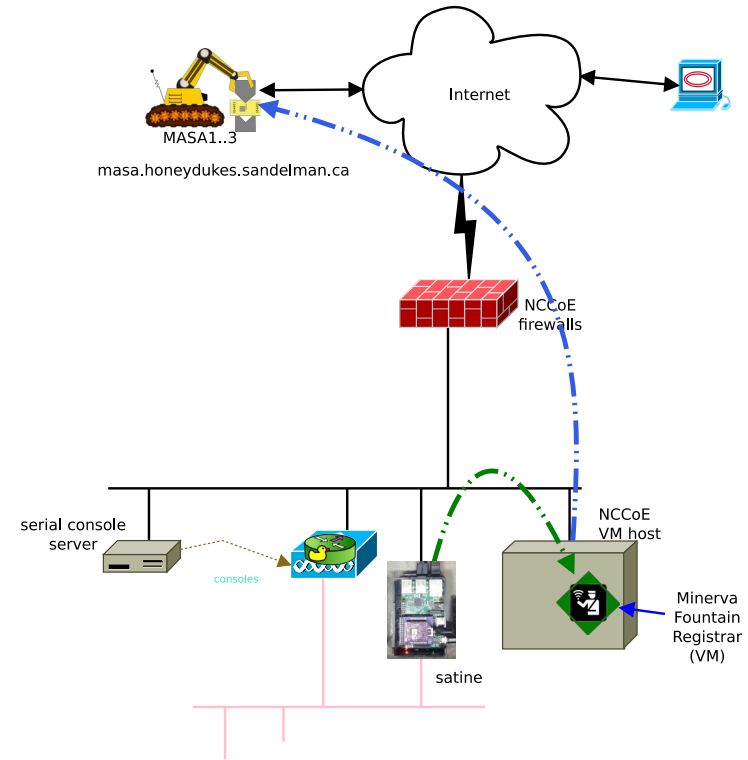# NCCoE IoT Onboarding

BRSKI – build 3 Operational Run Through

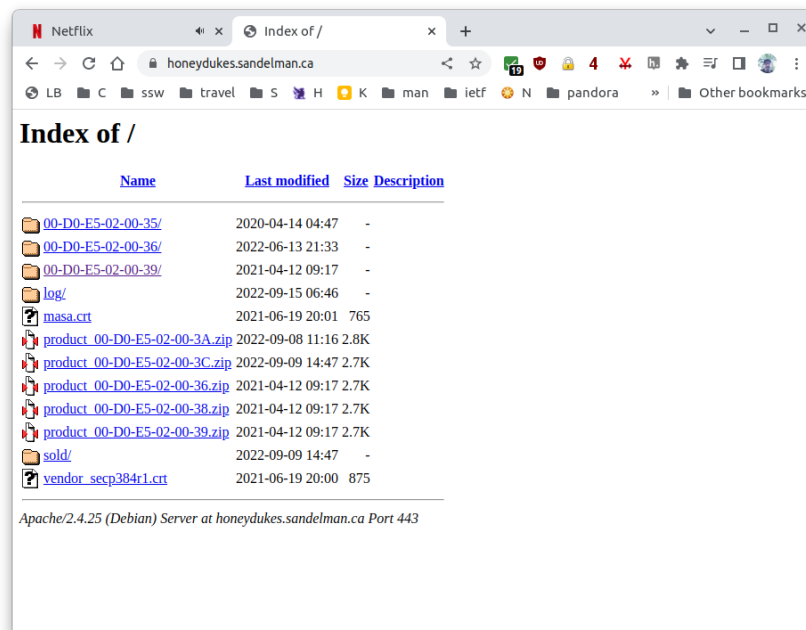# Sept 2022 - Network Diagram for Build 3

