AN1086: Using the Gecko Bootloader with the Silicon Labs *Bluetooth*® Applications

This version of AN1086 has been deprecated.

For the latest version, see docs.silabs.com.

****

This application note includes detailed information on using the Silicon Labs Gecko Bootloader with Silicon Labs Bluetooth applications for Gecko SDK (GSDK) 4.1.0 and higher. If you are not familiar with the basic principles of performing a firmware upgrade, or want more information about upgrading image files, refer to *UG103.6: Bootloader Fundamentals*.

KEY POINTS

- Gecko Bootloader overview
- Using Gecko Bootloader for BGAPI UART DFU
- Using Gecko Bootloader for Bluetooth OTA upgrade
- Using Gecko Bootloader to update firmware from the user application
- Delta DFU
- Post-Build Editor

1. Overview

The Silicon Labs Gecko Bootloader is a common bootloader for all the newer MCUs and wireless MCUs from Silicon Labs. The Gecko Bootloader can be configured to perform a variety of bootloader functions, from device initialization to firmware upgrades. The Gecko Bootloader uses a proprietary format for its upgrade images, called GBL (Gecko Bootloader). These images are produced with the file extension ".gbl". Additional information on the GBL file format is provided in *UG103.6: Bootloader Fundamentals*.

The Gecko Bootloader has a two-stage design, where a minimal first stage bootloader is used to upgrade the main bootloader. The first stage bootloader only contains functionality to read from and write to fixed addresses in internal flash. To perform a main bootloader upgrade, the running main bootloader verifies the integrity and authenticity of the bootloader upgrade image file. The running main bootloader then writes the upgrade image to a fixed location in flash and issues a reboot into the first stage bootloader. The first stage bootloader verifies the integrity of the main bootloader firmware upgrade image, by computing a CRC32 checksum before copying the upgrade image to the main bootloader location.

The Gecko Bootloader can be configured to perform firmware upgrades in standalone mode (also called a standalone bootloader) or in application mode (also called an application bootloader), depending on the software component configuration. Software components can be enabled and configured through the Simplicity Studio IDE.

This document describes how to configure and use the Gecko Bootloader for BGAPI UART device firmware upgrades and for Bluetooth OTA (over-the-air) upgrades.

The Gecko Bootloader does not come bundled into the application download image. Therefore, you must compile and load the bootloader separately from the application image.

2. BGAPI UART Device Firmware Upgrade (DFU)

This is the firmware upgrade used in Network Co-Processor (NCP) Bluetooth applications. For more information on NCP applications, refer to *AN1259: Using the v3.x Silicon Labs Bluetooth® Stack in Network Co-Processor*.

In the BGAPI UART DFU implementation a GBL image containing the new firmware is written to target device using UART as the physical interface.

2.1 UART DFU Options

The target device must be programmed with the Gecko Bootloader sample project **Bootloader - NCP BGAPI UART DFU**. Gecko Bootloader is configured automatically for the selected radio board. The BGAPI UART DFU bootloader is a standalone bootloader, so no storage area needs to be configured. During UART DFU upgrade the bootloader writes the new firmware image directly on top of the old firmware image and therefore no temporary download area is needed.

GPIO Settings

The default settings are suitable for testing with a WSTK (Wireless Starter Kit). These settings can be easily changed by through the Software Components tab. Select the Bootloader UART driver component. Here, Hardware Flow Control can be enabled or disabled, and the baud rate and pinout can be configured.

Flow control settings of the radio board and the WSTK must match. The WSTKs flow control can be configured the following way:

- • In Simplicity Studios Debug Adapters view, right click on the connected device.
- Select Launch Console.
- In the Admin tab, type 'serial vcom config handshake disable/enable', depending on if you want to disable or enable flow control.

NOTE: Add the two figures.

2.2 UART DFU Process

The basic steps involved in the UART DFU, using NCP, are as follows:

1. Boot the target device into DFU mode by calling the bootloader API `bootloader_rebootAndInstall()`. In NCP-mode, this can be achieved by calling `ssl_bt_user_reset_to_dfu()`. When using Series 1 devices, reset into DFU is achieved with `sl_bt_system_reset(1)`. Alternatively, if you have GPIO activation enabled in the bootloader, press the bootloader activation pin while the device is reset.
2. Wait for the `DFU boot` event.
3. Send the command `DFU Flash Set Address` to start the firmware upgrade.
4. Send the entire contents of the GBL upgrade image (using the command `DFU flash upload`).
5. After sending all data, the host sends the command `DFU flash upload finish`.
6. To finalize the upgrade, the host resets the target device into normal mode (by sending `sl_bt_system_reset(0)`).

A detailed description of the DFU-related BGAPI commands is found in the Bluetooth Software API Reference Manual.

At the beginning of the upgrade, the NCP host uses the command `Flash Set Address` to define the start address. The start address shall always be set as zero. During the data upload (step 4 above) the target device calculates the flash offset automatically.

The host does not need to explicitly set any write offset.

The UART DFU procedure may fail if the update image is either corrupted or data upload is interrupted for some reason. Failure due to either of these conditions is detected by the CRC check performed by the UART DFU bootloader before jumping into the main program. In this case, a `dfu_boot_failure` event is sent by the stack. The returned reason codes align with the sl_status codes, as shown in the platform documentation.

2.3 Creating Upgrade Images for the Bluetooth NCP Application

Building a C-based NCP project in Simplicity Studio does not generate the UART DFU upgrade images (GBL files) automatically. The GBL files need to be created separately by running a script located in the applicaton project's root folder. Before running the script, the application must be compiled.

Two scripts are provided in the SDK examples:

- **create_bl_files.bat** (for Windows)
- **create_bl_files.sh** (for Linux / Mac)

The GBL files can be generated by invoking the script from the project directory.

You need to define two environment variables, `PATH_SCMD` and `PATH_GCCARM`, before running the script, as shown in the following table.

NOTE: Add this "Table 1. Environment variables required for creating .gbl files"

Variable Name	Example Variable Value
PATH_SCMD	C:\SiliconLabs\SimplicityStudio\v5\developer\adapter_packs\commander
PATH_GCCARM	C:\SiliconLabs\SimplicityStudio\v5\developer\toolchains\gnu_arm\10.2_2020q4

Running the **create_bl_files** script creates multiple GBL files in a subfolder named output_gbl. The file named **full.gbl** is the upgrade image used for UART DFU. The other files are related to OTA upgrades, and they can be ignored.

If signing and/or encryption keys (named **app-sign-key.pem**, **app-encrypt-key.txt**) are present in the same directory, then the script also creates secure variants of the GBL files. More information on creating secure firmware for DFU can be found in our training document: Secure Firmware Upgrade using OTA.

2.4 UART DFU Host Example

The UART DFU host example is a C program that is located under the Bluetooth SDK examples in the following directory (the exact path depends on the installed SDK version).

In Windows this program can be built using MinGW. In Linux or Mac the program can be built using the GCC toolchain.

The project is built by running make (or mingw32-make) in the project root directory. After a successful build, an executable is created in the subfolder named **exe**. The executable filename is **bt_host_uart_dfu.exe**.

Before running the example, you need to check the COM port number associated with your NCP target. For more details, see *AN1259: Using the v3.x Silicon Labs Bluetooth® Stack in Network Co-Processor Mode*.

The **bt_host_uart_dfu.exe** program requires three command line arguments:

- COM port number
- Baud rate
- Name of the (full) GBL file

Furthermore, the device must be flashed with the BGAPI UART DFU Bootloader and an NCP-application.

Example usage and expected output in v4.0 or higher:

```
./bt_host_uart_dfu.exe -u COM42 -b 11520 full.gbl

[I] NCP host initialized.
[I] Reset NCP target in bootloader mode...
[I] DFU booted: v0x02010000
[I] Pressing Ctrl+C aborts the update process.
[I] WARNING! If the update process is aborted, the device will stay in bootloader mode.

207728/207728 (100%)
[I] DFU finished successfully. Resetting the device.
```

The number of bytes uploaded in one DFU flash upload command is configurable. The UART DFU host example included in the SDK uses a 48-byte payload. The maximum usable payload length is 128 bytes. The maximum number of bytes sent in one command is specified using a C preprocessor directive named MAX_DFU_PACKET. The value of MAX_DFU_PACKET must be divisible by four.

3. Bluetooth OTA Upgrade

This is the firmware upgrade method used in SoC-mode Bluetooth applications. A GBL-file containing new firmware is sent to a target device through a Bluetooth connection. The firmware upgrade image can be stored to an empty flash area and applied later by the user application, or immediately overwrite the original application using a component called Apploader. The main differences between application- and Apploader-based OTA are shown in the table below:

Feature	Apploader-based OTA	Application-based OTA
Implementation	Integrated into the bootloader	Implemented in the user application
Supported Devices	Series 1 and 2	Series 2 and 3
Storage slot required	No, the old firmware is directly overwritten	Yes, the new firmware must be stored in flash before overwriting
Supported PHY	1M	1M, 2M, Coded
Encryption	Not supported	Supported

Currently, it is recommended to use the application-based OTA as it enables improved security and customizability. Furthermore, Apploader is not supported in Series 3 devices. The two available options are described in more detail in the sections 3.1 and 3.2. An example of creating the GBL-files and using the application-based OTA is shown in section 3.3

3.1 AppLoader

A Bluetooth application developed with Silicon Labs Bluetooth SDK comprises two parts: AppLoader and the user application. AppLoader is a small standalone application that is required to support in-place OTA updates. AppLoader can run independently of the user application. It contains a minimal version of the Bluetooth stack, including only those features that are necessary to perform the OTA update. Any Bluetooth features that are not necessary to support OTA updates are disabled in AppLoader to minimize the flash footprint.

The AppLoader features and limitations are summarized below:

- Enables OTA updating of user application.
- The AppLoader itself can also be updated.
- Only one Bluetooth connection is supported, GATT server role only.
- Encryption and other security features such as bonding are not supported.
- PTI is not enabled so it is not possible to use the Network Analyzer with the AppLoader

Note: AppLoader in SDK v3.x or higher requires that the Gecko Bootloader version must be v1.11 or later to support OTA.

