Enersec

LAN usage and “cloud” enablement for nCipher Edge.

The nCipher Edge unit, as you are aware, is a portable, USB connected, low-volume transaction Hardware Security Module (HSM) which features as the cost-effective choice in the nShield product line.

The nCipher Edge unit works well in a single user environment, locally or via passthrough to a virtual machine with the relevant COM port mappings. With the logistic difficulties faced by COVID and a move to a more global workforce that want to leverage resources in a more cost-efficient way, it would be beneficial to be able to utilise an nCipher Edge unit in a remotely connected capacity.

This is NOT to replace performant Connect or XC HSMs, nor is it to replace nCiphers HSM as a service offering. It is a middle ground to allow for the maximum usage of an nCipher Edge over a large number of use cases in the new landscape we find ourselves in.

The details of how to undertake this is simply one approach, as always there are multiple ways to tackle a given problem.

This solution will use the following software and hardware to complete, remote sharing of an nCipher Edge to multiple clients where authorised:

- Raspberry PI
  - PI 3 B+
- Raspbian
  - Raspbian GNU/Linux 9 (stretch)
- nCipher Edge
  - FW 12.60.6 (will work with any I’m sure)
- VirtualHere
  - Limitation! - Generic Build of the VirtualHere Server on an unlimited number of computers and share a single USB device per computer server, with no payment required. To share more than one USB device simultaneously from a single server you must purchase an "Unlimited Device License".
- ZeroTier
  - "...directly connect the world’s devices and enable a new era of decentralized computing...”
- OpenVPN (Alternative to ZeroTier)
  - “….OpenVPN is open-source commercial software that implements virtual private network techniques to create secure point-to-point or site-to-site connections…”

The use of a PI is not necessary but does allow for a headless, low power, low cost and self-contained way to “share” the nCipher Edge device over a network for clients. Taking this into account the creation of a micro SD card with a Raspbian image is outside the scope of these notes.

Performance

This is a summary of times collected for some commands over the different connectivity options.

	Initunit	Newworld program	enquiry	nfkminfo	KEYGEN RSA2048	KEYGEN AES 256
Azure VIA ZeroTier	00:02:02	00:03:55	00:00:00	00:00:27	00:01:56	00:03:10
LAN	00:00:01	00:02:47	00:00:28	00:00:27	00:01:05	00:01:09
Local USB	00:00:37	00:02:25	00:00:00	00:00:25	00:02:32	00:00:39

All times in hh:mm:ss

It should be noted that LAN based tests were over 802.11AC Wifi connection and all Azure tests opted for 100Mbit wired connection, both with an effective 33Mbit Down and 8Mbit up to the internet from/to the PI/HOST.

VirtualHere Server

Log into your PI/Host OS and follow the commands below (also available from the vendors website https://www.virtualhere.com/oem_faq)

- cd ~
- mkdir vusb
- cd vsub
- wget https://www.virtualhere.co/smites/default/files/usbserver/vhusbdarm
- sudo chmod +x ./vhusbdarm
- sudo mv vhusbdarm /usr/sbin
- sudo vi /etc/systemd/system/virtualhere.service
- Put the following contents in the above file:
    - [Unit]
    - Description=VirtualHere USB Sharing
    - Requires=networking.service
    - After=networking.service
    - [Service]
    - ExecStartPre=/bin/sh -c 'logger VirtualHere settling...;sleep 1s;logger VirtualHere settled'
    - ExecStart=/usr/sbin/vhusbdarm

    - Type=idle
    - [Install]
    - WantedBy=multi-user.target
- Write and quit the file
- sudo systemctl daemon-reload
- sudo systemctl enable virtualhere
- sudo systemctl start virtualhere

nCipher Edge

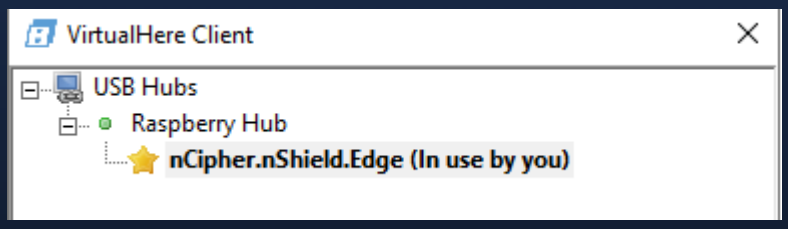
Connect the device to the PI via its provided USB A to B cable. Note the PI/Host will NOT require the install of any nCipher drivers or security world software.

nCipher Client install

It is now recommended to install the nCipher security world software on the client you wish to present the remote Edge device to. In this instance we want to use the Edge on a Windows server/ client. Mount the desired Security World ISO and install the desired components.

