

## BT800 Series HID Proxy

### BT800/BT820

#### Application Note

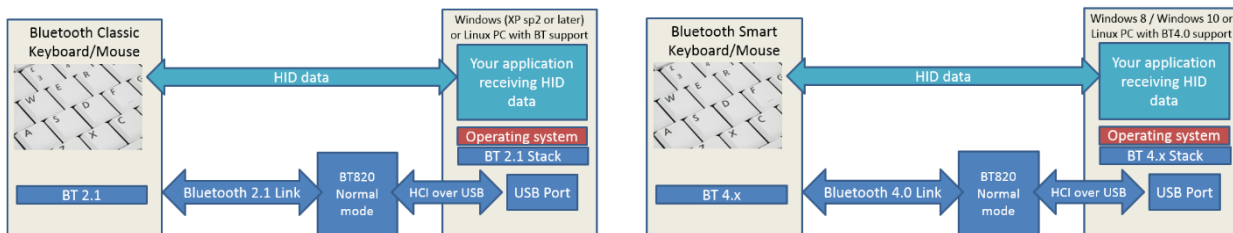
v1.4

## INTRODUCTION

Laird's BT800 series USB HCI devices support BLE HID proxy mode, a profile designed by Cambridge Silicon Radio that allows Bluetooth Low Energy HID devices to function on operating systems without the Bluetooth driver loaded. This functionality is present in the BT800, 810, and 820.

Both Classic Bluetooth and Bluetooth Low Energy have a similar problem with regards to the traditional HID profile. Until the host machine loads the Bluetooth driver, HID devices (such as a keyboard or mouse) cannot function. This makes certain tasks, like modifying the system BIOS, impossible with a Bluetooth mouse or keyboard. This is shown in [Figure 1](#).

**Note:** In the BT820, HID Proxy mode works with "Just Works" devices and will not pair with BT devices that require a pincode or passkey.



**Figure 1: Regular HID profile with Bluetooth Classic (left) and Bluetooth Smart (right)**

The BLE HID Proxy profile allows the BT800 Series device to process all the Bluetooth activity on its own and present itself to the host as a USB device with regular HID data traveling over USB. This onboard processing means a BLE HID device may communicate over USB to any host that supports USB input devices, even if the host is not running the Bluetooth stack. Bluetooth operations occur transparent to the host ([Figure 2](#)).

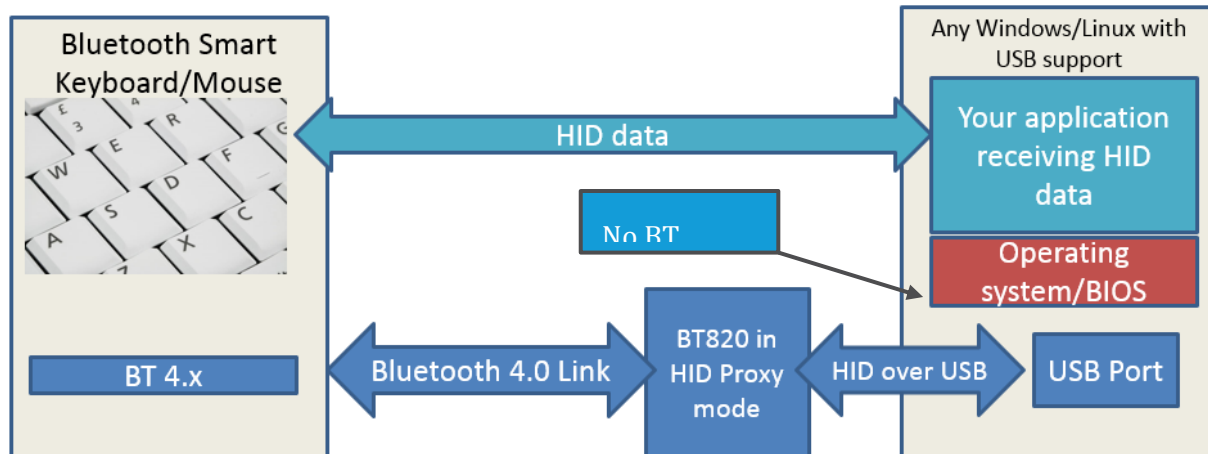


Figure 2: BLE HID Proxy profile abstracts Bluetooth operation away from the host

This application note illustrates how to enable this BLE HID proxy function by modifying a few keys in the Bluetooth Persistent Store. The function is not enabled in production.

**Note:** Due to the proprietary nature of the third party software (CSR BlueSuite) used for BLE HID proxy mode, we only support BLE HID proxy mode for OEMs and NOT for individual customers.

## REQUIREMENTS

- BT800 development board or BT820 USB dongle
- Windows PC

---

**Note:** Windows 8 is used in this guide. Windows 7 and XP can be used for the first time modification.

---

- CSR BlueSuite
- CSR USB driver or CSR USB-SPI adaptor for BT800 development kit.

---

**Notes:**

1. CSR BlueSuite is made available only to OEMs under a Laird NDA. OEMs should contact [LT-wirelessinfo@lairdtech.com](mailto:LT-wirelessinfo@lairdtech.com) to obtain the NDA. After BlueSuite is installed, PStools can be found under the CSR folder.
2. CSR USB driver is provided along with the CSR BlueSuite. The CSR USB-SPI adaptor is available at: <http://parts.digikey.com/1/parts/1406287-converter-usbspi-dev-sys-1808-1a.html>
3. Due to the proprietary nature of the third party software (CSR BlueSuite) used for BLE HID proxy mode, we only support BLE HID proxy mode for OEMs and NOT for individual customers.

