Silicon Labs is a leading vendor in Bluetooth hardware and software technologies, used in products such as sports and fitness, consumer electronics, beacons, and smart home applications. The core SDK is an advanced Bluetooth 5.3 compliant stack that provides all of the core functionality along with multiple API to simplify development. The core functionality offers both standalone mode allowing a developer to create and run their application directly on the SoC, or in NCP mode allowing for the use of an external host MCU.

These release notes cover SDK version(s):

4.0.0.0 GA released June 8, 2022

**Compatibility and Use Notices**

For information about security updates and notices, see the Security chapter of the Gecko Platform Release notes installed with this SDK or on the TECH DOCS tab on https://www.silabs.com/developers/bluetooth-low-energy. Silicon Labs also strongly recommends that you subscribe to Security Advisories for up-to-date information. For instructions as well as notes on using Secure Vault features, or if you are new to the Silicon Labs Bluetooth SDK, see Using This Release.

**Compatible Compilers:**

IAR Embedded Workbench for ARM (IAR-EWARM) version 9.20.4.

- Using wine to build with the iarBuild.exe command line utility or IAR Embedded Workbench GUI on macOS or Linux could result in incorrect files being used due to collisions in wine’s hashing algorithm for generating short file names.
- Customers on macOS or Linux are advised not to build with IAR outside of Simplicity Studio. Customers who do should carefully verify that the correct files are being used.

GCC (The GNU Compiler Collection) version 10.3-2021.10, provided with Simplicity Studio.
1 New Items

1.1 New Features

Added in release 4.0.0.0

Apploader as Bootloader communication plugin on EFR32M|BG2x devices

Beginning with Bluetooth SDK version 4.0.x on EFR32M|BG2x devices, the AppLoader is merged with Gecko Bootloader as a communication plugin. The binary size of the combined functionality could be 16K smaller than the size of standalone Apploader and default Bootloader binaries. See AN1086: Using the Gecko Bootloader with Silicon Labs Bluetooth Applications for the details and how to migrate from old version of Bootloader and Apploader.

The Apploader remains as a standalone application on EFR32M|BG1x devices.

Directed Advertising feature

The Bluetooth stack supports legacy and extended directed advertising PDUs.

L2CAP Connection Oriented Channels feature

The Bluetooth stack supports L2CAP Connection-Oriented Channels in the LE Credit Based Flow Control mode.

New components for legacy and extended scanner

The Bluetooth stack has two new components: the `bluetooth_feature_legacy_scanner` for scanning legacy advertising PDUs, and the `bluetooth_feature_extended_scanner` for scanning legacy and extended advertising PDUs. They supersede some scanner functionality in the base `bluetooth_feature_scanner` feature.

If the application does not need to scan extended advertising PDUs, by using the `bluetooth_feature_legacy_scanner` and excluding the `bluetooth_feature_extended_scanner`, the number of received advertisement reports are reduced if devices advertising extended advertising PDUs are in the radio range. Another benefit is reduced application size by eliminating the stack functionalities for the `bluetooth_feature_extended_scanner`.

The `sl_bt_scanner_set_timing()` and `sl_bt_scanner_set_mode()` commands are not available to use if either the `bluetooth_feature_legacy_scanner` or `bluetooth_feature_extended_scanner` component is included. They are superseded by the `sl_bt_scanner_set_parameters()` command.

Alpha Periodic Advertising Synchronization Transfer (PAST)

The Periodic Advertising Synchronization Transfer (PAST) feature is provided as Alpha. New components and APIs include `bluetooth_feature_past_receiver`, `bluetooth_featureAdvertiserPast`, `bluetooth_featureSyncPast`, and BGAPI classes "PAST Receiver", "Advertiser PAST" and "Sync PAST". The PAST feature is for evaluation purpose and the APIs are subject to change in a future release.

New option in command sl_bt_sm_configure

A new option is added in the `sl_bt_sm_configure()` command to require OOB data present from both devices when using secure connections OOB pairing.

