratories. All rights reserved.