---

## ENABLING THE BLE HID PROXY FUNCTION

### Changing the VID and PID

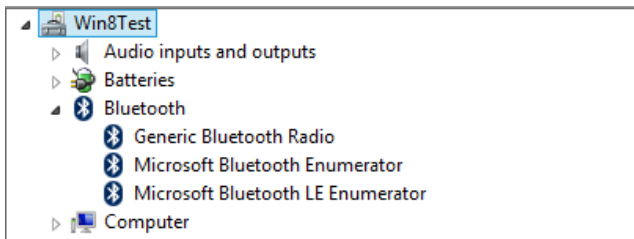
---

**Note:** This step (changing the VID and PID) is only required for the BT820 USB dongle. Please refer to the “*Modifying VID and PID for the BT820*” application note for information on this step.

---

## Installing CSR USB Driver

When the BT800 development board is first plugged in the PC USB port, Windows installs the driver automatically. It is recognized as the “Generic Bluetooth Radio” in the Windows device manager.



**Figure 3: Generic Bluetooth Radio in Device Manager**

Complete the following steps to install the CSR USB driver:

1. Right-click on **Generic Bluetooth Radio**, then click **Update Driver Software**.

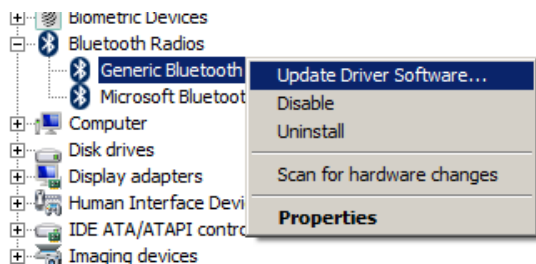


Figure 4: Contextual Rollout

2. Select the *Driver* tab and click **Update Driver**.

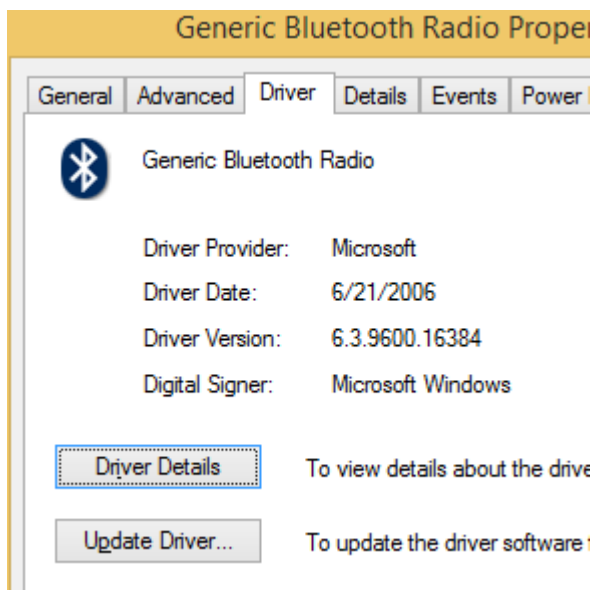


Figure 5: Update Driver button in Properties panel

3. Click **Browse my computer for driver software**.
4. Click **Let me pick from a list of device drivers on my computer**.
5. Click **Have Disk**.

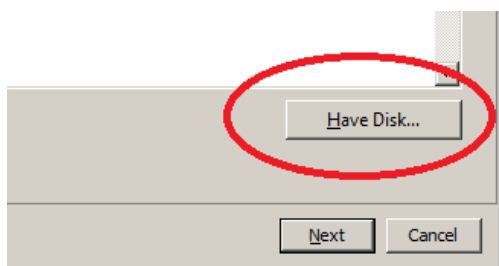
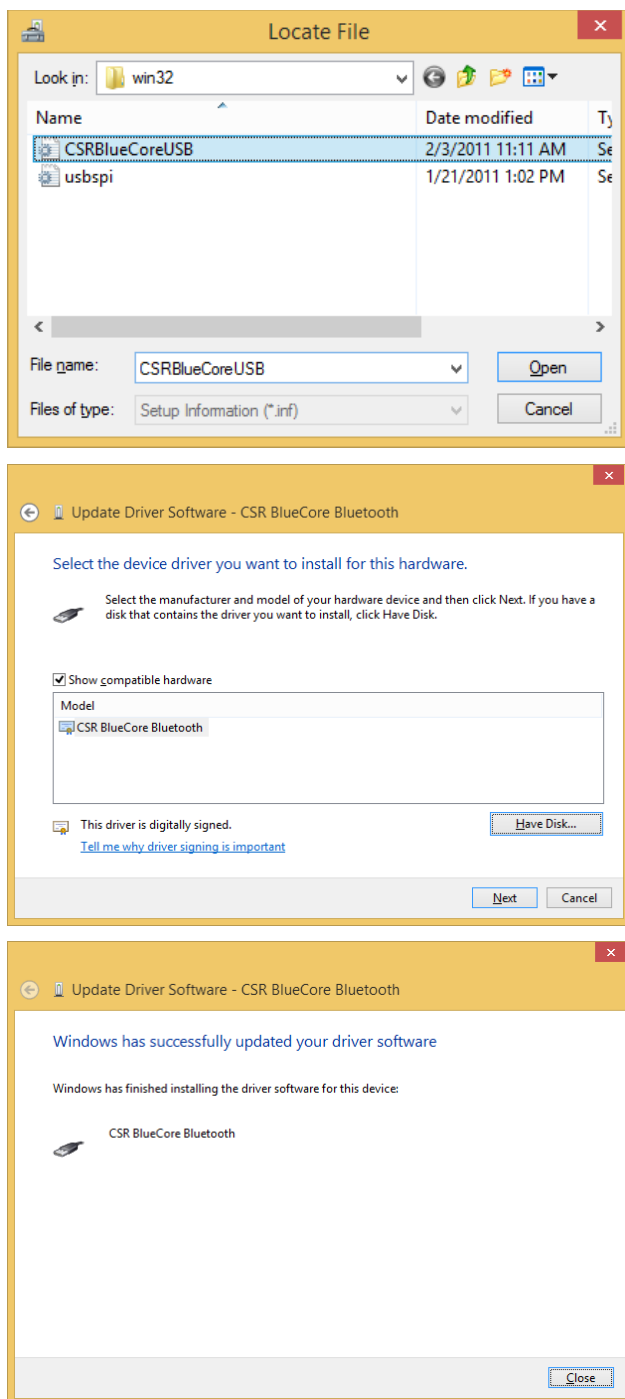


