OPEN CONNECTIVITY FOUNDATION®

Automated Development for Cross-Platform Internet of Things

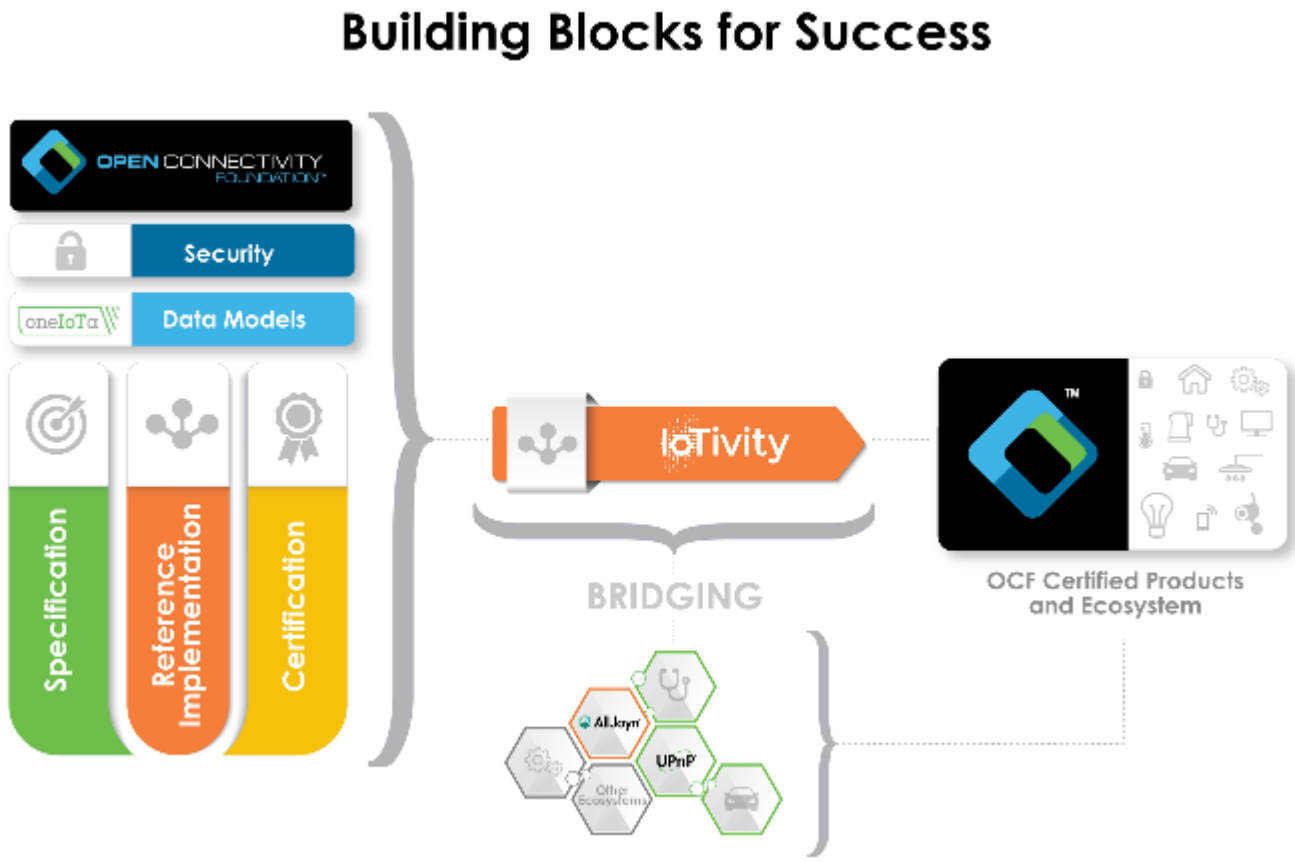
Develop a secure, certified hardware prototype in 15 minutes

Clarke Stevens
Shaw Communications
clarke.stevens@sjrb.ca

Shaw)