The user application is placed in code flash after AppLoader. The default linker script provided in the SDK places the user application so that it starts at the next flash sector following AppLoader. The user application contains a full-featured version of the Bluetooth stack, and it can run independently of the AppLoader. If in-place OTA update does not need to be supported, then the AppLoader can be removed completely to free up flash for other use (code space or data storage). Section 5. Implementing Device Firmware Update in the User Application describes how OTA can be implemented in application code, without any involvement of AppLoader.

For more details on AppLoader and the overall structure of a Bluetooth application, see *UG434: Silicon Labs Bluetooth® C Application Developers Guide for SDK v3.x* or *UG136: Silicon Labs Bluetooth® C Application Developers Guide for SDK v2.x*.

3.2 Gecko Bootloader Configuration up to SDK version 3.3.x

The Gecko Bootloader must be configured as an application bootloader. The OTA functionality is implemented almost entirely in the AppLoader, or alternatively in the user application. The Gecko Bootloader takes care of copying data from the download area to the final destination in flash. Additionally, AppLoader takes advantage of some features supported by Gecko Bootloader, for example, parsing the incoming GBL image.

Note: Gecko Bootloader has an *Application upgrade version* check component/plugin that can be included in the Bootloader project. This feature is used to check the version number and product ID of the application upgrade before applying it. However, this should not be used with AppLoader because the version comparison is done to AppLoader instead of the application.

For EFR32xG1, the **Bluetooth in-place OTA DFU Bootloader** configuration is used as a default. In this configuration, the upper half of the main flash, normally used to hold the Bluetooth application, is re-purposed as a storage area while a Bluetooth stack upgrade is downloaded.

For EFR32xG12 and later, any application bootloader configuration may be used that uses internal storage. The default example application configurations are suitable for Bluetooth OTA upgrades, and may be modified to fit the needs of the application. The following figure shows an example flash layout for EFR32xG1 and EFR32xG12 devices. For more information on flash organization, see *UG434: Silicon Labs Bluetooth® C Application Developers Guide for SDK v3.x* or *UG136: Silicon Labs Bluetooth® C Application Developers Guide for SDK v2.x*.

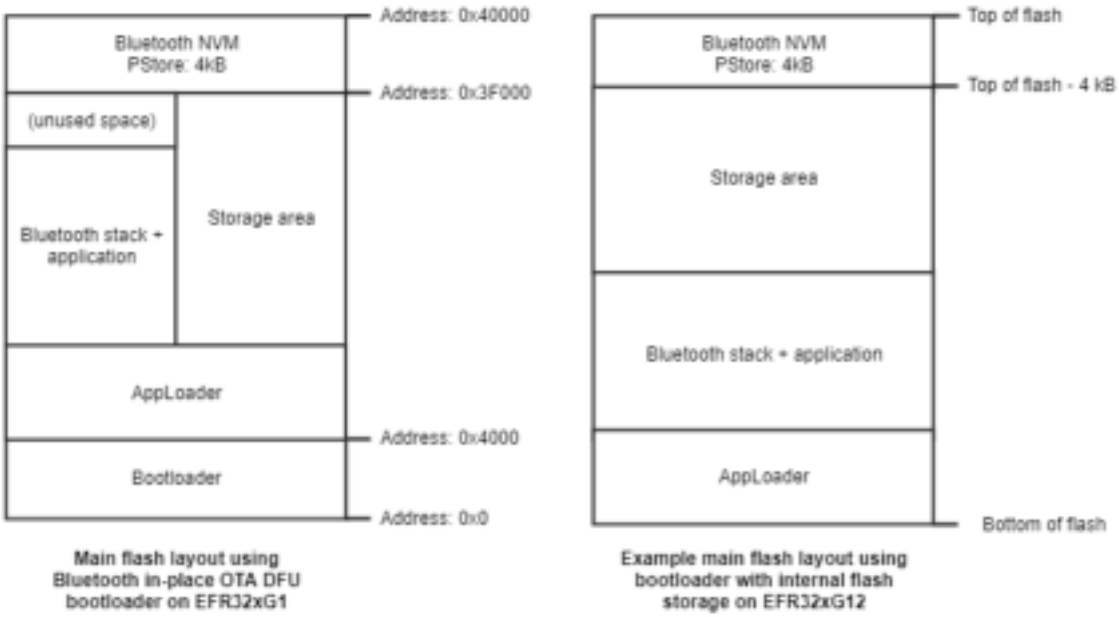
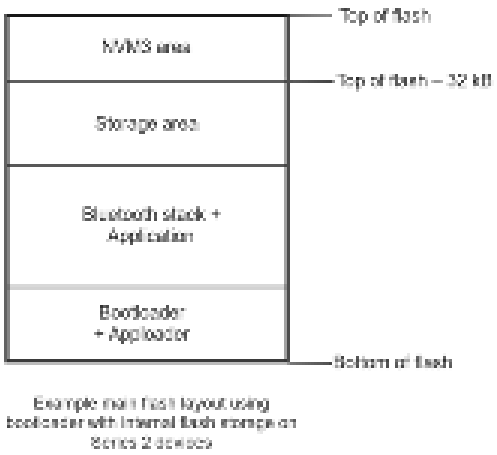


Figure 3.1. Examples of Main Flash Layout when Using Gecko Bootloader with Bluetooth OTA DFU

Note that on series 2 devices (EFR32xG2x) the default NVM solution is NVM3, and NVM3 might also be used instead of PS Store on series 1 devices. In this case the NVM area is larger than 4 kB, and therefore the slot size in the bootloader configuration must be reduced accordingly to avoid overwriting the NVM area.

3.3 Gecko Bootloader Configuration from SDK version 4.0

From Bluetooth SDK version v4.0, the AppLoader can also be included in the Bootloader. The following picture shows an example of this new layout:



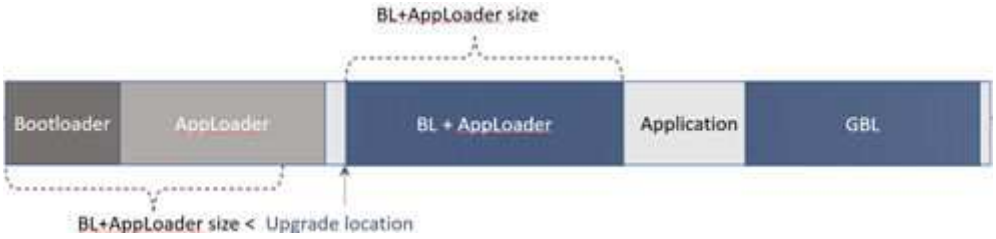
Example main flash layout using bootloader with internal flash storage on Series 2 devices

To use the AppLoader from the Bootloader, the start address of the Bootloader upgrade location needs to be changed so that there will be enough space for the Bootloader with the AppLoader. Unfortunately, this is not possible on Series 1 devices since the default Bootloader upgrade location is defined in the first stage Bootloader. So, this new method can only be used on Series 2 devices. For Series 2 devices, this is the new default configuration.

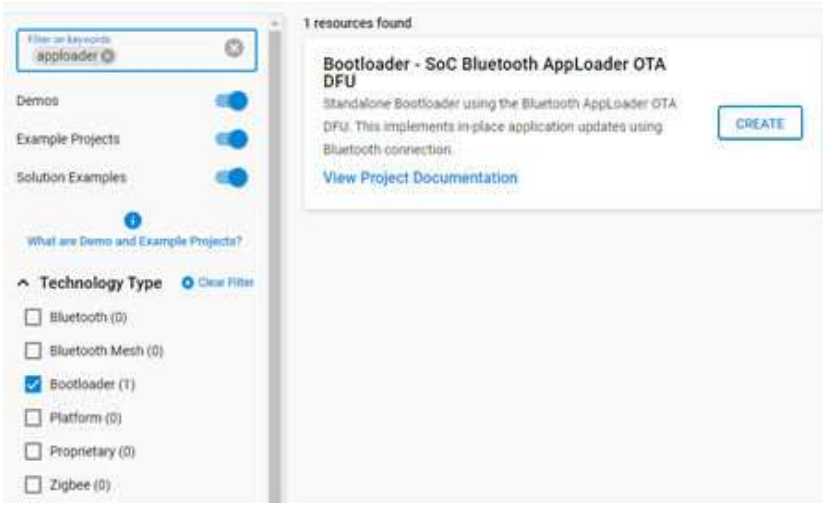
3.3.1 Configuring the Bootloader Project

In the Bootloader project, the Software Component “Bluetooth AppLoader OTA DFU” needs to be added:

After this component is added, the base address of the bootloader upgrade image needs to be updated in the Bootloader Core component. The recommended value is 0x18000 (98304), so that bootloader upgrade location will not overlap the bootloader with AppLoader. However, the projects can use any appropriate values based on their bootloader and application size.



Alternatively, you can use the new sample Bootloader project, SoC Bluetooth AppLoader OTA DFU, where all the necessary configurations are already set:



3.3.2 Configuring the Application

In the application project, only the **In-Place OTA DFU** component needs to be added so it can work with the new, combined Bootloader + AppLoader setup.

The **In-Place OTA DFU** component has dependencies:

- **AppLoader Support for Applications** component which on:
  - Series-1 devices adds AppLoader binary to the application.
  - Series-2 devices moves the application start address to give space for an AppLoader OTA DFU Bootloader. It also requires a Gecko Bootloader with an AppLoader OTA DFU plugin to be present on the device.
- **AppLoader Utility** component, which provides utility functions related to OTA DFU, such as a unified API for resetting the device to DFU mode.

