Draft-richardson-anima-smartpledge
BRSKI enrollment for Smart Pledges

Or:
How do I bootstrap operator-less Registrars

Michael Richardson*
Jacques Latour
Faud Khan

* All bad ideas are mine

https://www.sandelman.ca/SSW/ietf/anima/smartpledge/ietf103_smartpledge/ietf103_smartpledge.html

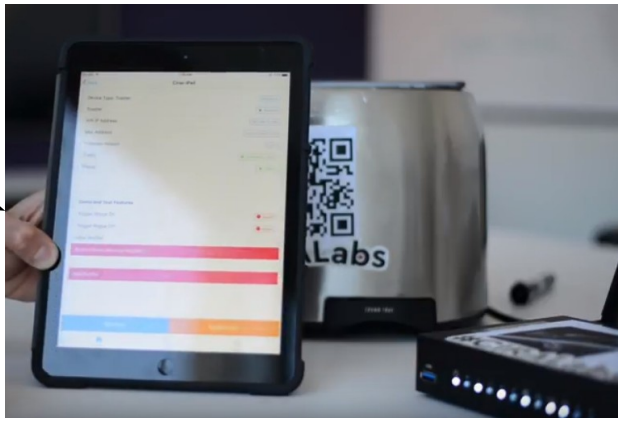
Agenda

1) what’s the problem.
2) Rough idea of solution.
3) Other ways considered
4) Questions.

