SECURE HOME GATEWAY PROJECT

- WHO AM I
- PROJECT VISION AND ORIGIN
- SYSTEM ARCHITECTURE
- MUD AND APIS
- CHALLENGES

SANDELMAN SOFTWARE WORKS

cira

BUILDING A BETTER
ONLINE CANADA

Initiated by:

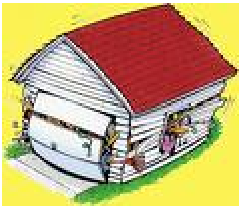
Jacques Latour, CTO, CIRA Labs
Canadian Internet Registration Authority

Presented by: Michael Richardson

<mcr@sandelman.ca>

These slides at:
https://tinyurl.com/udmq8ns

Who am I?



Xelerance Corp 2003-2007,2014-

xelerance

Internet technologist, doing IP since 1988. “Garage Entrepreneur”

SANDELMAN
SOFTWARE WORKS

1996-

SOLIDUM

(1998-2001)

FreeS/WAN (2001-2004)

Linux FreeS/WAN

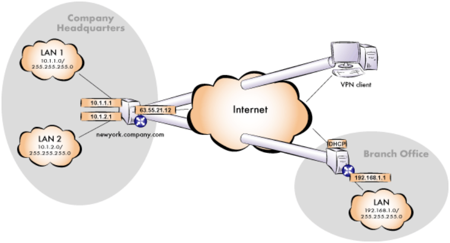
SIMtone
CORPORATION

(2007-2009)

}{ CENTRE DE RECHERCHE ET DÉVELOPPEMENT EXPÉRIMENTAL EN INFORMATIQUE LIBRE
CREDIL
CENTRE FOR RESEARCH AND EXPERIMENTAL DEVELOPMENT IN INFORMATICS LIBRE

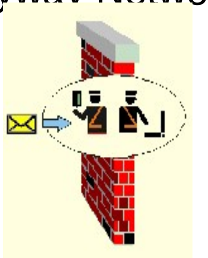
2009-2017

BRSKI
RFC8366



IETF standard security:IPsec/VPN

#4 at Milkyway Networks (1994)



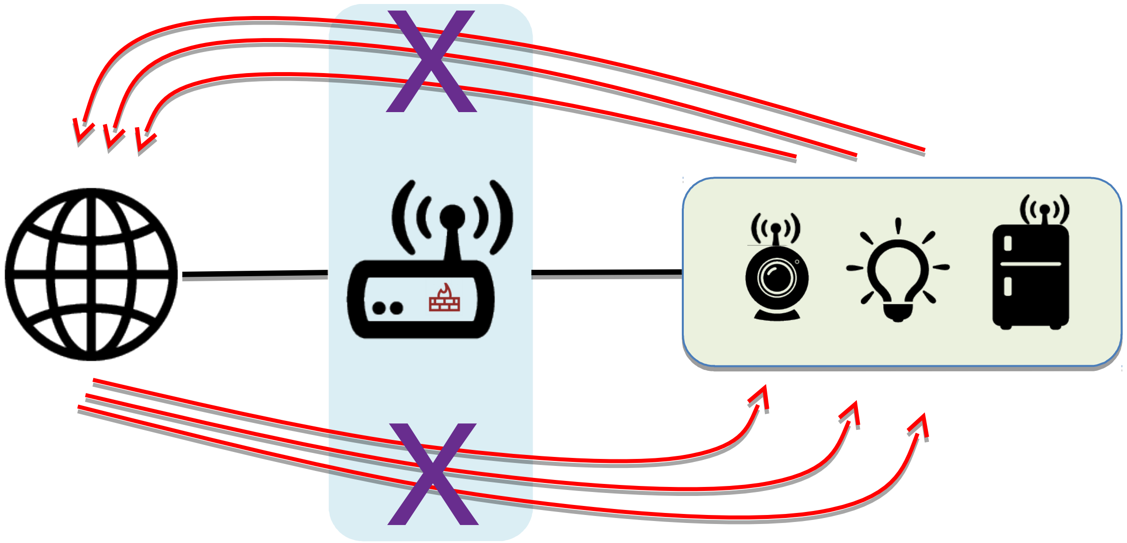
ROLL – RFC6550
2012-

6TiSCH

RFC4322
RFC4025
RFC5386
RFC8415
RFC7416
RFC8366
BRSKI
constrained-BRSKI

Secure Home Gateway (SHG)
Primary Project Goal

- The primary goal of this project is to develop a secure home gateway that;
  - **protects** the internet from IoT devices **attacks** and
  - **protects** home IoT devices from the internet **attacks**



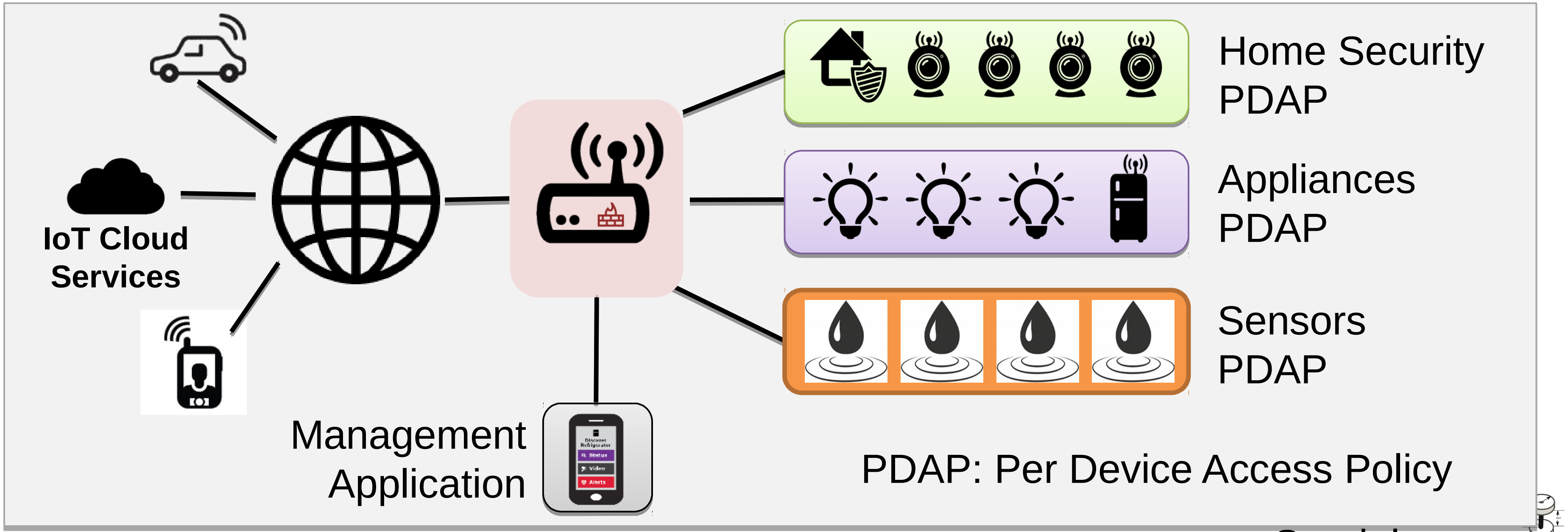
Why are we working on this?
-> Risk mitigation

- For many internet organizations like CIRA the #1 risk on the risk register is a large scale (Dyn like) DDoS attack.
- One of the mitigation mechanisms for this risk is to prevent ‘weaponization’ of IoT devices
- Tightly controlling access ‘to’ and ‘from’ IoT devices inside the home or small office network is key to preventing ‘weaponization’ and causing harm on the internet.
- The **threat** that **IoT devices** bring is the **scale of attacks**. The uncontrolled access of million/billions of IoT devices to and from the internet is the threat we need to mitigate.

How can we protect IoT devices?
-> Best practice & new standards

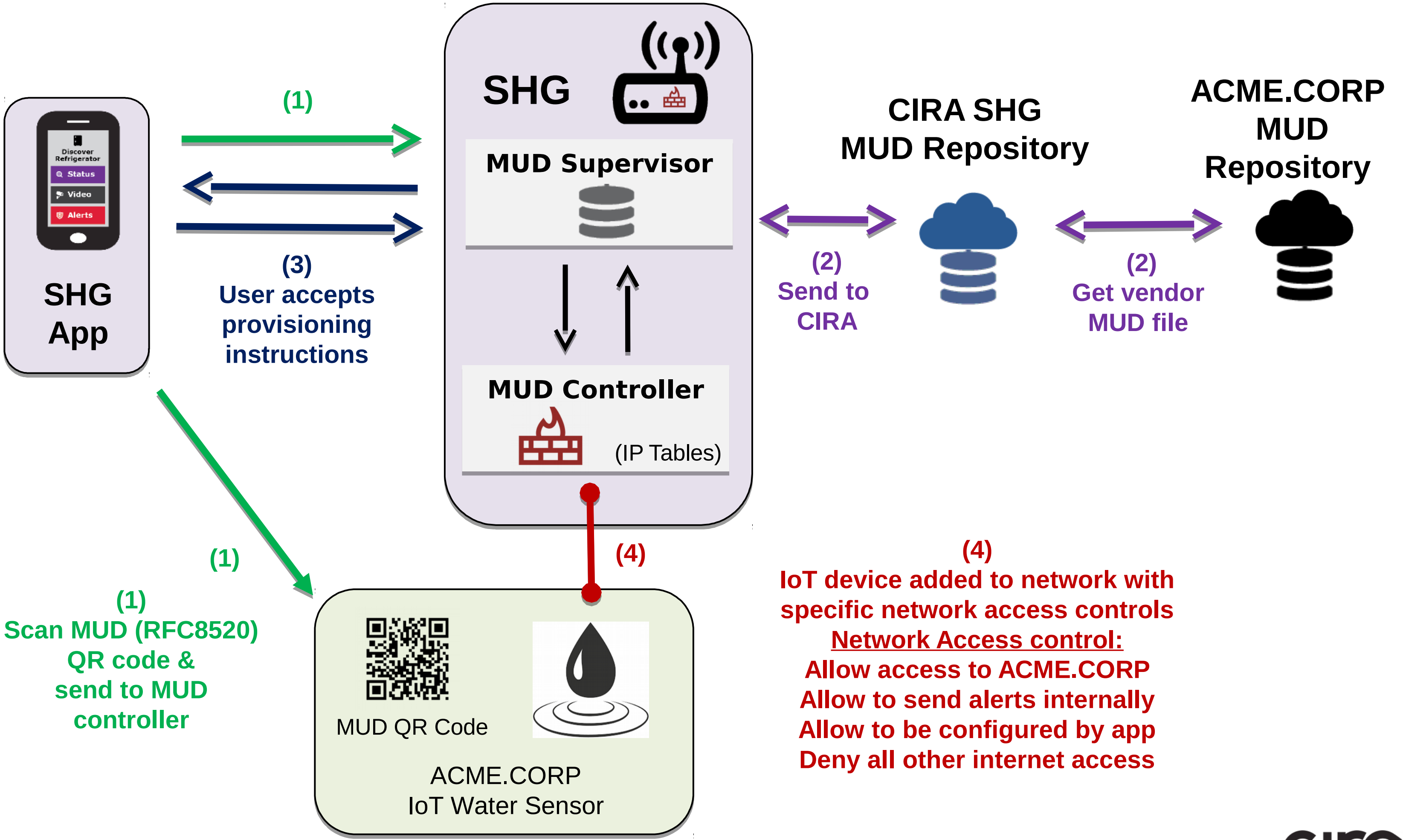
Manufacturer Usage Description RFC8520

- Rule #1: Identify IoT devices on your home network
- Rule #2: Place a policy around the IoT device that restricts it to a specific function (default is no access)
- Rule #3: Monitor for behavioural changes in the device and quarantine at the first sign of change.