Polarized antenna support in aoa_locator example

The AoA locator host example is extended with dual polarized antenna support.

New sample applications and components

New `bt_soc_app_ota_dfu` example is added to demonstrate background over-the-air (OTA) device-firmware-update (DFU) from the user application. New `app_ota_dfu` component is introduced for supporting freely adding the application OTA DFU to any component (e.g., `bt_soc_empty`).

Since the `app_ota_dfu` and `in_place_ota_dfu` (originally `ota_dfu`) components realize the same feature, only one can be selected by a project. Currently the `app_ota_dfu` component is an optional alternative to the `in_place_ota_dfu`.

New components `ots_server_core`, `ots_client` and `ots_server` are added for Object Transfer Service (Alpha).

New example is added for Certificate-Based Bluetooth Authentication and Pairing.

New example Certificate Signing Request Generator is added.
Custom vendor commands in RCP application

Custom HCI Command handlers are supported in RCP applications.

A new vendor-specific HCI command is added for specifying the PHYs that are allowed for use in extended scanning.

**COEX signal identifier on EFR32M|BG24**

The COEX signal identifier is supported on EFR32M|BG24.

### 1.2 New APIs

**Added in release 4.0.0.0**

Command `sl_bt_legacy_advertiser_start_directed`: Start directed legacy advertising on an advertising set.

Command `sl_bt_extended_advertiser_start_directed`: Start directed extended advertising on an advertising set.

**Event sl_bt_evt_scanner_legacy_advertisement_report**: Reports an advertising data or scan response packet from an advertising device that uses legacy advertising PDUs. This event is used for reporting advertisements only if the application includes the `bluetooth_feature_legacy_scanner` or `bluetooth_feature_extended_scanner` component.

**Event sl_bt_evt_scanner_extended_advertisement_report**: Reports an advertising or scan response packet from an advertising device that uses extended advertising PDUs. This event is used for reporting advertisements only if the application includes the `bluetooth_feature_extended_scanner` component.

Command `sl_bt_l2cap_open_le_channel`: Create and configure an L2CAP channel on a Bluetooth connection using the LE credit-based connection request packet.

Command `sl_bt_l2cap_send_le_channel_open_response`: Send an LE credit based connection response to an LE credit-based connection request.

Command `sl_bt_l2cap_channel_send_data`: Send data to the peer channel endpoint on a Bluetooth connection.

Command `sl_bt_l2cap_channel_send_credit`: Send flow control credits to the peer channel endpoint indicating that the local channel endpoint is capable of receiving more data.

Command `sl_bt_l2cap_close_channel`: Send a disconnect request to close a credit-based logical channel.

**Event sl_bt_evt_l2cap_le_channel_open_request**: Indicates that an LE credit-based connection request on a Bluetooth connection is received.

**Event sl_bt_evt_l2cap_le_channel_open_response**: Indicates that an LE credit-based connection response is received.

**Event sl_bt_evt_l2cap_le_channel_open_data**: Indicates that data is received on a channel.

**Event sl_bt_evt_l2cap_le_channel_credit**: Indicates that flow control credits are received on a channel informing that the peer channel endpoint is capable of receiving more data.

**Event sl_bt_evt_l2cap_le_channel_closed**: Indicates that a credit-based logical channel is closed by the local or peer device.

**Event sl_bt_evt_l2cap_command_rejected**: Indicates that the peer device rejected a command.

Command `sl_bt_connection_get_security_status`: Get the security mode, encryption key size and bonding handle of a Bluetooth connection.

Command `sl_bt_scanner_set_parameters`: Provides the functionality of `sl_bt_scanner_set_timing()` and `sl_bt_scanner_set_mode()`.