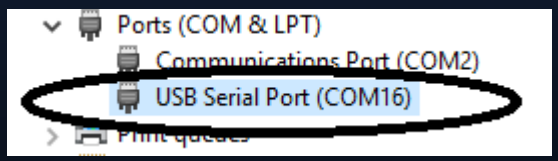
VirtualHere Client

Download the respective client (https://www.virtualhere.com/usb_client_software). In this case Windows x64, and execute, see the link above for an overview. The client should automatically find the VirtualHere server, as shown below. If not add the right click the top branch and “Specify Hubs” using the IP of your PI/Host.



Once found, right click the nCipher.nSheilf.Edge and select “use this device”.

Open device manager and specify a high COM port so not to cause issues with other devices, etc.



Modify the nCipher hardserver config file to reflect the new COM port, by adding “serial_dtpp_devices=COM16” to the file.

Restart the “nFast Server”

You may now use the nCipher Edge device over the local network.

Cloud or remote access

Latency is of high importance when using USB devices over a network, especially when you want to operate an nCipher Edge to a VM tenanted on a cloud provider. You use many different VPN technologies, but gaming based virtual network (peer) providers like Parsec and ZeroTier will provide a low latency "secure" connection that requires little to no network config, allowing full cloud access from a given guest to the PI Edge. ZeroTier will be used in this setup and its security information can be found https://www.zerotier.com/manual/#2_1_3

ZeroTier Initial setup

- Goto https://my.zerotier.com/ and register for a free account.
- Navigating to https://my.zerotier.com/network and clicking Create.
    - Note down the "NETWORK ID" and "NAME"
    - Access Control – Select "PRIVATE"
    - IPv4 Auto-Assign – Select "EASY" and select a subnet that does NOT conflict with you PI/HOST
- Install the PI/Host (as per the https://www.zerotier.com/download/)
    - SSH to the PI/Host
    - curl -s https://install.zerotier.com | sudo bash
    - sudo systemctl enable zerotier-one
    - sudo zerotier-cli info
        - Note down the "NODE ID"
    - Goto https://my.zerotier.com/netowork
    - Click on your "Network ID/NAME"
    - Locate the "Manually Add Member" section.
        - In the "NODE ID" box add PI/HOST "NODE ID" and press submit.
    - On the PI/Host run "sudo zerotier-cli join <NETWORK ID>"
    - Now check the PI/Host is connected "sudo zerotier-cli info"
- Install the Cloud VM / Client (as per the https://www.zerotier.com/download/) Windows in this case.
    - Install the MSI and note down the "NODE ID"
    - Goto https://my.zerotier.com/netowork
    - Click on your "Network ID/NAME"
    - Locate the "Manually Add Member" section.
        - In the "NODE ID" box add Cloud VM/Client "NODE ID" and press submit.

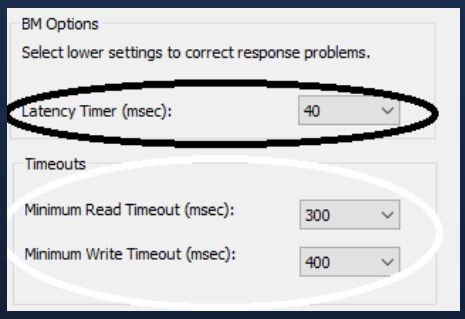
- Right click the task tray icon for zerotier and “Join Network”
- Enter the <NETWORK ID>, Tick allow global, allow managed and allow default. Then press OK.
- Right click the task tray icon for zerotier and select “show networks” Status should be “OK”

Cloud VM connect to the Edge

You should have administrator rights to this VM, the nCipher security world software should be installed and all module, card and world files should be present before continuing.

- Goto https://my.zerotier.com/netowork
  - Click on your “Network ID/NAME”
  - Select “Members”
    - Note the “Address” and “Managed IP” for the connected devices.
- Run the VirtualHere client (vhui64.exe) on the Cloud/VM
  - Right click the top branch and “Specify Hubs” using the IP of your PI/Host, “Managed IP” from zerotier.
  - Once found, right click the nCipher.nSheild.Edge and select “use this device”.

It is advised to modify the COM port Advance settings to allow for the added latency, some example values are shown in the screenshot below, which seem to give a consistent result when in use.



Visuals

Here is the finished standalone unit, just power required.