nRF5 SDK v11.0.0-2.alpha

BLE DFU Profile

This information applies to the following SoftDevices: ***S130, S132***

The Device Firmware Update (DFU) Profile is an example for a proprietary profile that can be used to update firmware files using *Bluetooth* low energy. This profile is not a standard profile. It is defined by Nordic Semiconductor to demonstrate how a typical Device Firmware Update can be achieved.

The DFU Profile is used to transfer application, SoftDevice, or bootloader images from a BLE central (for example, a computer or a smartphone) to a peripheral (for example, a Heart Rate Sensor) that supports Device Firmware Updates using the DFU Service.

Profile dependencies: This profile requires the Generic Attribute Profile (GATT).

Configuration

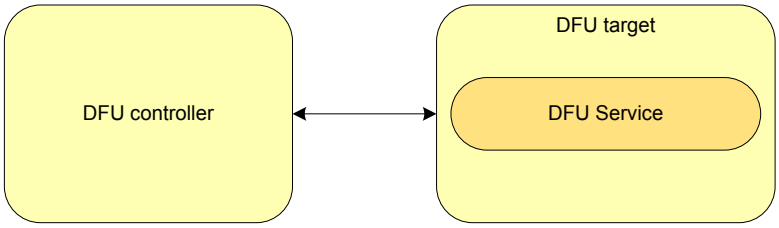
Roles

The profile defines two roles: DFU target and client (also referred to as DFU controller).

- The DFU target implements a GATT Server. This is the device that is updated by the DFU controller.
- The DFU controller implements a GATT client. This is the device that uploads a new firmware image to the DFU target.

Role/service relationships

The following diagram shows the relationships between services and the two profile roles.



Relationship between profile roles and services

A DFU target instantiates one instance of the DFU Service.

DFU controller role requirements

The DFU controller shall support the BLE DFU Service.

Service	DFU controller
Device Firmware Update Service	M

General error handling

The DFU controller shall be tolerant when receiving the following ATT Error Code defined in CSS Part B, Section 1.2 of Supplement to the *Bluetooth* Core Specification, Version 3 or later:

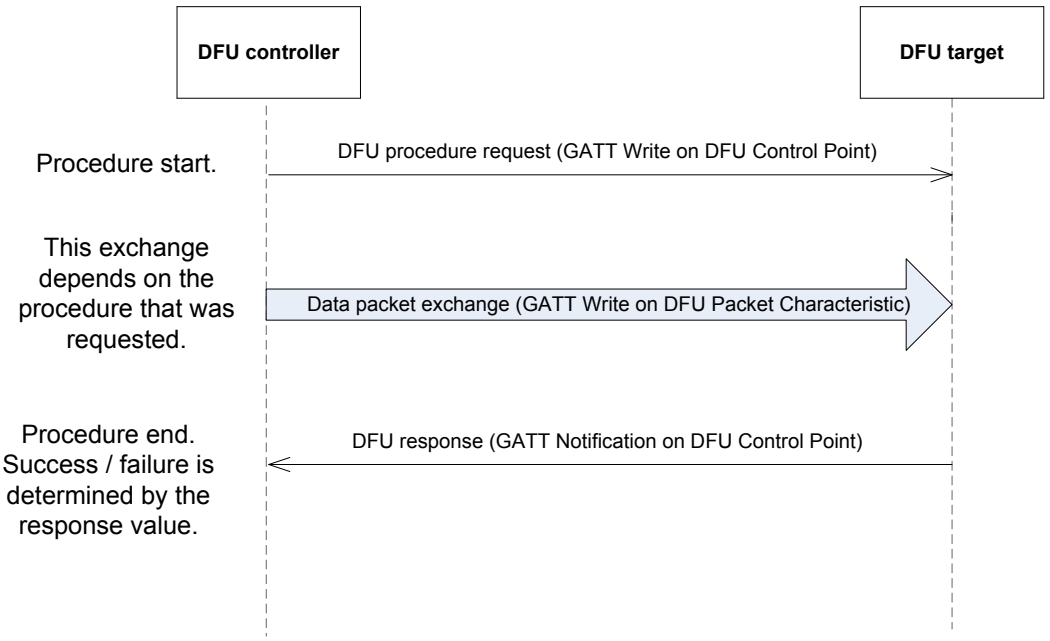
- Client Characteristic Configuration Descriptor Improperly Configured

DFU image transfer procedure

The DFU controller requests one of the procedures that are defined for a Device Firmware Update using the *DFU Control Point*. Each procedure requested by the controller is characterized by a request on the DFU Control Point, using the GATT Write procedure. This procedure may be followed by additional writes on the *DFU Packet* characteristic. The request to activate the image and reset the device ends the procedure. The DFU target for the procedure responds to this request using GATT notifications on the control point. The response code in the response packet contains information about the success or failure of the procedure. In case of failure, the response code provides an indication on the possible reason for the failure. See DFU Control Point for more details.

