RfidResearchGroup / **proxmark3** Public

Code Issues 84 Pull requests 12 Actions Projects Wik

master proxmark3 / doc / **bt_manual_v10.md** Go to file ···

[redacted]

[redacted]

MANUAL Bluetooth / Battery add-on 'Blue Shark'

rev. v1.1

Table of Contents

1. FEATURES

^Top

- Built-in Bluetooth 2.0 with EDR Bluetooth module, default baud rate 115200.
- Built-in 400 mAh polymer lithium-ion battery, typical standby time up to 3.5 hours.
- Additional heat dissipating fins can significantly reduce the

temperature when the HF antenna is in operation for a long time.
- Complete lithium charging management system, seamless switching power supply. Full overcharge and overdischarge protection.
- Bluetooth has an independent power switch that can be turned on or off.
- It's compact and easy to carry. The clamp structure is easy to install and replace.

It can easily connect to Bluetooth mobile phone, portable computer, etc. Without USB cable, complicated permissions or driver settings.

Built-in battery can support standalone mode, off-line sniffing, off-line reading & simulation, etc. The temperature of the device is stable.

2. PARAMETERS

^Top

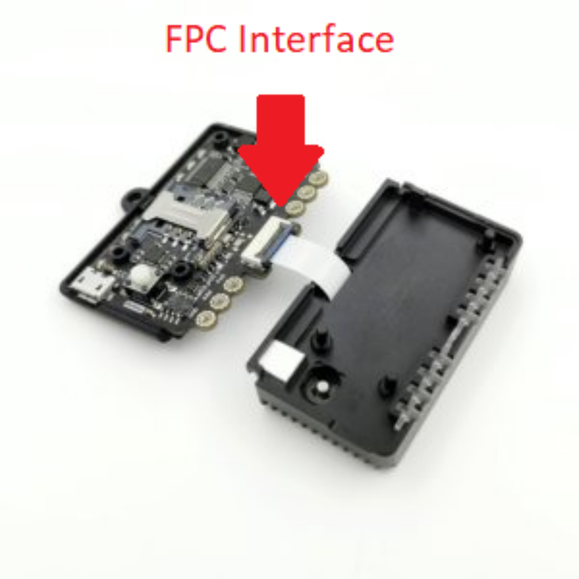
- Battery capacity: 400 mAh
- Standby time: 3.5h @ StandBy; 2.9h @ LF-On; 50min @ HF-On;
- Charging Current: 200mA (Plug in USB Default Charging)
- Charging time: 2.5h
- Num of charges: 400 -> 70% capacity (standard LIPO)
- Bluetooth power: 4dBm, -85 dBm @ 2Mbps
- Bluetooth distance: 6m (depending on the environment and device orientation)
- Size and weight: 54.4mm * 29.4mm * 13.5mm 24g

3. ASSEMBLY STEPS

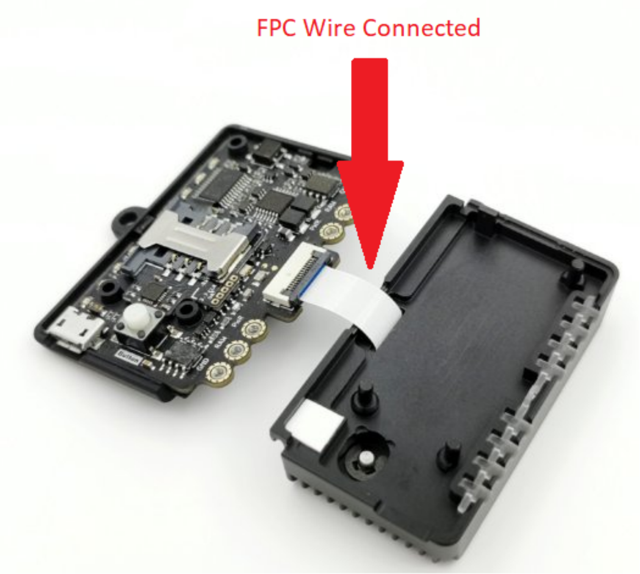
^Top

- Unplug your Proxmark3 RDV4.0 device from any usb cable.
- Remove the plastic upper case of Proxmark3 RDV4.0 with opener.