3.3.3 Upgrading from Internal Storage Bootloader to Bluetooth Apploader OTA DFU Bootloader

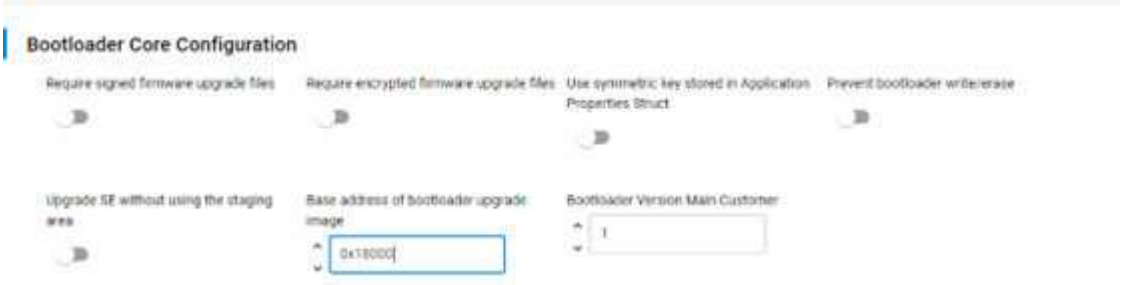
Up until Gecko SDK v4.0, AppLoader was a standalone application image that took place after the bootloader area and before the application in the flash memory. With Gecko SDK v4.1, AppLoader is part of the Gecko Bootloader project, and is provided as a communication plugin component instead of a separate application for series 2 devices. This means that:

- There is no need to flash the AppLoader image separately, as it is part of the Bootloader.
- The AppLoader cannot be upgraded by itself anymore. To upgrade the AppLoader, the Gecko Bootloader must be upgraded.
- The bootloader size is much bigger than that of a regular bootloader, and it does not fit into the regular bootloader area. Consequently, both the application start address, and the base address of the bootloader upgrade image, must be shifted.

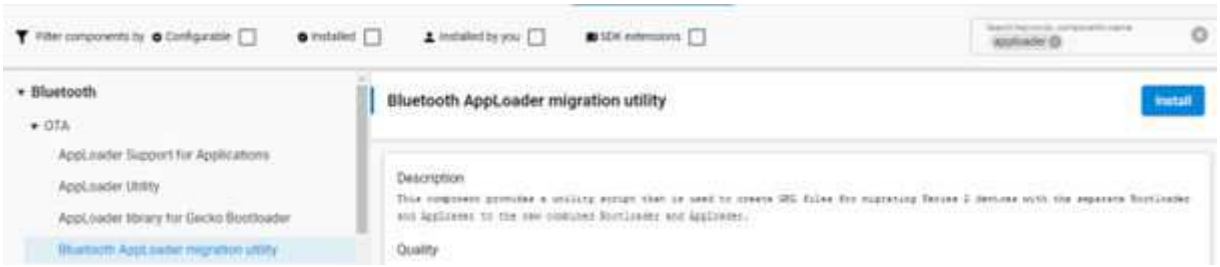
Due to these major changes, upgrading from a GSDK v4.0 separate Gecko Bootloader and AppLoader to a GSDK v4.1 combined Gecko Bootloader and AppLoader is not simple. Trying to update directly to the combined AppLoader and bootloader would fail, because the default upgrade location in the old bootloader is located so that the combined bootloader and AppLoader would overlap the update. This means that any problems with the update cause the device to be non-functional. The upgrade process, however, can be done successfully using the following steps:

Step 1: Create a GBL file containing AppLoader and bootloader where the upgrade location of the bootloader has been moved.

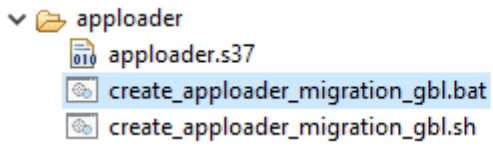
- In Simplicity Studio v5, using GSDK 4.1 (or higher), create the **Bootloader - SoC Internal Storage** project.
- Update `BTL_UPGRADE_LOCATION_BASE` to 0x18000UL in config/btl_core_cfg.h. Alternatively, use the **Platform > Bootloader Core** component configurator to update the base address.



- Install the **Bluetooth > Bluetooth AppLoader migration utility** component using the project configurator.



  This generates an “apploader” directory in the root folder of the bootloader project. The directory contains the correct AppLoader binary and a helper script for generating the needed GBL file. The AppLoader binary in this directory has support for GBL files containing only bootloader and no application.
- Build the project.
- Find the migration script inside the “apploader” folder, right click, and select **Open Command Line Here**.



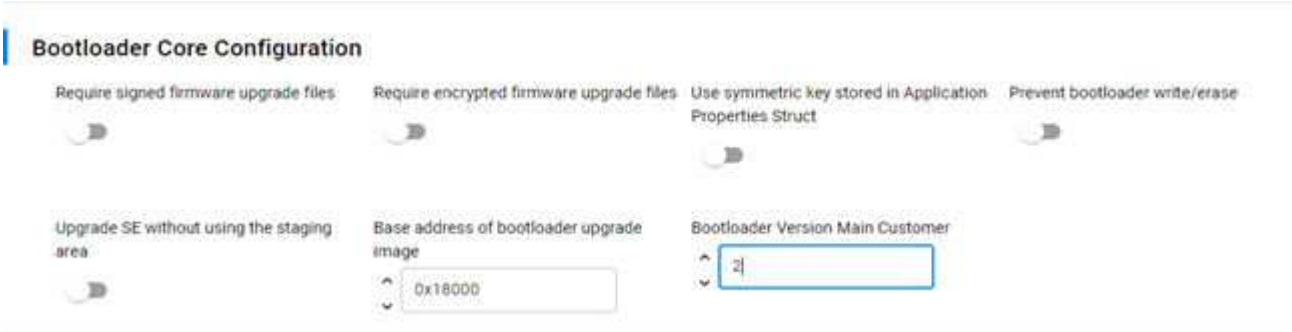
- Run the script by providing the path to the bootloader binary and the output GBL file:

```
create_apploader_migration_gbl.bat    "../GNU    ARM    v10.3.1    -    Default/bootloader-storage-internal-single-512k.s37" migration.gbl
```

  This process generates the migration.gbl file inside the “apploader” directory. The migration GBL file will be used in the OTA process to upgrade the bootloader with an updated bootloader version where the upgrade location is moved, but does not contain the AppLoader communication plugin.

Step 2: Create a GBL file for the new Bootloader which has the AppLoader communication plugin.

- In Simplicity Studio v5, using GSDK 4.1 (or higher), create the **Bootloader - SoC Bluetooth AppLoader OTA DFU** project.
- Increase the bootloader version number if you are using the same SDK version used for generating the migration GBL in Step 1. In config/btl_core_cfg.h, change the value of `BOOTLOADER_VERSION_MAIN_CUSTOMER`.



- Build the project.
- Find the output file (bootloader-apploader.s37) in the compiler's output folder, right click, and select **Open Command Line Here**.
- Generate the GBL file using the following command.

```
commander gbl create bootloader-apploader.gbl --bootloader bootloader-apploader.s37
```

This generates the `bootloader-apploader.gbl` file in the build directory of the project.

Step 3: Create a GBL file for an application upgrade.

- In Simplicity Studio v5, using GSDK 4.1 (or higher), create the **Bluetooth - SoC Empty** project.
- Build the project.
- Run the `create_bl_files.bat` script to generate the GBL file for the application upgrade, and find the `application.gbl` file in the output_gbl folder.

Step 4: Perform OTA updates.

- Copy `migration.gbl`, `bootloader-apploader.gbl` , and `application.gbl` created in steps 1 to 3 above into your phone.
- Start **EFR Connect** on your phone.
- Browse to your device and connect.
- In the context menu, find **OTA DFU**, select **PARTIAL OTA**, and upload `migration.gbl`. to upgrade to the new bootloader with a shifted bootloader upgrade location base address. This firmware also updates the AppLoader to a new version which supports GBL files containing only bootloader and no application.
- After disconnection, using **EFR Connect**, find the device advertising as OTA, and connect again.
- In the context menu, find **OTA DFU**, select **FULL OTA**, and use `application.gbl` and `bootloader-apploader.gbl` files to upgrade to the combined bootloader and AppLoader version and new application.

During the full OTA process, the device resets itself twice so there is no need for user interactions.

3.4 In-Place OTA Process

Most of the OTA functionality is handled autonomously by the AppLoader, which greatly simplifies application development. The minimum requirement for the user application is for a way to trigger a reboot into DFU mode. Rebooting into DFU mode in this context means that after the device is reset, the AppLoader is run instead of the user application. After the upload is complete, AppLoader will reboot the device back into normal mode.

Reboot into DFU mode can be triggered in a variety of ways. It is up to the application developer to decide which is most applicable. Most of the example applications provided in the Bluetooth SDK already have OTA support built into the code. In these examples, the DFU mode is triggered through the Silicon Labs OTA service that is included as part of the application's GATT database. The following sections explain in detail how this is done in the user application.

AppLoader supports two types of update:

- Full update: both AppLoader and the user application are updated
- Partial update: only the user application is updated

Note: In earlier stack versions (SDK v2.6.x and earlier), the meaning of partial and full update is different compared to the current OTA implementation. To avoid confusion, the main differences between the old and new OTA are summarized below.

	SDK v2.6.x and older	SDK v2.7.x and later
OTA update files generated	stack.gbl: Bluetooth stack and OTA update part (*supervisor*)	apploader.gbl: AppLoader (including minimal Bluetooth stack)
"	app.gbl: User application	application.gbl: user application (including full Bluetooth stack)
Partial update	Only user application is updated. Bluetooth stack remains the same. Application must be built with same SDK version that is currently installed in the target device.	User application is updated. The Bluetooth stack is part of the user application; therefore, the stack is also updated. The user application and AppLoader do not need to be built from the same SDK. (1)
Full update	Both the Bluetooth stack and the user application are updated in two phases (first stack, then application).	Both the AppLoader and user application (including Bluetooth stack) are updated in two phases (first AppLoader, then user application).