Goals of iteration 1

- Validation of Registrar
- Validation of MASA
- Verification of IDevID

Sept 2022 – Simulated Factory Provisioning

Provisioning of IDevID

- Factory generates private keys

- Signs IDevID certificates

- Maintains inventory of five un-owned devices

https://minerva.sandelman.ca/
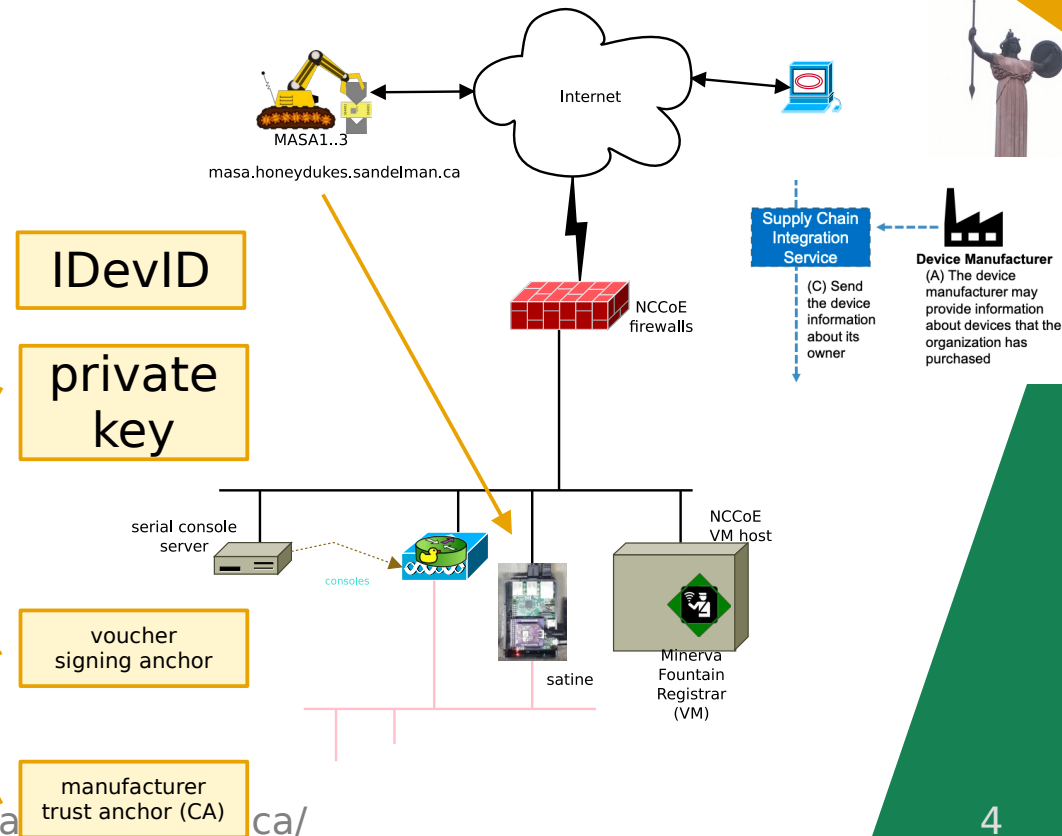
Sept 2022 – Provisioning Step

Provisioning of IDevID

- Download ZIP file to Pledge simulator
- Unzip into convenient place

```
nccoe@satine:~/reach$ ls -l 00-D0-E5-02-00-37

total 16

-rw-rw-r-- 1 nccoe nccoe 696 Apr 12  2021 device.crt

-r-------- 1 nccoe nccoe 227 Apr 12  2021 key.pem

-rw-rw-r-- 1 nccoe nccoe 733 Apr 12  2021 masa.crt

-rw-r--r-- 1 nccoe nccoe 810 Apr 12  2021 vendor.crt
```

IDevID

private key

voucher signing anchor

manufacturer trust anchor (CA)