PDAP: Per Device Access Policy

High Level MUD & IoT Device Provisioning Workflow



SHG App

(1)

(3)
User accepts provisioning instructions

SHG

MUD Supervisor

MUD Controller

(IP Tables)

(2)
Send to CIRA

CIRA SHG MUD Repository

(2)
Get vendor MUD file

ACME.CORP MUD Repository

(1)

(1)
Scan MUD (RFC8520) QR code &
send to MUD controller

(4)

MUD QR Code

ACME.CORP
IoT Water Sensor

(4)
IoT device added to network with specific network access controls
<u>Network Access control:</u>
Allow access to ACME.CORP
Allow to send alerts internally
Allow to be configured by app
Deny all other internet access

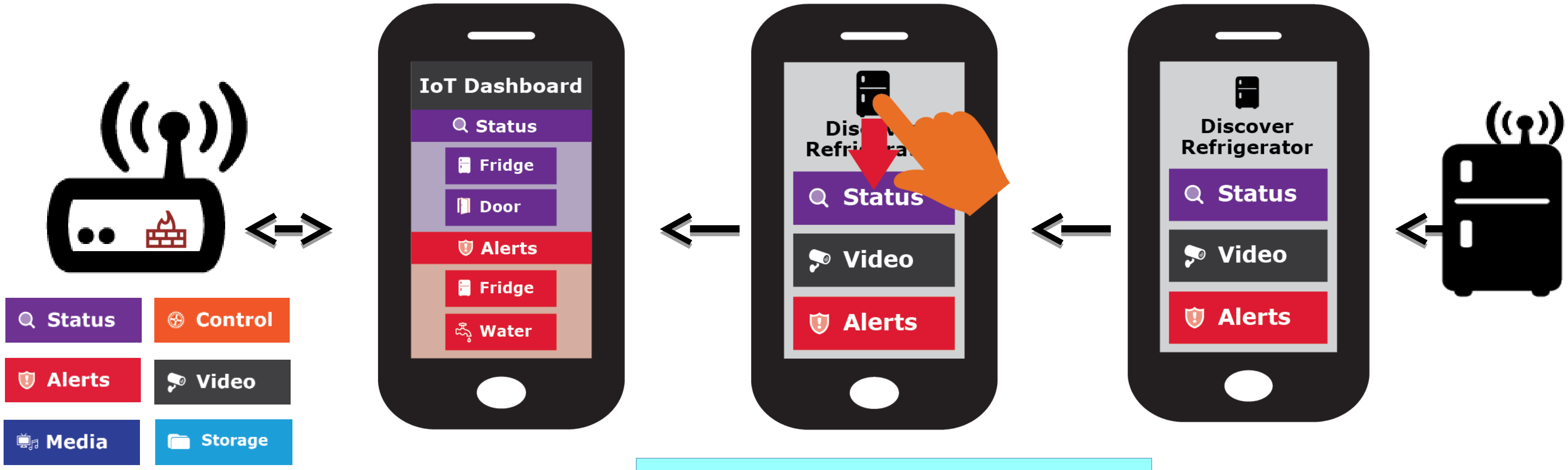
https://www.sandelman.ca/SSW/ietf/mud-links

cira

Sandelman Software Works

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!

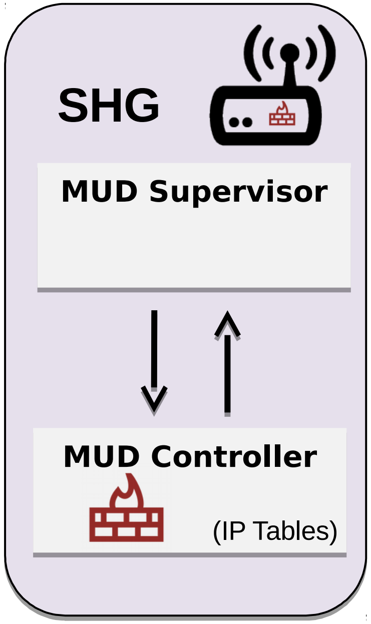
Sandelman Software Works

Risks for an API for MUD devices

GOOD GUYS

Discover Refrigerator
Status
Video
Alerts

SHG App



SHG

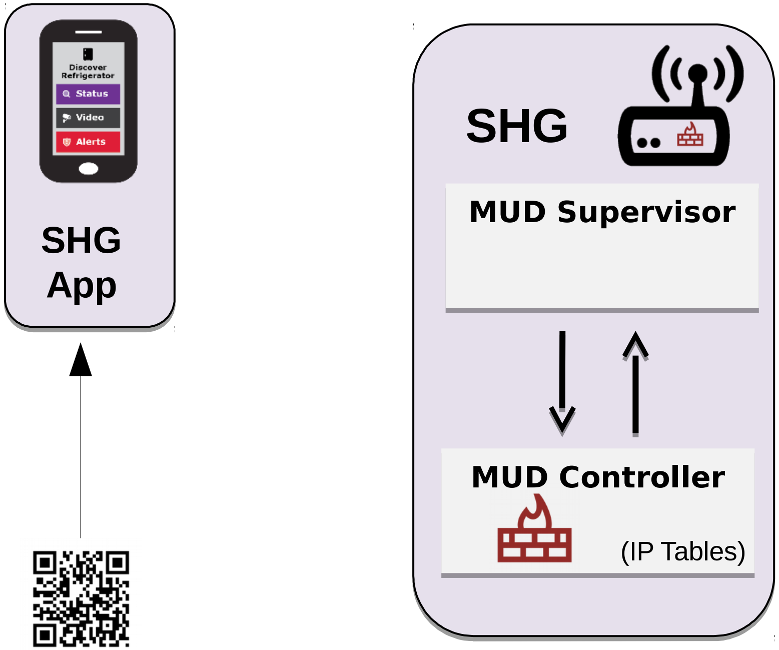
MUD Supervisor

MUD Controller

(IP Tables)

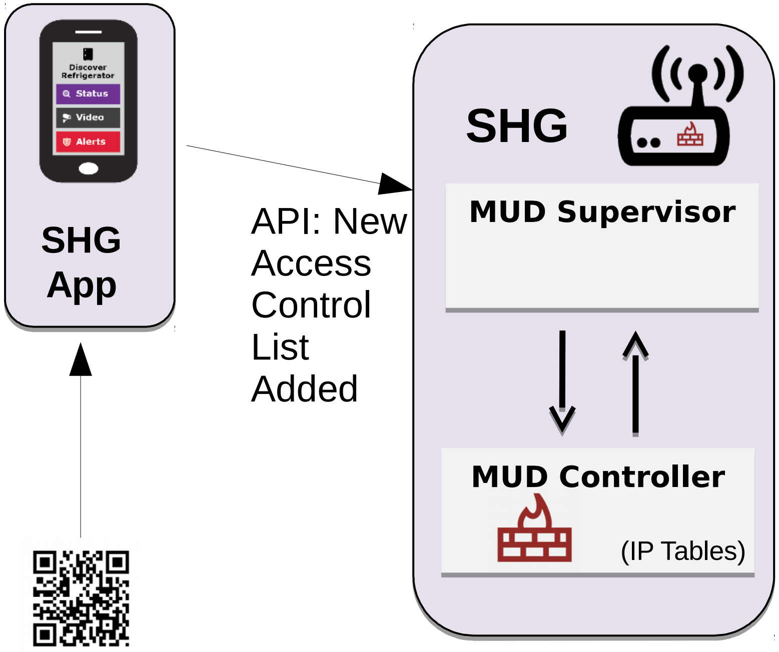
Risks for an API for MUD devices

GOOD GUYS



Risks for an API for MUD devices

GOOD GUYS



SHG App

API: New Access Control List Added

SHG

MUD Supervisor

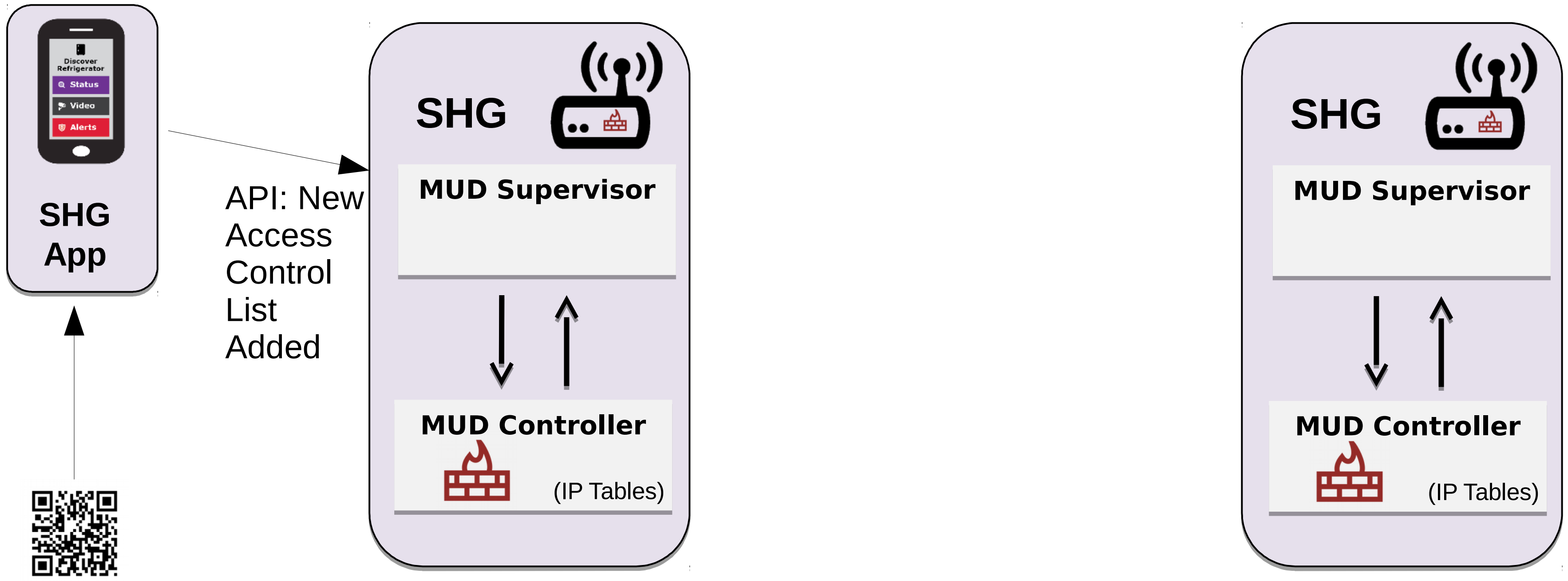
MUD Controller

(IP Tables)

Risks for an API for MUD devices

GOOD GUYS

BAD GUYS



SHG App

API: New Access Control List Added

SHG

MUD Supervisor

MUD Controller

(IP Tables)