(1) A full update is always recommended when moving from one SDK version to another. The size of AppLoader can vary depending on the SDK version. This may prevent a partial OTA update if the new application image overlaps with the old AppLoader version.

From the OTA client viewpoint, the overall OTA process is the same in both old and new versions. Full update is performed by uploading two GBL files into the target device. Partial update requires only one file. Because the mechanism of uploading GBL files over the air is identical, the OTA solution introduced in SDK 2.7.0 is backwards-compatible:

- Device running an application from SDK v2.6.x (or older, down to 2.0.x) can be upgraded to 2.7.x using OTA
- Device running v2.7.x firmware can be downgraded to 2.6.x or older using OTA
- Device running an application from SDK v2.7.x firmware and Gecko Bootloader v1.11 or later can be upgraded to SDK v3.x using OTA

The partial update process using AppLoader consists of following steps:

1. OTA client connects to target device.
2. Client requests target device to reboot into DFU mode.
3. After reboot, client connects again.
4. During the 2nd connection, target device is running AppLoader (not the user application).
5. New firmware image (application.gbl) is uploaded to the target.
6. AppLoader copies the new application on top of the existing application.
7. When upload is finished and connection closed, AppLoader reboots back to normal mode.
8. Update complete.

With partial update, it is possible to update the Bluetooth stack and user application. AppLoader is not modified during partial update.

Full update enables updating both the AppLoader and the user application. Full update is done in two steps. Updating the AppLoader always erases the user application and therefore AppLoader update must always be followed by application update.

The first phase of full update updates the AppLoader and it consists of following steps:

1. OTA client connects to target device.
2. Client requests target device to reboot into DFU mode.
3. After reboot, client connects again.
4. During the 2nd connection, target device is running AppLoader (not the user application).
5. New AppLoader image (apploader.gbl) is uploaded to the target.
6. AppLoader copies the image into the download area (specified in Gecko bootloader configuration).
7. When upload is finished and connection closed, AppLoader reboots and requests Gecko Bootloader to install the downloaded image.
8. Gecko Bootloader updates AppLoader using the downloaded image and reboots.
9. After reboot, the new AppLoader is started.

At the end of the AppLoader update, the device does not contain a valid user application and therefore AppLoader will remain in DFU mode. To complete the update, a new user application is uploaded following the same sequence of operations that were described for the partial update.

The SDK includes an example OTA client implementation that can be used to perform both full and partial updates. This example app is described in section 3.12 OTA DFU Host Example. Full and partial OTA can also be performed using the EFR Connect smartphone app.

3.4.1 Firmware Upgrade from PS Store to NVM3

If an application is already in the field using PS Store and should be upgraded to use NVM3, it can be upgraded using OTA DFU (over-the-air device firmware upgrade) with new firmware that already uses NVM3.

However, in this case the data stored in the PS Store cannot be preserved. All bonding information and stored user data will be lost. Nevertheless, the new application can reinitialize the NVM area (at the end of the main flash) to use NVM3 instead of PS Store, and after the upgrade NVM3 will work perfectly.

Upgrading software from PS Store to NVM3 is challenging, mostly due to the fact that the application provides information to the AppLoader through non-volatile memory (PS Store / NVM3), which gets upgraded as well. The following are the detailed steps to perform an OTA upgrade from PS Store to NVM3, where the device doing the upgrade is bonded with the device to be upgraded.

Note: The procedure illustrates the situation where the upgrader and the device to be upgraded are bonded to showcase all the challenges. Bonding is not a condition for upgrading from PS Store to NVM3.

1. The device uses an application with PS Store.
   - The application sets `random address OTA flag` and `OTA device name` in PS Store 10.2_2020q4.
2. The Smartphone opens a connection to this device and gets bonded (if not bonded already).
   - The application stores bonding information in PS Store.
3. The Smartphone resets the device into OTA mode by writing 0x00 into the OTA control characteristic.
4. AppLoader (with PS Store support) starts.
   - AppLoader advertises with a random address and the OTA device name.
5. The Smartphone connects and uploads a new AppLoader (with NVM3 support).
6. The device resets and applies the new AppLoader image.
7. The new AppLoader (with NVM3 support) starts.
   - The AppLoader advertises with the public address and with the default name ("Apploader"), because it cannot read the random address flag and the OTA device name from PS Store.
   - The Smartphone sees the device as bonded because bonding information is associated with the public address, but AppLoader does not support bonding.
8. The Smartphone removes bonding information for the device before re-connecting.
9. The Smartphone connects and uploads a new application (with NVM3 support).
10. The new application starts.
    - The application initializes NVM3 by reformatting the NVM area.
    - The application sets `random address OTA flag` and `OTA device name` in NVM3.
11. The Smartphone opens a connection and gets bonded (again).
    - The application stores bonding information in NVM3.

After this, NVM3 to NVM3 update will work normally.

1. The device uses an application with NVM3.
   - The application sets `random address OTA flag` and `OTA device name` in NVM3.
2. The Smartphone opens a connection to this device and gets bonded (if not bonded already).
   - The application stores bonding information in NVM3.
3. The Smartphone resets the device into OTA mode by writing 0x00 into the OTA control characteristic.
4. AppLoader (with NVM3 support) starts.
   - AppLoader advertises with a random address and the OTA device name.
5. The Smartphone connects and uploads a new AppLoader (with NVM3 support).
6. The device resets and applies the new AppLoader image.
7. The new AppLoader (with NVM3 support) starts.
   - AppLoader advertises with a random address and the OTA device name.
8. The Smartphone connects and uploads a new application (with NVM3 support).
9. The new application starts.
10. The Smartphone opens a connection and encrypts the connection with existing bonding information.
    - Bonding information is still stored in NVM3.

3.5 Silicon Labs OTA GATT service

The following XML representation defines the Silicon Labs OTA service. It is a custom service using 128-bit UUID values. The service content and the UUID values are fixed and must not be changed.

The OTA service characteristics are described in the following table. The UUID value of the service itself is `1d14d6eefd63-4fa1-bfa4-8f47b42119f0`.

Table 3.1. Silicon Labs OTA Service Characteristics

Characteristic	UUID	Type	Length	Support	Properties
OTA Control Attribute	F7BF3564-FB6D-4E53-88A4-5E37E0326063	Hex	1 byte	Mandatory	Write (4)
OTA Data Attribute (1)	984227F3-34FC-4045-A5D0-2C581F81A153	Hex	Variable; max 244 bytes	Mandatory	Write without response; Write
AppLoader version (2) (Bluetooth stack version 2,3)	4F4A2368-8CCA-451E-BFFF-CF0E2EE23E9F	Hex	8	Optional	Read
OTA version (2)	4CC07BCF-0868-4B32-9DAD-BA4CC41E5316	Hex	1	Optional	Read
Gecko Bootloader version (2)	25F05C0A-E917-46E9-B2A5-AA2BE1245AFE	Hex	4	Optional	Read
Application version	0D77CC11-4AC1-49F2-BFA9-CD96AC7A92F8	Hex	4	Optional	Read

Notes:

(1) This characteristic is excluded from the user application GATT database.

(2) Version information is automatically added by AppLoader when running in DFU mode. These are optional in the application GATT database.

(3) This characteristic exposes AppLoader version starting from SDK 2.7.0; was stack version in earlier versions.

(4) Silicon Labs highly recommends that the default property (i.e, write) be used only over bonded connections to prevent uploading of new firmware by untrusted/unknown devices.

Table 3.2. Possible Control Words Written to the OTA Control Characteristic

Hex value	Description
0x00	OTA client initiates the upgrade procedure by writing value 0.
0x03	After the entire GBL file has been uploaded the client writes this value to indicate that upload is finished.
0x04	Request the target device to close connection. Typically the connection is closed by OTA client but using this control value it is possible to request that disconnection is initiated by the OTA target device.
Other values	Other values are reserved for future use and must not be used by application.

In DFU mode, AppLoader uses the full OTA service described above. This allows a remote Bluetooth device to upload a new firmware image, as described later in this chapter. The GATT database of the user application includes only a subset of the full OTA service. The minimum application requirement is to include the OTA control characteristic. The application must not include the OTA data characteristic in its GATT database (unless the OTA update is implemented fully in application code, as described in section 5. Implementing Device Firmware Update in the User Application.

From the user application viewpoint, only the OTA control attribute is relevant. In the OTA host example reference implementation that is included in the SDK, the OTA procedure is triggered when the client writes value 0 to the OTA control attribute. The user application does not handle any data transfers related to OTA upgrades and therefore the OTA Data Attribute is excluded from the user application's GATT.

It is also possible to use an application-specific trigger to enter OTA mode, and therefore it is not absolutely necessary to include the OTA control attribute in the application's GATT database. If reboot into DFU mode is handled using some other mechanism, then it is possible to exclude the whole OTA service from the application GATT. However, it should be noted that to be compatible with the OTA host example from the SDK or the EFR Connect smartphone app the OTA trigger must be implemented as described above.

Note: AppLoader has its own GATT database that is independent of the user application's GATT database.

The presence of the OTA Data Attribute in the GATT database is used by the OTA host example application to check whether the target device is running in normal mode (user application) or DFU mode (AppLoader). Therefore, the OTA Data Attribute must not be included in the user application's GATT. The OTA-enabled examples in the Bluetooth SDK only expose the OTA Control Attribute.

The four characteristics after the OTA data attribute are automatically added in the GATT database that is used by AppLoader. These include version information that can be read by the OTA client before starting the firmware update. For example, by checking the AppLoader version, the OTA client may check if a full or partial update is needed.

The AppLoader version is a 8-byte value that consists of four two-byte fields, indicating the AppLoader version in the form <major>.<minor>.<patch>-<build>. For example, value 010000000000170b can be interpreted as version "1.0.0-2839".

The OTA version is a 1-byte value that indicates the OTA protocol version for compatibility checking. The OTA version number in SDK 2.7.0 is 3. This version number is incremented only when needed, if there are some changes in the OTA implementation that may cause backward compatibility issues.