Internet

MASA1..3
masa.honeydukes.sandelman.ca

NCCoE firewalls

Supply Chain Integration Service

(C) Send the device information about its owner

Device Manufacturer
(A) The device manufacturer may provide information about devices that the organization has purchased

serial console server

consoles

NCCoE VM host

satine

Minerva Fountain Registrar (VM)
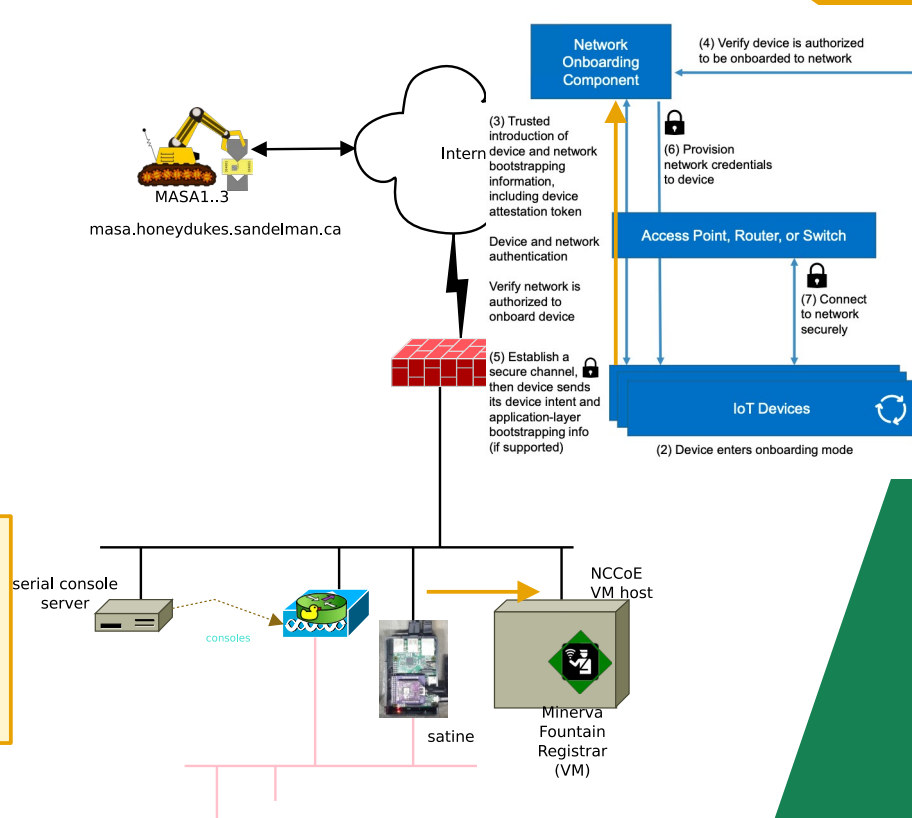
Sept 2022 – Voucher Request Step

Use IDevID to connect to Registrar

```
bundle exec rake
reach:enroll_http_pledge
PRODUCTID=00-D0-E5-02-00-3B
JRC=https://192.168.30.34:8443/
```

address/ port of Registrar

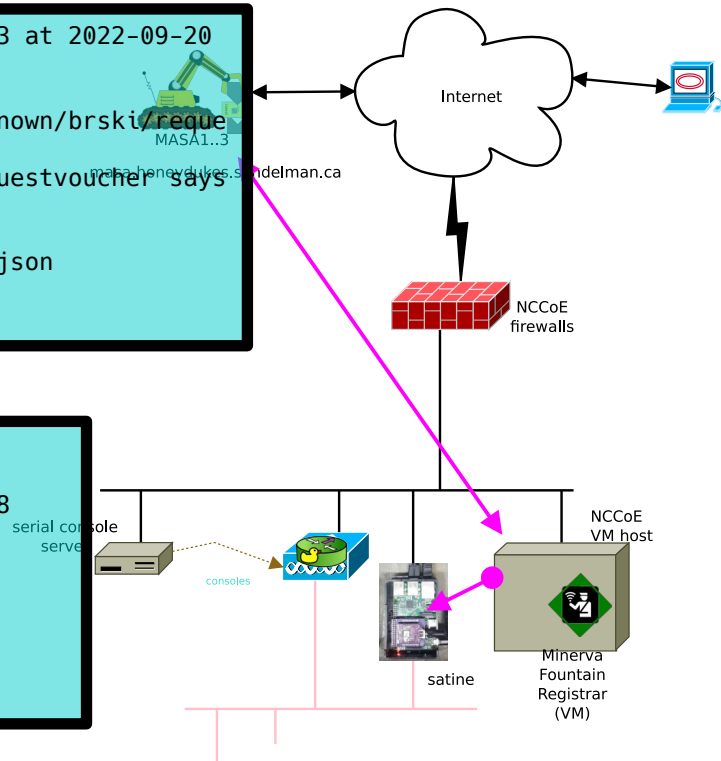Directory in which identity files are extracted