Figure 6: Have Disk button

6. Navigate to where the CSR driver is located on your computer, and select *CSRBlueCoreUSB.inf*. Proceed through the windows until software installation is complete.



**Figure 7: CSR USB Driver installation**

The BT800 development board is now recognized as *CSR BlueCore Bluetooth* in Windows device manager. It can be found by expanding “Universal Serial Bus controllers”.



**Figure 8: CSR BlueCore Bluetooth in Device Manager**

You can skip to [Open PStools](#) if you are not planning to use the SPI adaptor.

## CSR USB-SPI Adaptor

An RJ45 cable comes with the adaptor. Cut the RJ45 cable in half. Plug in the RJ45 jack into the adaptor and connect the open end to the development board.



**Figure 9: CSR USB SPI adaptor**

[Table 1](#) details RJ45 pins and their corresponding SPI signals.

**Table 1: RJ45 to SPI wiring**

Signal	RJ45 Connector Pin
SPI_CS8	1
SPI_MOSI	5
SPI_CLK	7
SPI_MISO	3
GND	8

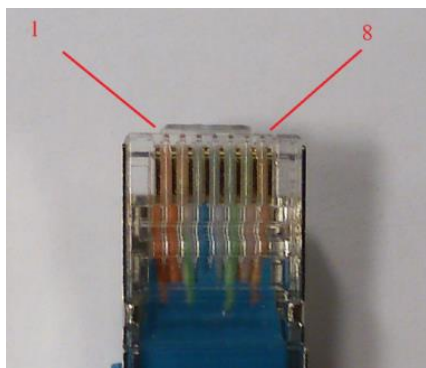


Figure 10: Wire numbering in RJ45 jack

## Open PStools

After invoking PStools, you must select either USB transport or SPI transport to access the PSkeys.

On the BT800 DVK board, there is a 10-pin header for SPI and WLAN Coexistence and a SPI/PCM switch. Be sure to put SPI/PCM switch on the SPI position before plugging the development board to your PC if an SPI interface will be used for opening PStools.

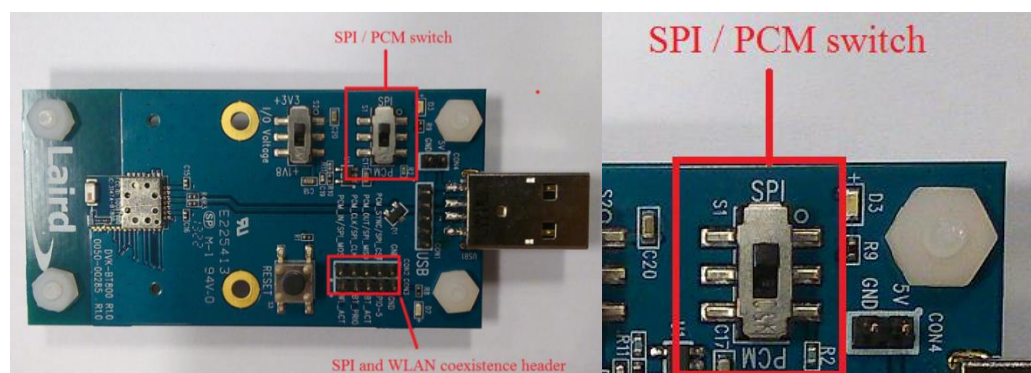


Figure 11: BT800 DVK Board, SPI/PCM switch set to SPI

In PStools, select either USB or SPI transport as shown in Figure 12 and Figure 13.

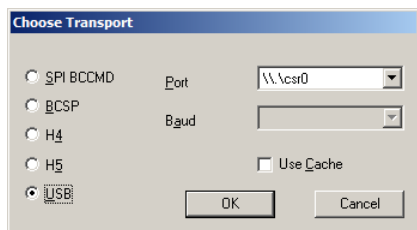


Figure 12: Selecting USB transport

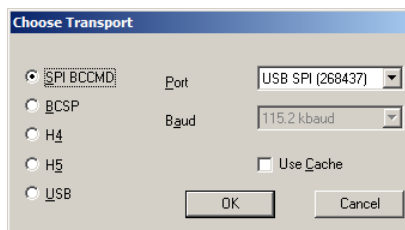


Figure 13: Selecting SPI transport

PStools first reads all the PSkeys from the module. This process takes about ten seconds and then the screen in Figure 14 appears with Bluetooth address highlighted on the list and the MAC address shown on the right.