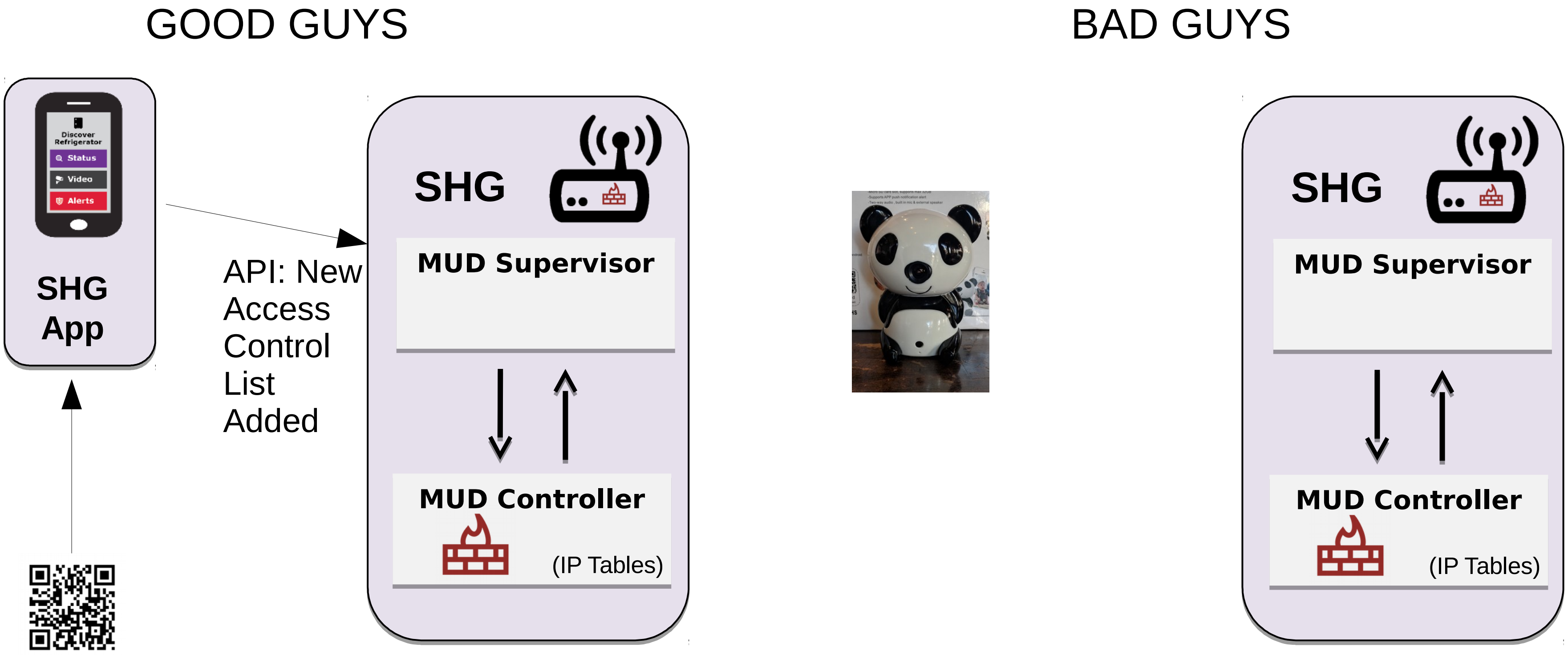
SHG

MUD Supervisor

MUD Controller

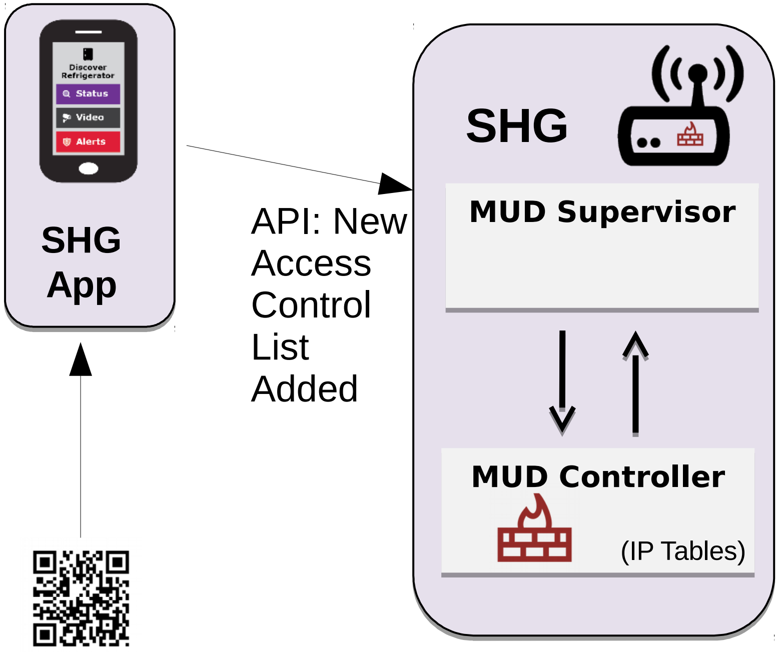
(IP Tables)

Risks for an API for MUD devices



Risks for an API for MUD devices

GOOD GUYS



SHG App

API: New Access Control List Added

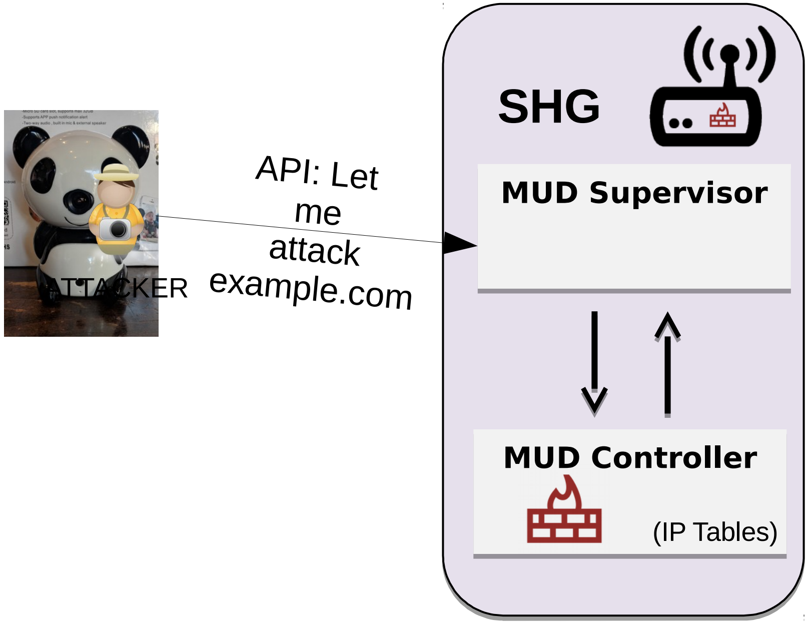
SHG

MUD Supervisor

MUD Controller

(IP Tables)

BAD GUYS



ATTACKER

API: Let me attack example.com

SHG

MUD Supervisor

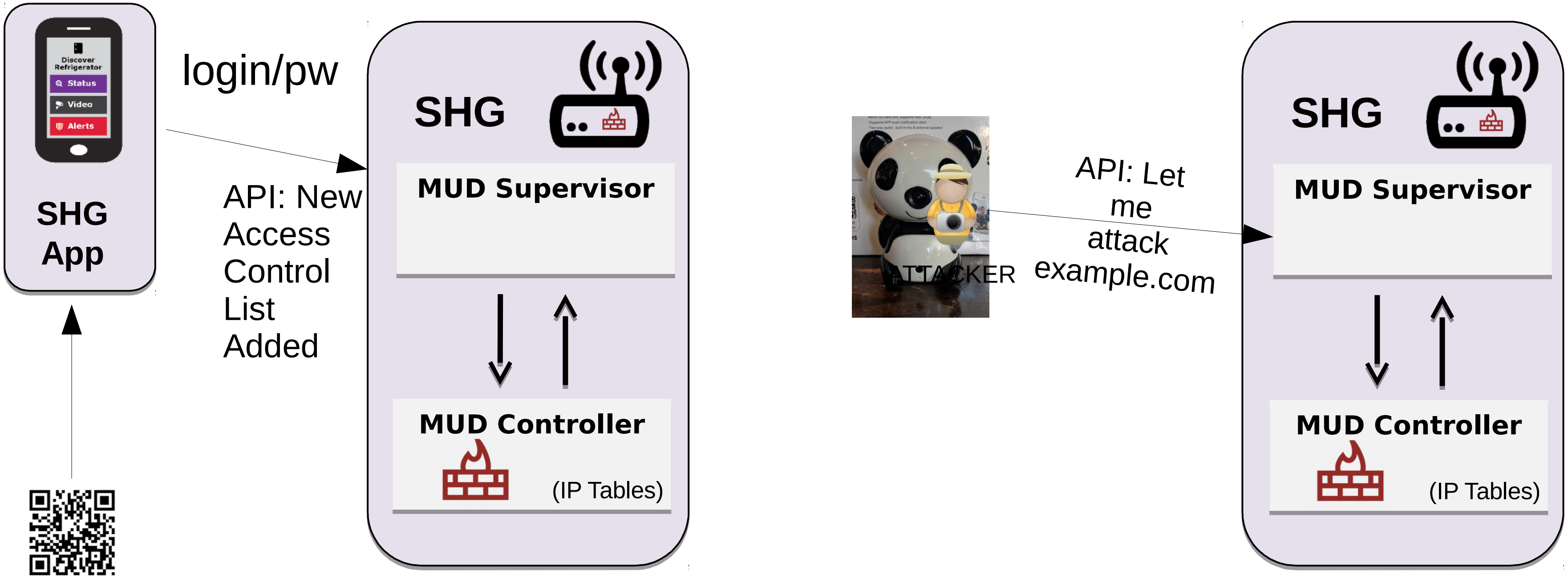
MUD Controller

(IP Tables)

Risks for an API for MUD devices

GOOD GUYS

BAD GUYS



SHG App

login/pw

API: New Access Control List Added

SHG

MUD Supervisor

MUD Controller

(IP Tables)

ATTACKER

API: Let me attack example.com

SHG

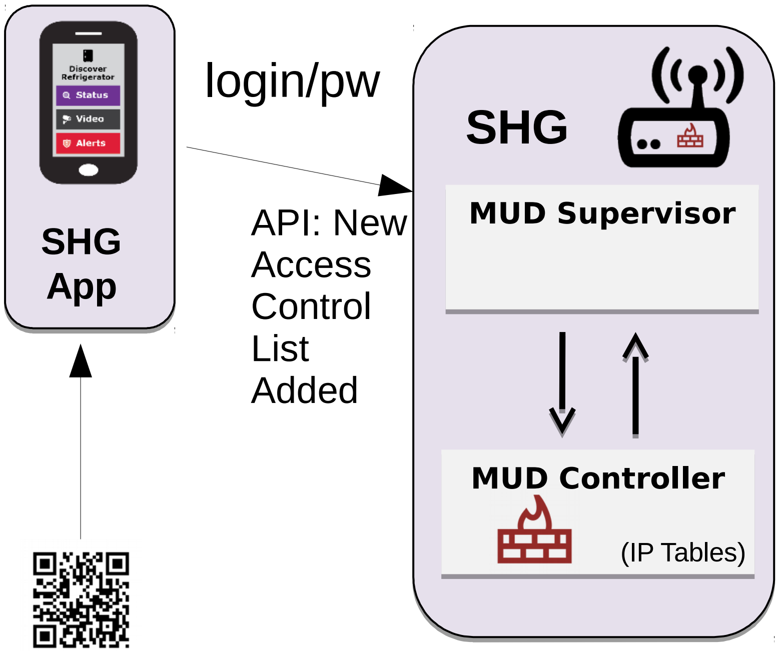
MUD Supervisor

MUD Controller

(IP Tables)

Risks for an API for MUD devices

GOOD GUYS



SHG App

login/pw

API: New Access Control List Added

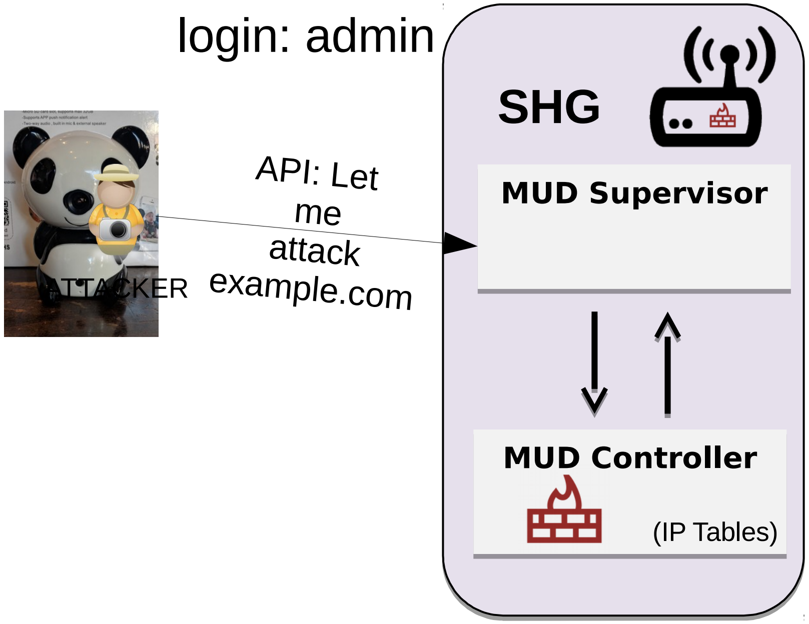
SHG

MUD Supervisor

MUD Controller

(IP Tables)

BAD GUYS



login: admin

ATTACKER

API: Let me attack example.com

SHG

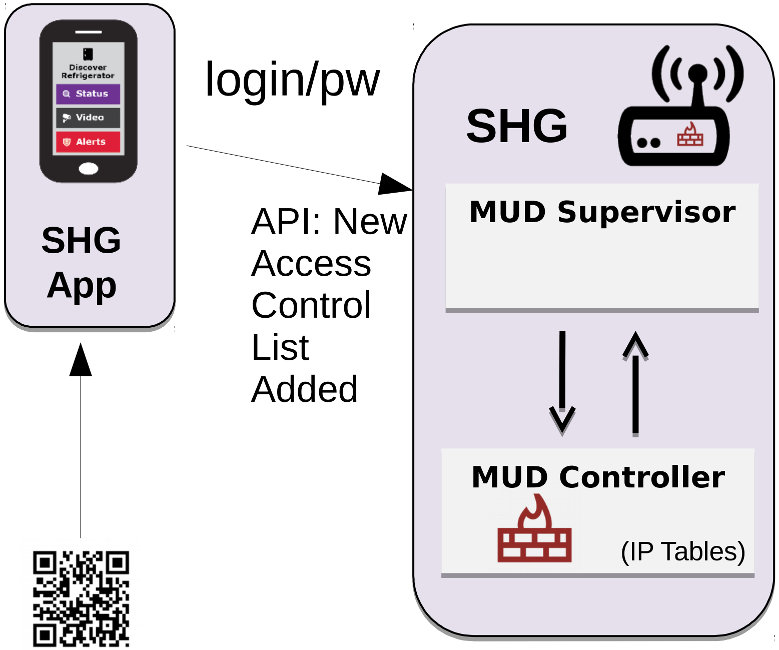
MUD Supervisor

MUD Controller

(IP Tables)