(4) Verify device is authorized to be onboarded to network

Network Onboarding Component

MASA1..3
masa.honeydukes.sandelman.ca

Internet

(3) Trusted introduction of device and network bootstrapping information, including device attestation token

Device and network authentication

Verify network is authorized to onboard device

(5) Establish a secure channel, then device sends its device intent and application-layer bootstrapping info (if supported)

(6) Provision network credentials to device

Access Point, Router, or Switch

(7) Connect to network securely

IoT Devices

(2) Device enters onboarding mode

serial console server

consoles

NCCoE VM host

satine

Minerva Fountain Registrar (VM)

2022-09-21

https://minerva.sandelman.ca/

5

Sept 2022 – MASA Interaction

Use IDevID to find MASA

device.crt ➡️ masa.honeydukes.sandelman.ca

```
nccoe@satine:~/reach$ openssl x509 -noout -text -in 00-D0-E5-02-00-3B/device.crt


    Certificate:
    ...
            Issuer: DC = ca, DC = sandelman, CN = Unstrung Highway CA
            Validity
                Not Before: Sep  9 12:47:22 2022 GMT
                Not After : Dec 31 00:00:00 2999 GMT
            Subject: serialNumber = 00-d0-e5-02-00-3b
    ...
            1.3.6.1.5.5.7.1.32:
                ..masa.honeydukes.sandelman.ca
        Signature Algorithm: ecdsa-with-SHA256
            30:65:02:30:75:15:8e:de:cd:13:58:ca:b3:1c:ef:03:9d:7c:
    ...     c9:b2:78:3d:36:29:b2:1f:85:f8:66:cd:8c
```

Sept 2022 – MASA Interaction

```
INFO -- : Started POST "/.well-known/brski/requestvoucher" for 192.168.30.103 at 2022-09-20
INFO -- : Processing by EstController#requestvoucher as HTML
INFO -- : voucher request from 192.168.30.103
INFO -- : Contacting server at: https://masa.honeydukes.sandelman.ca/.well-known/brski/reque
INFO -- : Asking for voucher of type: application/voucher-cms+json
INFO -- : MASA at https://masa.honeydukes.sandelman.ca/.well-known/brski/requestvoucher says
INFO -- : MASA provided voucher of type application/voucher-cms+json
INFO -- : device #3 (name: ) has been adopted
INFO -- : returning voucher #9 of size 1949 with ct=application/voucher-cms+json
INFO -- : Completed 200 OK in 952ms (Views: 0.5ms | ActiveRecord: 12.2ms)
```

```
nccoe@satine:~/reach$ sh er1
Writing Voucher Request to tmp/vr_00-d0-e5-02-00-3b.pkcs
MASA/JRC provided voucher of type application/voucher-cms+json; charset=utf-8
Voucher connects to /DC=ca/DC=sandelman/CN=minerva-fountain.example.com
vs:    /DC=ca/DC=sandelman/CN=minerva-fountain.example.com
Voucher authenticates this connection!
```