The DFU target processes one request at a time. Therefore, if a request is received on the target while it is already processing another request, an ATT error response ("Procedure Already In Progress") is received on the DFU controller. Asynchronous status information and information about the size of the received image is sent by the DFU target as GATT notifications on the control point.

The following message sequence chart shows a typical DFU Control Point procedure:



Typical DFU Control Point procedure

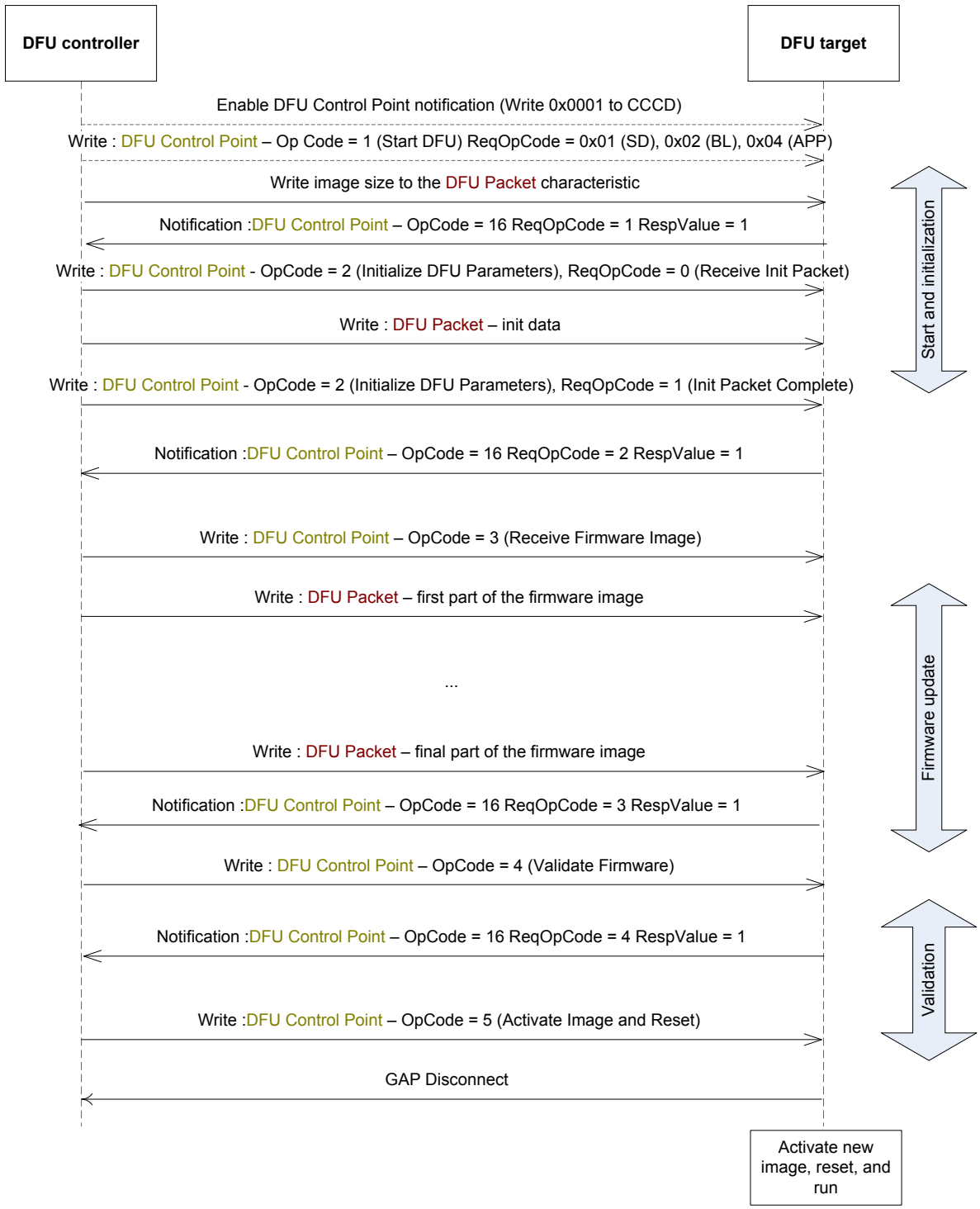
All defined DFU procedures are listed below:

DFU procedure	Description
Start DFU	Procedure to prepare the device for uploading the firmware. The size of the firmware image is provided in the request parameter. The response of the DFU target indicates if the device is ready for the next stage of the firmware update. The Start DFU procedure must be followed by a byte indicating the type of update.
Receive Init Data	Procedure to exchange information that must be exchanged before uploading the new firmware. Such information includes the device type, the revision type, the application version, hashs/public keys, and so on. See Safety-checking the image for more information.
Receive Image Data	Procedure to upload firmware, fragmented into DFU packets. The maximum size of each packet is (ATT_MTU - 3) octets. DFU packets can be of variable length with a minimum size of 1 octet; the length must be a multiple of the word size. The firmware is expected in binary format.
Validate	Procedure to validate the updated firmware image. The current implementation supports only CRC validation in addition to size validation (which is always performed). CRC validation is optional and uses the information provided in the Receive Init Data procedure.
Activate Image & Reset	Procedure to activate the new firmware and restart the device with the new firmware. This procedure results in a GAP Disconnect.
System Reset	Procedure to reset the system. This procedure result in a GAP Disconnect. This procedure can be requested at any stage. The system will then restart with the old application if the device had an existing application. Otherwise, the system will restart in DFU mode.
Report Received Image Size	Procedure to request the size of the received image. This procedure is particularly useful on reconnection after a link loss. See Link loss procedure for more information.
Packet Receipt Notification	Procedure to request notifications every time after receiving a certain number of packets. The number of packets is specified in the request by the controller. This procedure is not mandatory.

See DFU Control Point for more information about the procedures.

When the DFU target is in DFU mode, it is in *GAP General Discoverable mode* and is *connectable*. The 128-bit DFU Service UUID is advertised in the advertisement data, along with the full name (DfuTarg). When the DFU target is connected to the DFU controller, the DFU process can be started by requesting a Start DFU procedure.

The following message sequence chart shows a typical firmware update exchange between a DFU controller and a DFU target:



Transfer of an image to the DFU target

Idle mode procedure

If no connection is established with the DFU target after 60 seconds, the target device will restart in normal mode with the old application if the device had an existing application. Otherwise, the system will restart in DFU mode.

Image validation procedure

The post-validate function dfu_init_postvalidate in `dfu_init_template` validates the updated firmware image.

