

SECURE-DFU

Device Firmware Update

Secure-DFU

Contents

소개

Secure-DFU란?

빠른 Secure DFU 사용 가이드

Secure DFU

첫번째 : Secure-DFU 준비하기

두번째 : Security Key 생성

세번째 : Bootloader 컴파일

업데이트할 Firmware Package 생성하기

준비 사항

Package 생성

부가사항

양산을 위한 통합된 펌웨어 만들기

첫번째 : Bootloader Settings File 생성

두번째 : 하나의 파일로 통합 생성

Firmware Package UPDATE

Target Board에 펌웨어 다운로드

Mobile 또는 nRF Connect 를 통해 무선 펌웨어 업데이트

nRF Connect Desktop 이용한 방법

nRF Connect Mobile 을 이용한 방법

nrfutil.exe 를 이용하여 Command Line으로 업데이트하는 방법

Serial을 통한 유선 업데이트

참조 문서

Secure-DFU란?



Nordic SDK 에서 제공되는 Firmware Update 기능으로 Bluetooth Low Energy/Bluetooth Mesh/Thread/ZigBee와 같은 무선 프로토콜을 이용하는 OTA Upgrade 기능 및 UART/SPI와 같은 wired Serial Interface를 통해 생산 제품에 펌웨어를 업데이트 하는 기능

Secure DFU는 기존의 Device Firmware Upgrade 기능과는 다르게 Firmware 를 Signing하여 양단의 키 값이 맞지 않을 경우 사용하지 못하도록 하는 기능이 추가됨

- PC 버전과 Mobile App 버전에 대한 프로그램 및 소스코드 제공
 - Android Google Play
 - Apple App Store
 - PC version (nRF Connect)

빠른 SECURE DFU 사용 가이드

- 1. script를 이용하여 micro-ecc compile
- 2. nrfutil 설치
- 3. nrfutil를 이용하여 Private/Public key 생성
- 4. 생성된 Public Key를 DFU(Bootloader) firmware code에 삽입하여 DFU 예제 컴파일
- 5. nrfutil을 이용하여 bootloader settings 파일 생성
- 6. mergehex를 통해 bootloader settings, softdevice, application, bootloader 를 하나의 파 일로 통합
- 7. 통합된 펌웨어를 Target Device에 다운로드
- 8. nrfutil을 이용하여 새롭게 업데이트 할 Firmware package 생성
- 9. 생성된 Firmware Package를 nRF Connect for Mobile, nRF Connect for Desktop 또는 nRFToolBox App을 이용하여 Target Device에 무선으로 업데이트

첫번째 : Secure-DFU 준비하기

- Python PIP (PIP 가 설치되지 않았을 경우 참조 here) * Python 3.0 지원안됨
- ARM 용 GCC 컴파일러 설치 (4.9-2015-q3-update 이상)
- Make 설치 (use MinGW, GNU Make, or Xcode) 쉬운 설정을 위해 GNU Make를 설치를 권 장
- nrfutil

Python (2.7) 이 설치되어 있을 경우 (Windows/Linux 동일)

\$ pip install nrfutil

```
(base) C:\Users\Eugene≻pip install nrfutil
Installing collected packages: nrfutil
Successfully installed nrfutil-5.1.0
```

실행 파일 직접 <mark>다운로드</mark>

- micro-ecc library
 - SDK 에서 제공되는 Script File을 이용하여 Library Download 및 Build
 - 위치:nRF5_SDK_x.x.x_xxxxx\external\micro-ecc\
 - build_all.bat (Windows) 또는 build_all.sh (Linux/macOS) 실행
 - 빌드시 아래와 같은 에러가 날 경우 SDK에서 설정된 Compiler와 설치된 gcc 버 전의 차이가 있으므로 SDK 의 Makefile 관련 내용의 수정이 필요