**New option in command sl_bt_sm_configure**: Bit 6 for configuring that OOB data from both devices is required when using secure connections OOB pairing.
2 Improvements

2.1 Changed Items

**Changed in release 4.0.0.0**

**Assertion on Bluetooth stack initialization failure**

An error returned by the Bluetooth stack initialization function `sl_bt_stack_init` is now asserted using the EFM_ASSERT provided by the sl_assert component.

**Hardware revision in sl(bt_evt_system_boot) event**

The hardware revision information is reported in the boot event `sl_bt_evt_system_boot`. The major of the revision is in the the most-significant byte and the minor in the the least-significant byte.

**Radio PA removed from the Bluetooth configuration**

The radio PA configuration item has been removed from the Bluetooth configuration data structure `sl bt configuration_t`. The RAIL PA configuration is directly used by Bluetooth beginning with this release.

**Code optimization in the Bluetooth stack and example applications**

The Bluetooth stack has more code optimization in this release. Some example applications, such as `bt_soc_empty`, are optimized by using better-modularized software components. The size reduction could be from 2 to 7 KB depending on the device variants.

**Renamed examples**

All examples are renamed to follow new common naming convention.

**Refactored multilocator angle correlation**

Correlated angles component is refactored and renamed into a new, cleaner component: `angle_queue`.

**Deviation value field in AoA host examples**

Standard deviation value fields have been added to angle and position messages in the AoA host examples. Angle correction message format has been replaced with common angle message format.

**New dependency in RCP HCI**

In order to get a response to `HCI_Le_Read_Phy`, `HCI_Le_Set_Default_Phy` or `HCI_Le_Set_Phy` commands, the RCP-HCI application now requires the `bluetooth_feature_connection_phy_update` feature. This component conflicts with efr32M|BG1 devices because they only support LE 1M PHY.

**Security Disabled on RCP_CPC**

The security feature for CPC on RCP_CPC examples is disabled to save RAM.

To enable security, add the CPC SECURITY component.

2.2 Changed APIs

**Changed in release 4.0.0.0**

**Command sl(bt_system_reset)**

On EFR32M|BG2x devices, the `sl bt_system_reset()` command can only be used to boot to application mode. To boot to DFU mode, use the Bootloader API `bootloader_rebootAndInstall()`.

**Command sl(bt scanner_stop)**

This command now returns `SL_STATUS_OK` if the scanner is not enabled. Previously error `SL_STATUS_INVALID_STATE` was returned.
Command `sl_bt OTA_set_device_name`
This command no longer supports EFR32M|BG2x devices as the result of Apploader merging with Bootloader.

Command `sl_bt OTA_set_advertising_data`
This command no longer supports EFR32M|BG2x devices as the result of Apploader merging with Bootloader.

Command `sl_bt OTA_set_configuration`
This command no longer supports EFR32M|BG2x devices as the result of Apploader merging with Bootloader.
### Fixed Issues

