NILE

BT 5.0 + ZB/Thread + NFC-A Standalone Module

Secure DFU over Thread application note

Version 0.1

6141 Running Springs Rd
San Jose, CA 95135
www.ivativ.com

December 11, 2019

Email: info@ivativ.com
Ph: (408) 893 7812

Table of Contents

Table of Figures 2
1. Scope of the document 3
2. Overview 4
2.1 Introduction 4
2.2 Security 4
2.3 Reasons for firmware update 4
2.4 Types of OTA updates in Thread 4
3. Requirements 6
3.1 Hardware requirement: 6
3.2 Software requirements 6
4. Test setup 7
4.1 Procedure 7
5. Test results 11
6. References 12

Table of Figures

Figure 1: Starting of DFU (OTA) process 9
Figure 2: Update in progress 9
Figure 3: End of the firmware update 9

1. Scope of the document

The following article shows how to securely upgrade Thread application OTA (over-the-air) using signed encrypted files. The process is tested with nRF nRF5_SDK_for_Thread and Zigbee v3.2.0. This document explains the steps in DFU, keys generation, package preparation for a DFU.

2. Overview

2.1 Introduction

The ability to update the firmware of units already deployed in the field is a common requirement for many products. For example, it may be necessary to add new features into products after the first version has been launched.

Products that use Thread technology often designed to work with smart homes, or similar consumer electronic devices that are connected to the Internet. This makes it possible to implement OTA (Over-the-Air) firmware update capability without adding any extra cost or significant increase in the software complexity. The Internet of Things (IoT) also poses a challenge, because new types of devices and use cases are continually introduced, which can create unanticipated interoperability issues. For this reason, the ability to do OTA firmware updates is essential for any IoT device.

2.2 Security

Here we are using key, that key will be shared by the device and by the user. User need to add the key to his application which he is building. So when we do the update the device will check the key and accepts the incoming DFU request.

2.3 Reasons for firmware update

Firmware update needed for specific reasons like

For example, the Thread protocol under constant development, with different revisions of the protocol stack released over time. A revision may include new features, performance optimizations, and patches to bugs or interoperability issues. It may be desirable to use the OTA update procedures to change to the latest available stack revision, even if the user application itself remains unchanged.

2.4 Types of OTA updates in Thread

Thread OTA update process can be done in 2 ways

- Unicast mode
- Multicast mode

Unicast mode:

In unicast mode, the Thread DFU server sends a trigger packet with the mode bit set to 0. In this mode, the DFU server does not undertake any action on its own - it is the DFU client's responsibility to send appropriate requests to the server and download the image. All communication in this mode (with exception of the initial trigger packet) is sent through unicast messages. Therefore, each node must download the image individually. Use this mode when there is a single device to be updated. This mode is also used when the DFU process is initialized by the client.

Unicast mode is the default mode when no --address option is passed to nrfutil or when the passed address is a unicast address.

Multicast mode:

In multicast mode, the Thread DFU server sends a trigger packet with the mode bit set to 1. In this mode, the DFU server sends consecutive blocks of init packet and firmware package through multicast messages. Every DFU client node that receives the multicast DFU trigger packet decides whether to participate in the DFU process and store the firmware blocks. A client that recognizes that it missed one or more of the firmware blocks can send a request to the server for retransmission of these specific blocks. Use this mode when the firmware must be updated on several nodes at once.

You can select this mode by passing a realm-local multicast address as a parameter to nrfutil, for example, --address FF03::1.

NOTE: This document will explain about the **unicast** mode only.

Note: Assuming the reader of this document has expertise in Thread. The reader should have hands on using the Nordic SDK for thread and zigbee. The readers should have knowledge to install all the required tools by following the instructions in the link attached below.

3. Requirements

3.1 Hardware requirement:

- DVK – 2 Nos
- Windows PC
- Micro USB cables - 2 Nos

3.2 Software requirements

- nRF SDK
- nrfjprog tool
- nrfutil tool
- Jlink tool
- segger embedded studio
- micro-ecc

Note: All the tools and applications must be installed. Respective download links are attached herewith.

4. Test setup

Precondition: To test the Thread OTA Upgrade process, we need at least two NILE Development Kit boards. One of these boards will be an OTA Upgrade Server that distributes the new firmware. The others will play the role of OTA Upgrade Clients that are updated.