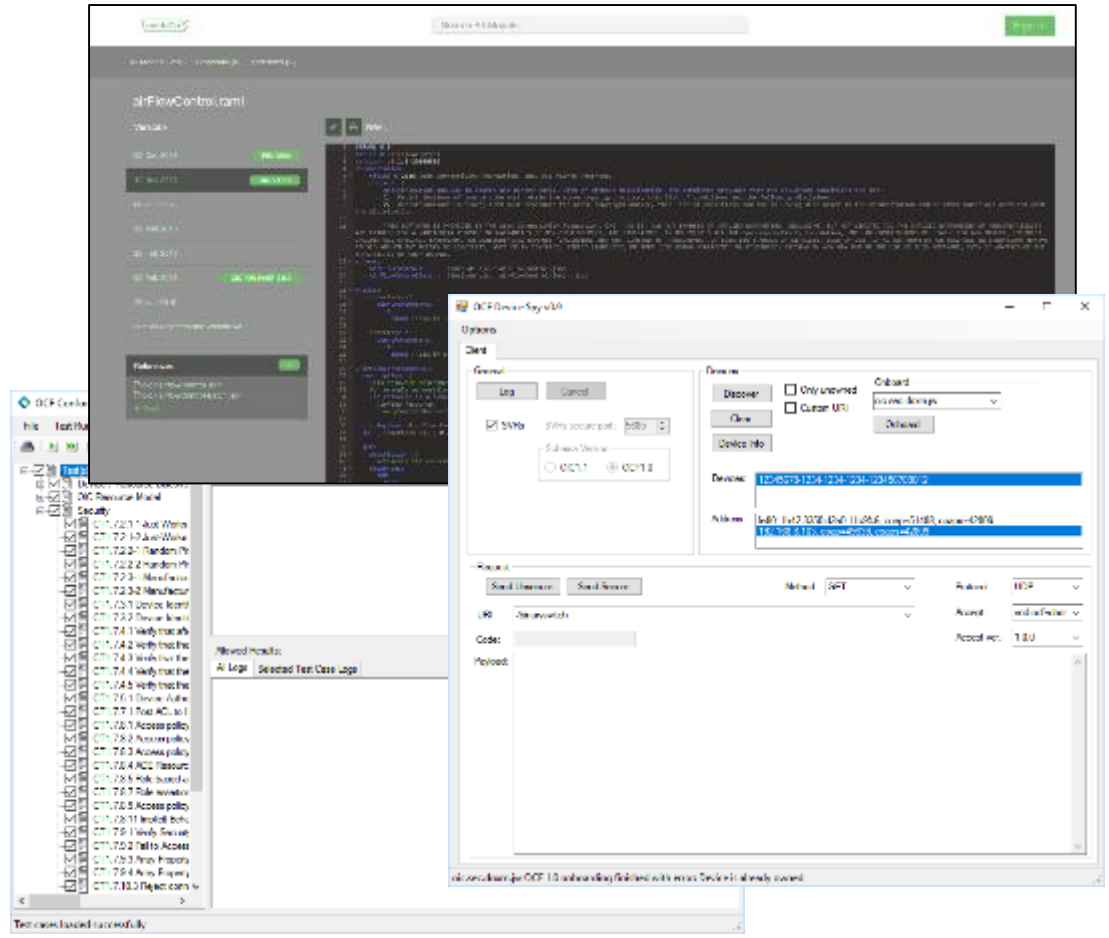
What is the Open Connectivity Foundation?

- Standards body for interoperable IoT
  - Strong security built in from the start
  - Works interoperably with existing ecosystems
  - Three pillar alignment
    - International specification
    - Open source implementation
    - Automated certification tool and international authorized test labs
  - Flexible, RESTful, data-model-based architecture