**Note:** The Bluetooth address of your module will be different than the one displayed in Figure 12 because this is a unique address. Do not attempt to change it or you might put the module in nonoperational condition.

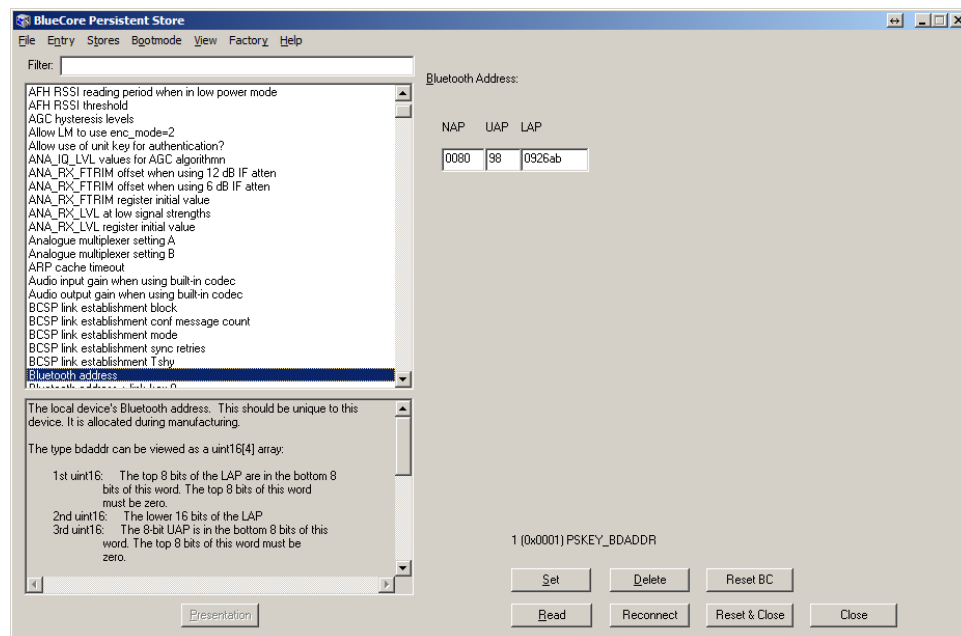


Figure 14: PStools opened successfully

## Modifying the pskeys for BLE HID Proxy Mode

There are several pskeys to be modified. To simplify the process, customers can merge the *HClanHIDKeys.psr*. To do this, follow these steps:

1. In the menu bar, select **File > Merge**.

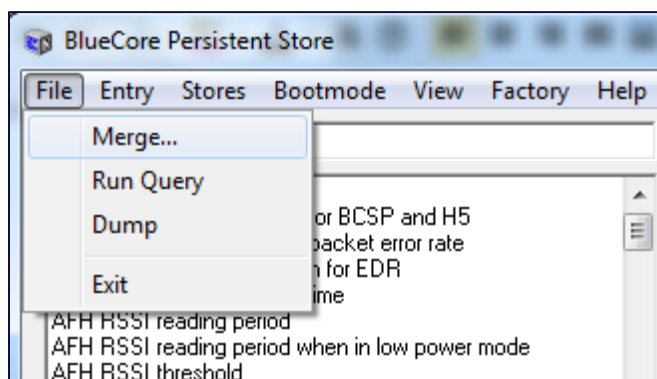


Figure 15: Merge psr file

2. Select the *HClanHIDKeys.psr* file and click **Open**.



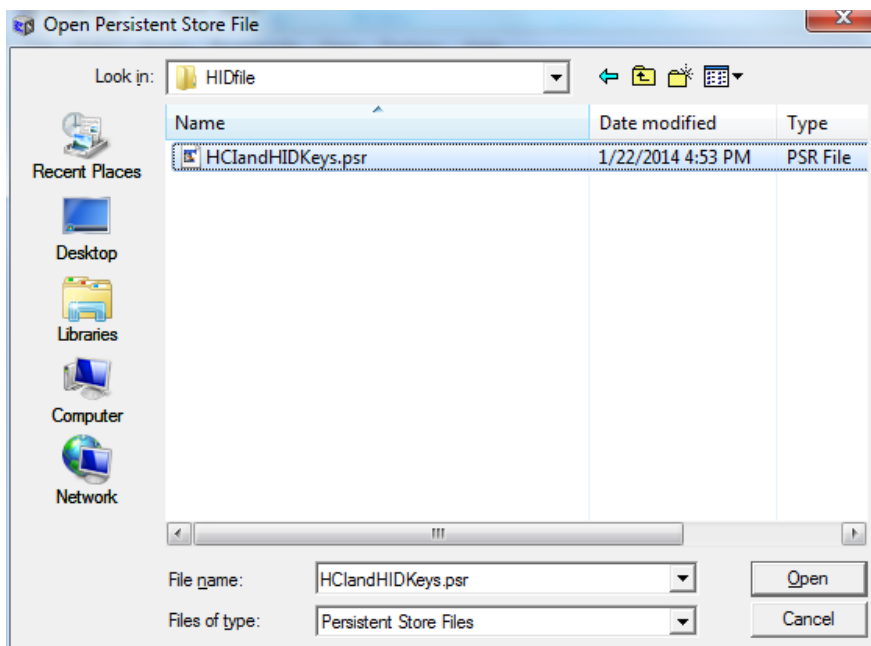


Figure 16: Select HClanHIDKeys.psr file

## Enabling HID Mode

The HCI and HID mode keys have been written to the module, but HID mode has not yet been selected. You can merge the *EnableHID.psr* file to select HID. However, it is very important to understand that the module must be in HCI mode before Pskeys can be accessed again with pstools if further changes are to be made.