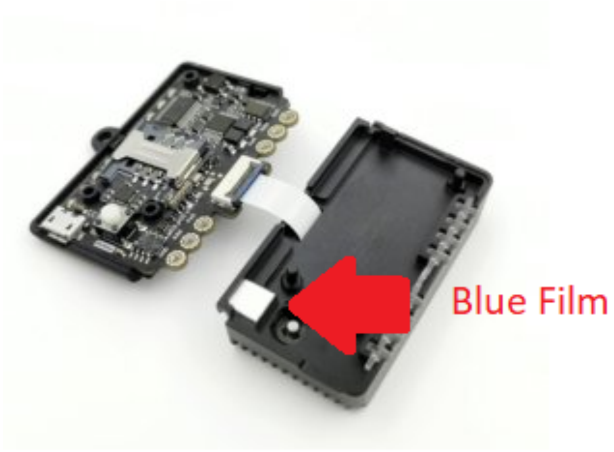
- Remove temporarily the antenna with a H5 (Hex/Allen) screwdriver to expose the FPC interface.



- Turn off all power switches, insert the FPC wire into the FPC connector, and lock the FPC connector.



- Tear off the blue film of heat conductive double-sided tape. Align the add-on to the hole positions and gently insert it into the case.



- Assembly finished!

4. COMPILATION / FLASHING

^Top

4.1 From Source

^Top

Please download the latest source code from Rfid Research Group's Github repo: https://github.com/RfidResearchGroup/proxmark3

To compile the client and firmware with FPC support, the easiest way is to

1. Copy the sample file: `Makefile.platform.sample` ⇒ `Makefile.platform`
   - `cp Makefile.platform.sample Makefile.platform`
2. Edit `Makefile.platform`, uncomment the line `#PLATFORM_EXTRAS=BTADDON` by removing the `#`
3. Recompile the project:
   - `make clean; make -j`
4. Flash the firmware
   - `./pm3-flash-fullimage`

You are now ready to run the client with the serial port you got from your BT device on your laptop etc.
See instructions below.

4.2 Homebrew (macOS)

^Top

From the homebrew-proxmark3 readme

1. `brew tap rfidresearchgroup/proxmark3`
2. `brew install --with-blueshark proxmark3`

5. CONNECT WITH BLUETOOTH

^Top

You can have both USB cable connect and BT active at the same time and connect to either serial port.
You can also switch serial port from inside the proxmark3 client using the new command `hw connect`.

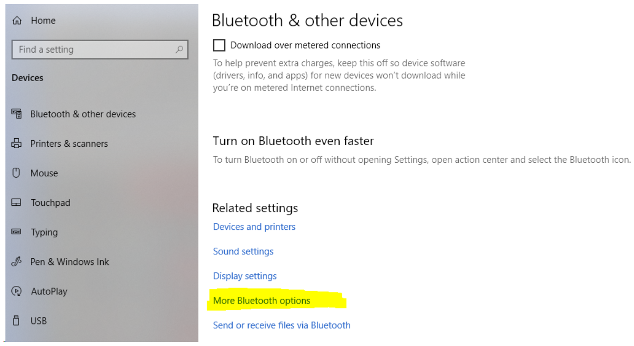
5.1 Windows

^Top

5.1.1 Connecting your RDV4.0 with Bluetooth on mobile phone or computer

^Top

- Open Bluetooth and search for a device named PM3_RDV4.0.
- Enter the paired password 1234 and establish the connection.
- The blue state LED on the add-on will keep blinking after the connection is established. Only when the mobile phone or computer opens the correct COM port, the blue LED turns on solid, indicating that the connection is successful.
- First time you do this you might need to go into Bluetooth more settings and add a outgoing com port. If so, follow these steps below.
- First open your bluetooth settings, click on "more options".



Bluetooth & other devices

□ Download over metered connections

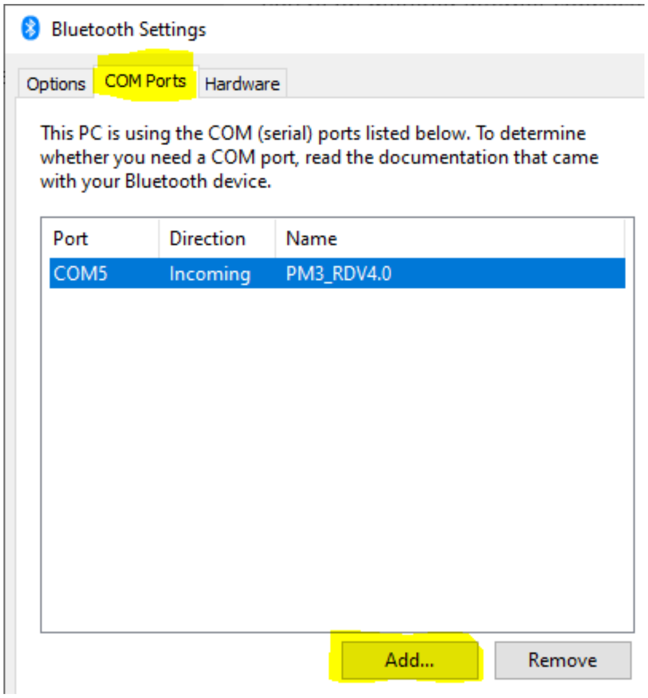
To help prevent extra charges, keep this off so device software (drivers, info, and apps) for new devices won't download while you're on metered Internet connections.