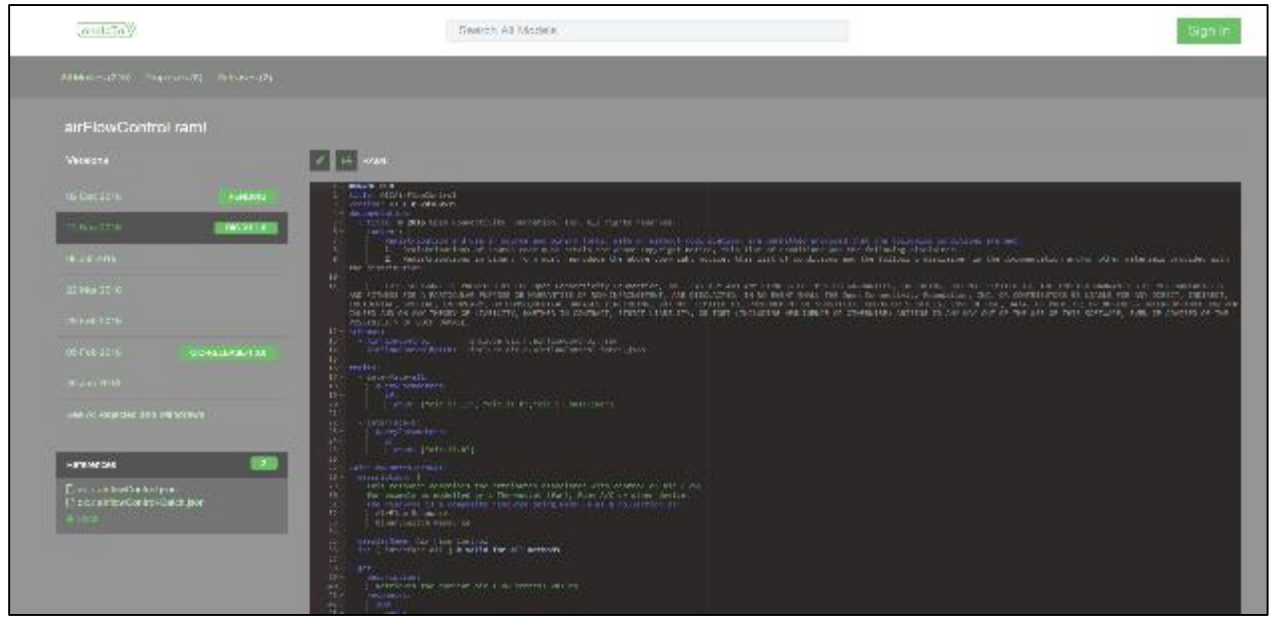
Complete suite of development tools

- Online tool for crowd-sourcing data models and building ecosystem interoperability
- Data models drive everything
- Automated tool chain creates
  - Server source code
  - Introspection file
  - Automated test case file
  - Secure onboarding file
  - Client tool user interface
- Several test and development tools



oneIoTa (oneiota.org)

- oneIoTa is an IDE and process management tool for the resource data models at the center of OCF.
  - OCF atomic resource models are entered in the editor windows in oneIoTa
  - More complex resources can be composed of atomic resources
  - Completed resources are submitted to an approval process for OCF (or partner organizations
  - Other organizations use the same approval process in oneIoTa
  - Mappings between OCF and other ecosystems are also entered in oneIoTa
  - Resource models are used to build specifications, devices, source code, GUIs, PICS files and bridges