**Fixed in release 4.0.0.0**

<table>
<thead>
<tr>
<th>ID #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>222747</td>
<td>There has been a feature request for the Apploader to be able to enter and stay in DFU mode for a certain time period on startup. On EFR32M</td>
</tr>
<tr>
<td>271312</td>
<td>There has been a feature request for the Apploader to support setting the TX power for OTA DFU. On EFR32M</td>
</tr>
<tr>
<td>7455025</td>
<td>There has been a feature request for the Apploader to support GPIO control in DFU mode. On EFR32M</td>
</tr>
<tr>
<td>290592</td>
<td>There has been an issue that MGM12P has poor signal strength when doing OTA with Apploader. On EFR32M</td>
</tr>
<tr>
<td>337467</td>
<td>There has been an issue that the OTA DFU using Apploader fails on devices that do not use DCDC. On EFR32M</td>
</tr>
<tr>
<td>742632</td>
<td>Fix a memory leak in the Bluetooth bonding OOB mode on EFR32M</td>
</tr>
<tr>
<td>744709</td>
<td>Fix a scanning issue with BGM220P and BGM220S modules in RCP applications.</td>
</tr>
<tr>
<td>753951</td>
<td>Fix an issue that opening a connection to an advertisement using extended advertising PDUs sometimes does not succeed.</td>
</tr>
<tr>
<td>757736</td>
<td>The aoa_locator host example now tolerates the failure of a periodic advertising synchronization opening when the number of synchronizations has reached the configured maximum value in SL_BT_CONFIG_MAX_PERIODIC_ADVERTISING_SYNC.</td>
</tr>
<tr>
<td>757740</td>
<td>The aoa_locator host example now tolerates the failure of a Bluetooth connection opening when the number of connections has reached the configured maximum value in SL_BT_CONFIG_MAX_CONNECTIONS.</td>
</tr>
<tr>
<td>774799</td>
<td>Fix IAR compilation warnings of unreachable code in the simple_timer_freertos and simple_timer_freertos_static components.</td>
</tr>
<tr>
<td>815083</td>
<td>Fix the issue in coex commands that causes the request pin held high during the BLE scan dwell time.</td>
</tr>
<tr>
<td>829662</td>
<td>Fix an issue that the coex BGAPI class is not added even if the RAIL Utility Coexistence component is installed. This issue caused unfunctional coex API calls at run time.</td>
</tr>
<tr>
<td>831505</td>
<td>Fix the issue that the advertiser only sends advertisement packets in one channel and does not respond to scan requests in the PTA mode.</td>
</tr>
<tr>
<td>835390</td>
<td>The Network Analyzer can now defragment Bluetooth extended advertisement packets correctly.</td>
</tr>
<tr>
<td>835393</td>
<td>The Network Analyzer can now detect Auxiliary Scan Responses correctly.</td>
</tr>
<tr>
<td>840603</td>
<td>Fix a memory allocation issue during parsing the antenna array configuration in the positioning host example.</td>
</tr>
<tr>
<td>842846</td>
<td>Fix an issue that the stack does not use the CE length values configured by the user application in responding to an L2CAP Connection Parameter Update request.</td>
</tr>
<tr>
<td>842924</td>
<td>Fix an issue on LE Coded PHY on EFR32M</td>
</tr>
</tbody>
</table>
## Known Issues in the Current Release

Issues in bold were added since the previous release. If you have missed a release, recent release notes are available on [https://www.silabs.com/developers/bluetooth-low-energy](https://www.silabs.com/developers/bluetooth-low-energy) in the Tech Docs tab.

<table>
<thead>
<tr>
<th>ID #</th>
<th>Description</th>
<th>Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>361592</td>
<td>The sync_data event does not report TX power.</td>
<td>None</td>
</tr>
<tr>
<td>368403</td>
<td>If setting CTE interval to 1, a CTE request should be sent in every connection interval. But it is sent only in every second connection interval.</td>
<td>None</td>
</tr>
<tr>
<td>641122</td>
<td>The Bluetooth stack component does not provide a configuration for RF antenna path.</td>
<td>This is an issue specifically for BGM210P. One workaround is to manually update the configuration in sl_bluetooth_config.h in text edit mode. If the OTA with Apploader is used, include the bluetooth_feature_ota_config component in application project. Call command sl_bt_ota_set_rf_path() to set the RF path for OTA mode.</td>
</tr>
<tr>
<td>650079</td>
<td>LE 2M PHY on EFR32[B</td>
<td>M]G12 and EFR32[B</td>
</tr>
<tr>
<td>682198</td>
<td>The Bluetooth stack has an interoperability issue on the 2M PHY with a Windows PC.</td>
<td>No workaround exists. For application development and testing, the disconnection can be avoided by disabling 2M PHY with sl_bt_connection_set_preferred_phy() or sl_bt_connection_set_default_preferred_phy().</td>
</tr>
<tr>
<td>730692</td>
<td>4-7% packet error rate is observed on EFR32M</td>
<td>BG13 devices when RSSI is between -25 and -10 dBm. The PER is nominal (as per the datasheet) both above and below this range.</td>
</tr>
<tr>
<td>756253</td>
<td>The RSSI value on a Bluetooth connection returned by the Bluetooth API is incorrect on EFR32M</td>
<td>B1, EFR32M</td>
</tr>
<tr>
<td>756562</td>
<td>The Bluetooth scanning has an issue on the LE Coded PHY on EFR32M</td>
<td>BG21 devices. After some time (minutes or hours) of scanning, a RAIL assertion (RAIL_ASSERT_FAILED_UNEXPECTED_STATE_RX_FIFO) may happen and the scanning stops.</td>
</tr>
<tr>
<td>773951</td>
<td>On EFR32M</td>
<td>BG24 devices, the CTE feature using 38.4MHz HFXO on the LE 2M PHY has an IQ sampling robustness issue that causes angle errors.</td>
</tr>
<tr>
<td>845506</td>
<td>When the Bluetooth_feature_afh component for AFH is included, the feature initialization always enables AFH.</td>
<td>To include the component but not to enable AFH at device boot, change the parameter value from 1 to 0 in the function call of sl_btctrl_init_afh() in sl_bt_stack_init.c.</td>
</tr>
<tr>
<td>848767</td>
<td>The documentation of the Apploader component is labeled as &quot;AppLoader application binary for EFR series 1 devices&quot;. However this component is also required by series 2 devices for reserving enough flash space for the new Bootloader that contains an Apploader library as the communication plugin.</td>
<td>Not required</td>
</tr>
</tbody>
</table>
5 Deprecated Items