The Gecko Bootloader version is a 4-byte value that is configured in a Gecko Bootloader project (file btl_config.h). The two most significant bytes are the major and minor numbers. The other two bytes are customer-specific and they can be set to indicate certain Gecko Bootloader configuration options (for example, whether secure boot is required or not). As an example, value 00000401 indicates that the Gecko Bootloader version is "1.4" and the customer-specific part is 0x0000 (this is the default if no customer-specific version info has been configured in the Gecko Bootloader project).

The application version is a 4-byte value and it is initialized to the same value that is defined in the file application_properties.c. The encoding of this value is application-specific. In the SDK example projects, the application_properties.c source is included but the application version is set to zero. In real applications it is highly recommended to use some meaningful application version so that it can be read over-the-air when the device is in OTA mode. The application properties file is discussed in more detail in section 3.8 OTA-Related Configurations in the v3.x Bluetooth Stack.

AppLoader does not include support for encryption or bonding and therefore there are no access restrictions on any of the characteristics listed in Table 3.1 Silicon Labs OTA Service Characteristics on page 15. Because the user application has its own GATT database it is possible to include additional security requirements there as needed. For example, the user application can require that the OTA control attribute is writable only by a bonded client so that only bonded client can trigger reboot into DFU mode.

For additional security, it is recommended to configure the Gecko Bootloader to use secure boot and signed GBL images.

3.6 OTA GATT Database and Generic Attribute Service

When booted into DFU mode, the AppLoader uses a GATT database that is different than the normal GATT used by the application.

The OTA DFU GATT database used by AppLoader contains following services:

- Generic Attribute (UUID 0x1801)
- Generic Access (UUID 0x1800)
- Silicon Labs OTA service (UUID 0x1d14d6ee-fd63-4fa1-bfa4-8f47b42119f0)

The Bluetooth specification requires that, if GATT-based services can change in the lifetime of the device, then the **Generic Attribute Service** (UUID 0x1801) and the **Service Changed** characteristic (UUID 0x2A05) shall exist in the GATT database. For details, please see Bluetooth Core specification, Version 5.2, Vol. 3, Part G, 7 DEFINED GENERIC ATTRIBUTE PROFILE SERVICE.

The Generic Attribute service is automatically included in the AppLoader GATT database used during OTA. To avoid any interoperability issues due to GATT caching, it is strongly recommended that the application GATT database used in normal mode also enables this service. Generic Attribute service is enabled by default in the SDK example applications.

Note: AppLoader does not generate a service changed indication when rebooting to DFU mode or rebooting back to normal mode.

Automatic service changed indication requires that the client is bonded and has enabled the indication for this characteristic. AppLoader does not support bonding and therefore the service changed indication is not generated.

The Generic Attribute Service can also be explicitly defined in the application's GATT database using the same XML notation that is used for other services. The Generic Attribute service must be the first service in the list, to ensure it is aligned with the Generic Attribute Service that is used during OTA. The Bluetooth specification requires that the attribute handle of the Service Changed characteristic shall not change and therefore this service must be first on the list (the same as in the OTA GATT database).

More details on the Generic Attribute Service can be found on the Bluetooth SIG website:

https://www.bluetooth.com/specifications/gatt/services

Note also that AppLoader does not support the GATT caching enhancements that were introduced in the Bluetooth Core Specification 5.1 and Silicon Labs Bluetooth SDK 2.11.1.

3.7 Triggering Reboot into DFU Mode from the User Application

The minimum functional requirement to enable OTA in the user application is to implement a 'hook' that allows the device to be rebooted into DFU mode. By default, this is done through the Silicon Labs OTA service.

The following code snippet is from the SoC Thermometer example supplied with the SDK. The code to enter DFU mode is similar in the other examples.

```
/////////////////////////////////////////////////////////////////////////////
// This event indicates that a remote GATT client is attempting to write //
// a value of a user type attribute in to the local GATT database.       //
/////////////////////////////////////////////////////////////////////////////
case sl_bt_evt_gatt_server_user_write_request_id:
  // If user-type OTA Control Characteristic was written, boot the device
  // into Device Firmware Upgrade (DFU) mode.
  if (evt->data.evt_gatt_server_user_write_request.characteristic == gattdb_ota_control) {
    // Set flag to enter OTA mode.
    boot_to_dfu = true;
    // Send response to user write request.                                    1
    sc = sl_bt_gatt_server_send_user_write_response(
      evt->data.evt_gatt_server_user_write_request.connection,
      gattdb_ota_control,
      SL_STATUS_OK);
    app_assert(sc == SL_STATUS_OK,
               "[E: 0x%04x] Failed to send response to user write request\n",
               (int)sc);
    // Close connection to enter to DFU OTA mode
    sc = sl_bt_connection_close(
      evt->data.evt_gatt_server_user_write_request.connection);
    app_assert(sc == SL_STATUS_OK,
               "[E: 0x%04x] Failed to close connection to enter to DFU OTA mode\n",
               (int)sc);
  }
  break;

/////////////////////////////////////////////////////////////////////////////
// This event indicates that a connection was closed.                      //
/////////////////////////////////////////////////////////////////////////////
case sl_bt_evt_connection_closed_id:
  // Check if need to boot to OTA DFU mode.
  if (boot_to_dfu) {
    // Reset MCU and enter OTA DFU mode.                                     2
    sl_bt_system_reset(2);
  }
  break;
```

Figure 3.2. Handling Write to OTA Control Characteristic in C Code in SDK v3.x or higher

```
case gecko_evt_le_connection_closed_id:
  /* Check if need to boot to dfu mode */
  if (boot_to_dfu) {                                    2.
    /* Enter to DFU OTA mode */
    gecko_cmd_system_reset(2);
  }
  else {
    ....


/* Checks if the user-type OTA Control Characteristic was written.
 * If written, boots the device into Device Firmware Upgrade (DFU) mode. */
case gecko_evt_gatt_server_user_write_request_id:
  if(evt->data.evt_gatt_server_user_write_request.characteristic==gattdb_ota_control) {
    /* Set flag to enter to OTA mode */
    boot_to_dfu = 1;                                                                1.
    /* Send response to Write Request */
    gecko_cmd_gatt_server_send_user_write_response(
      evt->data.evt_gatt_server_user_write_request.connection,
      gattdb_ota_control,
      bg_err_success);

    /* Close connection to enter to DFU OTA mode */
    gecko_cmd_endpoint_close(evt->data.evt_gatt_server_user_write_request.connection);
  }
  break;
```

Figure 3.3. Handling Write to OTA Control Characteristic in C Code in SDK v2.x

In v3.x and higher: The event with ID `sl_bt_evt_gatt_server_user_write_request_id` indicates that one of the characteristics (of type user) has been written by the remote Bluetooth client. This event handler is found in the **ota_dfu.c** file, which is part of the OTA DFU component.

In v2.x: The event with ID `gecko_evt_gatt_server_user_write_request_id` indicates that one of the characteristics (of type user) has been written by the remote Bluetooth client. This event handler is normally included in the **app.c** file of the sample projects.

In this example, the code simply checks if the OTA control characteristic was written and, if so, triggers a reboot into DFU mode. Before rebooting, the application closes the Bluetooth connection. The variable `boot_to_dfu` is set so indicate that DFU reboot has been requested. When the connection closed event is raised by the stack, the application checks the variable `boot_to_dfu` and if set, performs the DFU reboot by calling `sl_bt_system_reset(2)` in v3.x and higher, and `gecko_cmd_system_reset(2)` in v2.x. Parameter value 2 indicates that the device is to be rebooted into OTA DFU mode. The rest of the OTA upgrade is managed by AppLoader and no further actions are needed from the user application.

3.8 OTA-Related Configurations in the v3.x Bluetooth Stack

Besides implementing the hook to enter DFU mode, the user application must implement some additional OTA-related configurations. These include the OTA-flag, OTA-device name and the OTA-advertising data. For these configurations have an effect, the OTA Software component must be installed. This can be done in Simplicity Studio 5's Project Configurator.

Note: These commands are only valid if the application contains the apploader. If the apploader is used from the bootloader, these configurations must be implemented in the bootloader.

3.8.1 Setting OTA Flag in v3.x

You can use the run-time command `sl_bt_ota_set_configuration(flags)` to set OTA flags. The setting is stored in the persistent store.

`flags` is a 32-bit unsigned integer variable. Flags are defined as follows.

- Bit 0: Advertising address

  0: use public address.

  1: use static random address.
- Bit 1: Application update version check

  0: disable application version check.

  1: enable application version check.
- Bits 2-31: reserved.

`flags` value is given as a bitmask. Flag values are defined as follows.

- 0: use public device address and disable application version check.
- 1: use static random address and disable application version check.
- 2: use public device address and enable application update version check.
- 3: use static random address and enable application update version check.

Default value 0 is used if the user application does not set the flags, in which case the public device address is used and AppLoader does not perform any application version checking during OTA mode.

3.8.2 Setting OTA Device Name in v3.x

You can use the run-time command `sl_bt_ota_set_device_name(name_len, name)` to set the device name to be used during OTA update. The name is stored in the persistent store. The parameter `name` specifies the Bluetooth device name that is used when the device has been rebooted into DFU mode. Note that, in addition to specifying the name string, the application must also specify the exact number of characters in that string in the `name_len` parameter. Maximum name length is 17 bytes.

The device name used during OTA does not have to be static. The string can be dynamically generated, for example, based on the serial number of the device or some other value that uniquely identifies the device.

Default OTA device name "OTA" is used if it is not set in the user application.

3.8.3 Setting OTA Advertising Data in v3.x

Use the command `sl_bt_ota_set_advertising_data(packet_type, adv_data_len, adv_data)` to set the OTA advertising data.

The packet type identifies whether data is intended for advertising packets or to scan response packets.

- 2: OTA advertising packets
- 4: OTA scan response packets

You can set a maximum of 31 bytes of data.

Note: The OTA configuration commands must be called after NVM3 (PS) initialization has been done—that is, after `sl_bt_init()`.