Risks for an API for MUD devices

GOOD GUYS



SHG App

login/pw

API: New Access Control List Added

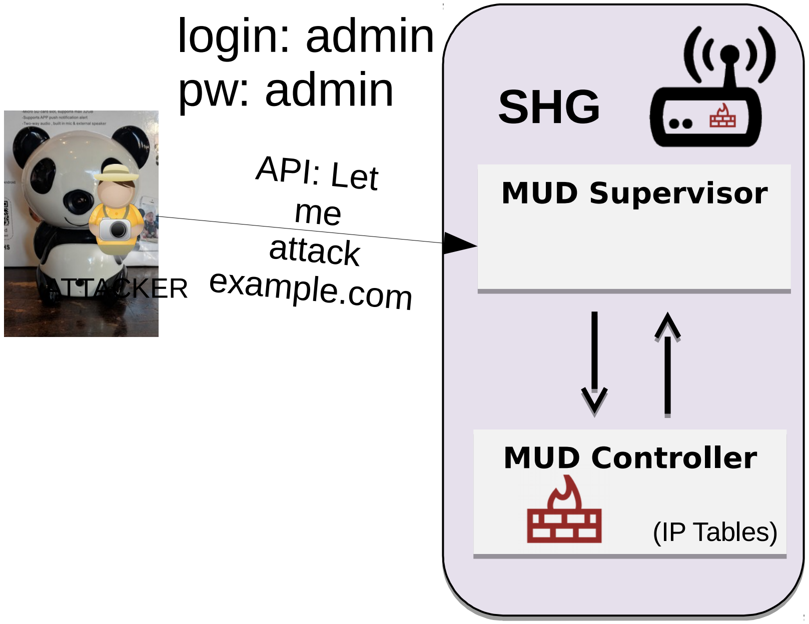
SHG

MUD Supervisor

MUD Controller

(IP Tables)

BAD GUYS



login: admin
pw: admin

API: Let me attack example.com

ATTACKER

SHG

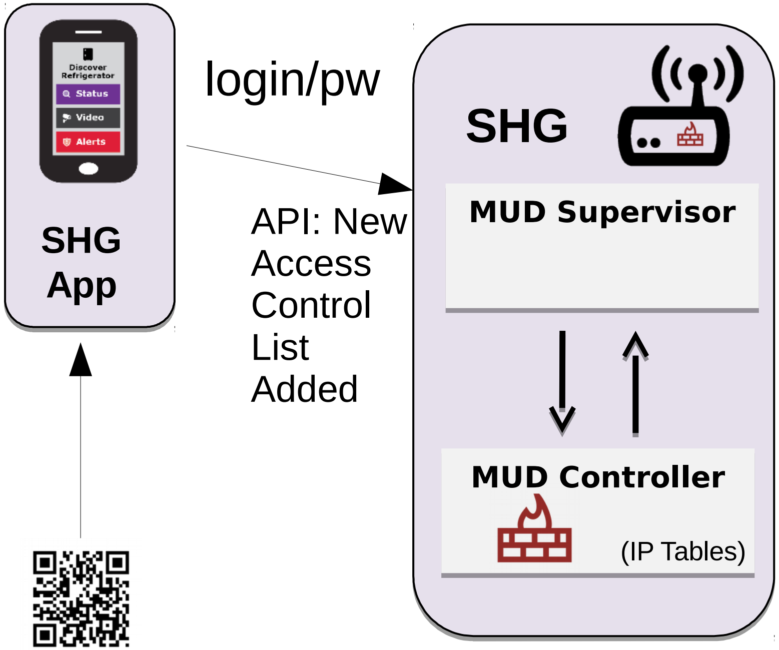
MUD Supervisor

MUD Controller

(IP Tables)

Risks for an API for MUD devices

GOOD GUYS



SHG App

login/pw

API: New Access Control List Added

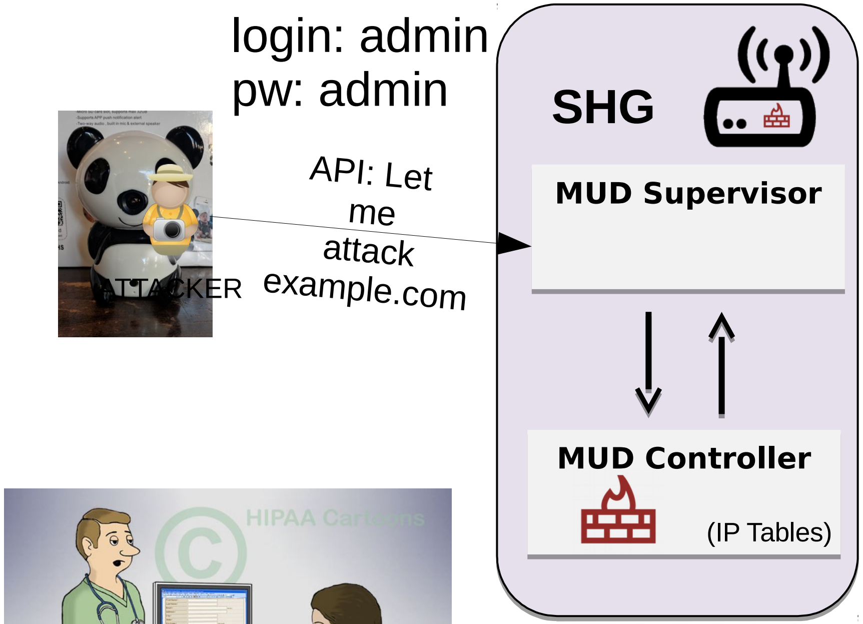
SHG

MUD Supervisor

MUD Controller

(IP Tables)

BAD GUYS



login: admin
pw: admin

ATTACKER

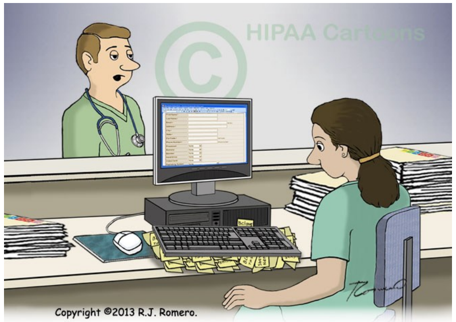
API: Let me attack example.com

SHG

MUD Supervisor

MUD Controller

(IP Tables)

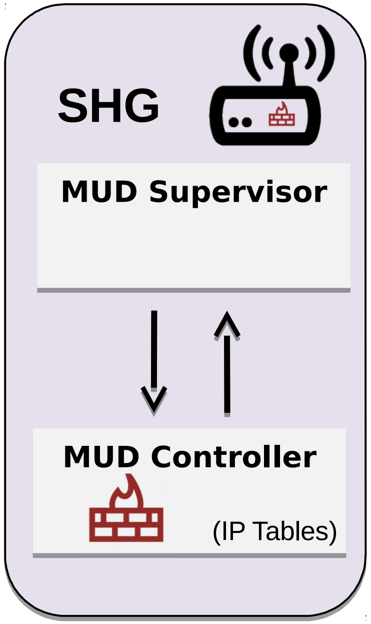


Copyright ©2013 R.J. Romero.

"Oh, that's for security. We all keep our user name and password on a sticky note hidden where it's safe."