**Deprecated in release 4.0.0.0**

Command `sl_btAdvertiser_set_phy`: deprecated and replaced by `sl_bt_extendedAdvertiser_set_phy()`.

Command `sl_btAdvertiser_set_configuration`: deprecated and replaced by `sl_btAdvertiser_configure()`.

Command `sl_btAdvertiser_clear_configuration`: Deprecated and replaced by `sl_btAdvertiser_configure()`.

Command `sl_btAdvertiser_set_data`: Deprecated and replaced by `sl_bt_legacyAdvertiser_set_data()` for legacy advertising PDUs, `sl_bt_extendedAdvertiser_set_data()` for extended advertising PDUs, and `sl_bt_periodicAdvertiser_set_data()` for periodic advertising PDUs.

Command `sl_btAdvertiser_set_long_data`: Deprecated and replaced by `sl_bt_extendedAdvertiser_set_long_data()` for extended advertising PDUs and `sl_bt_periodicAdvertiser_set_long_data()` for periodic advertising PDUs.

Command `sl_btAdvertiser_start`: Deprecated and replaced by `sl_bt_legacyAdvertiser_start()` and `sl_bt_extendedAdvertiser_start()`.

Command `sl_btAdvertiser_start_periodic_advertising`: Deprecated and replaced by `sl_bt_periodicAdvertiser_start()`.

Command `sl_btAdvertiser_stop_periodic_advertising`: Deprecated and replaced by `sl_bt_periodicAdvertiser_stop()`.

Commands `sl_btScanner_set_timing` and `sl_btScanner_set_mode`: This is a pre notice that the functionality of these two commands are replaced by new command `sl_btScanner_set_parameters()` and they will enter the deprecation notice period in the next major SDK release.
6 Removed Items

**Removed from release 4.0.0.0**

Example ncp_empty is removed, and replaced by bt_ncp example.

**Removed APIs**

The following APIs had been in deprecation notice period in the recent SDK versions, and the information of replacements can be found in v3.3 API reference manual.

- Command `sl_bt_sm_list_bonding_entry`
- Command `sl_bt_sm_list_all_bondings`
- Command `sl_bt_sm_set_oob_data`
- Command `sl_bt_sm_use_sc_oob`
- Command `sl_bt_sm_set_sc_remote_oob_data`
- Command `sl_bt_system_set_soft_timer`
7 Multiprotocol Gateway and RCP

7.1 New Items

Added in release 4.0.0.0

A new concurrent multiprotocol configuration is available: Zigbee NCP and OpenThread RCP running concurrently on the EFR32, using the Co-Processor Communication (CPC) architecture. It is released as alpha quality. See AN1333: Running Zigbee, OpenThread, and Bluetooth Concurrently on a Linux Host with a Multiprotocol RCP for details.

