Virtual Secure Engine Firmware Release Notes
For xG27 Products

Virtual Secure Engine (VSE) firmware is installed with the product. The firmware is upgradable through Gecko Bootloader and Simplicity Studio. Features and security updates available in the latest release are described in this document.

Contents

Using This Release

Virtual Secure Engine (VSE) firmware is factory installed with the product.

VSE firmware upgrade images are installed with Gecko SDK Suite in Simplicity Studio. This release contains the following.

- Upgrade image for Gecko Bootloader (.seu file)
- Upgrade application (.hex file)

Upgrade images are signed and encrypted.

Use of the upgrade image with Gecko Bootloader is described in *UG266: Silicon Labs Gecko Bootloader User's Guide, Section on Secure Engine Upgrade.*

To upgrade your device using the Upgrade application, program the .hex file to Flash using Simplicity Commander and then reset the device or use the upgrade feature in Simplicity Studio.

The Secure Engine Manager component in the Gecko SDK Suite provides an API to get the current VSE version from the device. The API reference guide is available on https://docs.silabs.com/gecko-platform/latest/service/api/group-sl-se-manager

1.1 Compatible Products

The firmware is compatible with the following Series-2 products:

- EFR32xG27 SoCs

1.2 Support

Development Kit customers are eligible for training and technical support. You can use the Silicon Laboratories web site https://www.silabs.com/products/development-tools/software to obtain information about software products and services, and to sign up for product support.

You can contact Silicon Laboratories support at www.silabs.com/support

Features and Security Updates

v2.2.4
- Fixed a bug where flashing a new application was not possible after a device erase, unless the device was reset beforehand.

v2.2.2
- Fixed an issue where data in internal VSE flash was encrypted using an uninitialized IV.
- Fixed an issue where certain debug restrictions could lead to a boot error on soft resets.
- Make the provisioned Secure Boot public key available to User code at runtime.

v2.2.1
- Prevent TrustZone specific debug lock configuration from being changed after debug access port lock has been applied.
- Changed the TrustZone Root Key automatic renewal. The key is now only renewed on Device Erase.
- Added OTP version to the status output field of the VSE mailbox.

v2.2.0
- Initial release for EFR32xG27 products.

Known Issues

– None

Legal

4.1 Disclaimer

Silicon Labs intends to provide customers with the latest, accurate, and in-depth documentation of all peripherals and modules available for system and software implementers using or intending to use the Silicon Labs products. Characterization data, available modules and peripherals, memory sizes and memory addresses refer to each specific device, and "Typical" parameters provided can and do vary in different applications.

Application examples described herein are for illustrative purposes only.

Silicon Labs reserves the right to make changes without further notice and limitation to product information, specifications, and descriptions herein, and does not give warranties as to the accuracy or completeness of the included information. Silicon Labs shall have no liability for the consequences of use of the information supplied herein. This document does not imply or express copyright licenses granted hereunder to design or fabricate any integrated circuits. The products are not designed or authorized to be used within any Life Support System. A "Life Support System" is any product or system intended to support or sustain life and/or health, which, if it fails, can be reasonably expected to result in significant personal injury or death. Silicon Labs products are not designed or authorized for military applications. Silicon Labs products shall under no circumstances be used in weapons of mass destruction including (but not limited to) nuclear, biological or chemical weapons, or missiles capable of delivering such weapons.

4.2 Trademark Information

Silicon Laboratories Inc.® , Silicon Laboratories®, Silicon Labs®, SiLabs® and the Silicon Labs logo®, Bluegiga®, Bluegiga Logo®, Clockbuilder®, CMEMS®, DSPLL®, EFM®, EFM32®, EFR, Ember®, Energy Micro, Energy Micro logo and combinations thereof, "the world's most energy friendly microcontrollers", Ember®, EZLink®, EZRadio®, EZRadioPRO®, Gecko®, ISOmodem®, Micrium, Precision32®, ProSLIC®, Simplicity Studio®, SiPHY®, Telegesis, the Telegesis Logo®, USBXpress®, Zentri, Z-Wave and others are trademarks or registered trademarks of Silicon Labs.

ARM, CORTEX, Cortex-M0+, Cortex-M3, Cortex-M33, Cortex-M4, TrustZone, Keil and Thumb are trademarks or registered trademarks of ARM Holdings.

Zigbee® and the Zigbee logo® are registered trademarks of the Zigbee Alliance.

Bluetooth® and the Bluetooth logo® are registered trademarks of Bluetooth SIG Inc.

All other products or brand names mentioned herein are trademarks of their respective holders.