문제현상



해결방안

```
위의 그림에서 가이드하는 바와 같이
nRF5_SDK\components\toolchain\gcc\Makefile.windows 의 내용중
Compiler 관련 내용을 사용자 환경에 맞게 변경하거나 SDK 맞는 버전을 다운로드
하여 설치
```

```
GNU_INSTALL_ROOT := C:/Program Files (x86)/GNU Tools
ARM Embedded/6 2017-q2-update/bin/
GNU_VERSION := 7.3.1
GNU_PREFIX := arm-none-eabi
```

```
두번째 : Security Key 생성
```

nrfutil 을 통한 Private Key 생성하기

nrfutil keys generate priv.pem

Private Key로 부터 Public Key 생성하기

```
nrfutil keys display --key pk --format code priv.pem --out_file
public_key.c
또는
nrfutil keys display --key pk --format code priv.pem
```

9x33, 9x69, 9xaa, 8x97, 9x5c, 9x33, 9x55, 9x44, 9xac, 9x29, 9x53, 9x83, 9x83, 9x83, 9x85, 9x66, 9x51, 9x8e, 9x17, 9x8e, 9x85, 9x56, 9x57, 9x54, 9x87, 9x58, 9x73, 9x89, 9x75, 9x89, 9x75, 9x85, 9x86, 9x51, 9x75, 9x85, 9x84, 9x73, 9x89, 9x82, 9x75, 9x85, 9x86, 9x51, 9x75, 9x85, 9x84, 9x83, 9x75, 9x85, 9x84, 9x83, 9x75, 9x85, 9x84, 9x83, 9x75, 9x85, 9x86, 9x51, 9x82, 9x82, 9x84, 9x43, 9x73, 9x89, 9x84, 9x73, 9x89, 9x84, 9x75, 9x85, 9x86, 9x51, 9x84, 9x73, 9x89, 9x84, 9x73, 9x88, 9x84, 9x73, 9x88, 9x84, 9x73, 9x88, 9x84, 9x73, 9x89, 9x84, 9x73, 9x85, 9x84, 9x83, 9x73, 9x85, 9x84, 9x83, 9x73, 9x85, 9x84, 9x83, 9x73, 9x85, 9x84, 9x83, 9x84, 9x83, 9x84, 9x84, 9x74, 9x88, 9x84, 9x73, 9x88, 9x84, 9x73, 9x88, 9x84, 9x84,

세번째 : Bootloader 컴파일

위 단계에서 생성된 Public Key 를 코드형태로 Bootloader Firmware (SDK\examples\dfu\bootloader_secure_ble)에 삽입(dfu_public_key.c)하여 컴파일

```
#include "sdk_config.h"
#include "stdint.h"
#include "compiler_abstraction.h"
#if NRF_CRYPTO_BACKEND_OBERON_ENABLED
/* Oberon backend is changing endianness thus public key must be kept
in RAM. */
#define _PK_CONST
#else
#define _PK_CONST const
#endif
/** @brief Public key used to verify DFU images */
__ALIGN(4) const uint8_t pk[64] =
{
    0xa3, 0x69, 0xaa, 0x07, 0xbc, 0x83, 0xf5, 0x94, 0xac, 0x2b, 0x58,
0x8a, 0x08, 0xa9, 0x0e, 0x85, 0x46, 0x51, 0x0e, 0x17, 0x8e, 0x88,
0x5f, 0xba, 0xdf, 0x59, 0x44, 0x84, 0x43, 0xc6, 0xf9, 0xd6,
    0x05, 0x3b, 0x19, 0xf0, 0xa4, 0xf3, 0xe1, 0xed, 0xab, 0x77, 0x98,
0x76, 0xf8, 0x00, 0xfa, 0xc8, 0xa2, 0xac, 0x44, 0xc7, 0x68, 0x7a,
0x80, 0xf3, 0xf5, 0x8e, 0xbf, 0xec, 0xb6, 0xb0, 0xef, 0xe3
};
```

준비 사항

- 업데이트 펌웨어 및 Private Key file
- Softdevice version information (예. S132 v6.1.1 == 0xB7)
 - https://github.com/NordicSemiconductor/pc-nrfutil#usage
 - o nrfutil를 통해서 확인

nrfutil pkg generate --help

Package 생성

```
nrfutil pkg generate --hw-version 52 --sd-req 0xB7 --application-
version 1 --application nrf52832_xxaa.hex --key-file priv.pem
app_dfu_package.zip
```