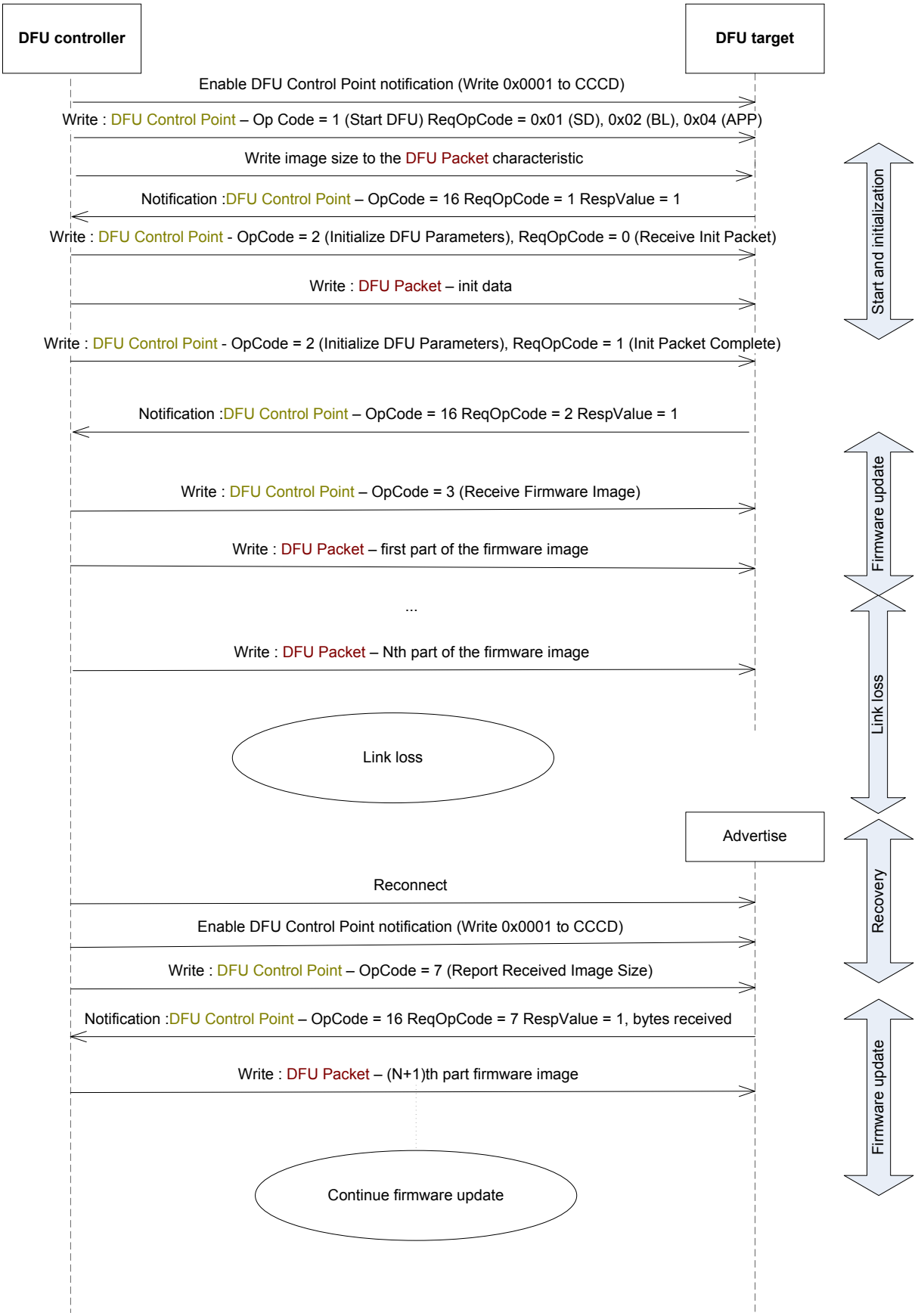
Idle connection procedure

When the bootloader example application detects that the connection has been idle for a certain period, thus if the DFU controller has not written any packets to continue the firmware update, the update is stopped. The connection is terminated and the previously valid application is started. If there is no valid application, the device remains in bootloader mode and waits for a reconnection from the DFU controller.

Link loss procedure

When the bootloader example application detects a link loss, the DFU state and image size is stored. When the controller connects again, the transfer can resume from where it stopped. The controller can request information about the size of the received image using the Report Received Image Size procedure and start thetransfer by applying the necessary offset. In the disconnected state after a link loss, the Idle mode procedure applies.

The following message sequence chart shows a typical link loss recovery procedure:



Recovery after link loss

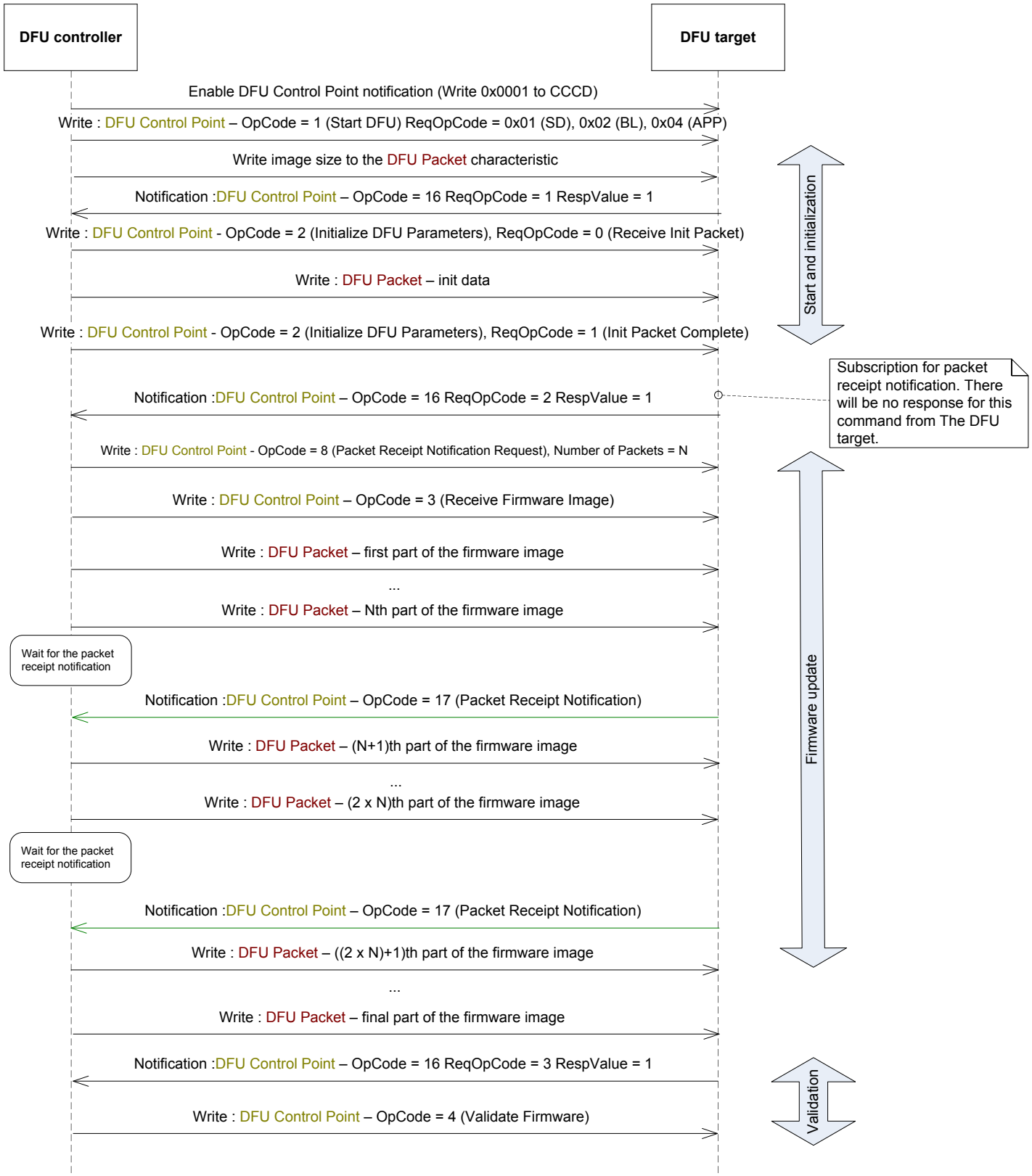
Packet Receipt Notification procedure

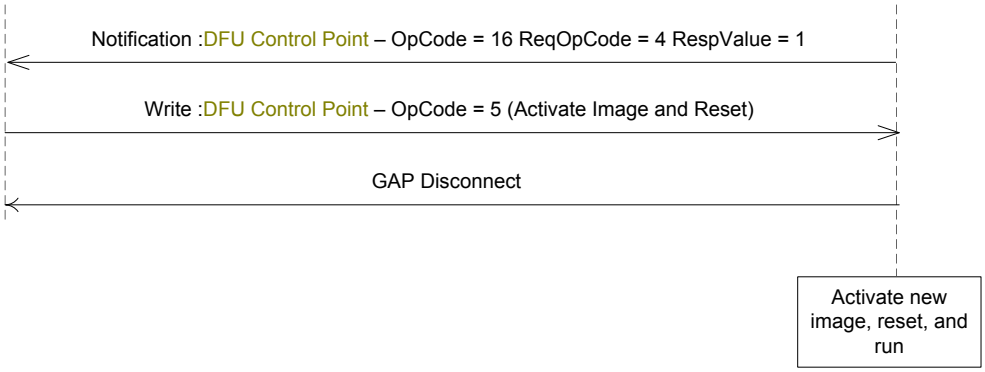
The DFU controller can subscribe to notifications from the DFU target, to be notified every time a given number of firmware packets has been received. To enable such notifications, the DFU controller must write the Op

Code 0x08 (Packet Receipt Notification Request) followed by the number of packets to the DFU Control Point. The DFU target will then send a notification of the DFU Control Point with Op Code 0x11 (Packet Receipt Notification) every time the specified number of firmware packets has been received. The DFU controller should wait for this notification every time after sending the specified number of firmware packets.

As part of the packet receipt notification, the DFU target also sends the total number of bytes of firmware data received so far. This information can be used for consistency checks by the DFU controller.

The following message sequence chart shows a typical Packet Receipt Notification procedure:





Packet Receipt Notification procedure

Security considerations

All supported characteristics specified by the DFU Service on the target are set to Security Mode 1 and Security Level 1.

This document was last updated on Fri Dec 18 2015.
Please send us your feedback about the documentation! For technical questions, visit the Nordic Developer Zone <https://devzone.nordicsemi.com/questions/>.