7.2 Improvements

Changed in release 4.0.0.0

CPC security is now enabled by default in the cpcd.conf file and in the SLCP project files. This means data sent over the serial line between the host and the EFR32 is encrypted. A security commissioning step is required to bind the host to the EFR32. See https://github.com/SiliconLabs/cpc-daemon/blob/main/readme.md for details.

For convenience, the run.sh script in app/host/multiprotocol/ zigbeed/multiprotocol-container/ includes a -K argument for commissioning cpcd security when using the multiprotocol docker container.

The multiprotocol container has been upgraded to use ubuntu 22.04 and BlueZ 5.64.

The zigbee_trust_center_backup component now supports migrating from a Zigbee Host + NCP setup to a Zigbee Host + Zigbeed + RCP setup. See AN1333: Running Zigbee, OpenThread, and Bluetooth Concurrently on a Linux Host with a Multiprotocol RCP for details.

Zigbeed built from GSDK sources no longer requires the /accept_silabs_msla_file at runtime. Only the Zigbeed binary from the multiprotocol docker container requires it.

7.3 Fixed Issues

Fixed in release 4.0.0.0

<table>
<thead>
<tr>
<th>ID #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>760596</td>
<td>Reduced the CPU consumption of Zigbeed when it is idle.</td>
</tr>
<tr>
<td>811566</td>
<td>Fixed an issue where Zigbee sleepy end devices failed to join an RCP parent.</td>
</tr>
<tr>
<td>817698</td>
<td>Fixed a Zigbeed crash due to a null buffer in the lower mac layer.</td>
</tr>
<tr>
<td>822233</td>
<td>Fixed an issue that caused dropped CPC packets over VCOM, especially at higher baud rates.</td>
</tr>
<tr>
<td>829614</td>
<td>The multi-PAN/multiprotocol 802.15.4 RCP now sets the radio tx power to the maximum of the power levels requested by all 15.4 host applications. This avoids the problem of one application reducing the power and inadvertently causing network connectivity problems for the other application.</td>
</tr>
<tr>
<td>830596</td>
<td>Fixed an issue where joining a sleepy end device to the multiprotocol RCP caused Z3Gateway to crash in some circumstances.</td>
</tr>
<tr>
<td>831689</td>
<td>Fixed an issue in Zigbeed that resulted in a fixed pan id and other parameters being chosen when forming a network.</td>
</tr>
</tbody>
</table>

7.4 Known Issues in the Current Release

<table>
<thead>
<tr>
<th>ID #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>828785</td>
<td>There is a known issue with the cpc-hci-bridge that causes the second HCI packet to be dropped if BlueZ sends two HCI packets to the RCP in rapid succession.</td>
</tr>
</tbody>
</table>

silabs.com | Building a more connected world.  Bluetooth 4.0.0.0 | 10
### 7.5 Deprecated Items

None

### 7.6 Removed Items

**Removed in release 4.0.0.0**

Pre-built ARM binaries for multiprotocol host applications are no longer distributed within the GSDK (cpcd, otbr-agent, zigbeed, Z3Gateway, etc). These should be built from sources on the target platform using the instructions in AN1333: *Running Zigbee, OpenThread, and Bluetooth Concurrently on a Linux Host with a Multiprotocol RCP*.

A copy of sl_cpc.h that was being included in the OpenThread sources as a convenience has been removed. This header file is placed in the standard system location when cpcd is installed.