Note that, if OTA advertising data is not set in the user application, a default OTA advertising data that includes the device name, TX power, advertising flags, and Bluetooth device address is used during OTA mode. The following text snippet illustrates typical default raw OTA advertising data and how it is dissected into different advertising data elements.

```
0x02010604094F5441081B005B7728E20A68020A00: raw OTA advertising data
02:                         length = 2bytes
01:                         type = flags
06:                         value = 6 (General Discoverable Mode, BR/EDR Not Supported)
-------------------------------------------------------------------------------
04:                         length = 4 bytes
09:                         type = complete local name
4F5441:                     value = OTA
-------------------------------------------------------------------------------
08:                         length = 8bytes
1B:                         type = BL device address
005B7728E20A68:             value = 00(public) 5B:77:28:E2:0A:68
-------------------------------------------------------------------------------
02:                         length = 2 bytes
0A:                         type = Tx Power
00:                         value = 0dBm
```

The Bluetooth device address that is used in OTA mode is determined as follows:

- Use a static random address if it has been enabled in the OTA configuration flags.
- If the user application has overridden the default Bluetooth address (using command `sl_bt_system_set_identity_address()`), then this address is also used during OTA (starting with SDKv2.8.0).
- The default Bluetooth address (programmed into the device in production) is used if neither a static random address nor custom address has been defined.

For series-1 devices, in OTA mode, the TX power is hardcoded to 0 dBm. For series-2 devices, the TX power level can be configured using the Bluetooth Apploader OTA DFU component inside the bootloader-apploader project.

3.9 OTA-Related Configurations in the v2.x Bluetooth Stack

Besides implementing the hook to enter DFU mode, the user application must implement some additional OTA-related configurations. These include the OTA-flag, OTA-device name and the OTA-advertising data.

3.9.1 Setting OTA Flag and OTA Device Name in v2.x

The user application initializes the Bluetooth stack by calling *gecko_init()*. This function takes one parameter, a pointer to a struct (of type *gecko_configuration_t*) containing various configuration parameters. The code snippet shown below is taken from the SoC Thermometer example from the Bluetooth C SDK. The three OTA-related configuration parameters are highlighted.

```
static const gecko_configuration_t config = {
  .config_flags=0,
  .sleep.flags=SLEEP_FLAGS_DEEP_SLEEP_ENABLE,
  .bluetooth.max_connections=MAX_CONNECTIONS,
  .bluetooth.heap=bluetooth_stack_heap,
  .bluetooth.heap_size=sizeof(bluetooth_stack_heap),
  .gattdb=&bg_gattdb_data,
  .ota.flags=0,
  .ota.device_name_len=3,
  .ota.device_name_ptr="OTA",
  #ifdef FEATURE_PTI_SUPPORT
  .pti = &ptiInit,
  #endif
};
```

Figure 3.4. OTA Configuration Parameters Passed to the v2.x Stack

The OTA parameters are collected in a smaller struct named *gecko_ota_config_t* that is part of *gecko_configuration_t*. The definition of *gecko_ota_config_t* is shown below.

```
typedef struct
{
    uint32_t flags;
    uint8_t  device_name_len;
    char     *device_name_ptr;
}gecko_ota_config_t;
```

Figure 3.5. OTA Configuration Struct in SDK v2.x

`flags` is a set of configuration flags. The following flag values, defined in **gecko_configuration.h**, are possible:

Flag	Description
GECKO_OTA_FLAGS_RANDOM_ADDRESS	If set, AppLoader will use the static random address during OTA mode.

`device_name_len` and `device_name_ptr` specify the Bluetooth device name that is used when the device has been rebooted into DFU mode. Note that, in addition to specifying the name string, the application must also specify the exact number of characters in that string in the device_name_lenparameter.

The device name used during OTA does not have to be static. The string can be dynamically generated, for example based on the serial number of the device or some other value that uniquely identifies the device. However, the name must be set when the stack is initialized (by calling `gecko_init()`).

An alternative way to define the OTA device name is to use the API call **cmd_system_set_device_name**. This method allows the name to be changed after the stack has been initialized.

3.9.2 Setting OTA Advertising Data in v2.x

OTA advertising data can be set using the command `gecko_cmd_le_gap_bt5_set_adv_data`. The same command is used to set user-defined data in advertising packets, scan response packets, or periodic advertising packets.

Note that, if OTA advertising data is not set in the user application, a default OTA advertising data that includes the device name, TX power, advertising flags, and Bluetooth device address is used during OTA mode. The following text snippet illustrates typical default raw OTA advertising data and how it is dissected into different advertising data elements.

```
0x02010604094F5441081B005B7728E20A68020A00: raw OTA advertising data
02:                         length = 2bytes
01:                         type = flags
06:                         value = 6 (General Discoverable Mode, BR/EDR Not Supported)
-------------------------------------------------------------------------------
04:                         length = 4 bytes
09:                         type = complete local name
4F5441:                     value = OTA
-------------------------------------------------------------------------------
08:                         length = 8bytes
1B:                         type = BL device address
005B7728E20A68:             value = 00(public) 5B:77:28:E2:0A:68
-------------------------------------------------------------------------------
02:                         length = 2 bytes
0A:                         type = Tx Power
00:                         value = 0dBm
```

The Bluetooth device address that is used in OTA mode is determined as follows:

- Use a static random address if it has been enabled in the OTA configuration flags.
- If the user application has overridden the default Bluetooth address (using command `cmd_system_set_identity_address()`), then this address is also used during OTA (starting with SDK v2.8.0).
- The default Bluetooth address (programmed into the device in production) is used if neither a static random address nor custom address has been defined.

3.10 Application Properties in OTA Mode

Before v3.3.x

The source file **application_properties.c** needs to be included in projects that use OTA and the Gecko Bootloader. This file is included in the SDK examples by default. Application properties are stored in a fixed location in code flash so that AppLoader can access the data when the device is running in OTA mode. The properties include a 32-bit version number that is application-specific. It is up to the application designer to decide how this value is encoded. This value is exposed in the GATT database used by AppLoader so that the OTA client can read it over the Bluetooth connection after the device has been rebooted into OTA mode.

The version information is set using following #define in **application_properties.c**:

```
/// Version number for this application (uint32_t) #define APP_PROPERTIES_VERSION 1
```

The default value is set to 1, but it is strongly recommended that meaningful version number information is added here so that the OTA client can check the exact version that is installed on the target device. This allows better management of OTA updates of units that are deployed in the field, especially in cases where units are running different versions of the application. If AppLoader does not detect any valid application at all, then the application version in the GATT database is initialized to value zero.

Note: Earlier SDK versions required that header file `aat.h` must be included by the user application. Beginning with SDK v2.7.0, this file is no longer needed, and it **must not be included**.

From v3.3.x and higher

From SDK version v3.3. the source file **application_properties.c** can be found in the folder: "…\platform\bootloader\app_properties".

3.11 Creating OTA Upgrade Images

Building a C-based Bluetooth application in Simplicity Studio does not generate the OTA DFU upgrade images (GBL files) automatically. The GBL files need to be created separately by running a script located in the project's root folder. Two scripts are provided in the SDK examples:

- **create_bl_files.bat** (for Windows)
- **create_bl_files.sh** (for Linux / Mac)

The GBL files can be generated by invoking the script from the project directory.

If you are using Gecko SDK Suite v3.x or higher, you need to define two environmental variables, PATH_SCMD and PATH_GCCARM, before running the script as shown in the following table.

Variable Name	Variable Value
PATH_SCMD	C:\SiliconLabs\SimplicityStudio\v5\developer\adapter_packs\commander
PATH_GCCARM	C:\SiliconLabs\SimplicityStudio\v5\developer\toolchains\gnu_arm\10.3_2021.10

Running the **create_bl_files** script creates six GBL files in a subfolder named `output_gbl`. The files named **application.gbl** and **apploader.gbl** are used for OTA DFU. The file **full.gbl** is related to UART DFU upgrade and can be ignored.

If signing and/or encryption keys (named **app-sign-key.pem**, **app-encrypt-key.txt**) are present in the same directory then the script also creates secure variants of the GBL files.

If a bootloader image (named **bootloader-second-stage.s37**) is present in the same directory then the script also creates a GBL file containing bootloader+apploader images. This GBL file can be used to upgrade the bootloader.

3.12 OTA DFU Host Example

The Bluetooth SDK includes an OTA host reference implementation. The example is written in C language and uses a Bluetooth development kit as modem in Network Co-Processor (NCP) mode. The OTA host application itself runs on the host computer. For more information on the NCP mode of operation, see *QSG169: Bluetooth® v3.x Quick Start Guide* or *QSG139: Bluetooth® v2.x Quick Start Guide*.

The following figure shows an overview of an OTA test setup. The OTA host application is running on a laptop that is connected to one Bluetooth development kit. These two together form the **OTA client**. The host program uses the development kit in NCP mode and communicates with it via a virtual serial port connection using the BGAPI protocol.

The target device to be upgraded over-the-air is shown on the right-hand side. It is identified by its Bluetooth address.

