Secure Engine Firmware Release Notes
For xG21 Products

Secure Engine (SE) 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

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

SE 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 SE 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:

- EFR32xG21 SoCs
- xGM21 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

v1.2.16

- Improved stability for xG21-C and xG21-D when operating close to -40°C.
- Adjusted the upper temperature limit for the temperature tamper signal to reflect the maximum junction temperature (135°C) instead of the maximum ambient temperature (125°C).

v1.2.15

- Reduced EM2 current consumption for the xG21-C and xG21-D family of devices.

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.
- Fixed a bug where using custom domain curves larger than 40 bytes would lead to a reset.

v1.2.13

- Security and stability fixes

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
- Increased internal watchdog timeout to prevent long operations from being interrupted
- Make the Device Erase command break the boot loop that could occur after a failed host upgrade
- Fixed an issue with the recovery logic following an interrupted host upgrade. The issue could quickly lead to the device outspending its allowed attempts, leaving it in an unusable state.
- X25519 and Ed25519 algorithms, along with related key management functionality, is now supported on Secure Vault Mid devices
- Added explicit validation of input and output length for commands that are sent without any input/output buffers from the mailbox interface. This causes a change in behavior of the SE Manager function `sl_se_roll_challenge`, which has been fixed in Gecko SDK v3.2.2. When applying the SE firmware upgrade to a device with an application compiled with an older version of the SDK, be aware that `sl_se_roll_challenge` will return an error code after the SE firmware upgrade, until the application is recompiled with the updated SDK.
- GCM support for input lengths larger than 0.5 GB.

v1.2.9

- Fixed an issue where the SE would fail to generate the correct public key for a given Ed25519 private key, affecting the 'export public key', 'generate signature', and 'verify signature' operations when called with a private key buffer. This bug exists in SE firmware versions between 1.2.2 and 1.2.8 (inclusive).
- Removed SE Manager function sl_se_upgrade_status_clear() and the corresponding functionality from the SE firmware. This function behaves erratically on older versions and was not in use by Gecko SDK components.

v1.2.8

- Fixed potential issue with the strength of crypto countermeasures under certain conditions
- Fixed a bug where the SE would fault on generating keys of non-word-aligned size
- Security and stability fixes

v1.2.6

- **Critical** stability fix to prevent devices becoming inoperable under certain conditions. A device whose SE 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
- Fixes an issue where tamper levels are not set to default level after issuing the disable tamper command

v1.2.4

- Allow EFR32xG21B devices to sign external content using the MCU identity key
- Fixed stability issue with the debug restriction command

v1.2.3

- Fixed issue where a public key could not be derived from a P-521 private key

- Maximum size for a 'RAW' key is now 512 bytes (previously 612)
- Fixed an issue preventing HMAC with null input
- Improved error handling in AES encryption and decryption operations
- Added certificate read support to mailbox interface
- The ReadRSTCAUSE command will now always return the reset cause observed at the previous boot
- When tamper reset threshold is reached, the device is now held in debug mode
- Security and stability fixes

v1.2.2

- 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.
- Fixed potential fault in the JPakeGenSessionKey command related to invalid password length
- Improved robustness of wrapped and volatile key handling
- Fixed potential starvation issue on the SE command interfaces
- Support for EFR32xG21 with die revision A0 is now removed. These were early engineering samples, not intended for production use. To check whether your device is revision A0, connect to the device using Simplicity Commander.
- Added support for Montgomery-type keys for use in ECDH on Vault parts
- Security and stability fixes

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
- Improved handling of run-time errors in the secure subsystem
- Volatile keys can now be used for multiple operations
- 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.
- Improved stability for REGDIS enable/disable command
- Improved EM2 entry/exit delay
- Added DCI command SE_COMMAND_READ_OTP to read non-reconfigurable user settings from the SE for Secure Boot with RTSL and Tamper Response
- Other security updates

v1.1.8

- Improved root key entropy

v1.1.7

- Security update

v1.1.6

- Stability fixes

v1.1.5

- Stability fixes

v1.1.4

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

v1.1.3

- Improved DCI error reporting on secure boot failure
- Increased reliability during boot-up sequence
- Added support for all allowed GCM tag lengths during GCM decrypt-and-verify
- Added functionality to keep SE awake on demand
- Added command to disable internal LDO (EFP support)
- Commands with reserved bits (i.e. unused bits from parameters/options) will now check these bits are set to zero
- Added workaround for a Cortex-M33 errata when exercising TrustZone debug lock bits

v1.1.2

- Added rollback prevention based on host application version number. The feature is enabled by the anti-rollback flag is in OTP settings

v1.1.1

- Fixed issue with having both Secure Boot and Secure Debug key installed, leading to problems with Secure Debug
- Fixed issue preventing Secure Unlock to function properly on Secure Boot failure
- If the SE has successfully booted an image that was signed with a certificate with version > 0, direct signing of a Secure Boot binary is no longer permitted by the SE. The SECURE_BOOT_VERIFY_CERTIFICATE flag in OTP can be used to require the use of certificates and disables the option to use directly signed binaries.

v1.1.0
- Added Secure Boot with RTSL (Root of Trust and Secure Loader) functionality
- Added extra protection against key leakage
- Added option to lock flash pages that have been validated by Secure Boot
- Other security fixes

v1.0.2
- Fixed an issue were subsequent DCI commands could share input parameters
- J-PAKE commands returns more granular error codes
- Fixed an issue where a J-PAKE input buffer could be overflown
- Fixed an issue where a device erase command could crash the device
- NVM sub-system longevity improvement

v1.0.1
- Security update fixing TRNG issue

v1.0.0
- GA release

v0.1.7
- Security update

v0.1.6
- DCI 'Get Status' command now returns the actual status of the debug locks in addition to the debug lock configuration

v0.1.5
- An implementation error in the ECDH acceleration code in mbedTLS (used in e.g. BLE) will start to produce an error in SE firmware v0.1.5. The update to ECDH in mbedTLS included in Gecko SDK Suite v2.5.2 resolves the issue. Users of BLE or ECDH separately needs to update to Gecko SDK Suite v2.5.2 before upgrading to an SE firmware version beyond v0.1.4.
- Fix potential data corruption when installing keys through host mailbox interface
- Increased timeout for DCI operations
- Security and stability updates

v0.1.4
- Improved responsiveness in EM2

v0.1.3
- Improved power consumption while sleeping in EM1
- Security and stability updates

v0.1.2
- Improved stability of device erase command

v0.1.1
- Energy consumption in EM2 improved for typical temperature range
- Improved various status codes for debug commands
- When using secure debug unlock, the debug port maintains the unlocked state across soft reset

v0.1.0 (first release for EFR32xG21 products)
- Stability update

Known Issues

- The PSA Initial Attestation Token available over mailbox implements the deprecated PSA_IOT_PROFILE_1 profile.
- The lifecycle claim in the PSA Initial Attestation Token is not correctly implemented with respect to the PSA Root of Trust (the SE), resulting in needlessly strict requirements to achieve the SECURED lifecycle state.

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.

4.3 License Information

This product contains the following sub-components, which are included according to their respective licenses:

4.3.1 t_cose

Copyright (c) 2019, Laurence Lundblade

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the copyright holder nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

4.3.2 QCBOR