부가사항

양산을 위한 통합된 펌웨어 만들기

첫번째 : Bootloader Settings File 생성

Application Firmware가 정상적으로 Flash 된 것인지를 확인하기 위해 사용되는 Setting 값들에 대한 파일을 생성

Firmware Download 시 Bootloader Settings 파일이 추가되지 않았을 경우 Bootloader에서 Application 영역으로 실행주소를 옮기지 못하는 문제가 발생되므로 반드시 생성해서 같이 Download 해야 함

nrfutil settings generate --family NRF52 --application
<application.hex> --application-version 1 --bootloader-version 1 --blsettings-version 1 bootloader_settings.hex

두번째 : 하나의 파일로 통합 생성

생성된 Bootloader Settings 파일은 Application Firmware 와 함께 통합하여 nRF5x 에 다운로드

```
mergehex -m <application.hex> <bootloader_settings.hex> -o <output
file.hex>
```

Softdevice 및 Bootloader를 하나로 통합할 경우

mergehex -m <application.hex> <bootloader_settings.hex>
<bootloader.hex> <softdevice.hex> -o <output file.hex>

FIRMWARE PACKAGE UPDATE

위에서 만든 Firmware Package와 Mergehex를 통해 통합된 펌웨어를 어떻게 업데이트 하는지에 대한 설명

Target Board에 펌웨어 다운로드

Bootloader Settings 와 함께 Mergehex 를 통해 통합된 펌웨어를 Programmer 또는 nrfjprog 를 통해 다운로드

nRF Connect v2.6	2 - Programmer		– 🗆 X
Ξ 0(251 +		
nRF52832	🕒 👔 File Memory Layout	File	•
			Add HEX file -
			Reload files
			Clear files
			Cical nics
		De	vice
			Erase all
			 Erase & write
			Save as file
		(Reset
			Write
		4	7 Read
			Auto read memory
Log		•	
16:45:18 181	RAM: 64KiB		
16:45:18 181	Flash: 512KiB in pages of 4KiB		
16:45:19 371	Reading device non-volatile memory. This may take a few seconds		
16:45:27 244	Non-volatile memory has been read 10 non-empty memory blocks identified		
16:45:27 690	SoftDevice detected id 0xAF (S132 v6 1 0)		
16:45:27 692	SoftDevice detected id 0xAF (S132 v6 1 0)	·····	
4			

또는

nrfjprog -f nrf52 --chiperase --reset --program <target firmware hex>

Mobile 또는 nRF Connect 를 통해 무선 펌웨어 업데이트

nRF Connect Desktop 이용한 방법

1. nRF Connect for Desktop을 설치

- 2. In-App 인 Bluetooth Low Energy 를 설치
- 3. nRF52-DK 또는 nRF52840-DK를 PC에 연결
- 4. Port Menu에서 연결된 DK의 Serial 을 선택한 후 Start Scan 하여 Target Device를 연결
- 5. 연결된 Target Device 항목에 DFU Icon을 눌러 업데이트할 펌웨어를 선택 후 업데이트

