Draft-richardson-anima-smarkaklink BRSKI enrollment with smart phones

Or:

How do I bootstrap operator-less Registrars

Michael Richardson*
Jacques Latour
Abhishek Joshi





* All bad ideas are mine

Agenda

- 1) what's the problem.
- 2) Rough idea of solution.
 - 1) Why the name change!
- 3) Questions.

SecureHomeGateway.ca

Internet

https://github.com/CIRALabs/Secure-IoT-Home-Gateway







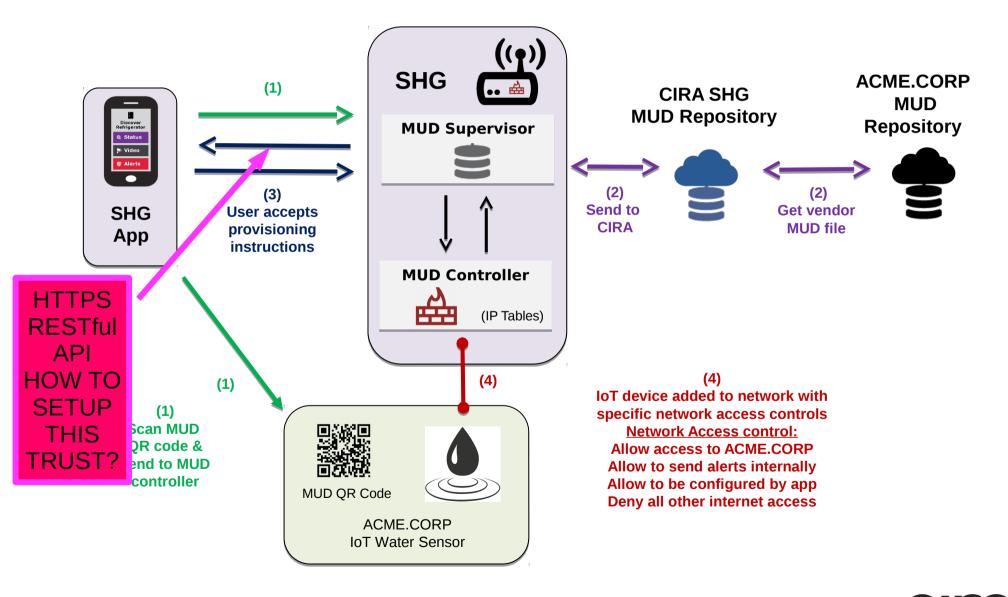
ICANN 2018 DEMO video

https://www.youtube.com/watch?v=LauvEBa4Z4s

RIPE 77 talk https://ripe77.ripe.net/archives/video/2309

ICANN 63 talk URL unknown

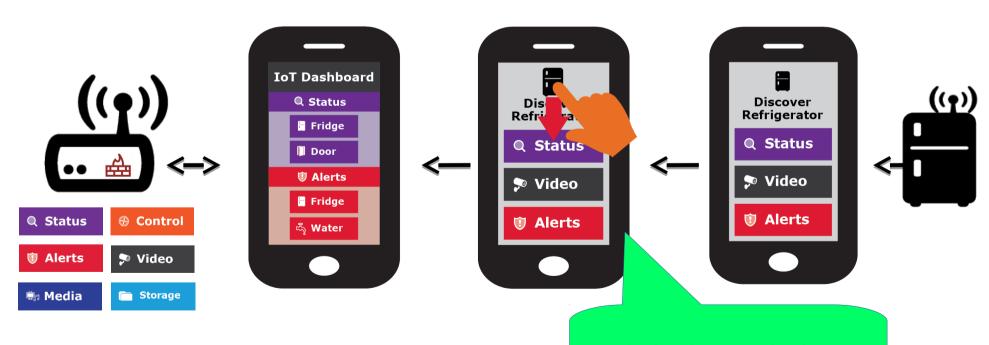
High Level MUD & IoT Device Provisioning Workflow





Simple user interface is key to this project: **Swipe UP, DOWN, LEFT and RIGHT**

 Gateway provisioning, device discovery, device provisioning must be as simple as possible, intuitive for non experienced users, available as framework for default open source app.



