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

Or:
How do I bootstrap operator-less Registrars

Michael Richardson*
Jacques Latour
Abhishek Joshi

* All bad ideas are mine

https://www.sandelman.ca/SSW/ietf/anima/smarkaklink/ietf104_smarkaklink/ietf104_smarkaklink.html
Agenda

1) what’s the problem.
2) Rough idea of solution.
   1) Why the name change!
3) Questions.
SecureHomeGateway.ca

Internet

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

https://github.com/CIRALabs/Secure-IoT-Home-Gateway
High Level MUD & IoT Device Provisioning Workflow

1. Scan MUD QR code & send to MUD controller
2. Get vendor MUD file
3. User accepts provisioning instructions
4. IoT device added to network with specific network access controls
   - Network Access control:
     - Allow access to ACME.CORP
     - Allow to send alerts internally
     - Allow to be configured by app
     - Deny all other internet access

MUD Supervisor
MUD Controller
(MUD Repository)

ACME.CORP MUD Repository

HTTPS RESTful API

HOW TO SETUP THIS TRUST?

CIRA SHG MUD Repository

MUD QR Code

ACME.CORP IoT Water Sensor

SHG App
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.

Tinder for IoT devices
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’

- 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.

MASA (2: request VR) voucher-request VR

Sorta seems like a registrar
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.

(4) RFC7030 EST /simplerenroll
(5) PKIX cert
Returned and pinned

Connection Authorized By voucher

Internet

MASA
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.
• 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
Time Sequence Diagram
Time Sequence Diagram
Time Sequence Diagram
Time Sequence Diagram
Time Sequence Diagram
Time Sequence Diagram

AR → Scan QR Code on → MASA
Time Sequence Diagram

AR → Scan QR Code on → Generate Self-signed → MASA
Time Sequence Diagram

AR

Scan QR Code on

Generate Self-signed
Use as ClientCertificate

MASA
Time Sequence Diagram

AR → Scan QR Code on → Generate Self-signed Use as ClientCertificate → Visit URL Given QR Do OAUTH2 dance? → MASA
Time Sequence Diagram

AR

Scan QR Code on

Generate Self-signed Use as ClientCertificate

Get Certificate (optional?) signed by MASA

Visit URL Given QR
Do OAUTH2 dance?

MASA
Time Sequence Diagram

Scan QR Code on

Generate Self-signed Use as ClientCertificate

Get Certificate (optional?) signed by MASA

Visit URL Given QR Do OAUTH2 dance?

Connect to BRISKI port /requestvouchersrequest (+ SPnonce)
Time Sequence Diagram

AR

Scan QR Code on

Encrypt (ECIES) With public Key of AR

Connect to BRSKI port /requestvoucherrequest (+ SPnonce)

Generate Self-signed Use as ClientCertificate

Get Certificate (optional?) signed by MASA

Visit URL Given QR

Do OAUTH2 dance?
Time Sequence Diagram

AR

Scan QR Code on

Generate Self-signed Use as ClientCertificate

Visit URL Given QR Do OAUTH2 dance?

Get Certificate (optional?) signed by MASA

Connect to BRSKI port /requestvoucharrequest (+ SPnonce)

Encrypt (ECIES) With public Key of AR

Receive voucherrequest (w/ SPnonce)
Scan QR Code on

Generate Self-signed Use as ClientCertificate

Visit URL Given QR Do OAUTH2 dance?

Get Certificate (optional?) signed by MASA

Send to voucherrequest To MASA

Encrypt (ECIES) With public Key of AR

Connect to BRSKI port /requestvoucherdemand (+ SPnonce)

Receive voucherrequest (w/ SPnonce)

Send to voucherrequest To MASA
Scan QR Code on

Generate Self-signed
Use as ClientCertificate

Get Certificate (optional?)
signed by MASA

Visit URL
Given QR
Do OAUTH2 dance?

Send to voucherrequest (w/ SPnonce)

Receive voucherrequest (w/ SPnonce)

Connect to BRSKI port
/requestvoucherrequest (+ SPnonce)

Encrypt (ECIES)
With public Key of AR

Encrypt (ECIES)
With public Key of AR
Scan QR Code on

Generate Self-signed Use as ClientCertificate

Visit URL Given QR Do OAUTH2 dance?

Get Certificate (optional?) signed by MASA

Encrypt (ECIES) With public key of AR

Connect to BRSKI port /requestvoucherrequest (+ SPnonce)

Receive voucherrequest (w/ SPnonce)

Send to voucherrequest To MASA Receive voucher
Scan QR Code on

Visit URL
Given QR
Do OAUTH2 dance?

Get Certificate (optional?) signed by MASA

Generate Self-signed Use as ClientCertificate

Encrypt (ECIES) With public Key of AR

Connect to BRSKI port /requestvouchерrequest (+ SP nonce)

Receive vouchерrequest (w/ SP nonce)

Send to vouchеrrequest To MASA
Receive vouchеr

Send voucher To AR
**Time Sequence Diagram**

1. Scan QR Code on AR
2. AR Connect to BRSKI port /requestvouchersrequest (+ SPnonce)
3. Receive voucherrequest (w/ SPnonce)
4. Encrypt (ECIES) With public Key of AR
5. Send voucher To AR
6. Receive reply, exit provisional state
7. Send to voucherrequest To MASA
8. Receive voucher
9. Get Certificate (optional?) signed by MASA
10. Do OAUTH2 dance?
11. Visit URL Given QR
12. Generate Self-signed Use as ClientCertificate
13. MASA
Scan QR Code on

Generate Self-signed Use as ClientCertificate

Visit URL Given QR Do OAUTH2 dance?

Get Certificate (optional?) signed by MASA

Encrypt (ECIES) With public Key of AR

Connect to BRSKI port /requestvouchercertificate (+ SPnonce)

Receive vouchercertificate (w/ SPnonce)

Send to vouchercertificate To MASA

Receive voucher

Send voucher To AR

Receive reply, exit provisional state

Send telemetry Reply to MASA
Time Sequence Diagram

EST7030 /simpleenroll
PKIX cert
Specific to this router

SHG specific
APIs

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?