SecureHomeGateway.ca

Internet

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

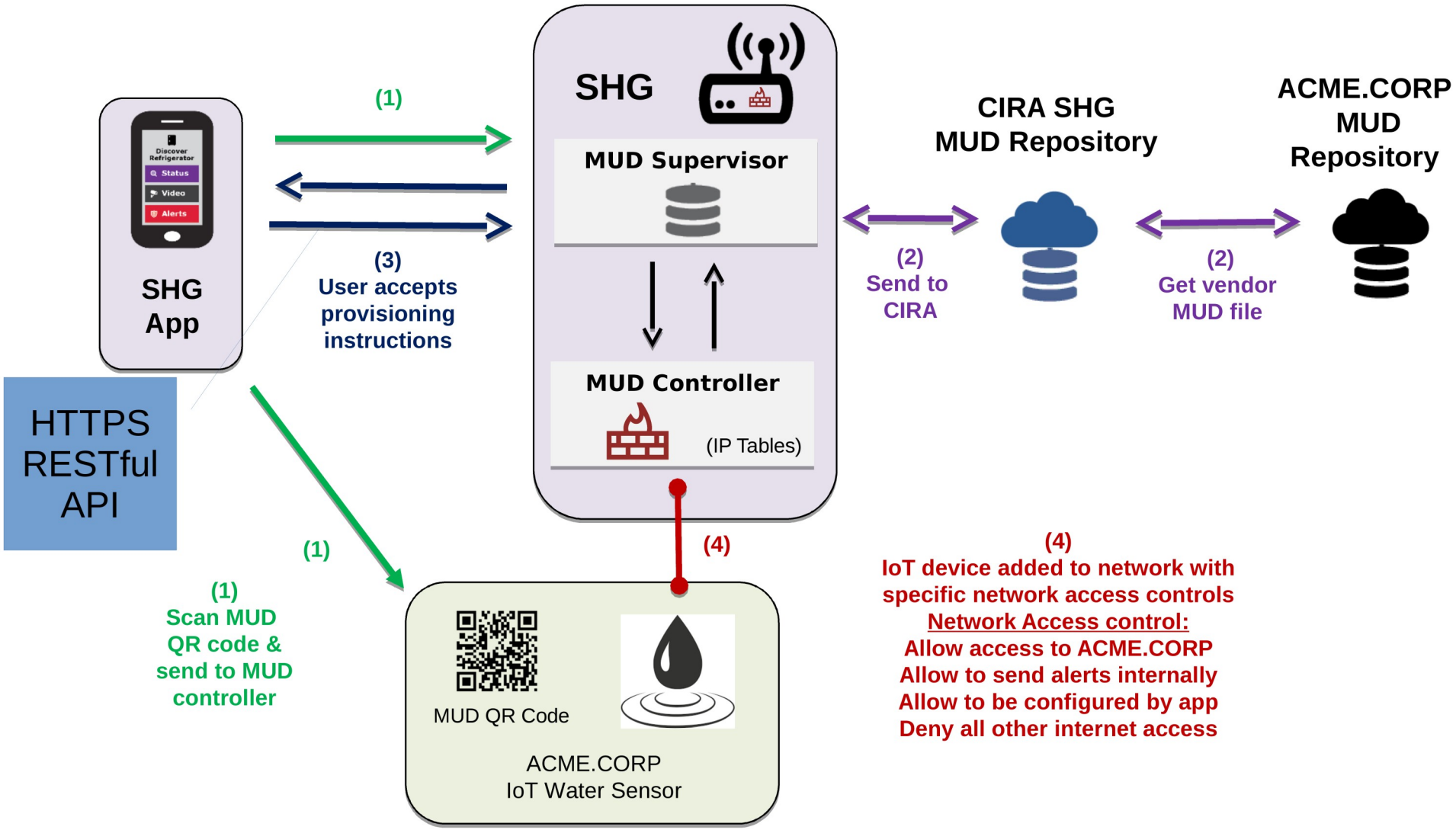


ICANN 2018 DEMO video
https://www.youtube.com/watch?v=LauvEBa4Z4s

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

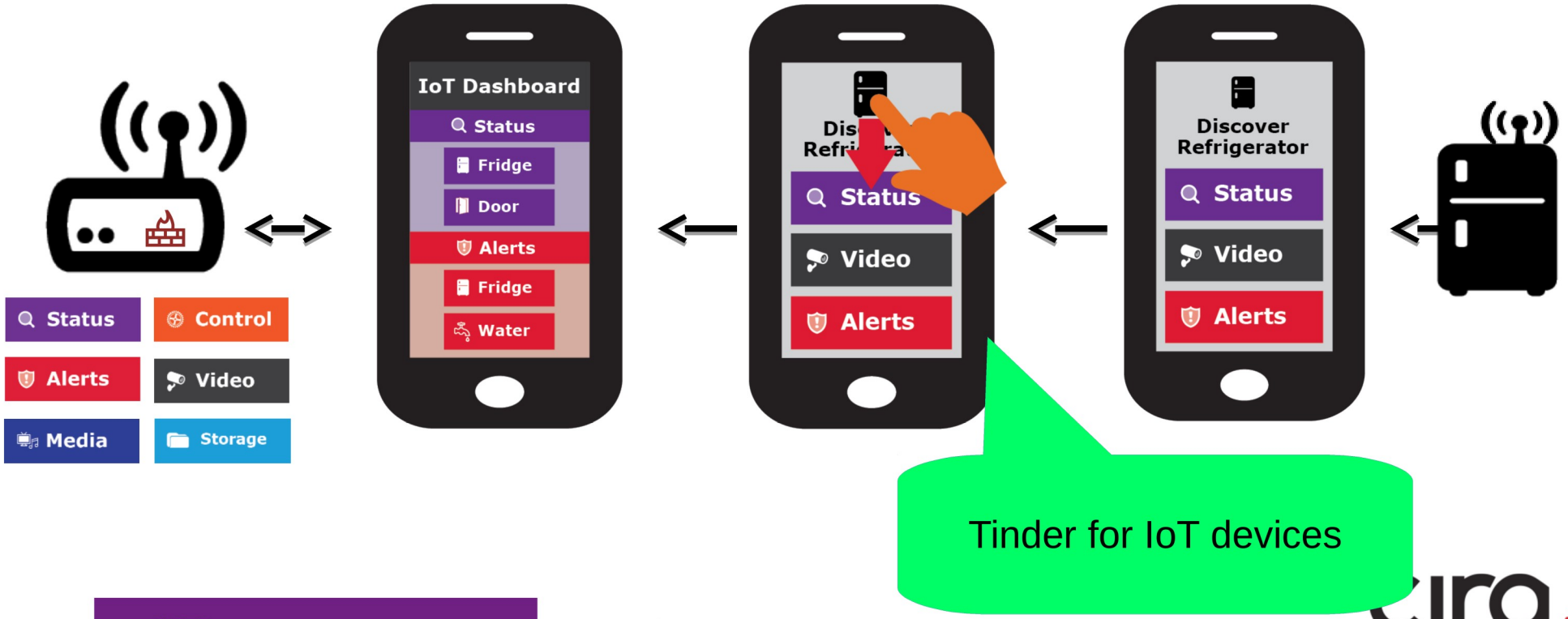