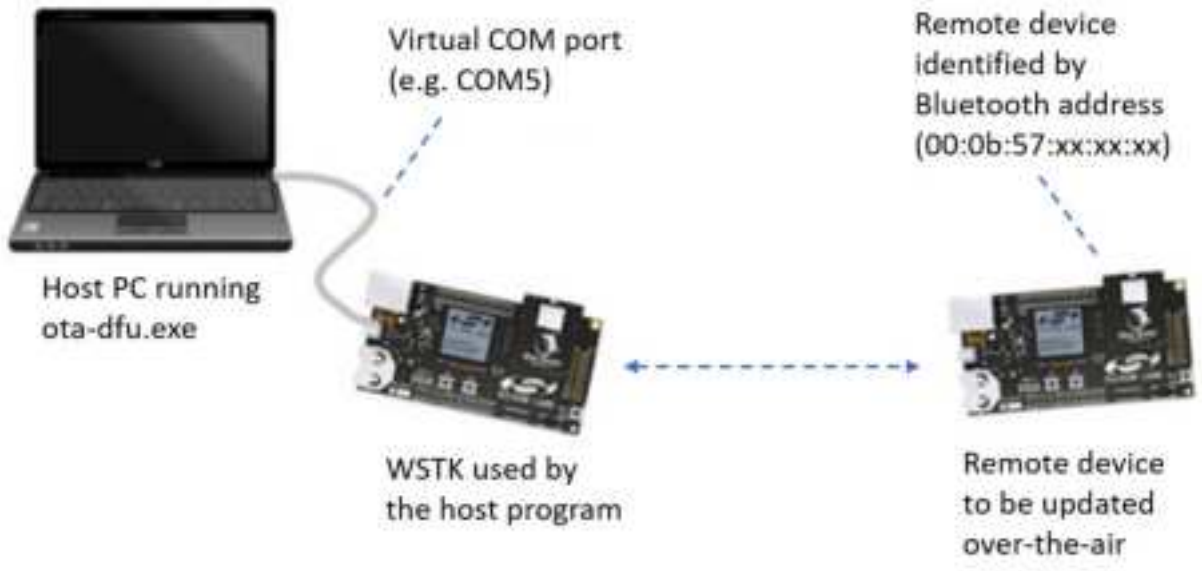


Figure 3.6. OTA test setup

3.12.1 Preparing the Development Kit for NCP Mode

The development kit that is used on the host side should be programmed with firmware that is suitable for NCP mode. The Bluetooth SDK includes an example project named **NCP – Empty Target** that can be used for this purpose.

The development kit main board features an on-board USB-to-UART converter. The board will be seen as a virtual COM port by the host computer.

3.12.2 Building the OTA Host Example Application

The OTA host example is found in the following directory under the Bluetooth SDK installation tree (the exact path depends on the installed SDK version):

v4.0:

```
C:\SiliconLabs\SimplicityStudio\v5\developer\sdks\gecko_sdk_suite\<version>\app\bluetooth\example_host
\bt_host_ota_dfu
```

v3.x:

```
C:\SiliconLabs\SimplicityStudio\v5\developer\sdks\gecko_sdk_suite\<version>\app\bluetooth\example_host\ota_dfu
```

v2.x:

```
C:\SiliconLabs\SimplicityStudio\v4\developer\sdks\gecko_sdk_suite\<version>\app\bluetooth\example_ncp_host
\ota_dfu
```

The project folder contains a makefile that allows the program to be built using for example MinGW (by running `mingw32-make`) or Cygwin (by running `make`). an executable file is created in subfolder named **exe**. The executable filename is:

- **bt_host_ota_dfu.exe** in v4.0 or higher
- **ota_dfu.exe** in v3.x
- **ota-dfu.exe** in v2.x

3.12.3 Running OTA with the NCP Host Example

The OTA host program expects the following command-line arguments:

- COM port number associated with the development kit used in NCP mode
- Baud rate (use fixed value 115200)
- Name of the GBL file to be uploaded into target device
- Bluetooth address of the target device
- (optional) force write without response (possible values 0 / 1, default is 0)

A full OTA upgrade is done in two parts, and it requires two separate GBL files, one for the AppLoader and another for the user application. Full OTA requires the host example program to be invoked twice. An example usage in v4.0 or higher is shown below:

```
./bt_host_ota_dfu.exe -u COM49 -b 115200 apploader.gbl 00:0B:57:0B:49:23
./bt_host_ota_dfu.exe -u COM49 -b 115200 application.gbl 00:0B:57:0B:49:23
```

If the application alone is going to be upgraded, then the host program is run once, with the **application.gbl** file passed as parameter. In other words, only the second of the two commands listed above is run.

Note: Starting from SDK 2.7.0, the user application also includes the Bluetooth stack and therefore the Bluetooth stack can be updated without full update. Full update is needed only if the AppLoader needs to be updated.

3.12.4 OTA Host Example Internal Operation

The OTA host example is implemented as a state machine. The key steps in the OTA sequence are summarized below. Note that the program execution is independent of the type of upgrade image that is used. The program simply uploads one GBL file into the target device. It is up to the user to invoke the program either once or twice, depending on the upgrade type (partial OTA or full OTA).

The following diagram illustrates the state transitions in the OTA host example program in a slightly simplified form.

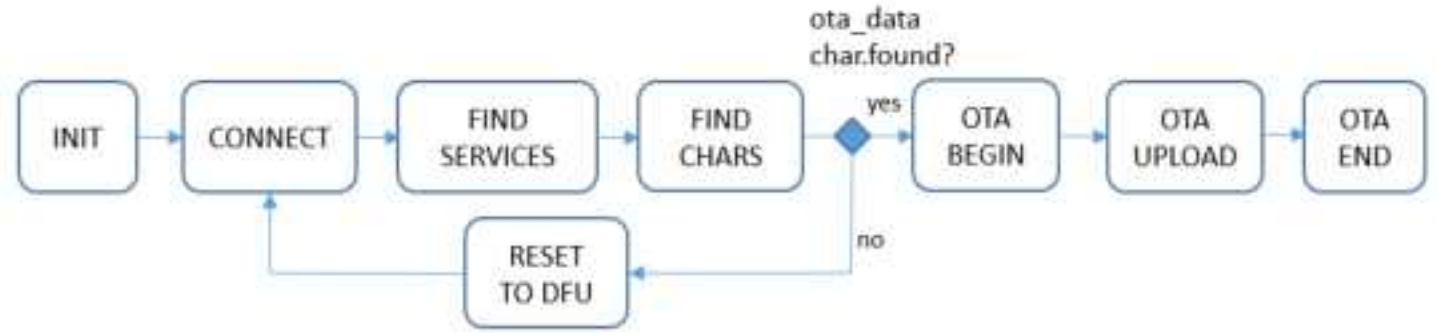


Figure 3.7. OTA Host Example State Transitions

In **INIT** state, the program checks the total size of the GBL file that is passed as a command-line parameter. The GBL file content is not parsed. It is enough to know the file size so that the entire content can be uploaded to target device.

In **CONNECT** state, the program tries to open a connection to the target device whose Bluetooth address is given as a command line parameter. The host program does not scan for devices. If the target device is not advertising, then the connection open attempt causes the program to be blocked.

After a connection has been established, the program moves to state **FIND SERVICES**, where it performs service discovery. In this case only the OTA service is of interest, and therefore the program performs discovery of services with that specific UUID (using the API call `sl_bat_gatt_discover_primary_services_by_uuid` in v3.x or higher, or `cmd_gatt_discover_primary_services_by_uuid` in v2.x).

After the service has been found the next state is **FIND CHARACTERISTICS**, where the characteristic of the OTA service are queried using API call `sl_bat_gatt_discover_characteristics` in v3.x or higher, or `gecko_cmd_gatt_discover_characteristics` in v2.x. The handle value for the **ota_control** needs to be discovered in order to proceed with the OTA procedure.

The **ota_data** characteristic may or may not be present, depending whether the target device is already in DFU mode or not. If the ota_data handle is not found, then the next state is **RESET TO DFU**. In this state the host program requests reboot into DFU mode by writing value 0x00 to the ota_control characteristic. The execution then jumps back to the **CONNECT** state.

If both ota_data and ota_control characteristic handles have been detected, the next state is **OTA BEGIN**. The host program initiates OTA by writing value 0x00 to the ota_control characteristic. This does not cause reboot or any other side effects because the target device is already in DFU mode.

The state following OTA_BEGIN is **OTA UPLOAD**. This is where the GBL file is uploaded to target device. The whole content of the GBL file is uploaded into the target device, by performing a number of write operations into the ota_data characteristic. The host program uses the write-without-response transfer type to optimize throughput. Note that even if the write-without-response operations are not acknowledged at the application level, error checking (and retransmission when needed) at the lower protocol layers ensures that all packets are delivered reliably to the target device.

When the whole GBL file has been uploaded, the next state is **OTA END**. In this state the host program ends the OTA procedure by writing value 0x03 to the ota_control characteristic. Finally, the program terminates.

Some error cases have been omitted from the state diagram for simplicity. For example, the program exits with an error code if the OTA service is not found when performing service discovery or if the ota_control characteristic is not discovered in **FIND CHARACTERISTICS** state.

Note: When the target device reboots into DFU mode, the host program must perform full service and characteristic discovery again. It is not possible to store the ota_control and ota_data characteristic handles in memory and use those cached values during the second connection. This is because the target device has two GATT databases that are independent of each other: one that is used by the application in normal mode and the other that is used by AppLoader in OTA DFU mode. While both of these GATT databases might include the Silicon Labs OTA service, the characteristic handles are likely to have different values. Therefore any kind of GATT caching cannot be used.

3.13 OTA Error Codes

When a new GBL file is being uploaded, the AppLoader performs various checks on it. AppLoader can signal possible errors to the OTA client in two ways:

1. Response to the OTA termination code (0x03) that is written to the OTA control characteristic.
2. Response to writes to the OTA_data characteristic.

Option 2) is not available if the client uses unacknowledged writes. In that case, the possible error code is not available until the entire file has been uploaded and client finishes the upload by writing to the OTA control characteristic.

The OTA client must always check the response value to the last write to the OTA control characteristic. Any non-zero value indicates that the update was not successful. In that case, the device is not able to boot into the main program but rather stays in OTA mode. This makes it possible to try the update again.

The following table summarizes the possible result codes returned by AppLoader.