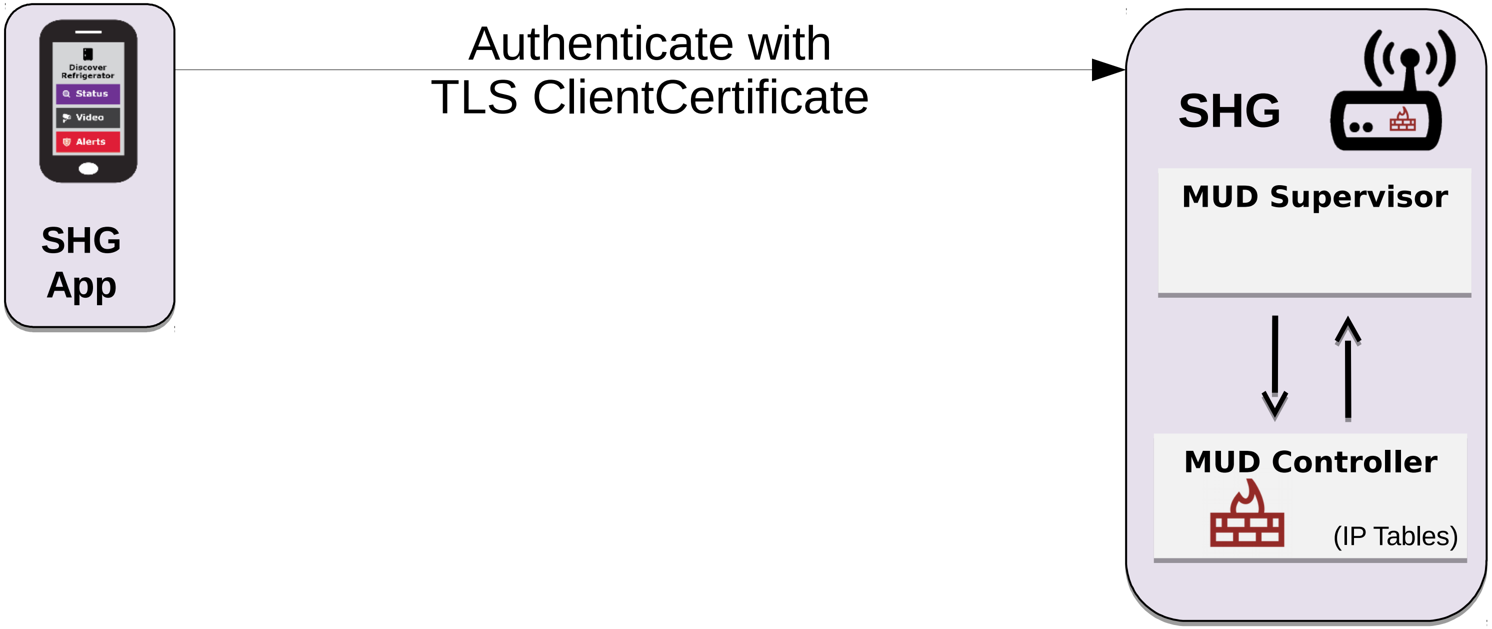
Solution: use some good crypto

Discover Refrigerator
Status
Video
Alerts
SHG
App



more info:
www.sandelman.ca/SSW/ietf/brski-links

Solution: use some good crypto



SHG App

Authenticate with TLS ClientCertificate

SHG

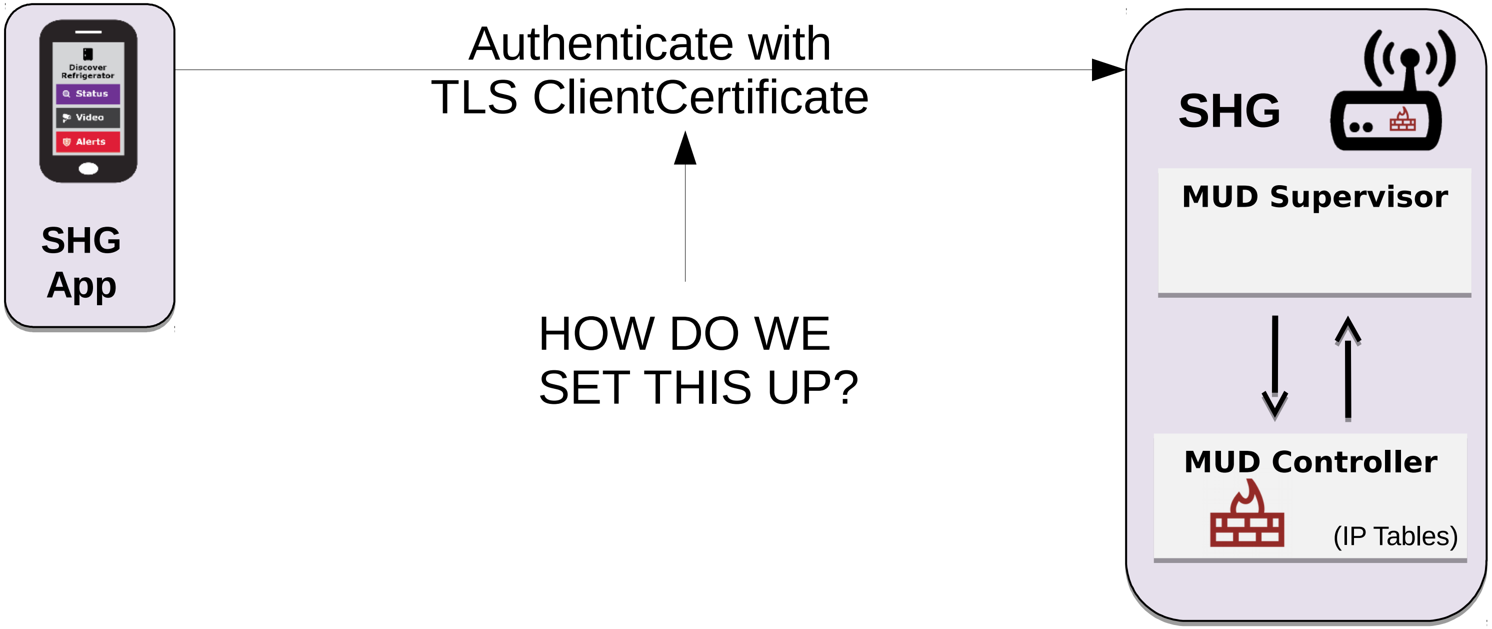
MUD Supervisor

MUD Controller

(IP Tables)

more info:
www.sandelman.ca/SSW/ietf/brski-links

Solution: use some good crypto



SHG App

Authenticate with TLS ClientCertificate

HOW DO WE SET THIS UP?

SHG

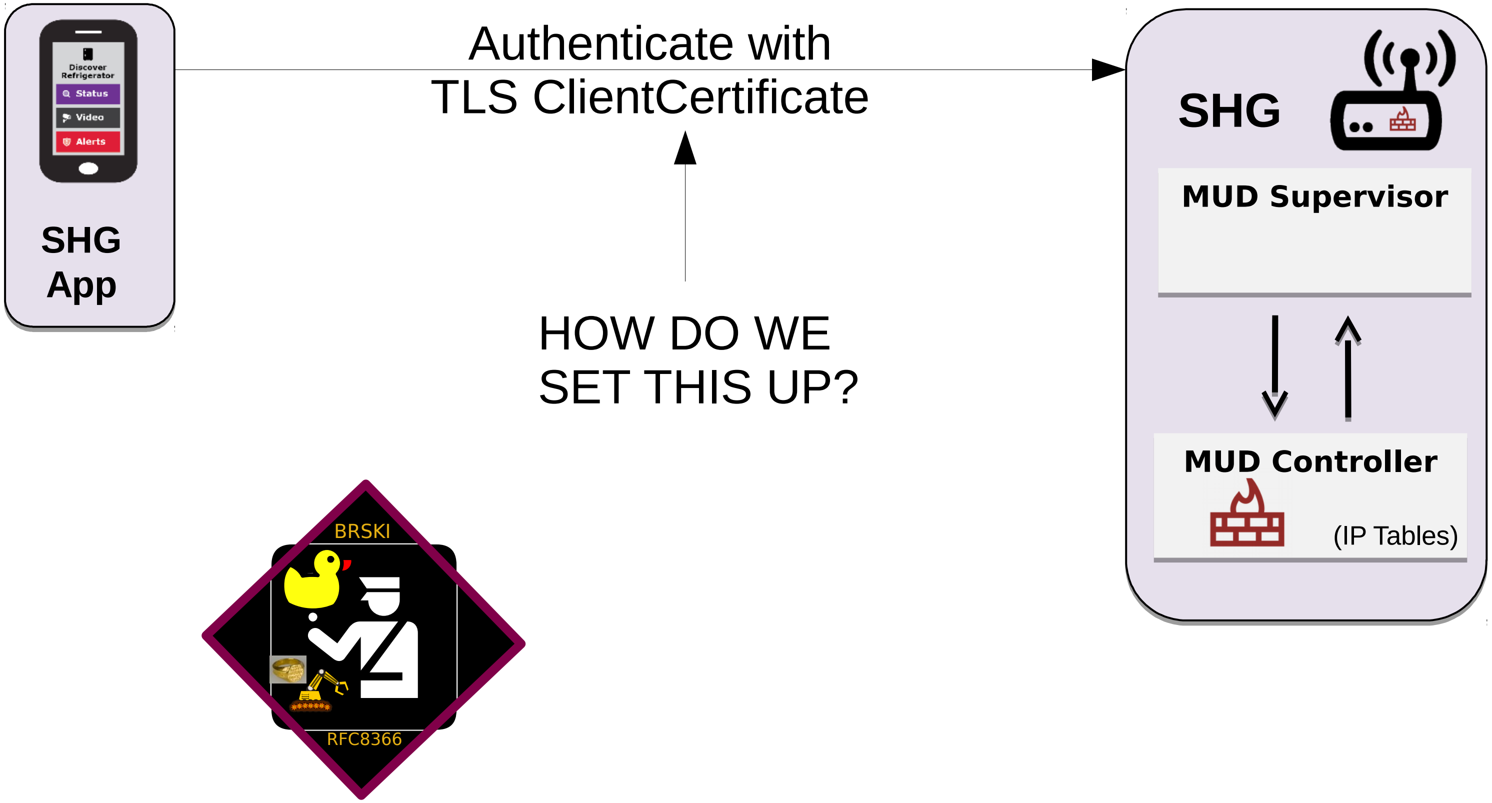
MUD Supervisor

MUD Controller

(IP Tables)

more info:
www.sandelman.ca/SSW/ietf/brski-links

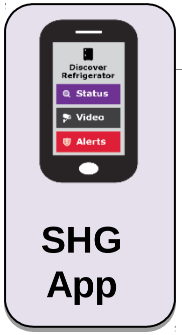
Solution: use some good crypto



HOW DO WE SET THIS UP?

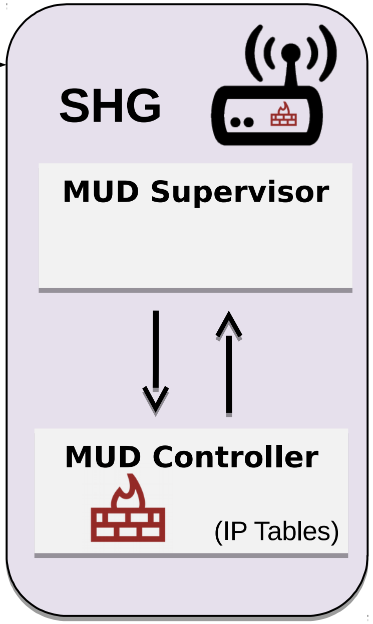
more info:
www.sandelman.ca/SSW/ietf/brski-links

Solution: use some good crypto



SHG App

Authenticate with TLS ClientCertificate



SHG

MUD Supervisor

MUD Controller

(IP Tables)

HOW DO WE SET THIS UP?

4th Annual Conference

Secure, Zero-Touch Bootstrap for the Internet of Things

Michael Richardson
Sandelman Software Works

www.iotsecurityfoundation.org #IoTSF2018 www.IoTSFConference.com

IET LONDON: SAVOY PLACE

"Secure Zero-Touch Bootstrap for the Internet of Things" Michael Richardson - IoTSF Conference 2018

Unlisted

13 views • Mar 18, 2019

4th Annual Conference

Authenticating Wireless nodes in Building Automation: Challenges & Approches

Prof. Andreas Rüst
Zurich University of Applied Sciences

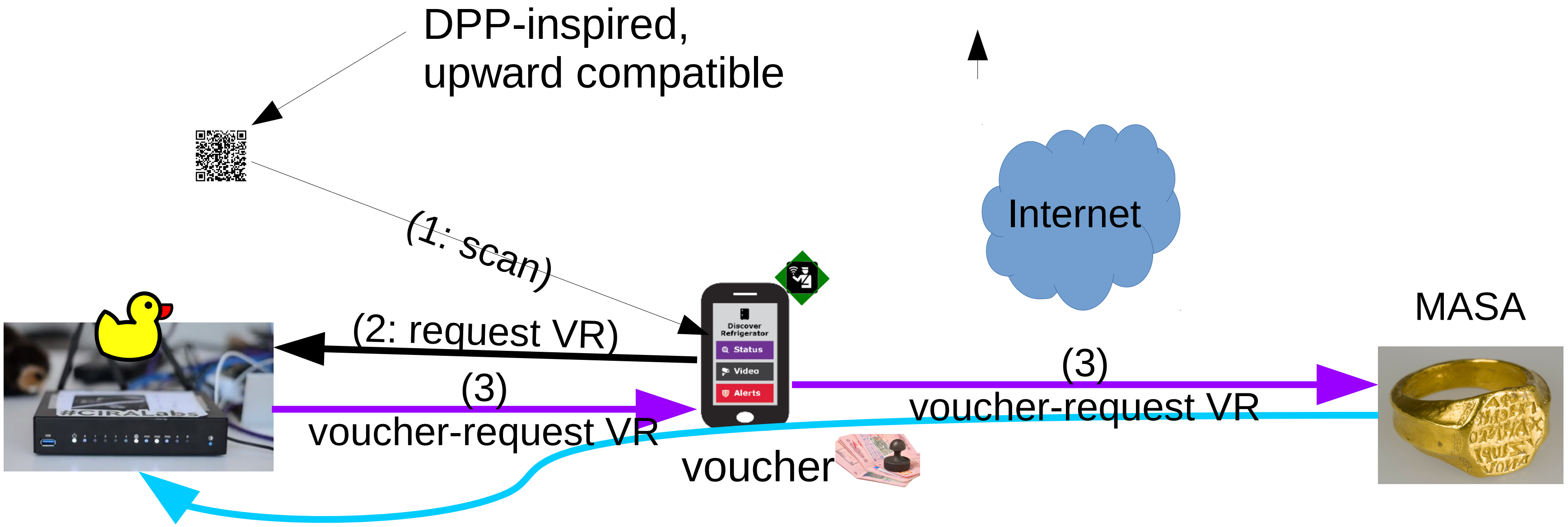
www.iotsecurityfoundation.org #IoTSF2018 www.IoTSFConference.com

IET LONDON: SAVOY PLACE

more info:
www.sandelman.ca/SSW/ietf/brski-links

Roles are a changin’