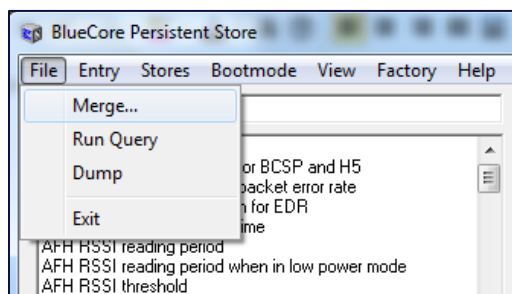


Figure 17: Merge psr file

After the *EnableHID.psr* file is merged, close the pstools and reinsert the BT800 development board or BT820 dongle into to the PC.

---

**WARNING:** Omitting "HClanHIDKeys.psr" will render the BT8XX non-operational.

---

The device is now a recognized USB Composite Device.

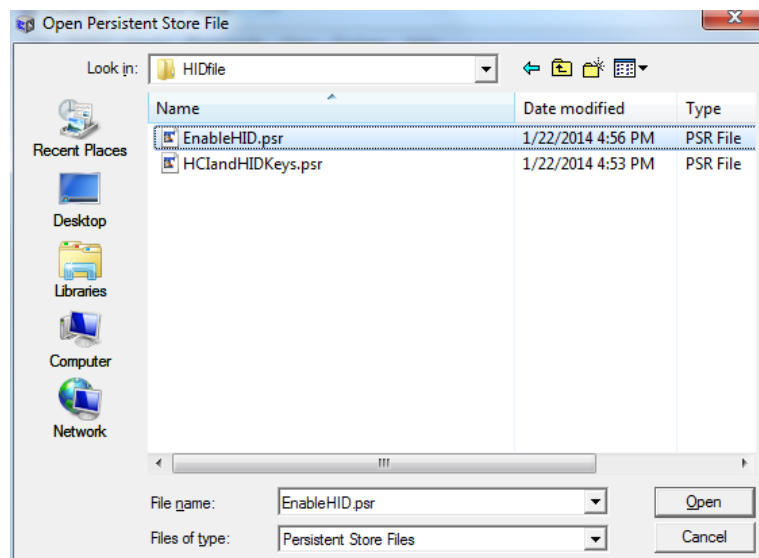


Figure 18: Select EnableHID.psr file

## Installing the Switcher Service

There is a service called VFPRadioSupportService provided by CSR. By enabling this service, Windows 8 is able to “switch” the HID device into HCI mode temporarily. Follow these steps to install the service:

1. Copy these two files (VFPRadioSupportService.exe and VFPRadioSupportService\_PS.dll) into the **C:\Windows\System32** directory. Note that administrative privileges are probably required.
2. Open a command prompt with Admin rights and navigate to the C:\Windows\System32 directory.

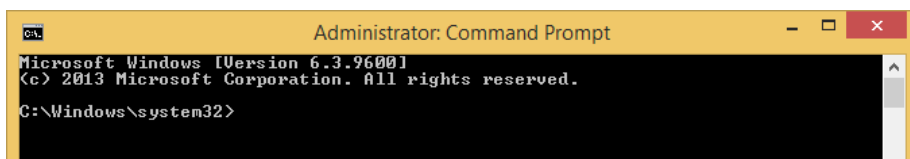


Figure 19: Open Command Prompt with Administrative right

3. Enter `sc create VFPRadioSupportService binPath="C:\Windows\System32\VFPRadioSupportService.exe` to create the service.

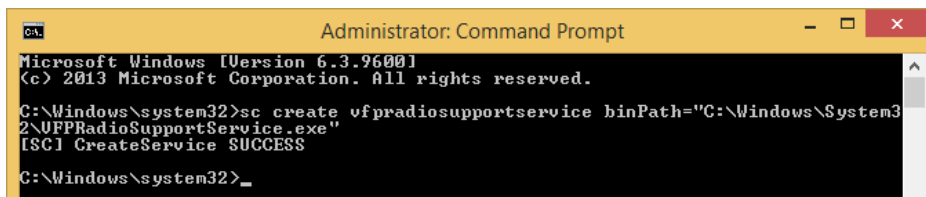
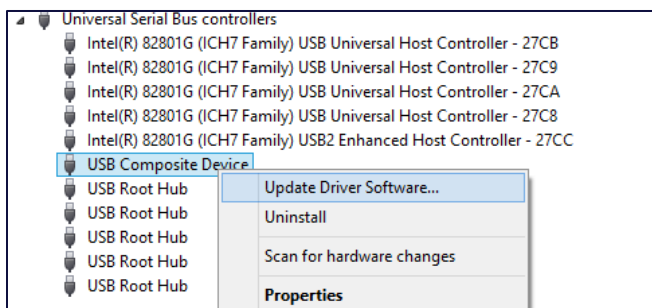


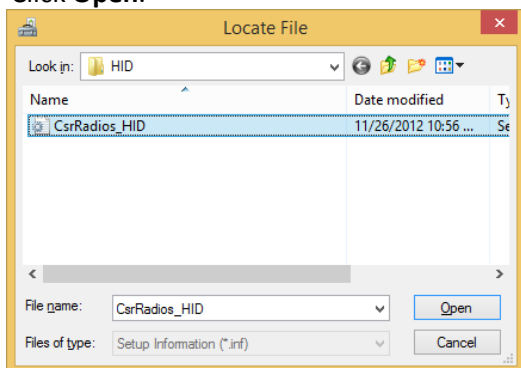
Figure 20: Create system service

4. Plug in the HIDenabled BT8xx device.
5. Open Device Manager, right click **USB Composite Device**, and select **Update Driver**.



