



Virtual Secure Engine Firmware Release Notes

For EFR32xG22 and xGM22 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

1	Using This Release	1
1.1	Compatible Products	1
1.2	Support.....	1
2	Features and Security Updates	2
3	Known Issues	4
4	Legal.....	5
4.1	Disclaimer.....	5
4.2	Trademark Information	5



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:

- EFR32xG22 SoCs
- EFM32PG22 MCUs
- xGM22 modules

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

v1.2.14

- 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.
- Patched vulnerability in security configuration of EFM32PG22 SoCs with date code earlier than 2239.
- Added OTP version to the status output field of the VSE mailbox.

v1.2.12

- Added support for TrustZone Root Key which can be used by TrustZone secure applications for secure storage. The key is renewed on OTP configuration, debug lock and device erase.

v1.2.11

- Fixed downgrade attack vulnerability
- Make the Device Erase command break the boot loop that could occur after a failed host upgrade

v1.2.7

- Security and stability fixes

v1.2.6

- **Critical** stability fix to prevent devices becoming inoperable under certain conditions. A device whose VSE firmware has been successfully upgraded at least once can become inoperable if the upgrade file is removed from flash after the upgrade and the device is subjected to a large cumulative number of resets. The exact number of reset cycles before failure varies due to process variations and operating temperature but would typically range between 50,000 and 200,000 cycles. **It is imperative that this fix be applied to every device to avoid latent failures.**
- Increase DCI output buffer size to be able to fit attestation tokens for all device configurations.
- Hardened the boot up process against partial RAM retention. If a mailbox command is issued to the VSE and followed by a momentary power failure whose duration is sufficient to cause only a few specific RAM bits to lose state, the POR boot process can terminate in a hard fault.

v1.2.5

- Added VSE mailbox support to enable debug lock. The debug lock status is stored in the status word upon each boot and can be read using the EMLIB API `SE_getConfigStatusBits()`. The SE Manager functions `sl_se_apply_debug_lock()` and `sl_se_get_debug_lock_status()` are also available for EFR32xG22 products from Gecko SDK version 3.0.1.

v1.2.2

- The output mailbox struct is populated with user OTP settings after reset.
- Added an option to manually upgrade the (V)SE firmware when the debug interface is locked and Secure Boot is enabled, as long as the device erase function has not been turned off.
- The error code returned over DCI on failure to validate the firmware during Secure Boot is now more granular as to the reason for failing Secure Boot.
- Security updates

v1.2.1

- Fixed issue that could cause the device to become unrecoverable with both Secure Boot with RTSL and Rollback Prevention enabled

v1.2.0

- Improved handling of fatal errors during chip boot-up sequence
- Access restrictions can now be set on the debug interface. The command `DBG_LOCK_SET_RESTRICTION` is added and status of individual restrictions is added to the status commands.

v1.1.8

- None for this product

v1.1.7

- Security update

v1.1.6

- Added DCDC configuration retention across soft reset

v1.1.5

- Stability fixes

v1.1.4

- Unauthenticated device recover will now also set all RAM words to 0

v1.1.3

- Commands with reserved bits (i.e. unused bits from parameters/options) will now check these bits are set to zero
- Fixed issue that prevented use of the UserData page
- Added workaround for a Cortex-M33 errata when exercising TrustZone debug lock bits
- Aligned DCI success status codes with EFR32xG21 products
- Resolved debug lock issue

v1.1.1 (first release for EFR32xG22 products)

- Fixed an issue where a device with Secure Boot turned on would not be able to be secure unlocked on secure boot failure
- Fixed issue preventing Secure Unlock to function properly on Secure Boot failure

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.