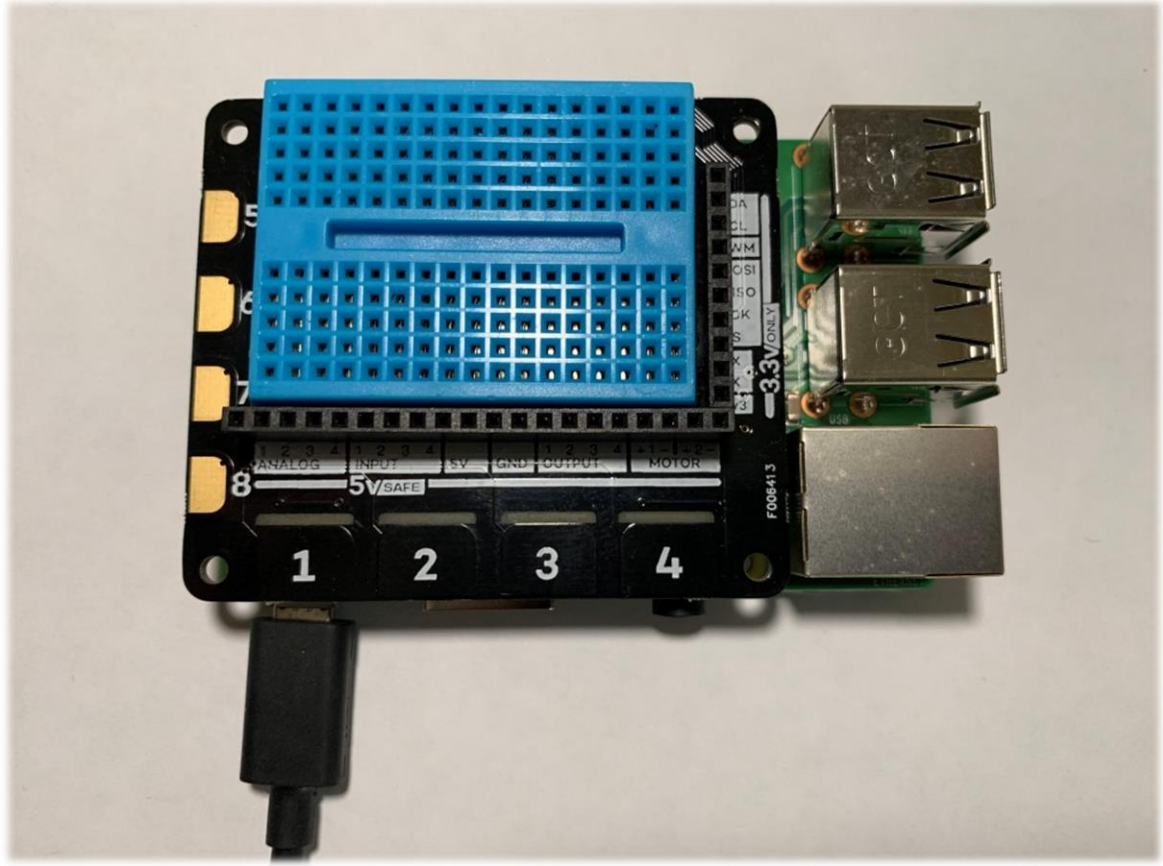


oneIoTa is the source of all resources you will need

- Go to http://www.oneiota.org
- Search for any resources you will need
- Use these descriptions when defining your device description file
- All devices consist of a list of resources
- All tools will consider oneIoTa as the authoritative source of resources

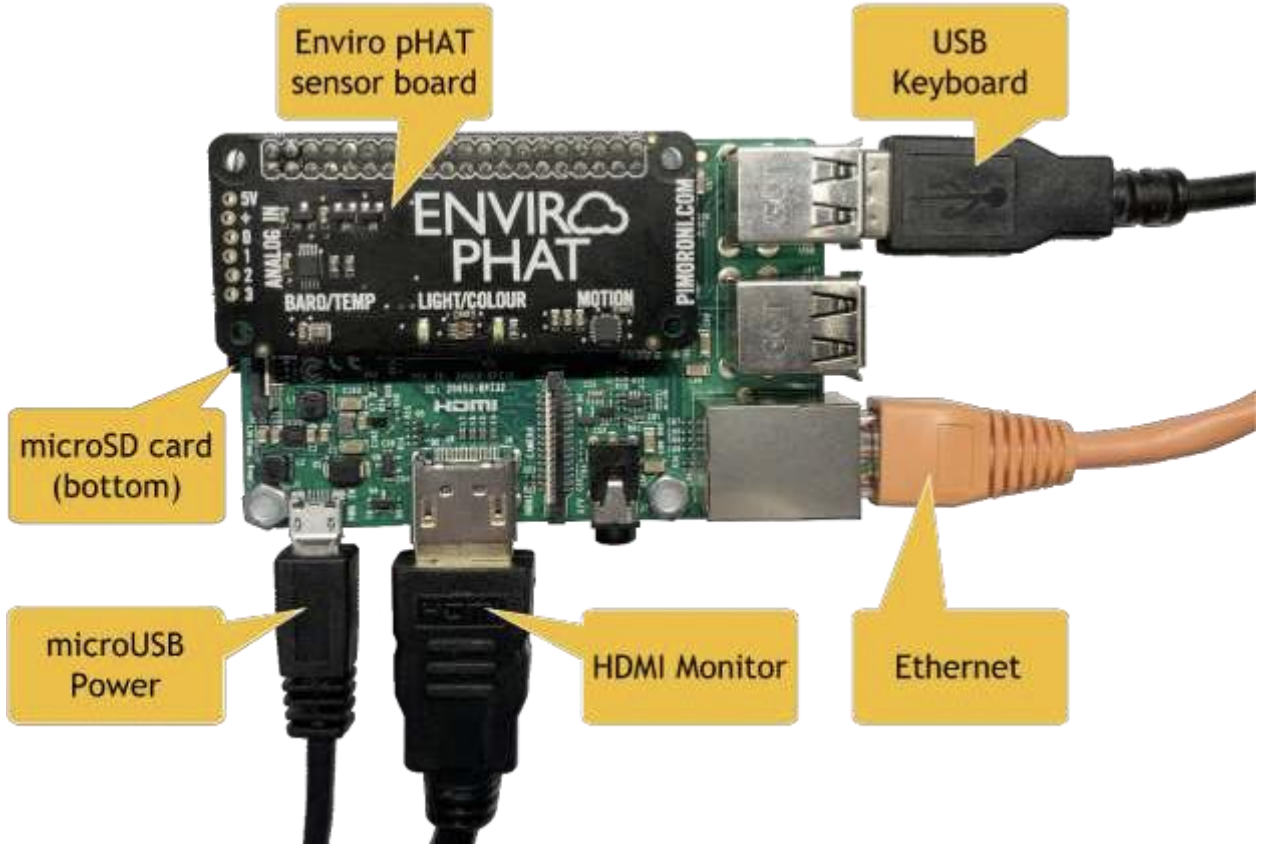
Set up the Hardware (Explorer Hat)