≡ 000682007919 - Ⅲ Co	onnection Map 🗧 Server Setup	
nRF5x Adapter 👸	1	Discovered devices
E3:DC:C8:9E:EB:88	ဗို	Clear
		Sort by signal strength
Generic Access	Peripheral 🙆 🗘	Filter: Device name or address
Generic Attribute	F3:74:F9:60:3B:72	Nordic_Buttonless -21 dBm .al
		F3:74:F9:60:3B:72 Connect @
	Generic Access	<unknown name=""> -33 dBm</unknown>
	Generic Attribute	5C:F7:6C:BF:0E:C8 Connect &
	Secure DFU	Details
		S2:D6:E2:D8:B0:28 Connect 2
		Details
		<unknown name=""> -47 dBm</unknown>
		Details
		<unknown name=""> .47 dBm .al</unknown>
		5E:32:5F:F9:F0:ED Connect &
		<unknown name=""> -47 dBm .al</unknown>
		6D:E0:C0:89:CB:E2 Connect P
		Details
.og		↓ 23:92:C4:B4:29:52 Connect <i>₽</i>
6:56:22 844 Disconnected from device	IUIE. UXUS, VAIUE (UX). 4E-0F-72-04-05-05-0F-40-02-4U	Details
6:57:13.092 Scan started		<unknown name=""> .48 dBm .all</unknown>
		7D:0B:9F:B5:84:F7 Connect 2
6:57:22.894 Connecting to device 6:57:23.029 Connected to device F3:	:74:F9:60:3B:72	7D:08:9F:B5:84:F7 Connect ∂ Details
6:57:22.894 Connecting to device 6:57:23.029 Connected to device F3: 16:57:23.347 Attribute value read, han	74:F9:60:38:72 dle: 0x03, value (0x): 4E-6F-72-64-69-63-5F-42-75-74-74-6F	
6.5722.894 Connecting to device F3 6.5723.029 Connected to device F3 6.5723.47 Attribute value read, han 6.5728.081 Connection parameters	74:F9:60:38:72 74:E:0x03, value (0x): 4E-6F-72-64-69-63-6F-42-76-74-74-6F updated for device F3:74:F9:60:38:72: interval 100ms, timeou	TO de sire 59.84.F7 Connect ♂ Connect ♂ Connect ♂ Connect ♂ Details
6.5723.02 6.5723.02 6.5723.02 6.5723.04 Connected to device F3. Attribute value read, han 6.5728.081 Connection parameters Device Firmware Upp Zip file D:\13 SDK NRF5\nRF5	74:F9:60:38:72 dile: 0x03, value (0x): 4E-6F-72:64-69:63:5F-42:75:74:74:6F updated for device F3:74:F9:60:38:72: interval 100ms, timeou grade (DFU) for device F3:74: 5 SDK 15:2.0 9412b96\examples\dfu	Tode sr by skift / Connect 2 Votes in 40 known name> 40 SA 40 40 00 Votes in 40 SA 40 40 Cotes in 40 SA 40 40 Cotes in 40 SA
6:5722.894 6:5723.029 6:5723.029 6:5723.04 Attribute value read, han 6:5728.081 Connection parameters Device Firmware Upp Zip file D:\13_SDK_NRF5\nRF5 Package info	74:F9:60:38:72 dile: (xx03, value (0x): 4E-6F-72:64-69-63-5F-42:75-74-74-6F updated for device F3:74:F9:60:38:72: interval 100ms, timeou grade (DFU) for device F3:74: 5_SDK_15.2.0_9412b96\examples\dfu	Tode sr by skift / Connect 2 Votes in today 40 SA 40 40 OF Votes in today 40 SA 40 OF Votes in today 40 SA 40 OF 40
6 6722 894 6 6723 029 6 6723 029 6 6723 029 6 5723 047 Attribute value read, han 6 5728 081 Connection parameters Device Firmware Upy Zip file D:\13_SDK_NRF5\nRF5 Package info	74:F9:60:38:72 dile: (xx03, value (0x): 4E-6F-72:64-69-63-5F-42:75-74-74-6F updated for device F3:74:F9:60:38:72: interval 100ms, timeou grade (DFU) for device F3:74: 5_SDK_15:2.0_9412b96\examples\dfu	Tode sr by skir / Connect 2 Votes in source 2 Vot