- Here the SDK refers to the nRF5_SDK_for_Thread and Zigbee v3.2.0
- Assume the 2 DK's named as
    - Client
    - Server

DFU client: A client that runs on a DFU target, which is the device that is being upgraded, and is responsible for downloading and installing the new firmware. The DFU client incorporates a DFU controller which manages the DFU process. This means that each DFU target might be in a different state regarding the DFU process at a given point of time.

DFU server: a server that provides a firmware package. For example, the DFU server could be a cloud service or NILE Development Kit in conjunction with **nrfutil**, or a mobile phone running an application.

Note: All the commands should be given from command line.

4.1 Procedure

1. After downloading the SDK for thread and zigbee. Go to the path from command line SDK\examples\thread\dfu
2. Need to create keys for secure update. So follow the below commands from command line to generate the keys
    a. Create a private key:
        - **nrfutil keys generate priv.pem**
    b. Create a public key in code format and store it in a file named dfu_public_key.c:
        - **nrfutil keys display --key pk --format code priv.pem --out_file dfu_public_key.c**
    c. The generated keys will be in the path of SDK\examples\thread\dfu
    d. Copy the dfu_public_key.c file to SDK\examples\dfu\ by replacing the existing file
3. Make sure that you are in the path of SDK\examples\thread\dfu
4. Build the bootloader by giving the command from the command line.
    - **make -C bootloader\pca10056\blank\armgcc**
5. Prepare the DFU client
    a. Compile the DFU client by running following command
        - **make -C client\pca10056\blank\armgcc**
    b. Make sure that you are the path of SDK\examples\thread\dfu and generate bootloader settings hex file
        - **nrfutil settings generate --family NRF52840 --application client\pca10056\blank\armgcc_build\nrf52840_xxaa.hex --application-version 1 --bootloader-version 1 --bl-settings-version 2 settings.hex**
    c. Merge the client and bootloader hex files by using the below command

- **mergehex -m client\pca10056\blank\armgcc_build\nrf52840_xxaa.hex settings.hex -o dfu_client.hex**

d. The file named dfu_client.hex file is generated in the path SDK\examples\thread\dfu