MASA1..3
masa.honeydukes.sandelman.ca

Internet

NCCoE firewalls

NCCoE VM host

serial console server

consoles

satine

Minerva Fountain Registrar (VM)

https://minerva.sandelman.ca/

Sept 2022 – MASA Interaction
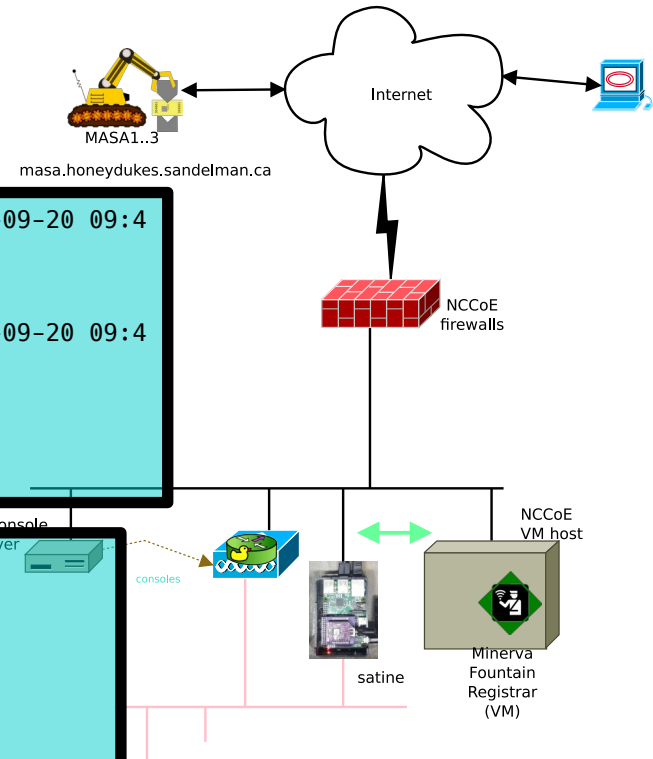
Use Resulting trust to enroll LDevID

```
INFO -- : Started GET "/.well-known/est/csrattributes" for 192.168.30.103 at 2022-09-20 09:4
INFO -- : Processing by EstController#csrattributes as */*
INFO -- : Completed 200 OK in 9ms (Views: 0.6ms | ActiveRecord: 1.3ms)

INFO -- : Started POST "/.well-known/est/simpleenroll" for 192.168.30.103 at 2022-09-20 09:4
INFO -- : Processing by EstController#simpleenroll as */*
INFO -- : Completed 200 OK in 69ms (Views: 0.7ms | ActiveRecord: 49.4ms)
```

```
csrattr_uri: https://192.168.30.34:8443/.well-known/est/csrattributes
Registrar returned CSR of type application/csrattrs; charset=utf-8
new device gets rfc822Name: rfc8994+fee4e924a8be596a64257f1e00000000+@acp
Registrar returned certificate of type application/pkcs7-mime;
                       charset=utf-8 [in tmp/certificate.der]
nccoe@satine:~/reach$
```

Internet

MASA1..3
masa.honeydukes.sandelman.ca

NCCoE
firewalls

serial console
server

consoles

NCCoE
VM host

satine

Minerva
Fountain
Registrar
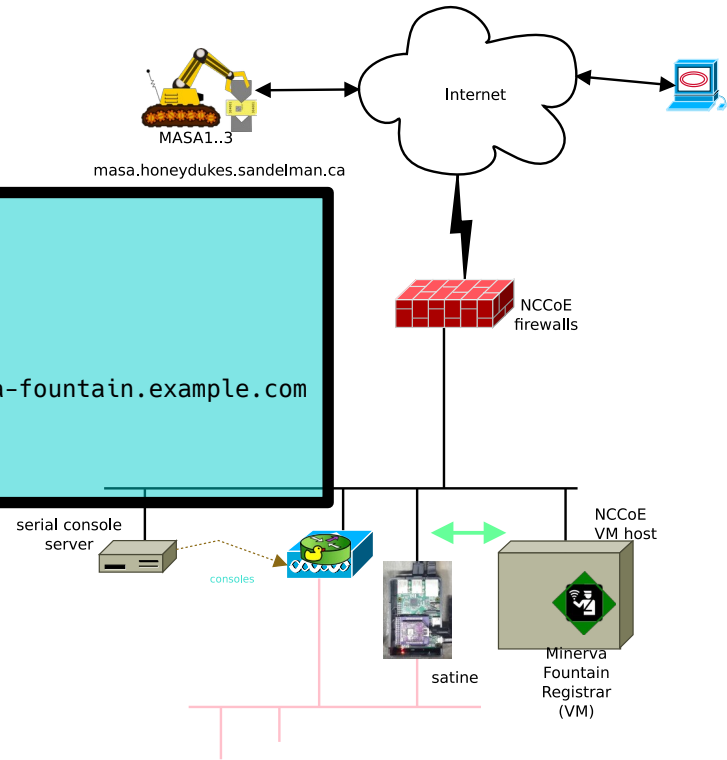(VM)