ICANN 63 talk
TBD

High Level MUD & IoT Device Provisioning Workflow



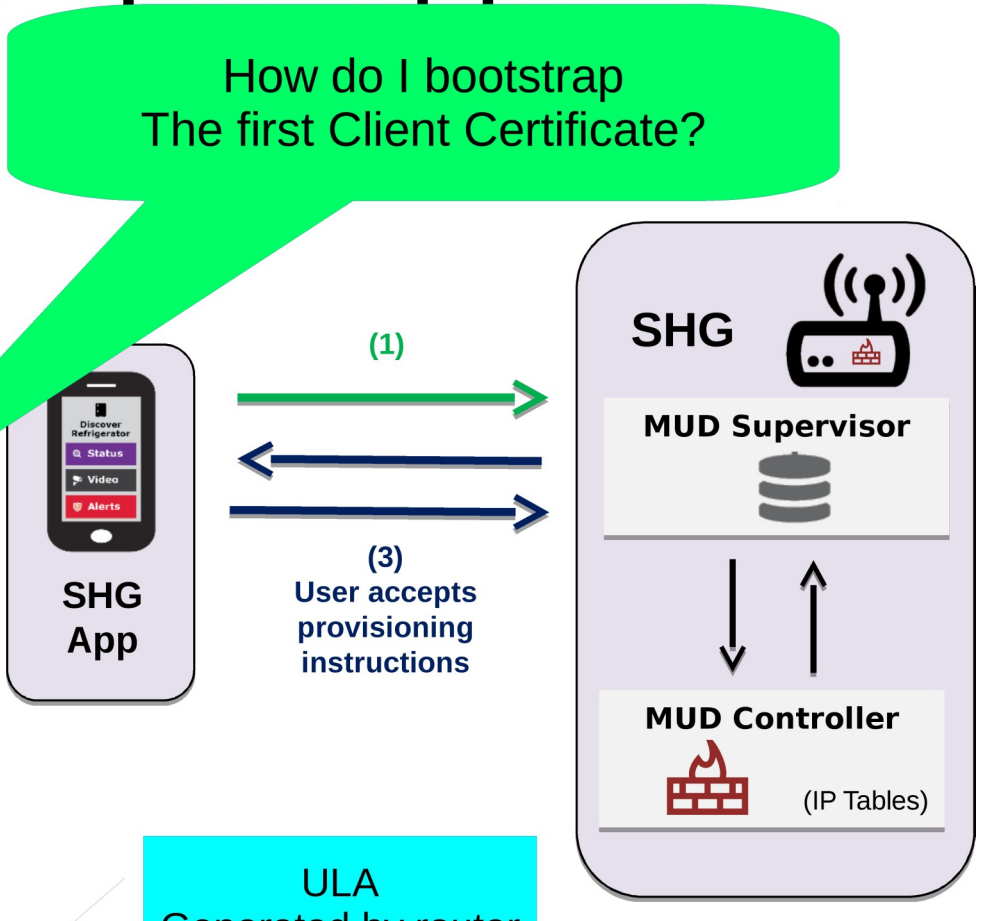
Simple user interface is key to this project: **Swipe UP, DOWN, LEFT and RIGHT**

- 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.