6. Load the dfu_client.hex file to the DK
   a. Connect the client DK to the PC and erase the flash by using below command
      - **nrfjprog -f nrf52 --eraseall**
   b. Flash the MBR to the DK using the command below
      - **nrfjprog -f nrf52 -r --program ..\..\..\components\softdevice\mbr\nrf52840\hex\mbr_nrf52_X.X.X.hex --chiperase**
   c. Flash the bootloader to the client DK using below command
      - **nrfjprog -f nrf52 -r --program bootloader\pca10056\blank\armgcc_build\nrf52840_xxxx.hex**
   d. Flash the merged DFU client by following the command
      - **nrfjprog -f nrf52 -r --program dfu_client.hex --sectorerase**
7. Prepare the firmware package for the DFU process
   a. To successfully perform the DFU process, you need to modify the DFU Client application, so that the new firmware has a different checksum. For example, add the following line to the main() .
   b. So go the path SDK\examples\thread\dfu\client\. Open the main.c file and add some changes like
      - **LEDS_ON(BSP_LED_3_MASK);**
   c. Compile the modified DFU client application by following below command. And also make sure that you are back to the same path SDK\examples\thread\dfu
      - **make -C client\pca10056\blank\armgcc**
   d. Prepare the firmware package with the updated application by using nrfutil
      - **nrfutil pkg generate --hw-version 52 --sd-req 0x00 --application-version 2 --application client\pca10056\blank\armgcc_build\nrf52840_xxaa.hex --key-file priv.pem app_dfu_package.zip**
   e. The package named as “app_dfu_package.zip” will be generated at the path SDK\examples\thread\dfu.
8. Now we need to run the DFU to update the updated application to client using the server.
   a. Connect the DFU server nRF52840 Development Kit board to your computer. This board serves as the connectivity IC to the Thread network. This board does not require installation of any firmware. It will be flashed by **nrfutil**.
   b. To make the DK-2 (server) to act as server it does not need any application or software to be deployed in it. It will acts as server based on the application we are using to update DFU.
   c. Now make sure the client is in ON state(power on or active state)
   d. Now the following command to start the DFU process over Thread, where COM3 is the DFU Server DK serial port
      - **nrfutil dfu thread -f -pkg app_dfu_package.zip -p COM3 --channel 11 --panid 43981**
   e. The update will take nearly couple of minutes.

```
C:\Users\THIS\Downloads\NILE_SDK's\nRF5SDKforThreadandZigbee20029775ac\examples\thread\dfu>nrfutil dfu thread -f -pkg app_dfu_package.zip -p COM30 --channel 11 --panid
43981
Address not specified. Using ff03::1 (all Thread nodes)
Using connectivity board at serial port: COM30
Flashing connectivity firmware...
Connectivity firmware flashed.
Waiting for NCP to promote to a router...
Thread DFU server is running... Press <Ctrl + D> to stop.

fdde:ad00:beef::ff:fe00:c800:   0%|                                                                                                  | 0/5447 [00:00<?, ?it/s]
fdde:ad00:beef::ff:fe00:c800:   0%|                                                                                                | 1/5447 [00:00<20:41,  4.39it/s]
fdde:ad00:beef::ff:fe00:c800:   0%|                                                                                                | 3/5447 [00:00<17:53,  5.07it/s]
fdde:ad00:beef::ff:fe00:c800:   0%|                                                                                                | 4/5447 [00:00<16:45,  5.41it/s]
fdde:ad00:beef::ff:fe00:c800:   0%|1                                                                                               | 6/5447 [00:00<13:38,  6.65it/s]
fdde:ad00:beef::ff:fe00:c800:   0%|1                                                                                               | 8/5447 [00:00<11:53,  7.63it/s]
fdde:ad00:beef::ff:fe00:c800:   0%|1                                                                                               | 9/5447 [00:01<11:43,  7.73it/s]
fdde:ad00:beef::ff:fe00:c800:   0%|1                                                                                              | 11/5447 [00:01<10:59,  8.24it/s]
fdde:ad00:beef::ff:fe00:c800:   0%|2                                                                                              | 12/5447 [00:01<10:26,  8.67it/s]
fdde:ad00:beef::ff:fe00:c800:   0%|2                                                                                              | 13/5447 [00:01<11:13,  8.07it/s]
fdde:ad00:beef::ff:fe00:c800:   0%|2                                                                                              | 14/5447 [00:01<11:42,  7.73it/s]
fdde:ad00:beef::ff:fe00:c800:   0%|2                                                                                              | 15/5447 [00:01<11:32,  7.85it/s]
fdde:ad00:beef::ff:fe00:c800:   0%|2                                                                                              | 16/5447 [00:01<11:59,  7.55it/s]
fdde:ad00:beef::ff:fe00:c800:   0%|3                                                                                              | 17/5447 [00:02<11:32,  7.84it/s]
fdde:ad00:beef::ff:fe00:c800:   0%|3                                                                                              | 18/5447 [00:02<11:21,  7.97it/s]
fdde:ad00:beef::ff:fe00:c800:   0%|3                                                                                              | 20/5447 [00:02<11:07,  8.13it/s]
fdde:ad00:beef::ff:fe00:c800:   0%|3                                                                                              | 22/5447 [00:02<10:19,  8.75it/s]
fdde:ad00:beef::ff:fe00:c800:   0%|4                                                                                              | 23/5447 [00:02<10:11,  8.87it/s]
```