Table 3.3. AppLoader Result Codes

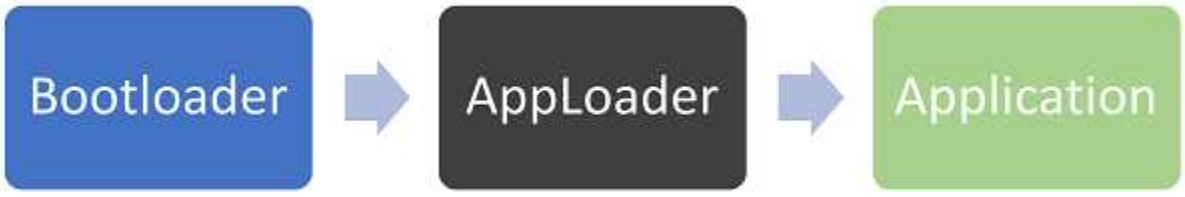
Result Code	Name	Description
0x0000	OK	Success / No errors found.
0x0480	CRC_ERROR	CRC check failed, or signature failure (if enabled).
0x0481	WRONG_STATE	This error is returned if the OTA has not been started (by writing value 0x0 to the control endpoint) and the client tries to send data or terminate the update.
0x0482	BUFFERS_FULL	AppLoader has run out of buffer space.
0x0483	IMAGE_TOO_BIG	New firmware image is too large to fit into flash, or it overlaps with AppLoader.
0x0484	NOT_SUPPORTED	GBL file parsing failed. Potential causes are for example:
"	"	1) Attempting a partial update from one SDK version to another (such as 2.3.0 to 2.4.0)
"	"	2) The file is not a valid GBL file (for example, client is sending an EBL file)
0x0485	BOOTLOADER	The Gecko bootloader cannot erase or write flash as requested by AppLoader, for example if the download area is too small to fit the entire GBL image.
0x0486	INCORRECT_BOOTLOADER	Wrong type of bootloader. For example, target device has UART DFU bootloader instead of OTA bootloader installed.
0x0487	APPLICATION_OVERLAP_APPLOADER	New application image is rejected because it would overlap with the AppLoader.
0x0488	INCOMPATIBLE_BOOTLOADER_VERSION	AppLoader in Bluetooth SDK v3.0 requires Gecko Bootloader v1.11.
0x0489 (1)	ATT_ERROR_APPLICATION_VERSION_CHECK_FAIL	AppLoader fails checking application version.

(1) Only in SDK v3.x or later.

Note that the error codes listed above are applicable only when testing with the NCP host example. The upper half of the result code (0x04**) is generated by the BLE stack running on the NCP host device. The size of the ATT error code that is transmitted over the air is one octet. Values in the range 0x80-0x9F are reserved for application-specific errors in the Bluetooth specification.

4. Working with AppLoader and Secure Boot

When employing secure boot, the AppLoader and application must be signed individually for the application to be allowed to run. This is because the AppLoader authenticates the application before allowing it to run, just as the bootloader authenticates the AppLoader before allowing it to run.



This section describes how to work with this capability in a production environment.

4.1 Creating a Single Signed Image with a Batch File

As described previously, a signed GBL file can be produced by executing `create_bl_files.bat`/`create_bl_files.sh` with a private signing key file, `app_sign_key.pem`, in the same folder. The resulting GBL file, `full.gbl`, can be flashed directly to the target device for a successful boot. This method is convenient for testing secure boot during the development process, but is not secure for production since it requires the private signing key to be available in plain PEM format, rather than isolating it in a Hardware Security Module (HSM) and does not support the use of bootloader certificates.

4.2 Signing Firmware Images for Production

For Series One Devices (EFR32xG1x):

To sign a firmware image using an HSM, the image must first be separated into the AppLoader and application parts as follows.

1. Extract the AppLoader portion with the following command: `objcopy -O srec -j .text_apploader* apploader.s37`.
2. Sign the AppLoader for secure boot. For specific instructions on signing images with an HSM, see 'Signing an Application for Secure Boot using a Hard Security Module' in *UG162*. It is also possible to sign the AppLoader with a certificate although direct signing is sufficient for most use cases. For instructions on signing with a certificate with an HSM, see "Signing an Application for Secure Boot using an Intermediary Certificate" in *UG162*.
3. Extract the application with the following command: `objcopy -O srec -R .text_apploader* -R .text_signature* application.s37`.
4. Sign the application for secure boot. The instructions for signing the apploader in step 2 above also apply to the application.
5. Combine the signed apploader and application into a single image as follows: `commander convert <signed apploader>.s37 <signed application>.s37 -outfile signed_fw_image.s37`.
6. Optionally, see "Creating a Partial Signed and Encrypted GBL Upgrade File for Use with a Hardware Security Module" and "Creating a Signed GBL File Using a Hardware Security Module" in *UG162*.

For series two devices (EFR32xG2x), the apploader can be included in the bootloader project as a software component. This makes it possible to sign the application and bootloader binaries without any need to perform steps 1 – 6 above.

For more information on secure boot, see *AN1218, Series 2 Secure Boot with RTSL*.

5. Implementing Device Firmware Update in the User Application

In addition to the basic UART and OTA DFU solutions discussed in previous chapters, it is possible to implement the firmware update functionality completely in the user application. This makes it possible to use a custom GATT service instead of the Silicon Labs OTA service. In case of UART DFU updates, the application can be designed to support some other protocol than BGAPI. The user application can be designed to support both OTA and UART DFU updates if needed and it is possible to support other interfaces such as SPI.

To use this update mechanism, any application bootloader configuration may be used, using internal or external storage. At least one download area must be defined and the area must be large enough to fit the full GBL file. Partial update is not supported. The download area must not overlap with the user application and therefore this DFU solution is not applicable to devices or modules based on the EFR32xG1 (see Figure 3.1 Examples of Main Flash Layout when Using Gecko Bootloader with Bluetooth OTA DFU on page 6).

5.1 Basic Steps to Update Firmware from the User Application

The general firmware upgrade sequence is explained in *UG489: Silicon Labs Gecko Bootloader User's Guide for GSDK 4.0 and Higher* and *UG266: Silicon Labs Gecko Bootloader User's Guide for GSDK 3.2 and Lower*. The basic steps are summarized below.

1. Application initializes the Gecko bootloader by calling `bootloader_init()`;
2. The download area is erased by calling `bootloader_eraseStorageSlot(0)`;
3. The update image (full GBL file) is received either over-the-air or through some physical interface like UART, application writes the received bytes to the download area by calling `bootloader_writeStorage()`
4. (optional) Application can verify the integrity of the received GBL file by calling `bootloader_verifyImage()`
5. Before rebooting, call `bootloader_setAppImageToBootload(0)` to specify the slot ID where new image is stored
6. Reboot and instruct Gecko bootloader to perform the update by calling `bootloader_rebootAndInstall()`

It is assumed here that only one download area is configured and therefore the slot index in the above function calls is set to 0.

Note that the erase procedure in step 2) above takes several seconds to complete. If the new image is downloaded over a Bluetooth connection then the supervision timeout must be set long enough to avoid connection drops. Alternatively, the download area can be erased in advance, before the Bluetooth connection is opened. A third alternative is to erase the download area one flash page at a time while the writing progresses. This can be done using `bootloader_eraseRawStorage()`.

5.2 Enabling Gecko Bootloader API

Gecko bootloader has an application interface exposed through a function table in the bootloader. To be able to call Gecko bootloader functions from your Bluetooth application, the following source files must be added into the project:

btl_interface.c (common interface)

btl_interface_storage.c (interface to storage functionality)

These files are found in the Gecko SDK suite in the following directory (exact path depends on installed SDK version):

```
\gecko_sdk_suite\<version>\platform\bootloader\api\
```

Starting with SDK v3.0, these files are copied to the sample projects by default but the corresponding include files must be added to the source file(s) that call any Gecko bootloader functions:

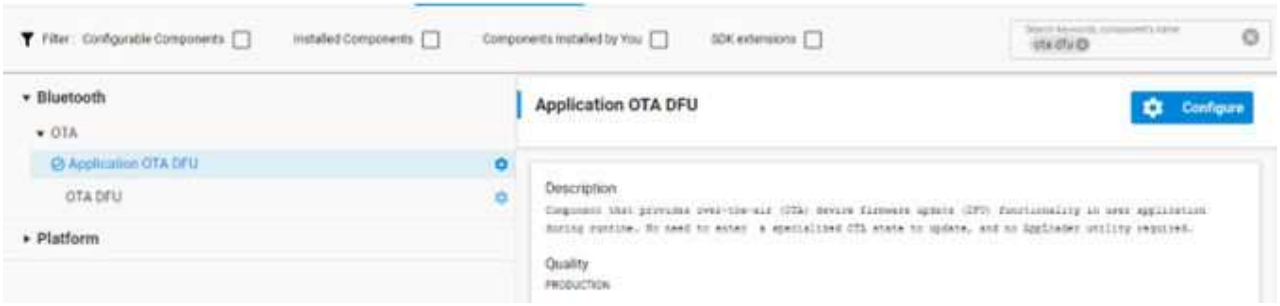
```
#include "btl_interface.h"
#include "btl_interface_storage.h"
```

In addition, if you are using v2.x, make sure that the following \platform\bootloader\ directory is added in the include paths. Using a symbolic path to the SDK installation, this can be configured by adding following strings to the include paths:

```
"${StudioSdkPath}/platform/bootloader"
"${StudioSdkPath}/platform/bootloader/api"
```

5.3 Example Implementation of Bluetooth OTA Update under Application Control

An example implementation of application-controlled OTA update is provided as a Software Component. To use it, simply add the “Application OTA DFU” component to the project:



Because AppLoader is not involved in this type of DFU implementation, it can be completely removed from the project to minimize flash usage.

In v3.x or higher: AppLoader can be removed from the SDK examples by uninstalling In-Place OTA DFU using the Project Configurator in Simplicity Studio 5.

In v2.x: AppLoader can be removed from the SDK examples by deleting **binapploader.o** from the project linker settings.

Simplicity Studio

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

IoT Portfolio
www.silabs.com/IoT

SW/HW
www.silabs.com/simplicity

Quality
www.silabs.com/quality

Support & Community
www.silabs.com/community

SILICON LABS

Silicon Laboratories Inc.
400 West Cesar Chavez
Austin, TX 78701
USA

www.silabs.com