Initial bootstrap of app

- HTTPS connection from app to SHG.
- NO PASSWORDS.
- TLS ClientCertificate (pinned in database, CA part irrelevant)
- Assume gateway has TLS ServerCertificate:
  - `mud.nc0a8fc4.router.securehomegateway.ca`



ULA
Generated by router
As per RFC7084

dooku-[~](system) mcr 10027 %dig +short mud.nc0a8fc4.router.securehomegateway.ca aaaa
fd2a:c0a:8fc4::18e

How the gateway gets a unique
Certificate and DNS
Name during manufacturing is another talk.

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)

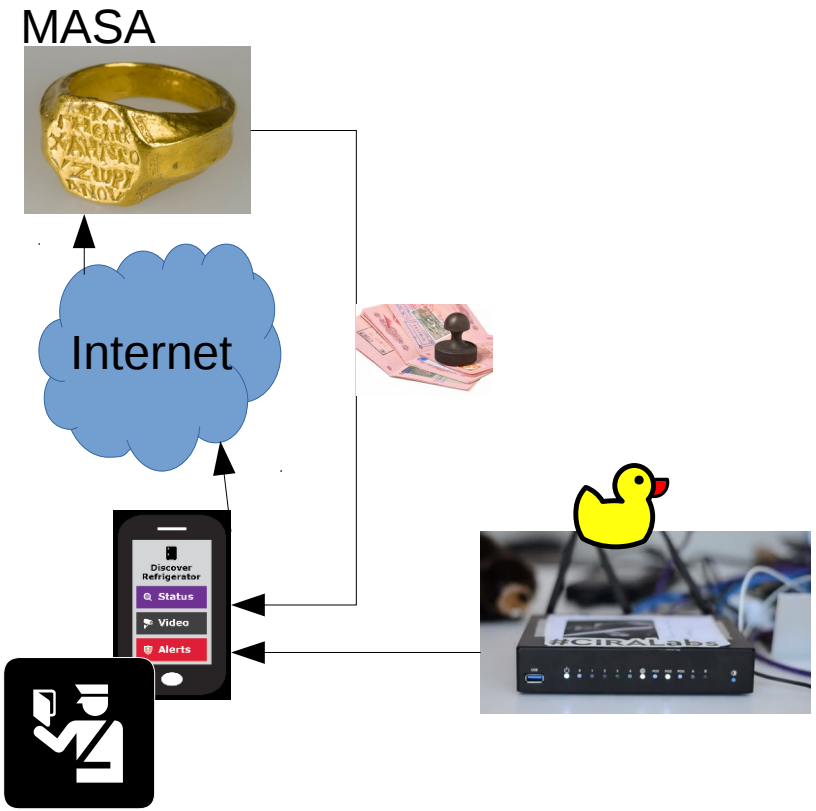
Assumptions

- Router has QR code on sticker
- Smartphone has LTE connection
- Router might have no Internet until end-user types in PPPoE password.

Who is who?