https://minerva.sandelman.ca/

Sept 2022 – MASA

MASA notes transfer of ownership with an email!


```
Subject: New cms_voucher voucher issued for Device 00-D0-E5-02-00-3B


Message from masa.honeydukes.sandelman.ca
============================

Device Device 00-D0-E5-02-00-3B was re-sold to /DC=ca/DC=sandelman/CN=minerva-fountain.example.com
to Registrar at 2610:20:60ce:230::34.
```

Sept 2022 – MASA

MASA notes depletion of inventory, creates new devices.


```
Subject: Cron <honeydukes@relay> $HOME/bin/inventory
Date: Fri,  9 Sep 2022 12:47:22 +0000 (UTC)

creating 1 devices to refill inventory to 5
Creating device 1 with mac 00-d0-e5-02-00-3b
Running: cd /honeydukes/app/highway/releases/20220603215622/db/devices &&
 zip -r /honeydukes/app/highway/current/db/inventory/product_00-D0-E5-02-00-3B.zip 00-D0-E5-02-00-3B
   adding: 00-D0-E5-02-00-3B/ (stored 0%)
   adding: 00-D0-E5-02-00-3B/device.crt (deflated 24%)
   adding: 00-D0-E5-02-00-3B/masa.crt (deflated 27%)
   adding: 00-D0-E5-02-00-3B/vendor.crt (deflated 34%)
   adding: 00-D0-E5-02-00-3B/key.pem (deflated 15%)
Marking /honeydukes/app/highway/current/db/inventory/product_00-D0-E5-02-00-37.zip
   as sold
```

https://minerva.sandelman.ca/
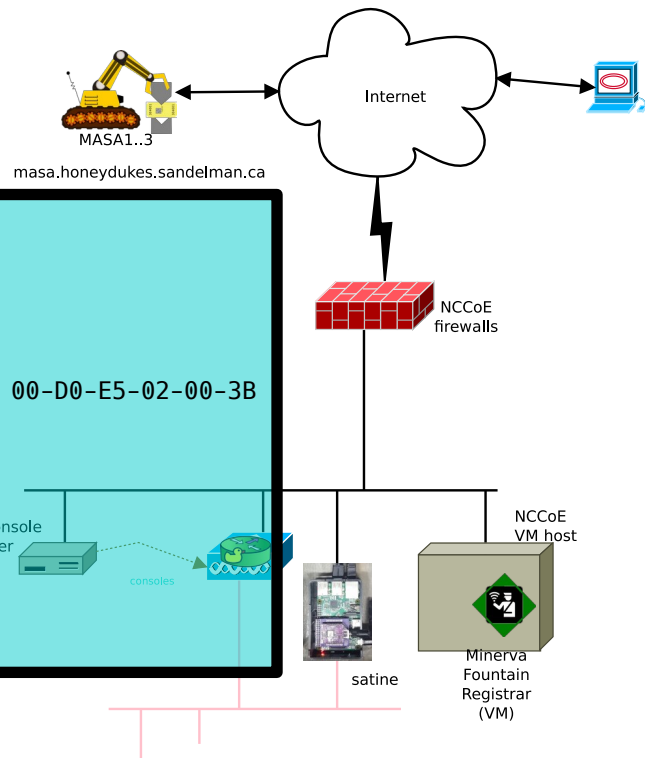
Build3 – BRSKI – Network/Application Onboarding

- A credential was provisioned by the manufacturer

- (similated by download of zip file)

- The device contacted the local onboarding infrastructure and was approved to join.

- An LDevID certificate was issued for the device

https://minerva.sandelman.ca/