- Install the ExplorerHat board on the GPIO header on the Raspberry Pi board
- Insert the microSD card
- Connect the network (automatic)
- Plug in the power
- Connect keyboard and monitor (or SSH)



Set up the Hardware (Automation pHat)

- Install the AutomationPhat board on the GPIO header on the Raspberry Pi board
- Connect a resistor and LED from 5V to output 1(+5-LED-resistor-output 1)
- Connect a switch between 5V and input 1 (+5-switch-input 1)
- Insert the microSD card
- Connect the network
- Plug in the power
- Connect keyboard and monitor (or SSH)



Set up the SD card for Raspberry Pi

- Install PiBakery on Windows or MacOS (https://www.pibakery.org)
- Run PiBakery and import this file (file reference)
- Enter the Wi-Fi credentials and a desired hostname in the provided fields
- Choose whether you want the desktop or the console version
- Insert an SD/SD Micro card, click “Write” to create the Raspbian card.
  - Choose if you want to install the full or lite version of Raspian
  - Wait for the write to finish, then eject the SD card from your computer

Boot and Connect to the Raspberry Pi

- Get a terminal view of the Raspberry Pi
  - Connect a monitor, keyboard and (optional) mouse to the Raspberry Pi, or
  - Connect from your computer using SSH
    - You can ping the Raspberry Pi (ping <your host name>.local) to verify that the Raspberry Pi is available
      - If it is taking a long time, try "sudo killall –HUP mDNSResponder" on MacOS
    - MacOS
      - Use the terminal program and "New Remote Connection
    - Windows
      - Use Putty on (or similar)
    - SSH to the Raspberry Pi using "ssh://pi@<your host name>.local"
- Default login: user: pi, password: raspberry

Alternative Set up of the SD card for Raspberry Pi (hard way)

- Go through the NOOBS process to install the headless Raspian Stretch Lite located here: https://www.raspberrypi.org/downloads/raspbian/
- Enable ssh: copy an empty file called "ssh" (no extension) to the SD card root directory (https://github.com/openconnectivity/Sample-Raspberry-Pi-Code/blob/master/ssh)
- Optionally set up a Wi-Fi connection by copying wpa_supplicant.conf to the SD card root directory and edit for your Wi-Fi (https://github.com/openconnectivity/Sample-Raspberry-Pi-Code/blob/master/wpa_supplicant.conf)
- It is convenient to use your computer as the terminal for the Raspberry Pi. In order to do this, you will need to know the IP address of the Raspberry Pi. The simplest was is to connect a monitor to the HDMI port. The IP address will print out near the end of the boot process.
- Boot the Raspbery Pi by inserting the SD card and powering the board on. Write the IP address down so you'll remember it.
- Get a terminal view using a monitor and keyboard or ssh. (Putty on Windows, or the Go menu on Mac will give you an SSH connection)
  - Default login: user: pi, password: raspberry

Set up the development environment (Network)

- This method will work you are on a network
- Install the development environment
  - Install all of this from the home directory: cd ~
  - IoTivity-lite development: curl https://openconnectivity.github.io/IOTivity-Lite-setup/install.sh | bash
  - Project scripts: curl https://openconnectivity.github.io/Project-Scripts/install.sh | bash
  - Raspberry Pi examples (answer "y" to all the prompts): curl https://openconnectivity.github.io/Sample-Raspberry-Pi-Code/pi-boards/install.sh | bash
  - Make sure the PATH is set: reboot or source ~/.bashrc

Set up the development environment (USB Stick)

- This method works if you have a USB stick set up by OCF
- Mount the USB stick on the Raspberry Pi
  - Create a mount point: sudo mkdir /mnt/myusb (you can name it something else)
  - Mount the drive: sudo mount –o uid=pi,gid=pi /dev/sda1 /mnt/myusb
- Install the development environment
  - Install all of this from the home directory: cd ~
  - IoTivity-lite development: cat /mnt/myusb/IOTivity-Lite-setup/install.sh | bash
  - Project scripts: cat /mnt/myusb/Project-Scripts/install.sh | bash
  - Raspberry Pi examples (answer "y" to all the prompts): cat /mnt/myusb/Sample-Raspberry-Pi-Code/pi-boards/install.sh | bash
  - Unmount the USB stick: umount /mnt/myusb
  - Make sure the PATH is set: reboot or source ~/.bashrc

Let's build a device (page 1)

- Create a directory for development (this can be anywhere, but we'll use the following):
  - cd ~
  - mkdir workspace
  - cd workspace
  - Create an OCF project (can be named anything, but we'll use the following):
    - create_project.sh myexample
    - cd myexample
  - We'll use a pre-built sample to start:
    - cp ~/Sample-Raspberry-Pi-Code/IoTivity-lite/explorer-hat-pro/setup.sh ./
    - ./setup

Let's build a device (page 2)

- Automatically generate the code, introspection file and security files:
  - gen.sh
- Build the project executiable:
  - build.sh
- Set the security to "ready for owner transfer method" (RFOTM):
  - reset.sh
- Run the server code on the Raspberry Pi:
  - run.sh
- You have successfully build an OCF device and it is ready to onboard!