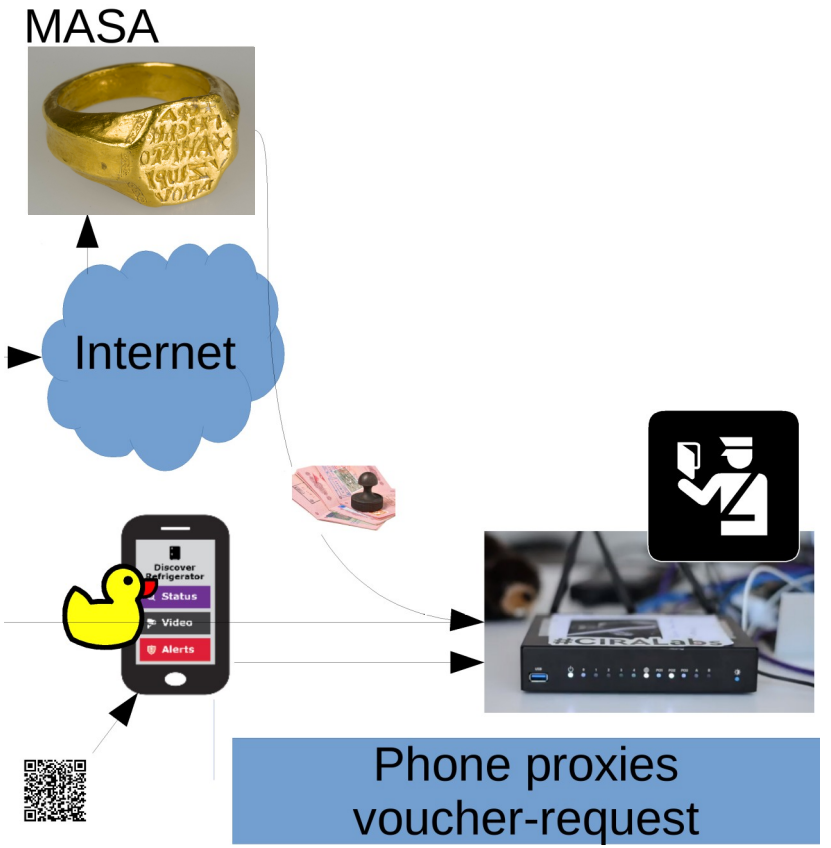
A: Router is Pledge

Smartphone is Registrar



B: Router is Registrar

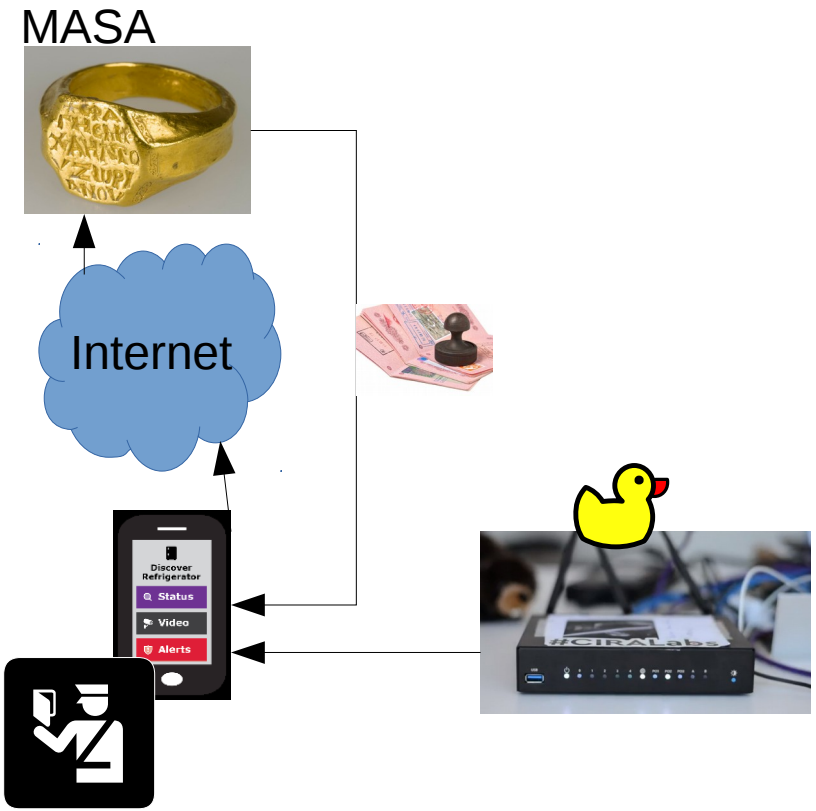
Smartphone is Pledge



Who is who?