<table>
<thead>
<tr>
<th>ID #</th>
<th>Description</th>
<th>Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>829675</td>
<td>Bi-directional Green Power Devices can’t pair with Z3GatewayGPCombo + Zigbeed + RCP.</td>
<td>A fix is being worked on for the next patch release.</td>
</tr>
<tr>
<td>834191</td>
<td>There is a known issue with the cpc-hci-bridge consuming excessive CPU time.</td>
<td>A fix is targeted for the next patch release.</td>
</tr>
<tr>
<td>811732</td>
<td>Custom token support is not available when using Zigbeed.</td>
<td>Support is planned in a future release.</td>
</tr>
</tbody>
</table>
8 Using This Release

This release contains the following
- Silicon Labs Bluetooth stack library
- Bluetooth sample applications

For more information about the Bluetooth SDK see QSG169: Bluetooth® SDK v3.x Quick Start Guide. If you are new to Bluetooth see UG103.14: Bluetooth LE Fundamentals.

8.1 Installation and Use

The Bluetooth SDK is provided as part of the Gecko SDK (GSDK), the suite of Silicon Labs SDKs. To quickly get started with the GSDK, install Simplicity Studio 5, which will set up your development environment and walk you through GSDK installation. Simplicity Studio 5 includes everything needed for IoT product development with Silicon Labs devices, including a resource and project launcher, software configuration tools, full IDE with GNU toolchain, and analysis tools. Installation instructions are provided in the online Simplicity Studio 5 User’s Guide.

Alternatively, Gecko SDK may be installed manually by downloading or cloning the latest from GitHub. See https://github.com/SiliconLabs/gecko_sdk for more information.

Simplicity Studio installs the GSDK by default in:
- (Windows): C:\Users\<NAME>\SimplicityStudio\SDKs\gecko_sdk
- (MacOS): /Users/<NAME>/SimplicityStudio/SDKs/gecko_sdk

Documentation specific to the SDK version is installed with the SDK. Additional information can often be found in the knowledge base articles (KBAs). API references and other information about this and earlier releases is available on https://docs.silabs.com/.

8.2 Security Information

Secure Vault Integration

When deployed to Secure Vault High devices, sensitive keys such as the Long Term Key (LTK) are protected using the Secure Vault Key Management functionality. The table below shows the protected keys and their storage protection characteristics.

<table>
<thead>
<tr>
<th>Wrapped Key</th>
<th>Exportable / Non-Exportable</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Long Term Key (LTK)</td>
<td>Non-Exportable</td>
<td></td>
</tr>
<tr>
<td>Local Long Term Key (legacy only)</td>
<td>Non-Exportable</td>
<td></td>
</tr>
<tr>
<td>Remote Identity Resolving Key (IRK)</td>
<td>Exportable</td>
<td>Must be Exportable for future compatibility reasons</td>
</tr>
<tr>
<td>Local Identity Resolving Key</td>
<td>Exportable</td>
<td>Must be Exportable because the key is shared with other devices.</td>
</tr>
</tbody>
</table>

Wrapped keys that are marked as “Non-Exportable” can be used but cannot be viewed or shared at runtime.

Wrapped keys that are marked as “Exportable” can be used or shared at runtime but remain encrypted while stored in flash.

For more information on Secure Vault Key Management functionality, see AN1271: Secure Key Storage.
Security Advisories

To subscribe to Security Advisories, log in to the Silicon Labs customer portal, then select Account Home. Click HOME to go to the portal home page and then click the Manage Notifications tile. Make sure that ‘Software/Security Advisory Notices & Product Change Notices (PCNs)’ is checked, and that you are subscribed at minimum for your platform and protocol. Click Save to save any changes.

8.3 Support

Development Kit customers are eligible for training and technical support. Use the Silicon Labs Bluetooth LE web page to obtain information about all Silicon Labs Bluetooth products and services, and to sign up for product support.

You can contact Silicon Laboratories support at http://www.silabs.com/support.
Simplicity Studio

One-click access to MCU and wireless tools, documentation, software, source code libraries & more. Available for Windows, Mac and Linux!