Requirements

Goal

- Enroll a smartphone into PKI/database in Registrar of Home Router
- First administrator can enable additional administrators or other roles with less rights (Role-Based Access control)

Assumptions

- Router has QR code on sticker attached
- Smartphone has LTE connection, or can move to another WiFI
- Router might have no Internet until end-user types in PPPoE password.
 - Fries & Oskar: Device might NOT have Internet until home is occupied, or might never have Internet.

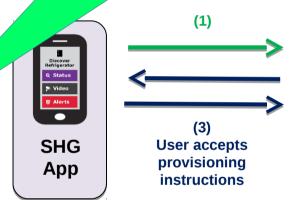
Initial bootstrap of app

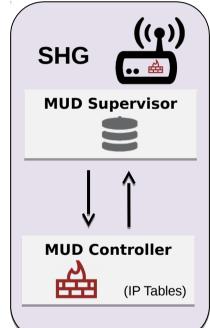
HTTPS connection from app to SHG.

- NO PASSWORDS.
- TLS ClientCertificate

 (pinned in database, CA part irrelevant)
- TLS ServerCertificate:
 - mud.nc0a8fc4.r.securehomegateway.ca

How do I bootstrap
The first Client Certificate?





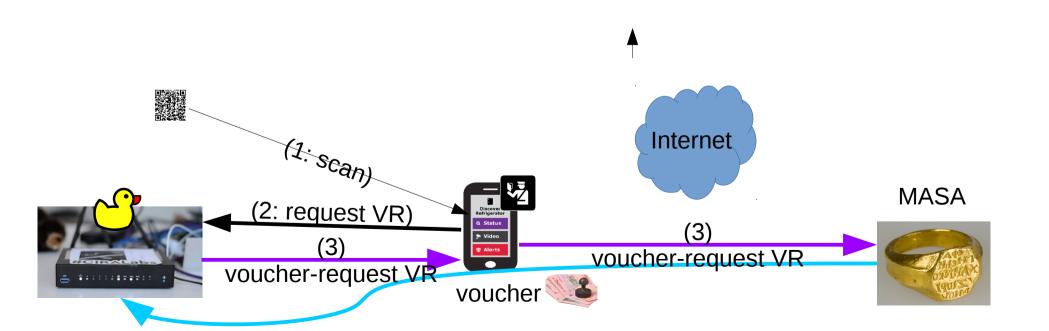
ULA
Generated by router
As per RFC7084
WebPKI certificate
Installed at factory
W/ DNS name

%dig +short mud.nc0a8fc4.router.securehomegateway.ca aaaa fd2a:c0a:8fc4::18e

Roles are a changin'

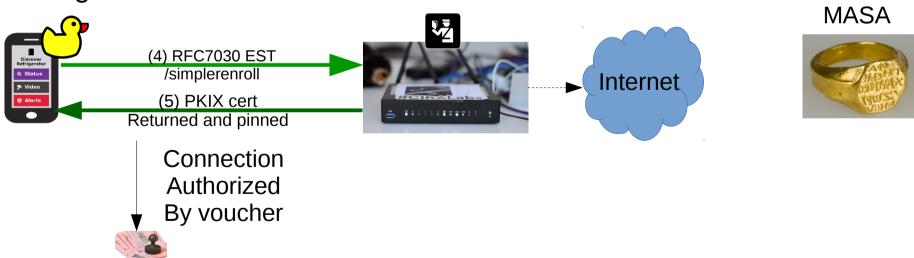
Sorta seems like a registrar

- Consider new (adolescent) router to be a Pledge at first.
- Consider Smartphone to be a new type of Join Proxy at first
- Change roles later on.



Smartphone becomes client!

- Smartphone now becomes the EST client
- Router now becomes a registrar
- Smartphone uses authorized TLS connection as secure transport for enrollment of new identity. As first device, becomes administrator, configures the device.