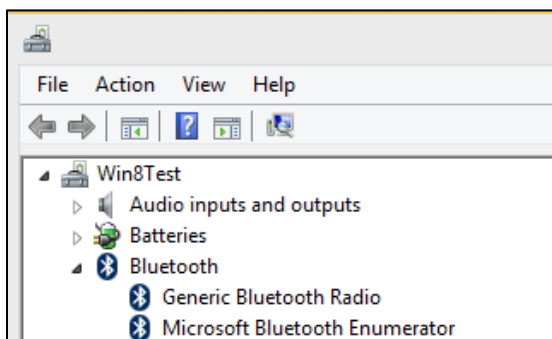
**Figure 21: Update Driver Software with “CsrRadios\_HID.inf”**

6. Navigate to where *CsrRadios\_HID.inf* is located and select it.
7. Click **Open**.



**Figure 22: Select CsrRadios\_HID.inf file**

The BT8XX device is now recognized as Generic Bluetooth Radio.



**Figure 23: Select “CsrRadios\_HID.inf” file**

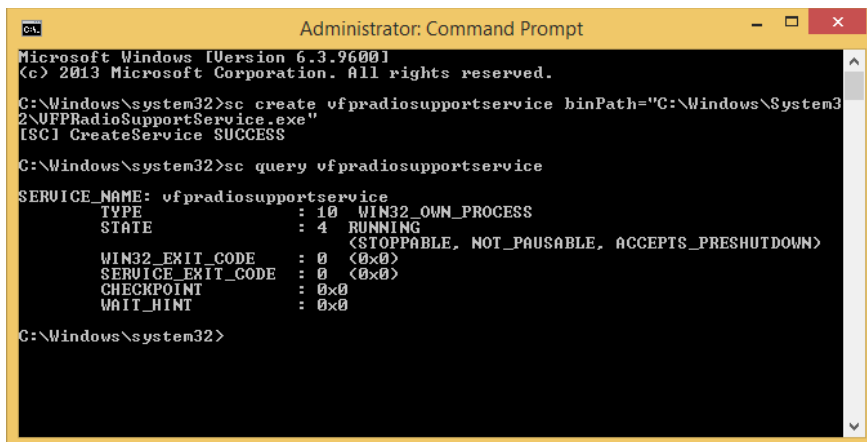


Figure 24: Vfpradiosupportservice service is now running.

- By updating the driver with the CSR USB driver again as shown in previous section, it is possible to access the pskeys again.

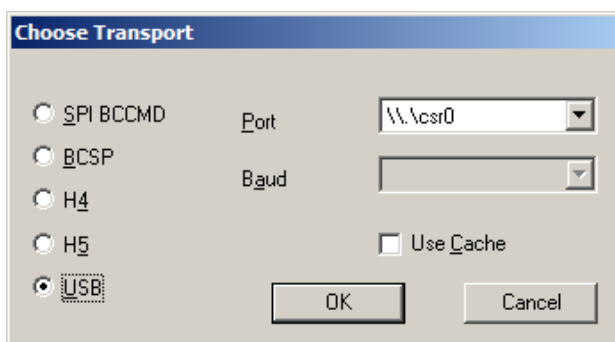


Figure 25: Select USB transport

## Enabling the HCI Mode

You can merge *EnableHCI.psr* to select HCI mode. The BT8Xxx is recognized as Generic Bluetooth Radio even after the switcher service has been stopped.

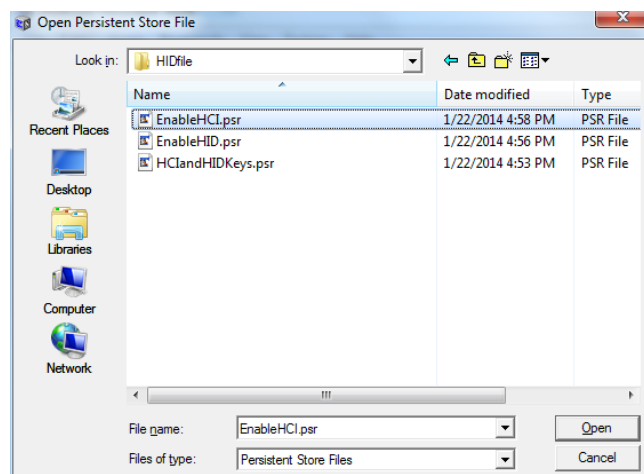
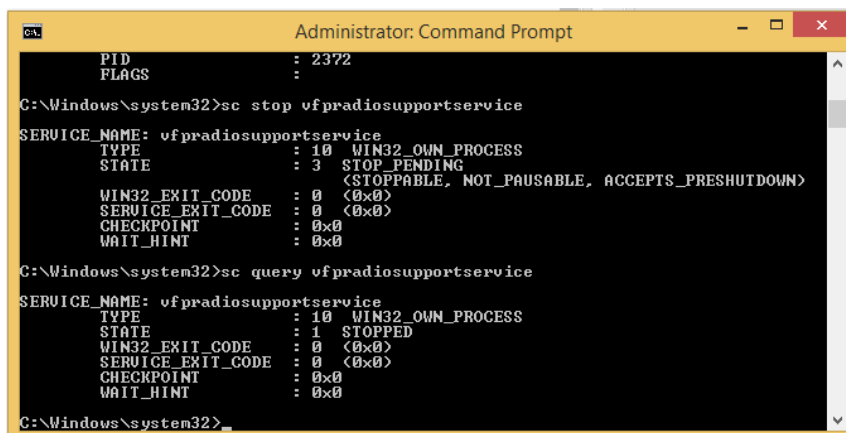