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



Time Sequence Diagram

Time Sequence Diagram

AR

Time Sequence Diagram

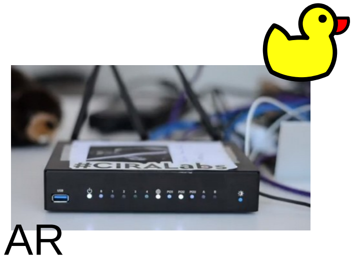
AR

Time Sequence Diagram

AR

MASA

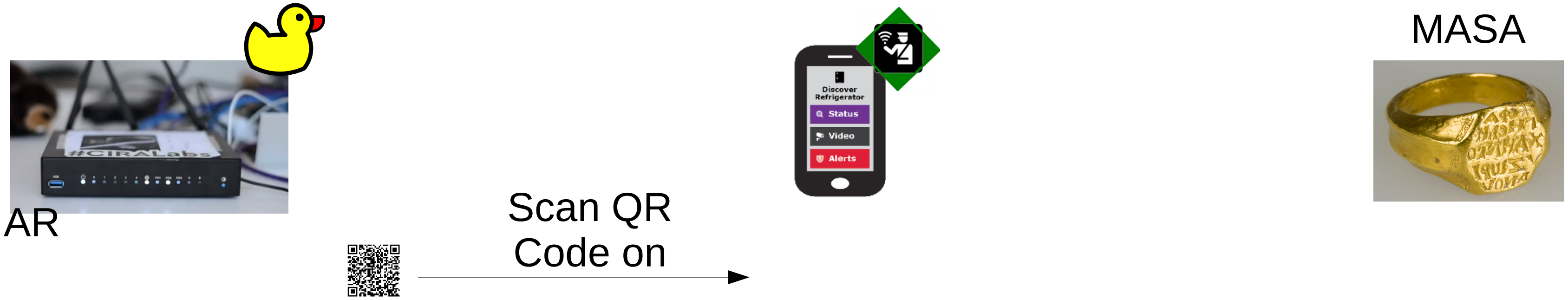
Time Sequence Diagram



AR

MASA

Time Sequence Diagram

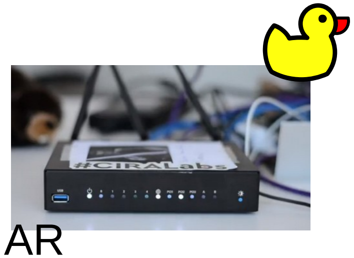


MASA

AR

Scan QR Code on

Time Sequence Diagram



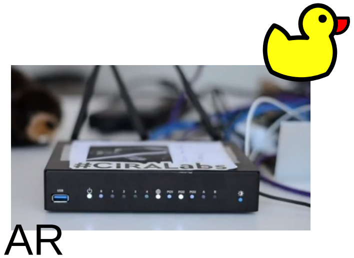
AR

MASA

Scan QR Code on

Generate Self-signed

Time Sequence Diagram



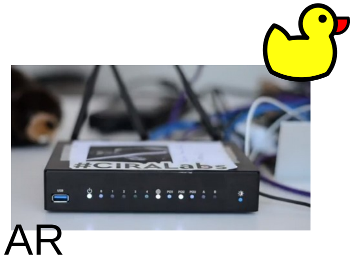
AR

MASA

Scan QR Code on

Generate Self-signed
Use as ClientCertificate

Time Sequence Diagram



AR

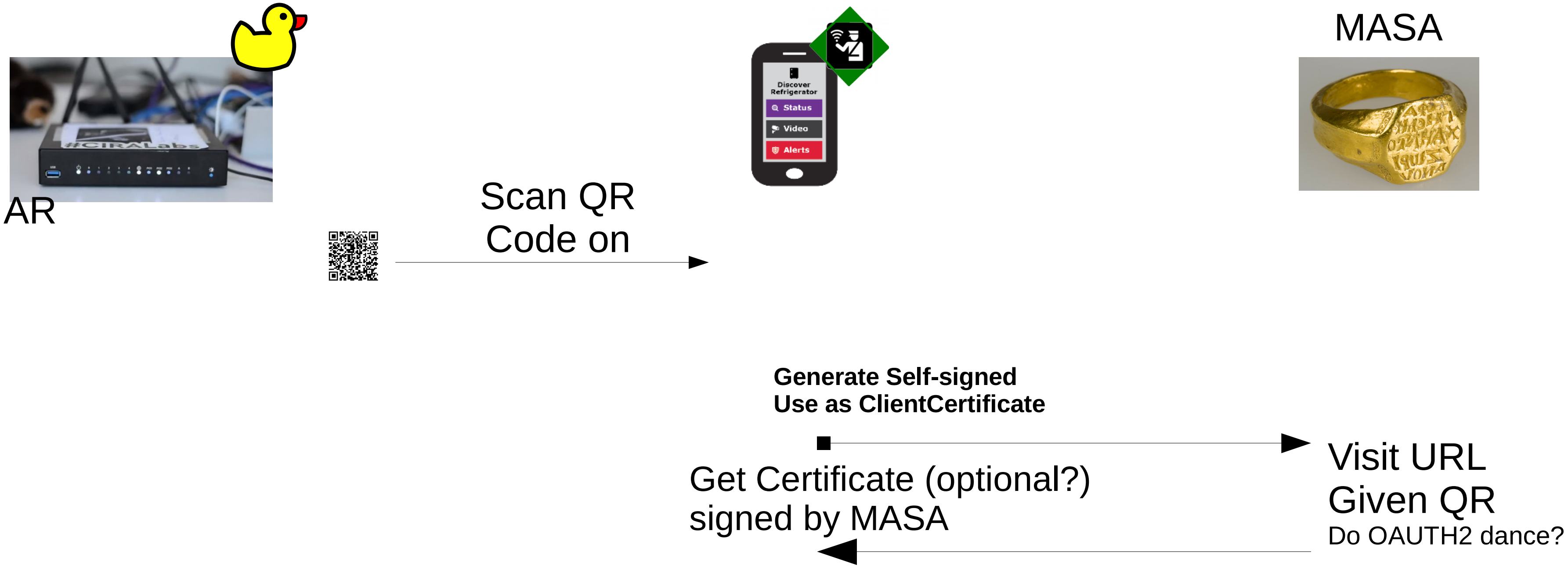
MASA

Scan QR Code on

Generate Self-signed
Use as ClientCertificate

Visit URL
Given QR
Do OAUTH2 dance?

Time Sequence Diagram



MASA

AR

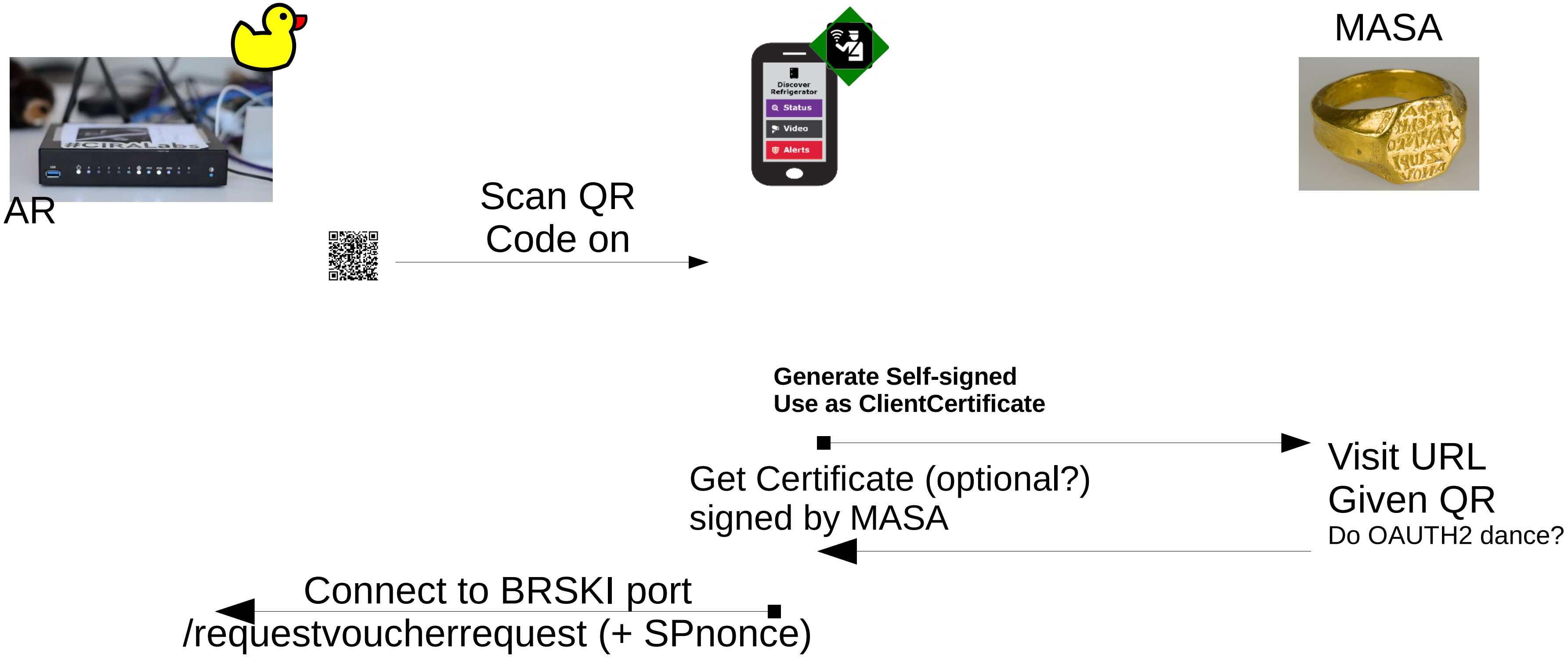
Scan QR
Code on

Generate Self-signed
Use as ClientCertificate

Visit URL
Given QR
Do OAUTH2 dance?

Get Certificate (optional?)
signed by MASA

Time Sequence Diagram



MASA

AR

Scan QR Code on

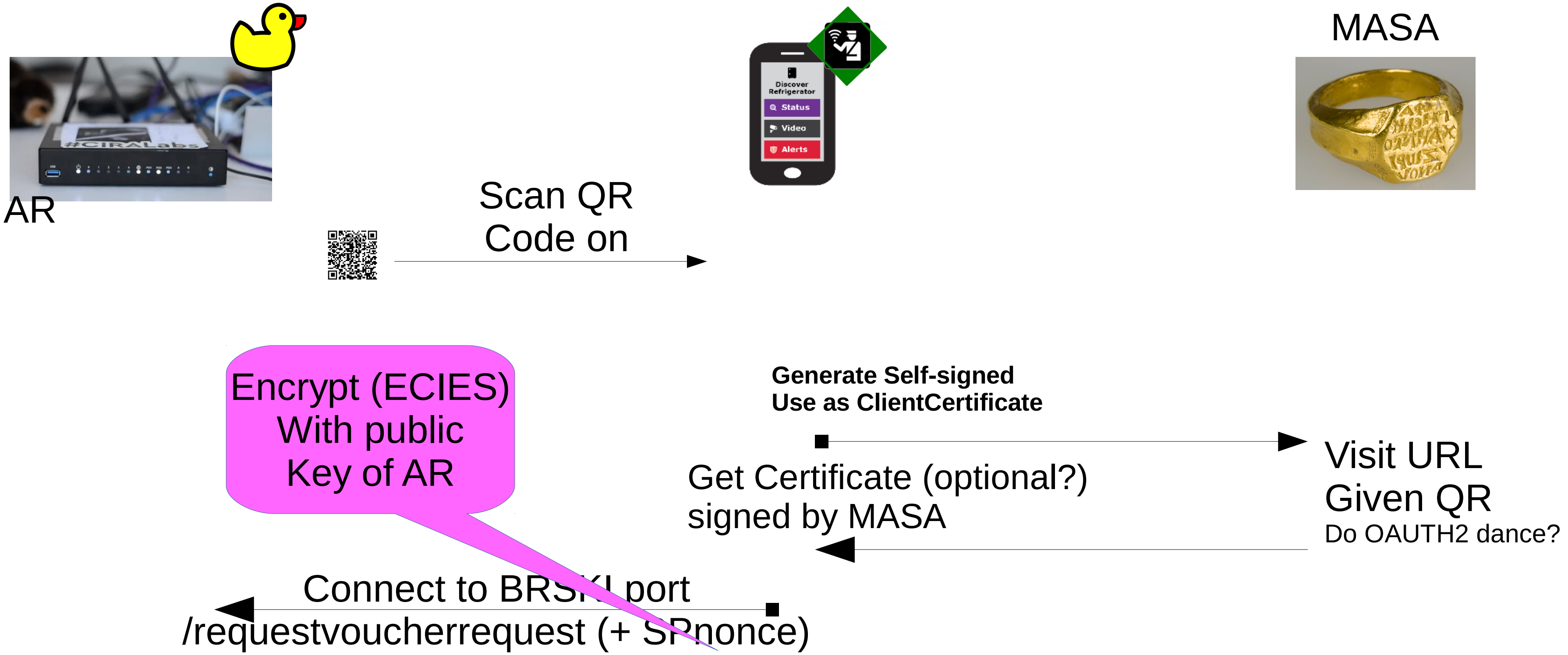
Generate Self-signed
Use as ClientCertificate

Visit URL
Given QR
Do OAUTH2 dance?