6:5723 894 Connecting to device 6:5723 029 Connected to device F3: 6:5723 04 Attribute value read, han 6:5728 081 Connection parameters Device Firmware Upy Zip file D:\13_SDK_NRF5\nRF5 Package info application :	74:F9:60:38:72 rdle: (xx03, value (0x): 4E-6F-72:64:69:63:5F-42:75:74:74:6F updated for device F3:74:F9:60:38:72: interval 100ms, timeou grade (DFU) for device F3:74: 5_SDK_15:2:0_9412b96\examples\dfu	Tode sress 4.17 Connect 2 Votes and 2 Vote
6.5728.094 Connecting to device 6.5723.029 Connected to device F3. 6.5723.047 Attribute value read, han 6.5728.081 Connection parameters Device Firmware Upy Zip file D:\13_SDK_NRF5\nRF5 Package info application: bin_file: nrf52832_>	74:F9:60:38:72 Idle: (xx03, value (0x): 4E-6F-72:64:69:63:5F-42:75:74:74:6F updated for device F3:74:F9:60:38:72: interval 100ms, timeou grade (DFU) for device F3:74: 5_SDK_15:2:0_9412b96\examples\dfu	Tode sress 4.17 Connect 2 Votes is 50.417 Votes is 50.417 Votes is 50.44 Votes 4.000 F Votes is 50.440 40.54.40.40.00 F Votes 5 Votes 5 Vo
6.5728.094 Connecting to device 6.5723.029 Connected to device F3. 6.5728.081 Connection parameters 6.5728.081 Connection parameters Device Firmware Upy Zip file D:\13_SDK_NRF5\nRF5 Package info application: bin_file: nrf52832_x dat_file: nrf52832_x	74:F9:60:38:72 Idle: (XX3, value (IXX): 4E-6F-72:64:69:63:5F-42:75:74:74:6F updated for device F3:74:F9:60:38:72: interval 100ms, timeou grade (DFU) for device F3:74: 5_SDK_15:2:0_9412b96\examples\dfu cxaa.bin cxaa.bin cxaa.dat	Tode sr by skift / Connect 2 Vote site Vote site Vot
6:72284 Connecting to device 6:572302 Connected to device F3: 6:572307 Attribute value read, han 6:5728081 Connection parameters Device Firmware Upy Zip file D:\13_SDK_NRF5\nRF5 Package info application: bin_file: nrf52832_x dat_file: nrf52832_x	74:F9:60:38:72 dde: (xx03, value (0x): 4E-6F-72:64:69:63:5F-42:75:74:74:6F updated for device F3:74:F9:60:38:72: interval 100ms, timeou grade (DFU) for device F3:74: 5_SDK_15:2:0_9412b96\examples\dfu cxaa.bin cxaa.dat	Tode sr by safer Poelais Connect 2 Voltage str by safer Connect 2 Voltage str by safer Choose
6:72284 6:572302 6:572307 Attribute value read, har 6:5728081 Connection parameters Device Firmware Upy Zip file D:\13_SDK_NRF5\nRF5 Package info application: bin_file: nrf52832_x dat_file: nrf52832_x	74:F9:60:38:72 Idle: (XX3, value (IXX): 4E-6F-72:64:69:63:5F-42:75:74:74:6F updated for device F3:74:F9:60:38:72: interval 100ms, timeou grade (DFU) for device F3:74: 5_SDK_15:2:0_9412b96\examples\dfu xxaa.bin xxaa.bin	Tode sress 4.17 Connect 2 Votes is 5.4.17 Connect 2 Votes is 5.4.14 Votes is 5.4.4 0.4 0.0 of Connect 2 Votes is F9:60:3B:72 Vsecure_dfu_1 Choose
16:57:23:894 Connecting to device 16:57:23:029 16:57:23:029 Connected to device 17:3 16:57:23:081 Connection parameters Device Firmware Upg Zip file D:\13_SDK_NRF5\nRF5 Package info application: bin_file: bin_file: nrf52832_x Progress Completed	74:F9:60:38:72 Idle: (XX3, value (IX): 4E-6F-72:64:69:63:5F-42:75:74:74:6F updated for device F3:74:F9:60:38:72: interval 100ms, timeou grade (DFU) for device F3:74: 5_SDK_15:2:0_9412b96\examples\dfu xxaa.bin xxaa.dat	Tode sress 4.17 Connect 2 Votes sress 4.17 Connect 2 Votes and to the second state of the second state o