Onboard and control the server with OTGC

- Install OTGC on an Android device (make sure you're on the right LAN):
  - (download and run the APK or get it from the OCF USB stick)
  - Launch the OTGC application
- Click the discover button to search for OCF devices on the LAN
  - Arrow in circle icon
- Onboard the discovered server
  - "+" icon associated with the server device
- Get the UI to control the Raspberry Pi server from the Android OTGC
  - Gear icon
  - Use the UI to turn on and off any of the lights on the ExplorerHat board
  - Use the AI to turn on "observe" on any of the switches, then watch the terminal as you press the button on the ExplorerHat board
- <u>You have successfully onboarded and controlled your OCF Device!</u>

What we did

- Started with an OCF configuration file:
  - edit_config.sh
- Created an OCF input file:
  - edit_input.sh
- Created the server code, introspection file and sercurity files:
  - edit_code.sh
  - ls
- Used OTGC to discover, onboard and control the device
  - OTGC

Let's try a more complicated example (page 1)

- Create a new OCF project (can be named anything, but we'll use the following):
  - cd ~/workspace
  - create_project.sh automationphatlite
  - cd automationphatlite
- We'll use another pre-built sample:
  - cp ~/Sample-Raspberry-Pi-Code/IoTivity-lite/automation-phat-example/setup.sh ./
  - ./setup
- This time, setup will also copy over hardware interface files
  - Explore what is now in the bin directory: ls bin

Let's build a more complicated device (page 2)

- The same as before
  - Automatically generate the code, introspection file and security files:
    - gen.sh
  - Build the project executiable:
    - build.sh
  - Set the security to "ready for owner transfer method" (RFOTM):
    - reset.sh
  - Run the server code on the Raspberry Pi:
    - run.sh
- Run OTGC to
  - Control the hardware light on the Raspberry Pi
  - Turn on observe and the switch will change on the client when you switch it in hardware

Here's how you can do it on your own (page 1)

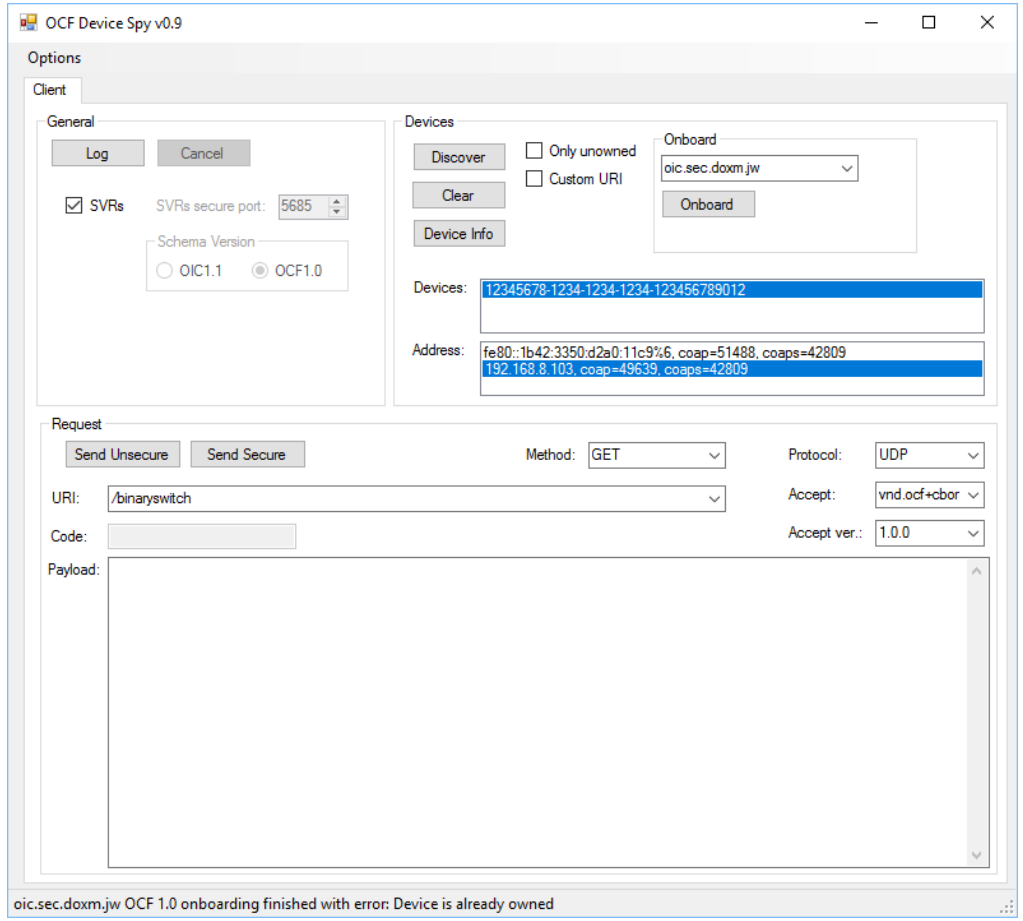
- Create a new OCF project (can be named anything, but we'll use the following):
  - cd ~/workspace
  - create_project.sh mytestproject
  - cd mytestproject
- Edit the configuration file for your specific device:
  - edit_config.sh
- Automatically generate the code, introspection file and security files (this usually only needs to be done once unless the config file is changed):
  - gen.sh