Get Certificate (optional?)
signed by MASA

Connect to BRSKI port
/requestvoucherrequest (+ SPnonce)

Time Sequence Diagram



MASA

AR

Scan QR Code on

Generate Self-signed
Use as ClientCertificate

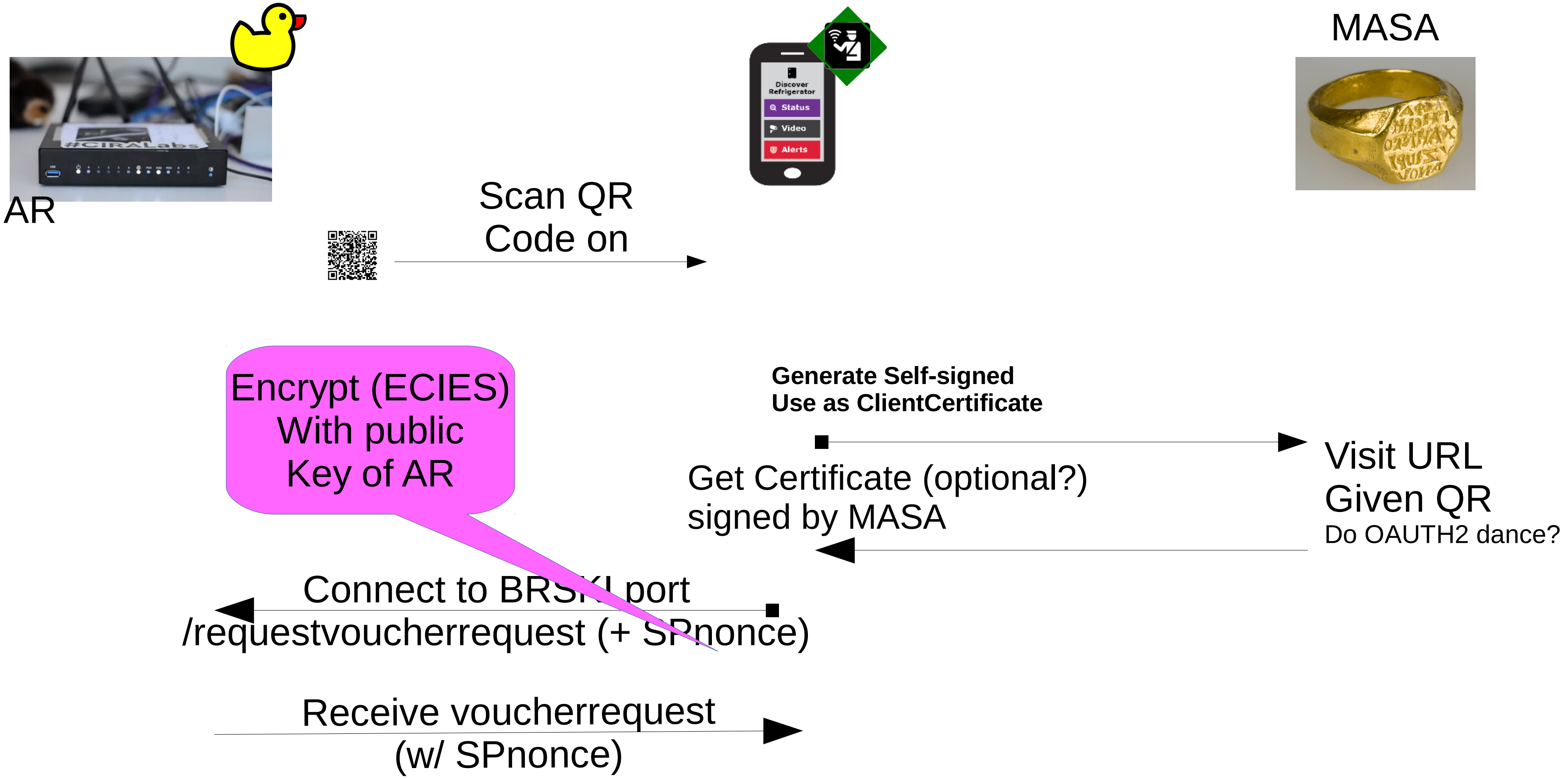
Visit URL
Given QR
Do OAUTH2 dance?

Get Certificate (optional?)
signed by MASA

Encrypt (ECIES)
With public
Key of AR

Connect to BRSKI port
/requestvoucherrequest (+ SPnonce)

Time Sequence Diagram



AR

MASA

Scan QR Code on

Encrypt (ECIES) With public Key of AR

Generate Self-signed
Use as ClientCertificate

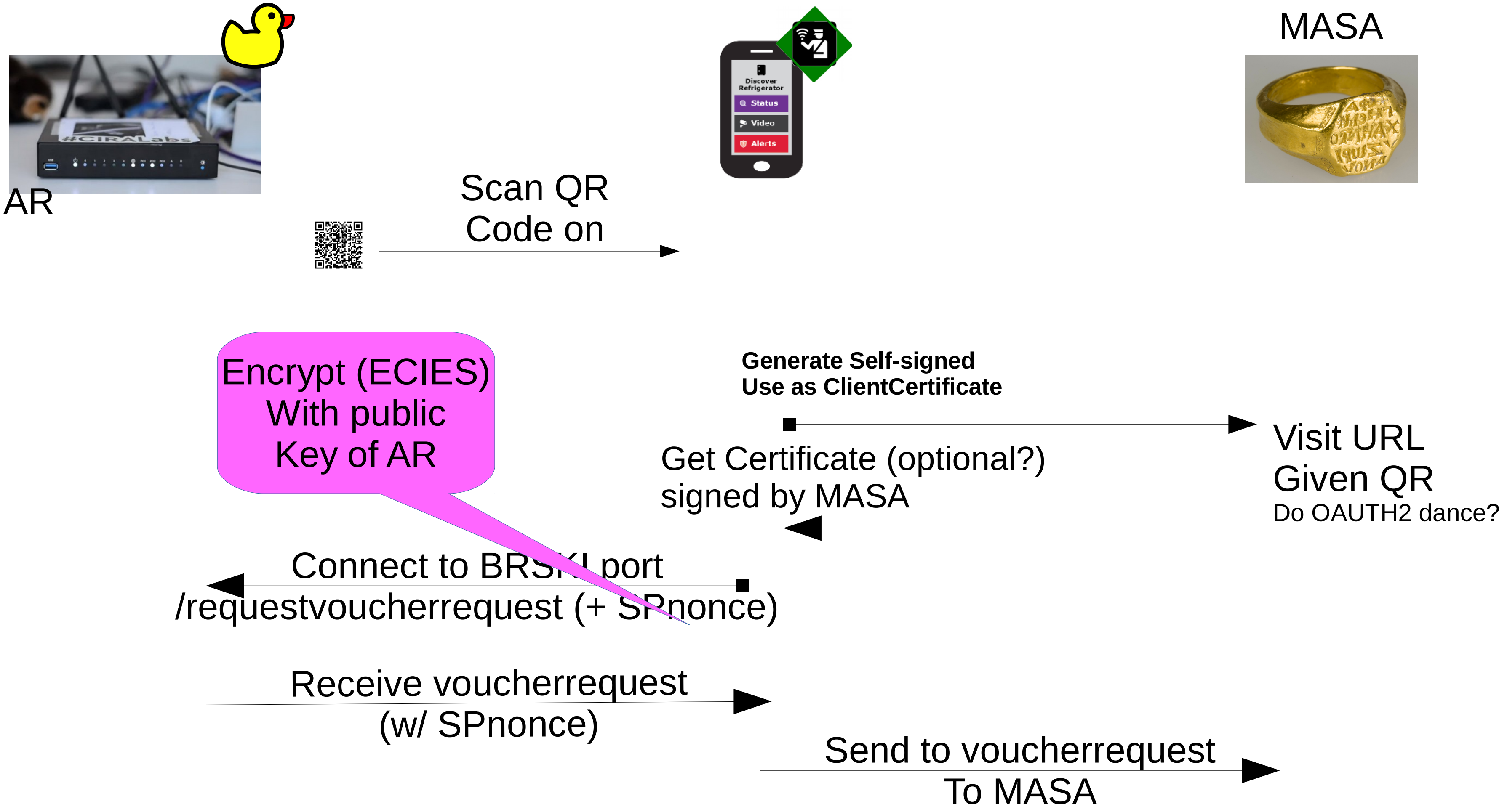
Visit URL
Given QR
Do OAUTH2 dance?

Get Certificate (optional?)
signed by MASA

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
Do OAUTH2 dance?

Get Certificate (optional?)
signed by MASA

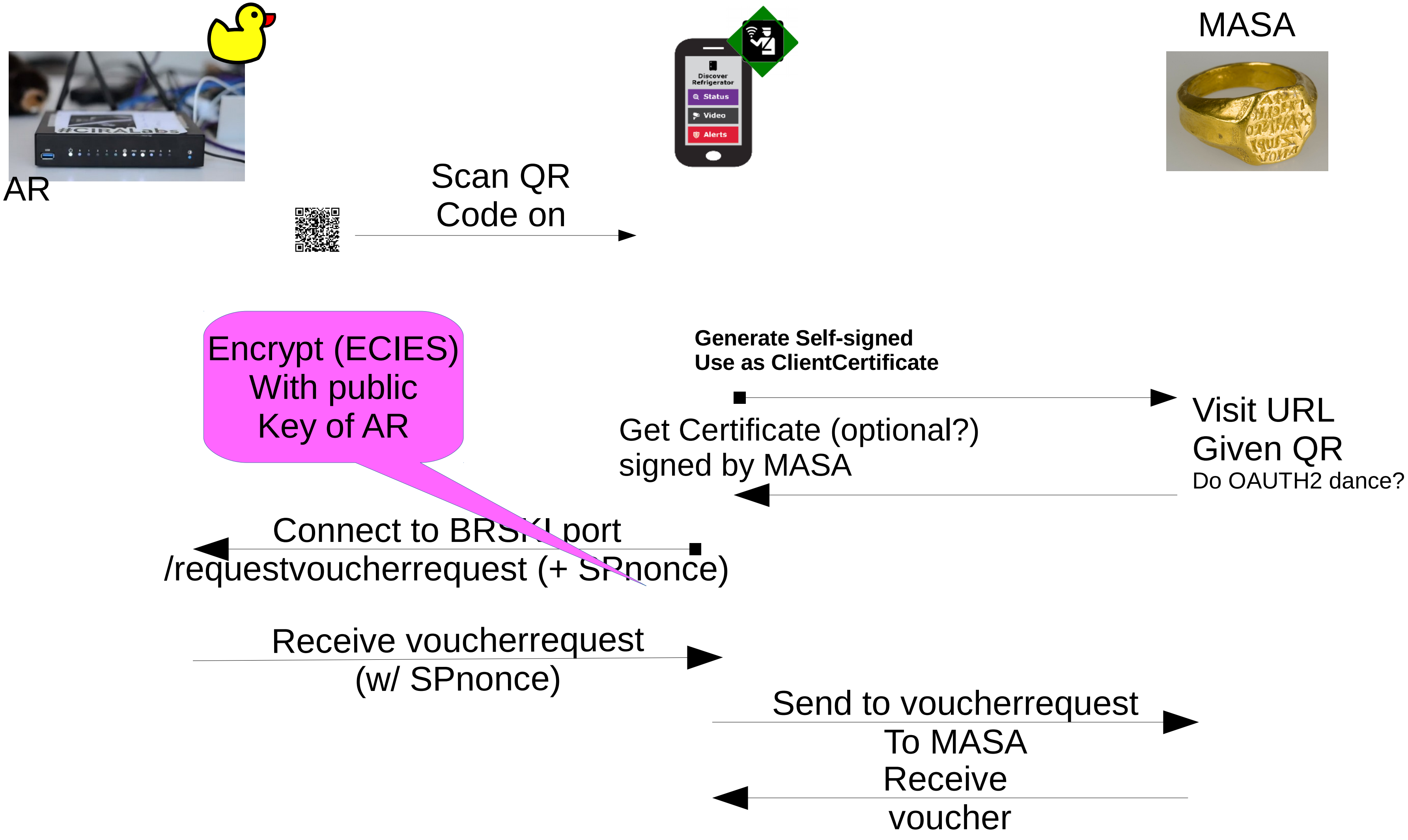
Encrypt (ECIES)
With public
Key of AR

Connect to BRSKI port
/requestvoucherrequest (+ SPnonce)

Receive voucherrequest
(w/ SPnonce)

