Secure Engine Firmware Release Notes
For xG25 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:

- EFR32xG25 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

v2.2.5

-   Accept host upgrade attempts where the size of the upgrade binary includes the CRC32 checksum of Gecko Bootloader. This is a mitigation for a defect in Gecko Bootloader present in GSDK versions 3.2.0 through 3.2.9 and 4.0.0 through 4.0.2.

v2.2.4

-   Improved current consumption of Active Mode. Making active mode only exitable through the interface with which it was entered.
-   Improved SE wakeup time from EM2/3.
-   Time to execute a device erase has been reduced by ~50 percent.
-   Fixed a bug where flashing a new application was not possible after a device erase, unless the device was reset beforehand.
-   Fixed a bug where the setting of "Enable M33 Lockup reset" bit in EMU led to timeout when issuing a device erase command.
-   Reduced secure boot time by 0.2-0.4 ms when considering a 0x6000 byte host application.

v2.2.2

-   Improved boot time by about 1 ms.
-   Reduced duration of Secure Boot validation of host application by around 1 ms depending on application size.
-   Fixed an issue where data in internal SE flash was encrypted using an uninitialized IV.
-   Fixed an issue where the get_tamper_reset_cause command would return an incorrect value when the tamper reset threshold in OTP was configured to 0.
-   Fixed an issue where certain debug restrictions could lead to a boot error on soft resets.

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 get_tamper_reset_cause command to output which tamper source caused a tamper reset. The command is available over mailbox.

v2.2.0

-   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.
-   Fixed a bug where TrustZone specific debug locks where not retained across soft resets after being opened through Secure Debug unlock.
-   Fixed an issue where executing a host upgrade with a large image could cause a watchdog timeout.
-   Security and stability updates

v2.1.7

-   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
-   X25519 and Ed25519 algorithms, along with related key management functionality, is now supported on Secure Vault Mid devices
-   Randomize the operating frequency between every command also when active mode is enabled
-   GCM support for input lengths larger than 0.5 GB

v2.1.5

-   Startup time improvements. For typical device configurations, this change could save 5-6 ms of boot time. With Secure Boot enabled and debug ports locked, the estimated boot time savings can be as much as 10 ms. Prior to this change, startup time could increase over time based on the history of the device. For example, performing a successful host upgrade or device erase command on a debug locked part could permanently increase boot time by a few milliseconds. In a worst-case scenario, these effects could add up to a total of 300 ms additional boot time.

v2.1.4

-   Fixed a bug where using volatile keys together with a custom ECC curve did not work
-   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.

```
    -    Improved fault injection hardening
```

v2.1.3 (first release for EFR32xG25 products)
```
    -    Secure Vault High features
```

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

Copyright (c) 2016-2018, The Linux Foundation.
Copyright (c) 2018-2020, 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 Linux Foundation nor the names of its contributors, nor the name "Laurence Lundblade" may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER 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.