6:72284 Connecting to device 6:5723302 Connected to device F3: 6:5723307 Attribute value read, han 6:5728.081 Connection parameters Device Firmware Upy Zip file D:\13_SDK_NRF5\nRF5 Package info application: bin_file: nrf52832_> dat_file: nrf52832_> Progress Completed	74:F9:60:38:72 Idle: (XX3, value (IX): 4E-6F-72:64:69:63:5F-42:75:74:74:6F updated for device F3:74:F9:60:38:72: interval 100ms, timeou grade (DFU) for device F3:74: 5_SDK_15:2:0_9412b96\examples\dfu xxaa.bin xxaa.dat	Tode sress 4.17 Connect 2 Votes is 40 harown names 40 SA 40 40 00 F Votes is 40 SA 40 40 00 F Votes is 40 SA 40 40 00 F Connect 2 Votes is 40 SA 40 0 F Connect 2 Votes is 40 SA 40 Connect 2 Votes
16:5723.02 16:5723.02 Connecting to device F3: 16:5723.02 Connection parameters: Device Firmware Upy Zip file D:\13_SDK_NRF5\nRF5 Package info application: bin_file: nrf52832_x dat_file: nrf52832_x Progress Completed 100%	74 F9 60 38 72 Idle: (xx3, value (0x): 4E-6F-72-64-69-63-5F-42-75-74-74-6F updated for device F3.74-F9 60 38 72: interval 100ms, timeou grade (DFU) for device F3:74: 5_SDK_15.2.0_9412b96\examples\dfu cxaa.bin cxaa.dat	Secure_dfu_1 Choose
16:5723.02 16:5723.02 16:5723.02 Connecting to device F3: 16:5723.04 Connection parameters: Device Firmware Upy Zip file D:\13_SDK_NRF5\nRF5 Package info application: bin_file: nrf52832_x dat_file: nrf52832_x Progress Completed 100%	74 F9 60 38 72 Idle: (xx3, value (0x): 4E-6F-72-64-69-63-5F-42-75-74-74-6F updated for device F3.74-F9 60 38 72: interval 100ms, timeou grade (DFU) for device F3:74: 5_SDK_15.2.0_9412b96\examples\dfu cxaa.bin cxaa.dat	Tode sress 44.7 Connect 2 Votes is 40 harown names 40 SA 40 40 00 F Votes is 40 SA 40 40 00 F Votes is 40 SA 40 40 00 F Votes is 40 SA 40 40 00 F Connect 2 Votes is 40 SA 40 0 F Connect 2 Votes is 40 SA 40 Connect 2 Votes is 40 S
6 6728 094 Connecting to device 6 6 6 723 029 Connecting to device F3 6 5 723 047 Attribute value read, har 6 5 728 081 Connection parameters Device Firmware Upy Zip file D:\13_SDK_NRF5\nRF5 Package info application: bin_file: nrf52832_x dat_file: nrf52832_x Progress Completed 100%	74 F9 60 38 72 Idle: 0x03, value (0x): 4E-6F-72-64-69-63-5F-42-75-74-74-6F updated for device F3 74-F9-60 38 72: interval 100ms, timeou grade (DFU) for device F3:74: 5_SDK_15.2.0_9412b96\examples\dfu xaa.bin cxaa.bin cxaa.dat	Secure_dfu_1 Choose

nRF Connect Mobile 을 이용한 방법

- 1. nRF Connect for Mobile을 App store 또는 Play Market을 통해 다운로드
- 2. nRF Connect for Mobile을 실행하여 연결하고자 하는 디바이스를 검색하여 연결
- 3. DFU Menu를 선택하여 Distribution packet(ZIP) 을 선택하여 펌웨어 업데이트



nrfutil.exe 를 이용하여 Command Line으로 업데이트하는 방법

PC에 nRF52-DK,nRF52840-DK 또는 nRF52840-Dongle을 연결하여 디바이스를 업데이트 (COM port 3를 이용할 경우)

```
nrfutil dfu ble -ic NRF52 -pkg app_dfu_package.zip -p COM3 -n "MyDevice" -f
```

Serial을 통한 유선 업데이트

COM port를 통해 연결된 디바이스를 nrfutil.exe를 통해서 아래의 커맨드로 업데이트 (COM port 3를 이용할 경우)

nrfutil dfu serial -pkg app_dfu_package.zip -p COM3

참조 문서

- BLE Secure DFU Bootloader Guide
- Getting started with Nordic's Secure DFU bootloader, a step by step guide
- https://github.com/NordicSemiconductor/pc-nrfutil#commands