Turn on Bluetooth even faster

To turn Bluetooth on or off without opening Settings, open action center and select the Bluetooth icon.

Related settings

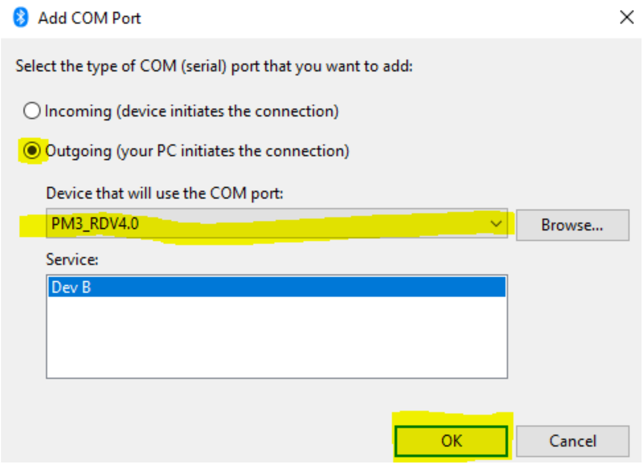
* Go to second tab and view the list of current bluetooth comports. If you don't have an outgoing com port setup, click 'add'


Bluetooth Settings

This PC is using the COM (serial) ports listed below. To determine whether you need a COM port, read the documentation that came with your Bluetooth device.

Port	Direction	Name
COM5	Incoming	PM3_RDV4.0

* Select `outgoing comport` and select the Proxmark3 RDV4.0 device. Click `OK` when done.


Add COM Port

Select the type of COM (serial) port that you want to add:

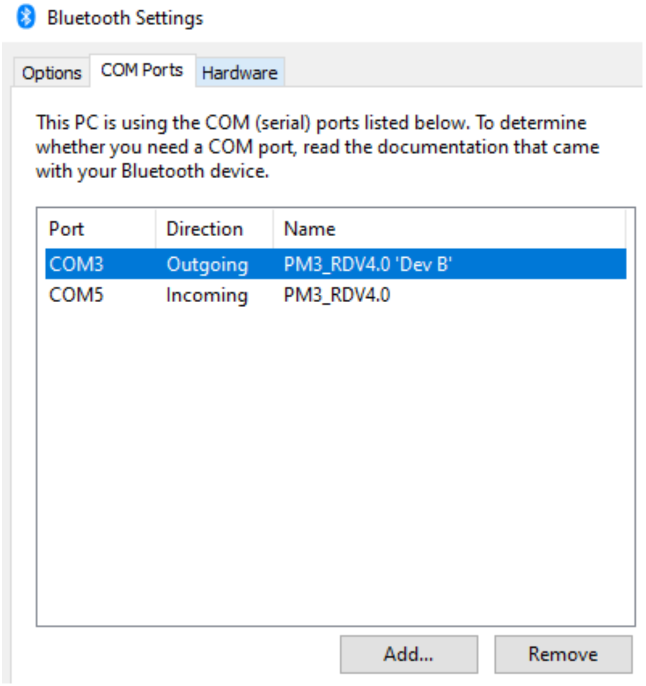
○ Incoming (device initiates the connection)

● Outgoing (your PC initiates the connection)

Device that will use the COM port: PM3_RDV4.0

Service: Dev B

* Verify that you now have a outgoing comport. Remember this com port when you want to use your Proxmark3.



This PC is using the COM (serial) ports listed below. To determine whether you need a COM port, read the documentation that came with your Bluetooth device.

Port	Direction	Name
COM3	Outgoing	PM3_RDV4.0 'Dev B'
COM5	Incoming	PM3_RDV4.0

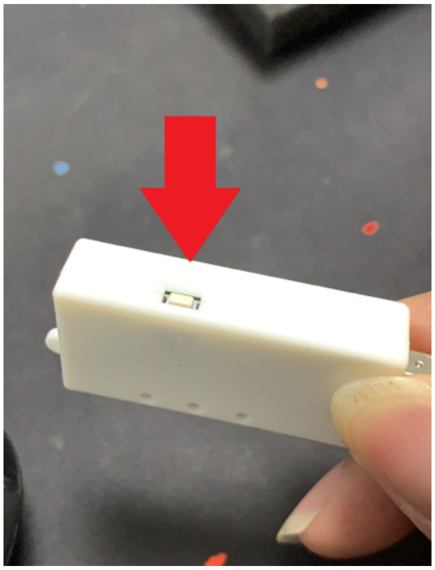
* done!

