



Secure Engine Firmware Release Notes

For SixG301 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	1
1.1 Compatible Products	1
1.2 Support	1
Features and Security Updates	2
Known Issues	4
Legal	5
4.1 Disclaimer	5
4.2 Trademark Information	5
4.3 License Information	5
4.3.1 t_cose	5
4.3.2 QCBOR	6
4.3.3 P99	6



SILICON LABS

Using This Release

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

SE firmware upgrade images are installed with SiSDK Suite in Simplicity Studio. This release contains the following.

- Upgrade image for Gecko Bootloader (.seuv2 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 SiSDK 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/5.1.2/platform-security-api/sl-se-manager>.

1.1 Compatible Products

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

- SixG301 products

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

v3.3.6

- Flash encryption stabilization. This fixes issues with flash encryption in either EXiP or AXiP modes. In either of the modes, data could be incorrectly encrypted before written to the external flash. This was a rare issue, only occurring once every few thousand code region write attempts.
- Users are advised to upgrade their SE FW to v3.3.5 before performing application or bootloader upgrades. Bundling an SE FW upgrade into the same GBL as other upgrade files is also okay, as the SE FW upgrade is always applied first by the bootloader.
- Bug fix in the DeleteKey command for KSU keys. The command erroneously prevented the KSU from being used after DeleteKey was called. This issue is now fixed.

v3.3.2

- Updates to the PSA Initial Attestation Token creation and Secure Debug unlock.
 - o The lifecycle claim is updated to contain information on whether or not the SE CPU has been unlocked during manufacturing.
 - o A Secure Debug unlock of the SE CPU after the device has experienced any customer init commands is now tracked permanently in OTP.
 - o The device will erase its attestation keys and will never generate new attestation tokens.
- An EnterEOL command has been added. This command allows the user to trigger a full erasure of all SE protected secrets and optionally log a trace code in OTP. The device will not be operational after entering EOL.
- A command to wipe the host AES key used by the SiSDK Bootloader is added. This command allows users to erase their secrets from OTP without rendering the device non-functional.
- Upgrade to ROM patch 5.3
- Improved the polling operation for the external flash to optimize flash erase speed and response time for flash pause and resume commands.
- Improved handling of new commands when flash operations are in progress.
- Allow transfers to KSU if the DPA_REQUIRED flag is set in the key metadata, as all KSU consumers have DPA protections.

v3.3.1

- Enables DPA countermeasures for EdDSA and Montgomery point multiplication.
 - o With DPA CM enabled, only points on the curve are supported as public keys for ECDH (Curve25519). Attempting other values as public keys will result in unusable output. Valid ECDH public keys will always be points on the curve.
 - o DPA countermeasures increase the duration of these operations with approximately 20 %.

v3.3.0

- Added non-blocking command options for flash write and erase commands. The non-blocking options make the command return immediately. To check the status of the flash operation, the user must check the GetFlashStatus command.
 - o Commands that erase a code region require that the flash status is checked by the user before responding to any other commands.
 - o While flash is busy, all SE commands not related to flash handling are unavailable.
- Added new commands related to flash handling: GetFlashStatus, PauseFlash and ResumeFlash.
- Updated key metadata format for KSU, including supporting crypto engine ID for transfers and imports to KSU.
- Fixed a bug in the HMAC multipart update command that reported BUS_ERROR

v3.2.0

- Added support for HMAC-AES-MMO.
- GetOTPRollbackCounter command can now read out SE rollback counter.
- Added new return status: EOL(0xE). This status is returned when the SE has run out of OTP space to update its rollback counter.
- Fixed an issue where the SE could get into a bad state if Debug Lock was applied after both Device Erase and Secure Debug Unlock was disabled.
- Security updates.

v3.1.1

- Improved bootup time for devices with a full MTP storage area.
- Added command for partial erase of host region.
- Added command for disabling code region AXiP IV roll, permanently entering a non-secure state.
- Support transferring NVM3 key to KSURAM.
- Fix an issue where the device would reset about 240 ms after waking up from EM4.

- Improved QSPI calibration logic.
- Updates ROM patch to 5.2.

v3.1.0

- Support for Secure Boot, on-par with Series 2.
 - o Note that the "narrow" and "wide" page lock options no longer make sense for Series 3 and are removed.
 - o In order to validate the Secure Boot signature, SE FW requires that region 0 is locked. This can be achieved through "commander security closeregion 0" command in Simplicity Commander. Only close a region after flashing a validly signed application to region 0.
- EraseHostFlash command is now available through mailbox.
- ReadSecureTraceFlags command is now available through mailbox.
- Get/IncrementHostRollbackCounter command is now available through mailbox.
- KSU support.
- Unlocking a host code region is no longer possible to do through the ApplyCodeRegionConfig command. To unlock a region, one must either erase the region over mailbox or trigger a device erase command.
- System wide bus lock is no longer applied when changing QSPI clock configuration.
- Re-calibration of QSPI delay line on delay tap drift.

v3.0.1

- Fixed a bug where the DeviceErase command could brick a device.

v3.0.0

- Initial release

Known Issues

- The PSA Initial Attestation Token available over mailbox implements the deprecated `PSA_IOT_PROFILE_1` profile.

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®, ISModem®, 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.

4.3.3 P99

Copyright (c) 2010-2012, Jens Gustedt, INRIA, France, <http://www.inria.fr/>.

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License.

You may obtain a copy of the License at

<http://www.apache.org/licenses/LICENSE-2.0>

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

See the License for the specific language governing permissions and limitations under the License.