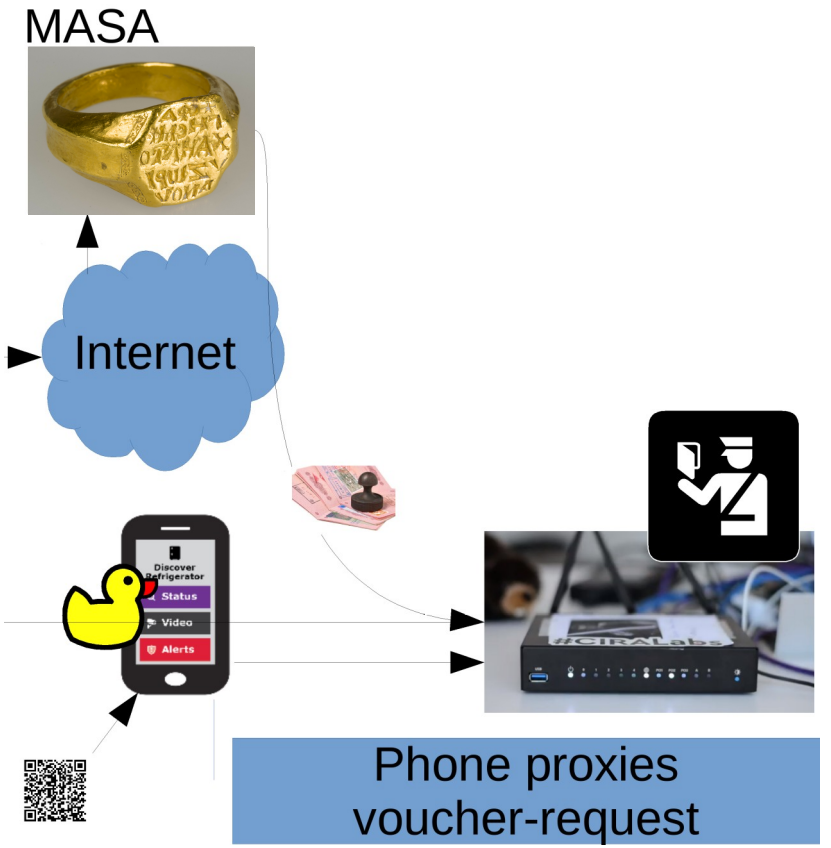
A: Router is Pledge

~~Smartphone is Registrar~~



B: Router is Registrar

Smartphone is Pledge



Rough idea of solution.

- Use BRSKI
- Our MUD supervisor is already a Registrar
  - Because MUD URLs from IoT devices can arrive by IDevID.
    - And because running-code!
-

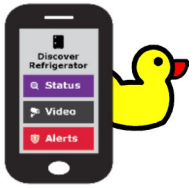
Who else uses QR code?

- 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, inaccessible on current smartphone OSes.
- 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.

smartpledge-00

- 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.

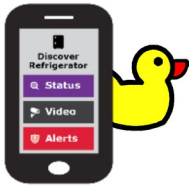
Time Sequence Diagram



AR

MASA

Time Sequence Diagram

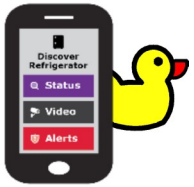


Scan QR Code on

AR

MASA

Time Sequence Diagram



Scan QR
Code on

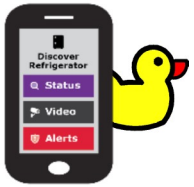
AR

MASA

Generate Self-signed
Use as ClientCertificate

Visit URL
Given QR

Time Sequence Diagram



AR

MASA

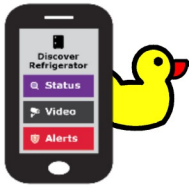
Scan QR
Code on

Generate Self-signed
Use as ClientCertificate

Visit URL
Given QR

Get Certificate signed by MASA

Time Sequence Diagram



AR

MASA

Scan QR
Code on

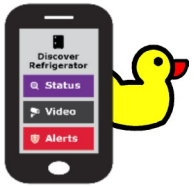
Generate Self-signed
Use as ClientCertificate