Here's how you can do it on your own (page 2)

- Use the same development loop as before, but edit the code as necessary:
  - Edit the code:
    - edit_code.sh
  - Build the project executiable:
    - build.sh
  - Set the security to "ready for owner transfer method" (RFOTM):
    - reset.sh
  - Run the server code on the Raspberry Pi:
    - run.sh
  - Run OTGC and control the server on the Raspberry Pi

Testing with Device Spy (as an alternative to OTGC)

- Device Spy is a lower level client that allows you to construct the actual payloads that are sent. It is only available on Windows.
  - Discover the device by clicking the [Discover] button
  - Onboard the device by clicking SVRs, selecting an address and clicking the [Onboard] button
  - Inspect the resource payload by setting the resource URI, selecting the GET method and clicking the [Send Secure] button
  - Change the value of the resource (e.g. false to true) by selecting the POST message and clicking the [Send Secure] button
  - The state of the light should change accordingly



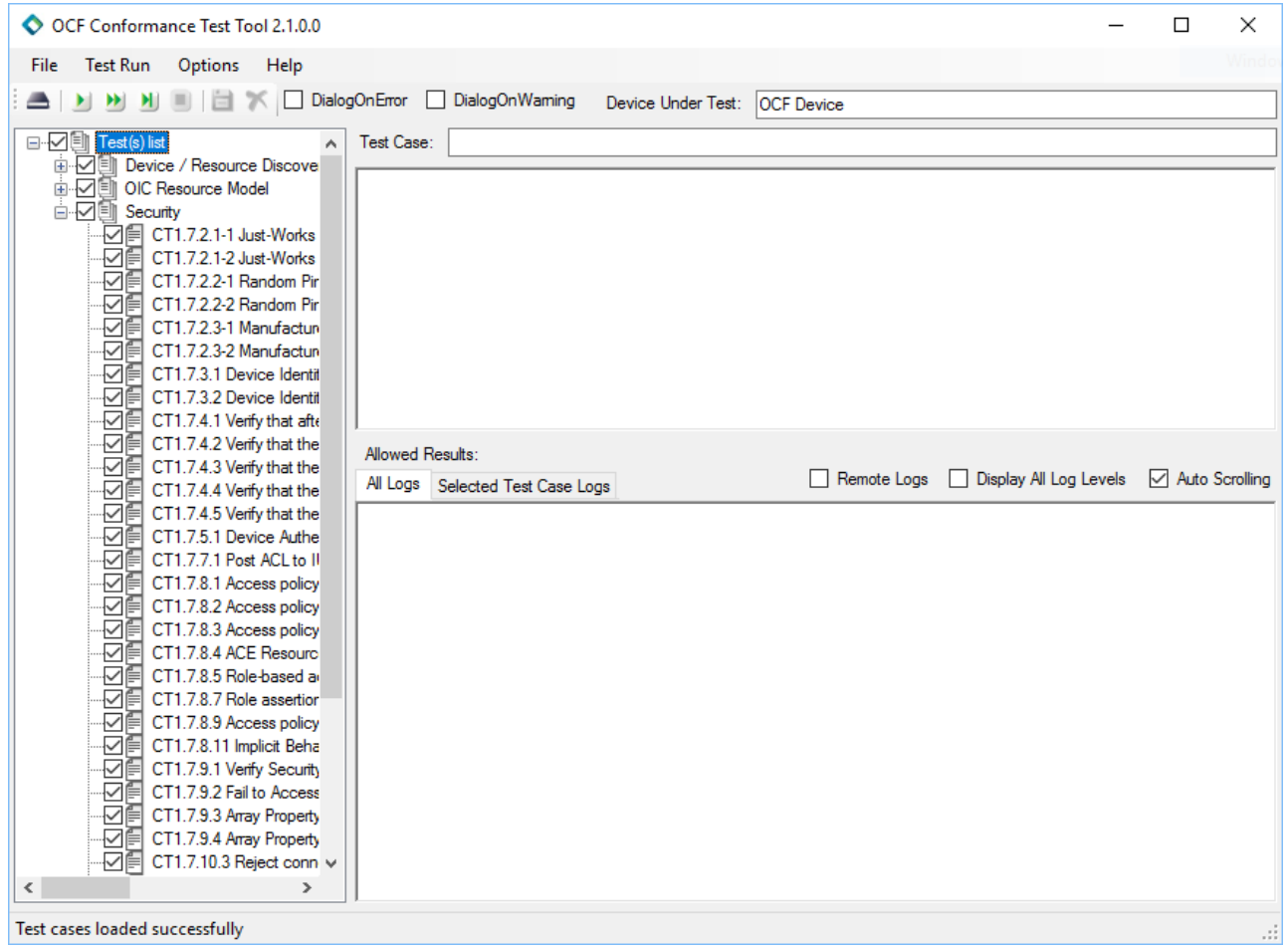
Simple device description input file

```
[
   {
     "path" : "/binaryswitch",
     "rt"   : [ "oic.r.switch.binary" ],
     "if"   : ["oic.if.a", "oic.if.baseline" ],
     "remove_properties" : [ "range", "step" , "id", "precision" ]
   },
   {
     "path" : "/oic/p",
     "rt"   : [ "oic.wk.p" ],
     "if"   : ["oic.if.baseline", "oic.if.r" ],
     "remove_properties" : [ "n", "range", "value", "step", "precision", "vid"  ]
   }
]
```