Figure 26: Merge EnableHCI.psr



```
Administrator: Command Prompt

PID          : 2372
FLAGS        :

C:\Windows\system32>sc stop vfprradiosupportservice

SERVICE_NAME: vfprradiosupportservice
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 3  STOP_PENDING
                        (STOPPABLE, NOT_PAUSABLE, ACCEPTS_PRESHUTDOWN)
        WIN32_EXIT_CODE        : 0  (0x0)
        SERVICE_EXIT_CODE     : 0  (0x0)
        CHECKPOINT            : 0x0
        WAIT_HINT             : 0x0

C:\Windows\system32>sc query vfprradiosupportservice

SERVICE_NAME: vfprradiosupportservice
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 1  STOPPED
        WIN32_EXIT_CODE        : 0  (0x0)
        SERVICE_EXIT_CODE     : 0  (0x0)
        CHECKPOINT            : 0x0
        WAIT_HINT             : 0x0

C:\Windows\system32>
```

Figure 27: Vfprradiosupportservice service is stopped

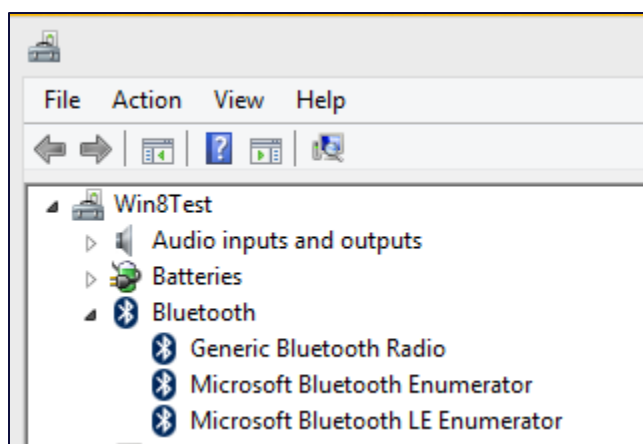
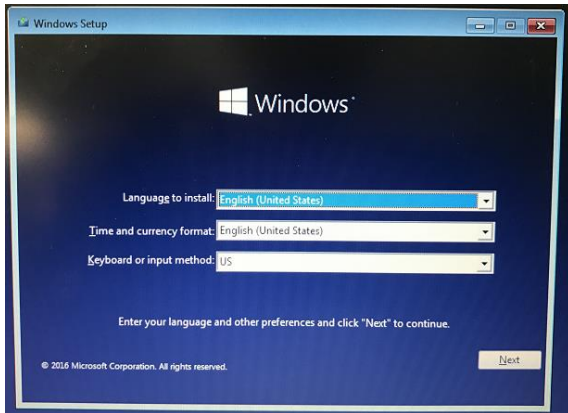


Figure 28: BT8XX is recognized as Generic Bluetooth Radio

## WORKING WITH A BLE HID DEVICE

### Connecting to a BLE Mice

To begin, you'll need a Windows installation USB thumb drive. Insert the drive into your device, and select "BOOT from USB" in your PC's boot screen (Figure 29).



**Figure 29: Windows setup screen**

Once the Windows set up screen is shown, insert the BT820 dongle which is already configured in BLE HID proxy mode. Press the “pairing button” on the BLE mouse (Figure 30). In this example, we’re using the ELECOM M-BT11BB.



**Figure 30: Put the BLE mice to advertise ADV\_IND packet**

After few seconds, the BT820 connects to the mouse automatically. No host BT/BLE stack is involved in the process (Figure 31).

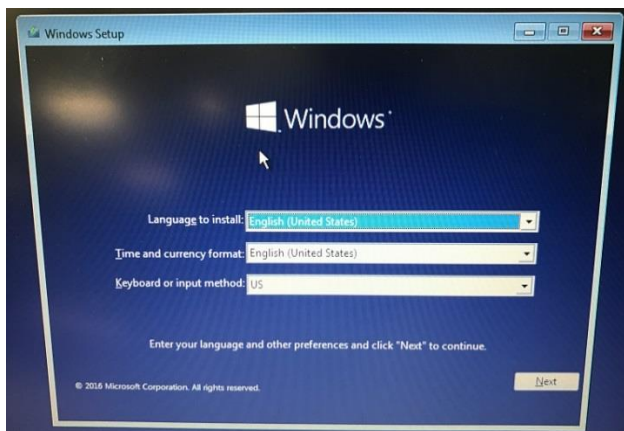


Figure 31: BT800 connects to the BLE mouse and the cursor appears

## Clearing the pairing entry

Once a connection has taken place, the pairing is saved. The BT820 will always try to connect to same BLE device it has last connected to. The pairing entry needs to be cleared before it will connect to a new BLE device.