5.1.2 Fast connection using dedicated USB Bluetooth adapter under Windows

^Top

- Install driver: http://www.silabs.com/products/developmentbe connected.

- The adapter button can be used to delete memory so that other add-on can be searched and connected.



- After the connection is established, the blue state LED on add-on will turn on solid.
- look for *CP2104 USB tp UART bridge controller* under devices in order to get the assigned serial port

5.2 Linux

^Top

5.2.1 Connecting rdv4.0 with Bluetooth on Linux computer via native Bluetooth support in the client

^Top

This requires to have compiled the client with Bluetooth support.

Be sure your user has permissions to use Bluetooth

- On most distributions, you've to be part of group `bluetooth` : `sudo adduser $USER bluetooth` then log out and log in
- else, run the following commands as root : `sudo ...`

1. Find the MAC address of the Bluetooth add-on, named PM3_RDV4.0.

```
hcitool scan
Scanning ...
  aa:bb:cc:dd:ee:ff PM3_RDV4.0
```

Instead of `aa:bb:cc:dd:ee:ff`, you'll see your MAC address.

If you don't have `hcitool`, you can use `bluetoothctl` and `scan on` as shown in next section.

2. Use Proxmark client with Bluetooth MAC address as bt:

```
./proxmark3 -p bt:aa:bb:cc:dd:ee:ff
```

The first time, your OS will ask you for pairing. The default PIN is 1234. If PIN is not typed in quickly, the client might timeout. Simply restart it again after pairing.

If your OS doesn't prompt you for pairing or if the device connects and immediately disconnects, you can pair it in command line, e.g. (again, replace with your addon MAC address):

```
bluetoothctl
[bluetooth]# remove aa:bb:cc:dd:ee:ff
[bluetooth]# pairable on
[bluetooth]# scan on
Discovery started
...
[CHG] Device aa:bb:cc:dd:ee:ff Name: PM3_RDV4.0
[bluetooth]# trust aa:bb:cc:dd:ee:ff
[bluetooth]# pair aa:bb:cc:dd:ee:ff
[agent] Enter PIN code: 1234
```

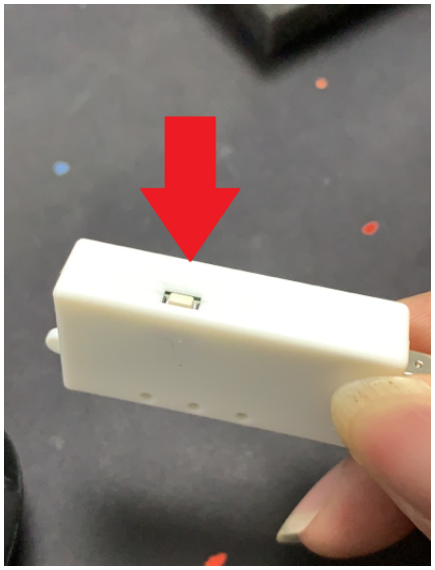
```
[bluetooth]# quit
```

5.2.2 Fast connection using dedicated USB Bluetooth adapter under Linux

^Top

1. Insert the adapter into the USB port. The adapter will search automatically and establish the connection. The adapter will remember the device that was first connected and after that the same device will be connected.

2. The adapter button can be used to delete memory so that other add-on can be searched and connected.



3. After the connection is established, the blue state LED on add-on will turn on solid.

4. a serial port `/dev/ttyUSB0` will be created, use Proxmark3 client on it

```
./proxmark3 -p /dev/ttyUSB0
```

5.2.3 (deprecated) Connecting rdv4.0 with Bluetooth on Linux computer via rfcomm

^Top

rfcomm is a deprecated tool which might be unavailable in your Linux distribution.

1. Find the MAC address of the Bluetooth add-on, named PM3_RDV4.0.

```
hcitool scan
Scanning ...
  aa:bb:cc:dd:ee:ff PM3_RDV4.0
```

Instead of `aa:bb:cc:dd:ee:ff`, you'll see your MAC address.

2. Bind your BT add-on MAC address to a serial port

```
sudo rfcomm bind rfcomm0 aa:bb:cc:dd:ee:ff
```

Replace `aa:bb:cc:dd:ee:ff` by your MAC address.