Run the Certification Test Tool

- The Certification Test Tool is and automated test too that devices must pass to get OCF certification
  - Run the CTT
  - Select the PICS file generated by gen.sh
  - Select the discovered device and the interface to use
  - Click the play button to start the tests
  - Go get coffee
  - But don't take too long because you will need to change the onboarding state to RFOTM a few times
  - Pass the CTT and work with a certified lab to get official certification.

Available to OCF members



What to do next

- Define your own input file
- Run the tooling!
- Build it… and see if it works
- Change the code, to what you want it to do

What else?

- The DeviceBuilder can be modified for any programming language using templates
- The OTGC will be available on Android, iOS, Linux and Windows soon
- The OTGC will be available as open source, so you can use a product that is already OCF certified as the basis for your own client tool on multiple operating systems
- There is a node.js version of IoTivity available
- IoT boards from other companies are supported with these tools
  - Samsung EagleEye
  - Linux emulator using Glade for UI
  - More to be added soon

Acknowledgments and references

- All of this has been developed by the dedicated volunteers and contractors of Open Connectivity Foundation (http://openconnectivity.org)
- Wouter van der Beek of Cisco is the Chair of the OCF Technical Steering, is responsible for key architectural design and personally developed the DeviceBuilder and the key scripts in this presentation.
- Dekra created the OTGC tool under contract to OCF. The tool will be available as open source on Android, iOS, Linux and Windows in the Fall.
- Comarch created the CTT and DeviceSpy under contract to OCF. These tools are available to OCF members.
- For complete summarized instructions, look here: https://github.com/openconnectivity/Project-Scripts/blob/master/One%20Page%20Complete%20Setup%20Instructions.md

OPEN CONNECTIVITY FOUNDATION®

Connect to the Raspberry Pi

- MacOS
  - Start terminal: (command-K from finder) or “terminal” from Spotlight
  - Enter SSH address: ssh://pi@<hostname>.local
  - Refresh DNS: sudo killall –HUP mDNSResponder
- Windows
  - Start terminal: run putty
  - Get the IP address from someone with linux or a Mac
  - Enter SSH address: ssh://pi@<IP address>
  - Refresh DNS: ipconfig /flushdns
- Linux
  - Start terminal: usually in sidebar, but can type terminal in search applications
  - Enter SSH command: ssh pi@<hostname>.local
  - Refresh DNS: sudo /etc/init.d/dns-clean restart
- Default login: user: pi, password: raspberry