The pairing can be removed with HID "SET\_FEATURE\_REQ" command over USB – "0x06 0x0 0x0 0x0 0x0 0x0 0x0 0x0". For testing purposes, there is an exe file to remove the pairing. If the switcher service has been installed and is running, the service must be stopped with "sc stop vfpradiosupportservice" in command prompt (Figure 32). You must have administrative permissions.

```

C:\Windows\system32>sc stop vfpradiosupportservice

SERVICE_NAME: vfpradiosupportservice
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 2   START_PENDING
                               (STOPPABLE, NOT_PAUS
        WIN32_EXIT_CODE       : 0   (0x0)
        SERVICE_EXIT_CODE   : 0   (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x0
```

Figure 32: Stop vfpradiosupportservice if the BT800 is not seen as a USB composite device



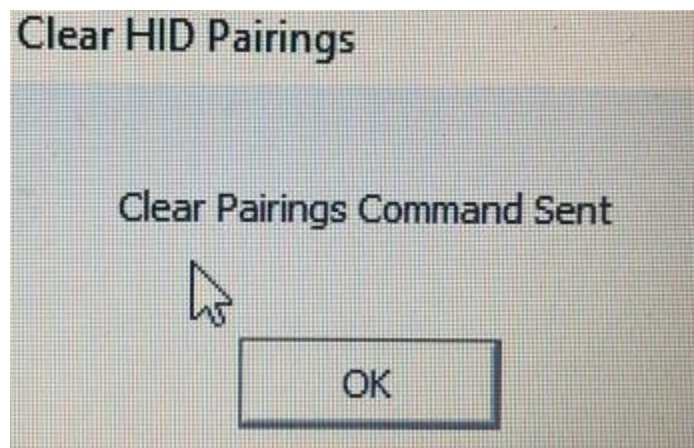


Figure 33: Clear the pairing in BT800 BLE HID proxy mode

## BLE HID proxy mode pairing requirement

The BLE HID device must allow the “Just Works” as I/O CAP. It is not possible for the BT800/BT820 to provide any IO capability other than the “Just Works” option. Some market available BLE keyboards require I/O CAP “Display” option, and it will reject the pairing if such security level is not met. Below is the sniffer trace showing the BLE keyboard and BT800 rejecting the pairing.

```

247 20.133017 f8:9a:68:a4:7a:3f <broadcast> BLE ADV ADV_IND
248 20.170821 f8:9a:68:a4:7a:3f <broadcast> BLE ADV ADV_IND
249 20.221709 f8:9a:68:a4:7a:3f <broadcast> BLE ADV ADV_IND
250 20.223932 Ezurio_0a:1d:70 f8:9a:68:a4:7a:3f BLE ADV CONNECT_REQ
251 20.303004 Master Slave ATT Rcvd Read By Type Request, Boot Keyboard Input Report, Handles: 0x0001..0xffff
252 20.304568 Slave Master BLE Data Empty Data PDU
253 20.381450 Master Slave BLE Data Empty Data PDU
254 20.384027 Slave Master ATT Rcvd Error Response - Insufficient Authentication, Handle: 0x0022
255 20.461861 Master Slave ATT Rcvd Read By Type Request, Peripheral Privacy Flag, Handles: 0x0001..0xffff
256 20.463196 Slave Master BLE Data Empty Data PDU
257 20.541426 Master Slave BLE Data Empty Data PDU
258 20.542978 Slave Master ATT Rcvd Error Response - Attribute Not Found, Handle: 0x0001
259 20.621774 Master Slave SMP Rcvd Pairing Request: Bonding, No MITM, Initiator Key(s): , Responder Key(s): LTK
260 20.623092 Slave Master BLE Data Empty Data PDU
261 20.701572 Master Slave BLE Data Empty Data PDU
262 20.703122 Slave Master SMP Rcvd Pairing Failed: Authentication Requirements
263 20.781400 Master Slave BLE Data Empty Data PDU
264 20.782713 Slave Master BLE Data Empty Data PDU
265 20.861459 Master Slave BLE Data Empty Data PDU
266 20.862752 Slave Master BLE Data Empty Data PDU
267 20.941354 Master Slave BLE Data Empty Data PDU
268 20.942695 Slave Master BLE Data Empty Data PDU
269 21.021504 Master Slave BLE Data LL_Control PDU: LL_TERMINATE_IND
270 21.023317 Slave Master BLE Data Empty Data PDU
271 21.025777 f8:9a:68:a4:7a:3f <broadcast> BLE ADV ADV_IND
272 21.027277 52:9c:4a:52:2c:89 f8:9a:68:a4:7a:3f BLE ADV SCAN_REQ

```

Figure 34: A BLE keyboard rejects the pairing because of insufficient authentication.

## REVISION HISTORY

Revision	Date	Description	Approved By
1.0	18 Feb 2014	Initial Release	Jonathan Kaye
1.1	26 Mar. 2014	Minor Edits	Jonathan Kaye
1.2	11 Nov 2015	Expanded introduction on HID vs BLE HID Proxy	Jonathan Kaye
1.3	1 Dec 2016	Addition of example	Raymond Au
1.4	15 Aug 2017	Added clarifying note that BT820 HID Proxy only works with “Just Works” devices	Jonathan Kaye