Figure 1: Starting of DFU (OTA) process

```
dde:ad00:beef::ff:fe00:c800:  56%|#####################################################4                                          | 3032/5447 [05:15<04:55,  8.16it/s]
dde:ad00:beef::ff:fe00:c800:  56%|#####################################################4                                          | 3033/5447 [05:15<05:16,  7.63it/s]
dde:ad00:beef::ff:fe00:c800:  56%|#####################################################4                                          | 3034/5447 [05:15<05:14,  7.68it/s]
dde:ad00:beef::ff:fe00:c800:  56%|#####################################################5                                          | 3036/5447 [05:16<04:36,  8.71it/s]
dde:ad00:beef::ff:fe00:c800:  56%|#####################################################5                                          | 3038/5447 [05:16<03:58, 10.09it/s]
dde:ad00:beef::ff:fe00:c800:  56%|#####################################################5                                          | 3040/5447 [05:16<04:00, 10.02it/s]
dde:ad00:beef::ff:fe00:c800:  56%|#####################################################6                                          | 3042/5447 [05:16<03:50, 10.45it/s]
dde:ad00:beef::ff:fe00:c800:  56%|#####################################################6                                          | 3044/5447 [05:16<04:05,  9.80it/s]
dde:ad00:beef::ff:fe00:c800:  56%|#####################################################6                                          | 3046/5447 [05:16<03:59, 10.03it/s]
dde:ad00:beef::ff:fe00:c800:  56%|#####################################################7                                          | 3048/5447 [05:17<04:23,  9.12it/s]
dde:ad00:beef::ff:fe00:c800:  56%|#####################################################7                                          | 3050/5447 [05:17<04:33,  8.76it/s]
dde:ad00:beef::ff:fe00:c800:  56%|#####################################################7                                          | 3052/5447 [05:17<04:01,  9.90it/s]
dde:ad00:beef::ff:fe00:c800:  56%|#####################################################8                                          | 3054/5447 [05:17<03:39, 10.89it/s]
dde:ad00:beef::ff:fe00:c800:  56%|#####################################################8                                          | 3056/5447 [05:17<03:40, 10.83it/s]
dde:ad00:beef::ff:fe00:c800:  56%|#####################################################8                                          | 3058/5447 [05:18<03:36, 11.06it/s]
dde:ad00:beef::ff:fe00:c800:  56%|#####################################################9                                          | 3060/5447 [05:18<04:23,  9.06it/s]
dde:ad00:beef::ff:fe00:c800:  56%|#####################################################9                                          | 3061/5447 [05:18<04:56,  8.06it/s]
dde:ad00:beef::ff:fe00:c800:  56%|#####################################################9                                          | 3063/5447 [05:18<04:39,  8.52it/s]
dde:ad00:beef::ff:fe00:c800:  56%|#####################################################                                           | 3065/5447 [05:18<04:05,  9.68it/s]
dde:ad00:beef::ff:fe00:c800:  56%|#####################################################                                           | 3067/5447 [05:19<04:21,  9.11it/s]
dde:ad00:beef::ff:fe00:c800:  56%|#####################################################                                           | 3069/5447 [05:19<04:09,  9.53it/s]
dde:ad00:beef::ff:fe00:c800:  56%|#####################################################1                                          | 3071/5447 [05:19<04:12,  9.41it/s]
dde:ad00:beef::ff:fe00:c800:  56%|#####################################################1                                          | 3072/5447 [05:19<04:25,  8.94it/s]
dde:ad00:beef::ff:fe00:c800:  56%|#####################################################1                                          | 3073/5447 [05:19<05:41,  6.94it/s]
dde:ad00:beef::ff:fe00:c800:  56%|#####################################################1                                          | 3074/5447 [05:20<05:16,  7.49it/s]
dde:ad00:beef::ff:fe00:c800:  56%|#####################################################1                                          | 3075/5447 [05:20<05:17,  7.48it/s]
dde:ad00:beef::ff:fe00:c800:  56%|#####################################################2                                          | 3076/5447 [05:20<04:56,  8.00it/s]
dde:ad00:beef::ff:fe00:c800:  57%|#####################################################2                                          | 3078/5447 [05:20<04:20,  9.09it/s]
dde:ad00:beef::ff:fe00:c800:  57%|#####################################################2                                          | 3079/5447 [05:20<04:14,  9.32it/s]
dde:ad00:beef::ff:fe00:c800:  57%|#####################################################3                                          | 3081/5447 [05:20<04:00,  9.82it/s]
dde:ad00:beef::ff:fe00:c800:  57%|#####################################################3                                          | 3083/5447 [05:20<04:06,  9.58it/s]
dde:ad00:beef::ff:fe00:c800:  57%|#####################################################3                                          | 3084/5447 [05:21<04:23,  8.97it/s]
dde:ad00:beef::ff:fe00:c800:  57%|#####################################################3                                          | 3085/5447 [05:21<04:21,  9.03it/s]
dde:ad00:beef::ff:fe00:c800:  57%|#####################################################3                                          | 3086/5447 [05:21<04:42,  8.37it/s]
```