SmartPledge -> Smarkaklink

- "SmartPledge" name was trying to be some kind of portmanteau of smartphone pledge
 - But, smartphone is not always the pledge, the router is.
- Smartphone has multiple roles

- SmarKaklink invokes sound of wine glasses clinking.
- Redrew images according to BRSKI left(pledge) to right (MASA) view.



Some notes

 Smartphone, as pseudo-registrar can still access audit-log from MASA!



- Smartphone identity is pseudonymous, but MASA still logs it, so smartphone can recognize "itself"
- Opportunity for further enrollment provided via OAUTH2 interaction between MASA and Smartphone

What about this QR code? Who else uses QR code?

- WiFi Alliance DPP
 - Released in summer
 - Crypto done by Dan Harkins.
 - Uses Public Key privated on QR code
 - Runs over new management frames in 802.11, presently inaccessible on current smartphone Oses.
 - We are writing code today.

- EAP-NOOB
 - Been around for awhile.
 - Requires dynamic QR code ... or
 - Maybe leverage many LEDs on front of router?
 - Not interested in AAA back-end, it would have to be co-located in phone.

smarkaklink-01

- Leverages DPP QR code format
 - Want to leverage all of the crypto with the goal of "upgrading" to DPP when smartphone APIs become available.
 - (Extends DPP QR code, despite WiFi Alliance not providing "IANA Considerations")
- Tweaks BRSKI to include a /requestvoucherrequest to avoid need for Registrar to contact MASA directly.



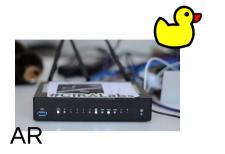














MASA















Scan QR Code on









Scan QR Code on

Generate Self-signed







Scan QR
Code on

Generate Self-signed Use as ClientCertificate











Generate Self-signed Use as ClientCertificate

Visit URL Given QR Do OAUTH2 dance?





MASA



Scan QR Code on

Generate Self-signed Use as ClientCertificate

Get Certificate (optional?) signed by MASA

Visit URL
Given QR
Do OAUTH2 dance?





MASA





Generate Self-signed Use as ClientCertificate

Get Certificate (optional?) signed by MASA

Visit URL
Given QR
Do OAUTH2 dance?

/requestvoucherrequest (+ SPnonce)







Encrypt (ECIES)
With public

Key of AR

Generate Self-signed Use as ClientCertificate

Get Certificate (optional?) signed by MASA

Visit URL
Given QR
Do OAUTH2 dance?

Connect to BRSKL port
/requestvoucherrequest (+ SPnonce)

Scan QR

Code on









Scan QR Code on

Encrypt (ECIES)
With public
Key of AR

Generate Self-signed Use as ClientCertificate

Get Certificate (optional?) signed by MASA

Visit URL
Given QR
Do OAUTH2 dance?

Connect to BRSKL port
/requestvoucherrequest (+ SPnonce)

Receive voucherrequest (w/ SPnonce)







Encrypt (ECIES)
With public
Key of AR

Generate Self-signed Use as ClientCertificate

Get Certificate (optional?) signed by MASA

Visit URL
Given QR
Do OAUTH2 dance?

Connect to BRSKL port
/requestvoucherrequest (+ SPnonce)

Receive voucherrequest (w/ SPnonce)

Scan QR

Code on

Send to voucherrequest
To MASA





MASA



Encrypt (ECIES) With public

Key of AR

Generate Self-signed Use as ClientCertificate

Get Certificate (optional?) signed by MASA

Visit URL Given QR Do OAUTH2 dance?

Connect to BRSK! port /requestvoucherrequest (+ SPnonce)

Scan QR

Code on

Receive voucherrequest (w/ SPnonce)

Send to voucherrequest To MASA Receive voucher







Encrypt (ECIES)
With public
Key of AR

Generate Self-signed Use as ClientCertificate

Get Certificate (optional?) signed by MASA

Visit URL
Given QR
Do OAUTH2 dance?