3. The blue state LED on the add-on will keep blinking after the connection is established. Only when the Proxmark3 client opens the `/dev/rfcomm0` port, the blue LED turns on solid, indicating that the connection is successful.

4. Use Proxmark client on BT-serial port

```
./proxmark3 -p /dev/rfcomm0
```

See instructions above (method 1) for initial pairing.

5.3 MacOS

^Top

5.3.1 Connecting rdv4.0 with Bluetooth on MacOS

^Top

With MacOS Mojave 10.14.5 you could experience some continuously disconnecting and difficult to reconnect the device at the system wakeup, to avoid this problem do a PRAM reset before to add your Proxmark3 RDV4 Blue Shark:

1. Open a Terminal and execute this command: sudo rm -R /Library/Preferences/com.apple.Bluetooth.plist.
2. Shut down your Mac.
3. Then turn it on and immediately press and hold these four keys together: Option, Command, P, and R.
4. You can release the keys after about 20 seconds, during which your Mac might appear to restart.

After reboot you can go ahead to pairing your Proxmark3 RDV4 Blue Shark:

5. Make sure the Blue Shark BT switch is turned ON
6. On your Mac, choose Apple menu -> System Preferences, then click Bluetooth.
7. Select the device in the list, then click Connect and add the 1234 pwd.
8. A serial port like `/dev/tty.PM3_RDV40-DevB` will be created, use Proxmark3 client on it

```
./proxmark3 -p /dev/tty.PM3_RDV40-DevB
```

5.4 Android

^Top

5.4.1 Fast connection using dedicated Bluetooth (HC-06 Master + CP2102) adapter under Android with Termux

^Top

1. Make sure you already followed this tutorial https://github.com/RfidResearchGroup/proxmark3/blob/master/doc/termux_notes.md#setup and have Termux with an running Proxmark3 client ready. You need additional the `cp210x` serial usb driver enabled and working, like the `USB_ACM` driver to communicate wireless.
2. Insert the Bluetooth adapter with an fitting USB-C/Micro-USB converter into your Android USB port and a serial port `/dev/ttyUSB0` will be created. To see if it's working, run `tsudo ls /dev/ttyU*` and it should list `/dev/ttyUSB0`.
3. The adapter will search automatically and establish the connection to BlueShark. The adapter will remember the device that was first connected and after that the same device will be connected. After the connection is established, the blue state LED on add-on will turn on solid.
4. If you see this, congratulations, you can run your Proxmark3 client in

Termux with `tsudo proxmark3/client/proxmark3 -p /dev/ttyUSB0`

6. OTHER NOTES

^Top

6.1 Default settings

^Top

Settings of the Blue Shark add-on and of the white dongle:

1. Serial: `115200 8N1`
2. Name: `PM3_RDV4.0`
3. Pin: `1234`

If you bought your Bluetooth adapter dongle somewhere else, make sure to set the baud rate to 115200 `AT+BAUD8`, the name `AT+NAMEPM3_RDV4.0` and PIN `AT+PIN1234` correctly.

6.2 UART and LED behavior

^Top

Bluetooth is connected to Proxmark3 RDV4.0 via UART. The USB and UART interfaces of RDV4.0 can coexist without conflict, and no special switching is required.

The following link has helpful notes on UART usage and baud rates: https://github.com/RfidResearchGroup/proxmark3/blob/master/doc/uart_notes.md

6.3 Disassembly

^Top

There is a heat conductive double-sided tape inside the add-on, which has strong adhesive force. Therefore, if add-on needs to be removed, it needs to be pulled out from the heat sink end with greater efforts. Each disassembly will reduce the viscidity of double-sided tape. When double-sided tape is well protected, it will not affect the second use. Thermal conductivity will be slightly worse and will therefore have a direct impact on the thermal performance of the heat sink.

6.4 Battery charging

^Top

The battery charging circuit is turned on by default. Any time a USB cable is inserted, the battery will be automatically charged. The red LED will remain bright when charging. The red LED will be extinguished when charging is completed.

6.5 Get better signals

^Top

For the better heat dissipation, we have used a cast metal enclosure for the add-on. As a result Bluetooth wireless signals are sacrificed. For example, if the back of add-on is facing the Bluetooth host, the signal is very bad and the distance will be reduced. The best signal strength can be obtained when the front glass faces the Bluetooth host.

If the Proxmark3 is not responding, it may be due to a poor Bluetooth connection. To improve performance, try repositioning the Proxmark3 so the glass face is directed toward the host.