Figure 2: Update in progress

```
fdde:ad00:beef::ff:fe00:c800:  99%|#################################################################################################| 5391/5447 [09:32<00:06,  8.88it/s]
fdde:ad00:beef::ff:fe00:c800:  99%|#################################################################################################| 5393/5447 [09:32<00:05, 10.21it/s]
fdde:ad00:beef::ff:fe00:c800:  99%|#################################################################################################| 5395/5447 [09:32<00:05,  9.24it/s]
fdde:ad00:beef::ff:fe00:c800:  99%|#################################################################################################1| 5397/5447 [09:33<00:05,  9.05it/s]
fdde:ad00:beef::ff:fe00:c800:  99%|#################################################################################################1| 5399/5447 [09:33<00:04, 10.17it/s]
fdde:ad00:beef::ff:fe00:c800:  99%|#################################################################################################1| 5401/5447 [09:33<00:05,  9.11it/s]
fdde:ad00:beef::ff:fe00:c800:  99%|#################################################################################################2| 5403/5447 [09:33<00:04, 10.61it/s]
fdde:ad00:beef::ff:fe00:c800:  99%|#################################################################################################2| 5406/5447 [09:33<00:03, 11.95it/s]
fdde:ad00:beef::ff:fe00:c800:  99%|#################################################################################################3| 5408/5447 [09:33<00:03, 12.31it/s]
fdde:ad00:beef::ff:fe00:c800:  99%|#################################################################################################3| 5410/5447 [09:34<00:03, 11.67it/s]
fdde:ad00:beef::ff:fe00:c800:  99%|#################################################################################################3| 5412/5447 [09:34<00:02, 11.85it/s]
fdde:ad00:beef::ff:fe00:c800:  99%|#################################################################################################4| 5414/5447 [09:34<00:03, 10.88it/s]
fdde:ad00:beef::ff:fe00:c800:  99%|#################################################################################################4| 5416/5447 [09:34<00:02, 11.69it/s]
fdde:ad00:beef::ff:fe00:c800:  99%|#################################################################################################5| 5419/5447 [09:34<00:02, 12.25it/s]
fdde:ad00:beef::ff:fe00:c800: 100%|#################################################################################################5| 5421/5447 [09:34<00:02, 12.05it/s]
fdde:ad00:beef::ff:fe00:c800: 100%|#################################################################################################5| 5423/5447 [09:35<00:02, 10.72it/s]
fdde:ad00:beef::ff:fe00:c800: 100%|#################################################################################################6| 5425/5447 [09:35<00:02, 10.71it/s]
fdde:ad00:beef::ff:fe00:c800: 100%|#################################################################################################6| 5427/5447 [09:35<00:01, 11.27it/s]
fdde:ad00:beef::ff:fe00:c800: 100%|#################################################################################################6| 5429/5447 [09:35<00:01, 10.80it/s]
fdde:ad00:beef::ff:fe00:c800: 100%|#################################################################################################7| 5431/5447 [09:36<00:01,  9.77it/s]
fdde:ad00:beef::ff:fe00:c800: 100%|#################################################################################################7| 5433/5447 [09:36<00:01, 10.02it/s]
fdde:ad00:beef::ff:fe00:c800: 100%|#################################################################################################7| 5435/5447 [09:36<00:01, 10.21it/s]
fdde:ad00:beef::ff:fe00:c800: 100%|#################################################################################################8| 5437/5447 [09:36<00:00, 10.88it/s]
fdde:ad00:beef::ff:fe00:c800: 100%|#################################################################################################8| 5439/5447 [09:36<00:00,  9.82it/s]
fdde:ad00:beef::ff:fe00:c800: 100%|#################################################################################################8| 5441/5447 [09:37<00:00,  8.63it/s]
fdde:ad00:beef::ff:fe00:c800: 100%|#################################################################################################9| 5443/5447 [09:37<00:00,  9.78it/s]
fdde:ad00:beef::ff:fe00:c800: 100%|#################################################################################################9| 5445/5447 [09:37<00:00,  8.98it/s]
fdde:ad00:beef::ff:fe00:c800: 100%|#################################################################################################9| 5446/5447 [09:37<00:00,  8.32it/s]
fdde:ad00:beef::ff:fe00:c800: 100%|##################################################################################################| 5447/5447 [09:37<00:00,  8.22it/s]

Thread DFU upload complete
```

Figure 3: End of the firmware update

9. After successful DFU, the board will reset and loads with the new application

5. Test results

Observed that the thread client is updated with the new application via OTA. With the help of thread server.

6. References

Info center - https://infocenter.nordicsemi.com/index.jsp

Nordicsemi – https://www.nordicsemi.com/

Nrfutil - https://github.com/NordicSemiconductor/pc-nrfutil