Connect to BRSKL port
/requestvoucherrequest (+ SPnonce)

Receive voucherrequest (w/ SPnonce)

Scan QR

Code on

Send to voucherrequest
To MASA
Receive
voucher







Scan QR Code on

Encrypt (ECIES)
With public
Key of AR

Generate Self-signed Use as ClientCertificate

Get Certificate (optional?) signed by MASA

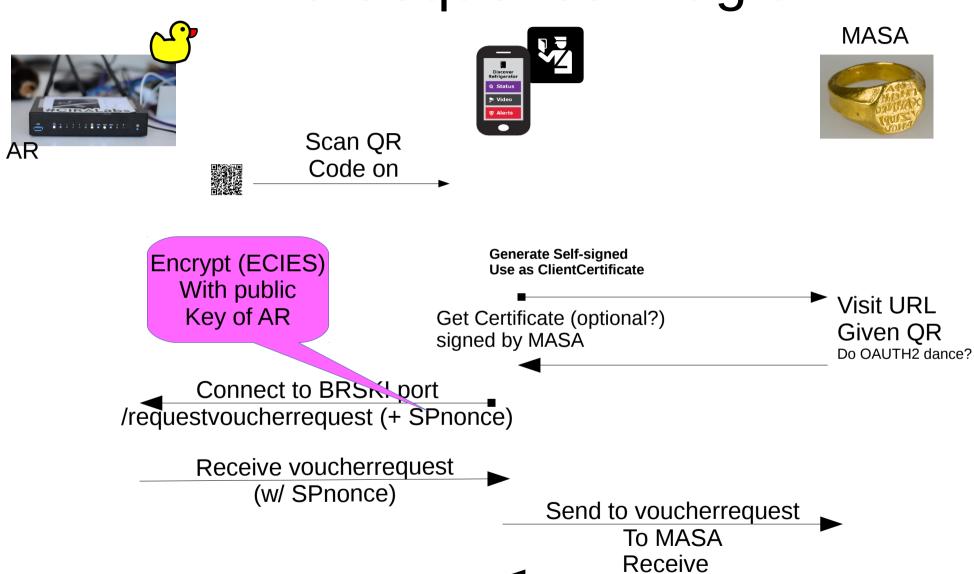
Visit URL
Given QR
Do OAUTH2 dance?

Connect to BRSK! port
/requestvoucherrequest (+ SPnonce)

Receive voucherrequest (w/ SPnonce)

Send to voucherrequest
To MASA
Receive
voucher

Send voucher To AR



Send voucher
To AR
Receive reply,
exit provisional state

voucher





MASA

Encrypt (ECIES)
With public
Key of AR

Generate Self-signed Use as ClientCertificate

Get Certificate (optional?) signed by MASA

Visit URL
Given QR
Do OAUTH2 dance?

Connect to BRSKL port
/requestvoucherrequest (+ SPnonce)

Scan QR Code on

Receive voucherrequest
(W/ SPnonce)

Send to voucherrequest
To MASA
Receive
Voucher
To AR
Receive reply,
exit provisional state

Send to voucherrequest
Voucher
Receive reply,
Receive reply,
Receive Reply to MASA

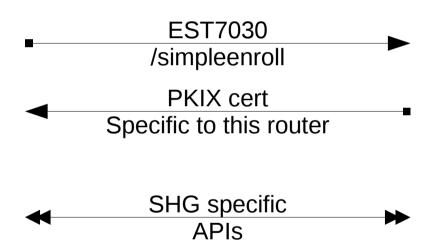




MASA



Registrar



DNSSEC and Advanced Homenet Naming

 Device will come with "coupon" for delegated DNS for home:

allthegoodnames.securehomegateway.ca

 Delegated DNS will be secured with DNSSEC, and use RFC8078 after initial setup via HTTPS API. Initially, this was going to Come in the form of a QR code

Somehow this could

Be done as part

Of enrollment, resulting in

A single QR code, but

Unclear how.

Questions/Discussion

I'm not sure this belongs in ANIMA, but if not, where?