Visit URL
Given QR

Get Certificate signed by MASA

Connect to BRSKI port
/requestvoucherrequest (+ SPnonce)

Time Sequence Diagram



AR

MASA

Scan QR
Code on

Generate Self-signed
Use as ClientCertificate

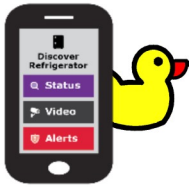
Visit URL
Given QR

Get Certificate signed by MASA

Connect to BRSKI port
/requestvoucherrequest (+ SPnonce)

Encrypt
With public
Key of AR

Time Sequence Diagram



AR

MASA

Scan QR
Code on

Generate Self-signed
Use as ClientCertificate

Visit URL
Given QR

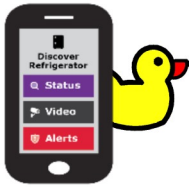
Get Certificate signed by MASA

Encrypt
With public
Key of AR

Connect to BRSKI port
/requestvoucherrequest (+ SPnonce)

Receive voucherrequest
(w/ SPnonce)

Time Sequence Diagram



AR

MASA

Scan QR
Code on

Generate Self-signed
Use as ClientCertificate

Visit URL
Given QR

Get Certificate signed by MASA

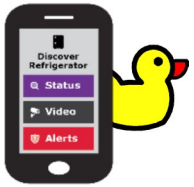
Encrypt
With public
Key of AR

Connect to BRSKI port
/requestvoucherrequest (+ SPnonce)

Receive voucherrequest
(w/ SPnonce)

Send voucherrequest
To MASA

Time Sequence Diagram



AR

MASA

Scan QR
Code on

Generate Self-signed
Use as ClientCertificate

Visit URL
Given QR

Get Certificate signed by MASA

Encrypt
With public
Key of AR

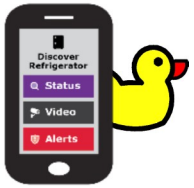
Connect to BRSKI port
/requestvoucherrequest (+ SPnonce)

Receive voucherrequest
(w/ SPnonce)

Send voucherrequest
To MASA

Receive
voucher

Time Sequence Diagram



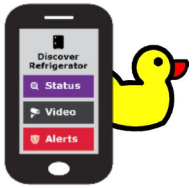
AR

MASA

Send voucherrequest
To MASA

Receive
voucher

Time Sequence Diagram



AR

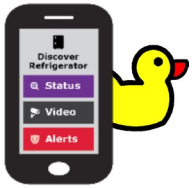
MASA

Send voucherrequest
To MASA

Receive
voucher

Send to voucher
to router

Time Sequence Diagram



AR

MASA

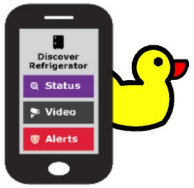
Send voucherrequest
To MASA

Receive
voucher

Send to voucher
to router

Receive reply,
exit provisional state

Time Sequence Diagram



AR

MASA

Send voucherrequest
To MASA

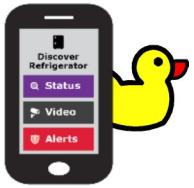
Receive
voucher

Send to voucher
to router

Receive reply,
exit provisional state

EST-rfc7030
/simpleenroll

Time Sequence Diagram



AR

MASA

Send voucherrequest
To MASA

Receive
voucher

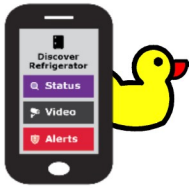
Send to voucher
to router

Receive reply,
exit provisional state

EST-rfc7030
/simpleenroll

RFC7030
certificate

Time Sequence Diagram



AR

MASA

Send voucherrequest
To MASA

Receive
voucher

Send to voucher
to router

Receive reply,
exit provisional state

EST-rfc7030
/simpleenroll

RFC7030
certificate

First Administrator now pinned!

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?