Send to voucherrequest
To MASA

Time Sequence Diagram



AR

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

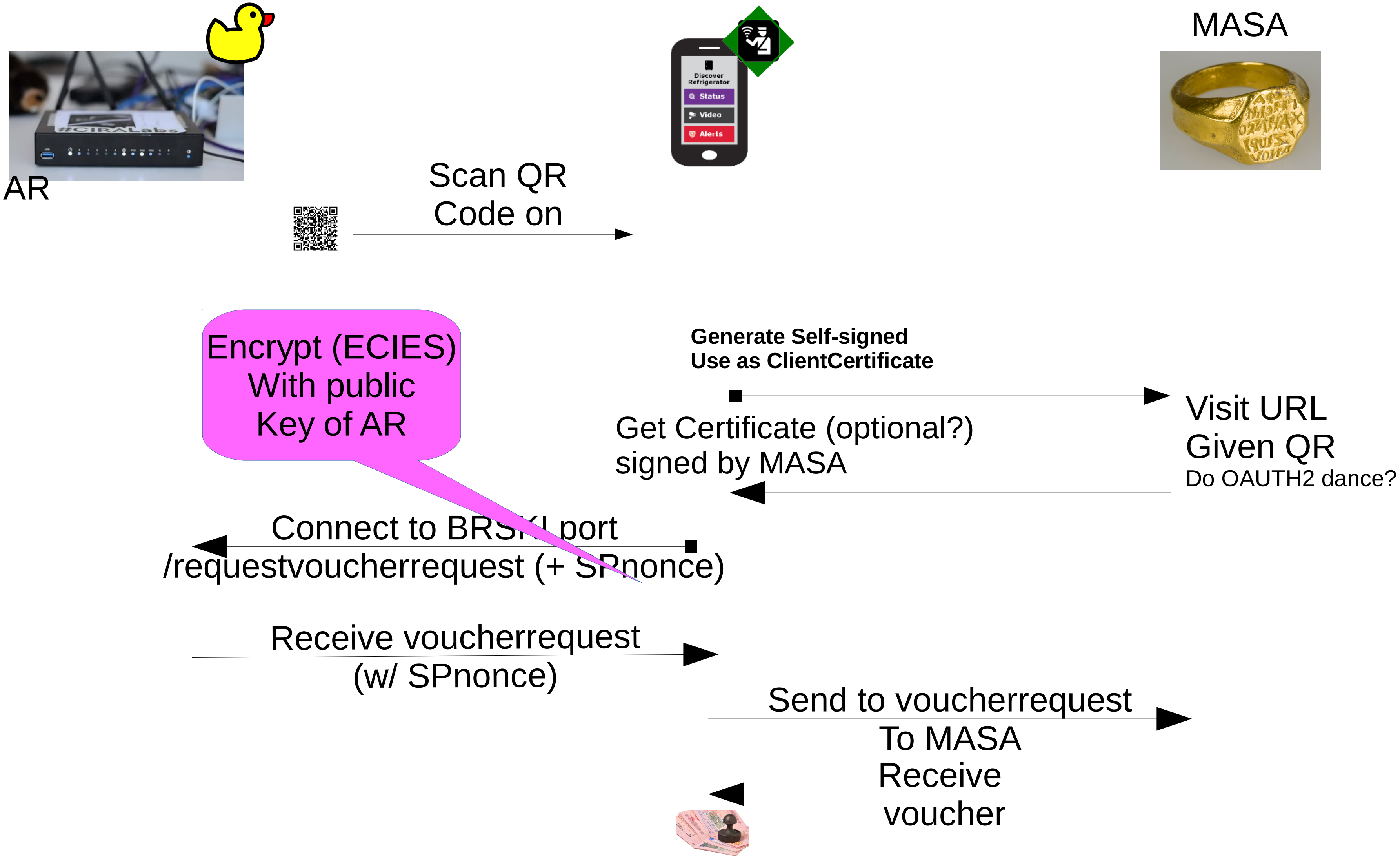
Connect to BRSKI port
/requestvoucherrequest (+ SPnonce)

Receive voucherrequest
(w/ SPnonce)

Send to voucherrequest
To MASA

Receive
voucher

Time Sequence Diagram



AR

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

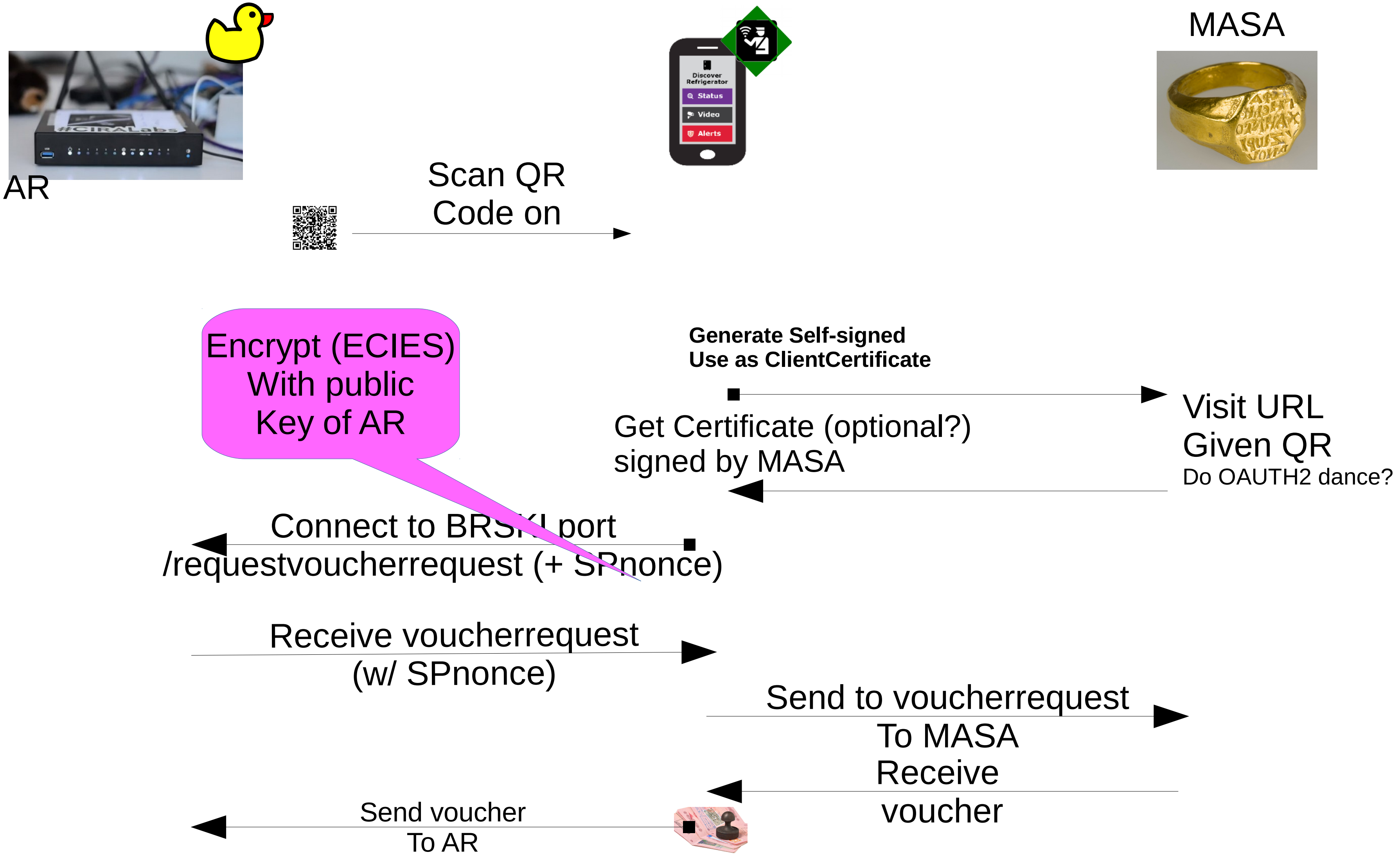
Connect to BRSKI port
/requestvoucherrequest (+ SPnonce)

Receive voucherrequest
(w/ SPnonce)

Send to voucherrequest
To MASA

Receive
voucher

Time Sequence Diagram



MASA

AR

Scan QR
Code on

Encrypt (ECIES)
With public
Key of AR

Generate Self-signed
Use as ClientCertificate

Visit URL
Given QR
Do OAUTH2 dance?

Get Certificate (optional?)
signed by MASA

Connect to BRSKI port
/requestvoucherrequest (+ SPnonce)

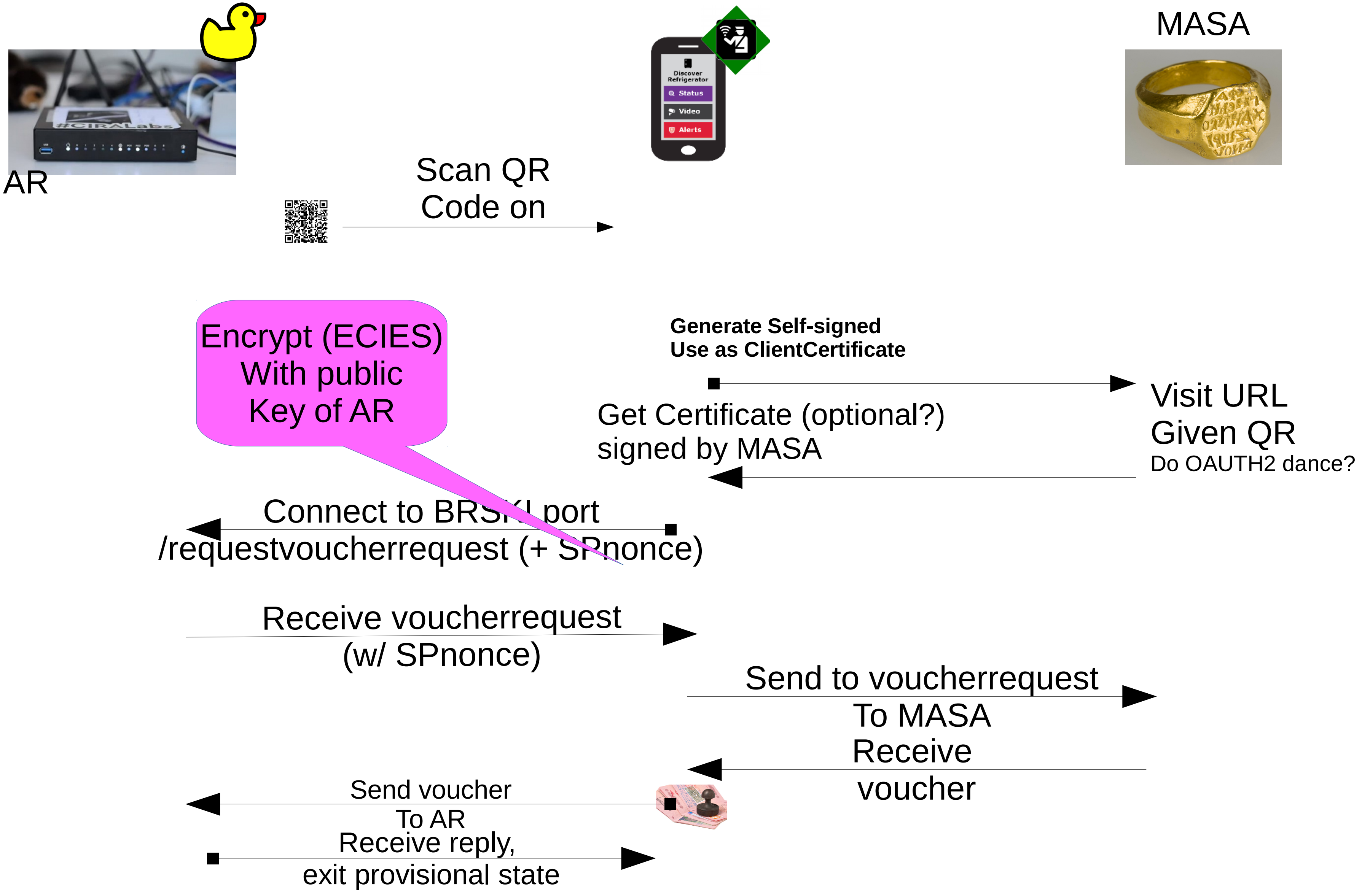
Receive voucherrequest
(w/ SPnonce)

Send to voucherrequest
To MASA

Receive
voucher

Send voucher
To AR

Time Sequence Diagram



AR

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
/requestvoucherrequest (+ SPnonce)

Receive voucherrequest
(w/ SPnonce)

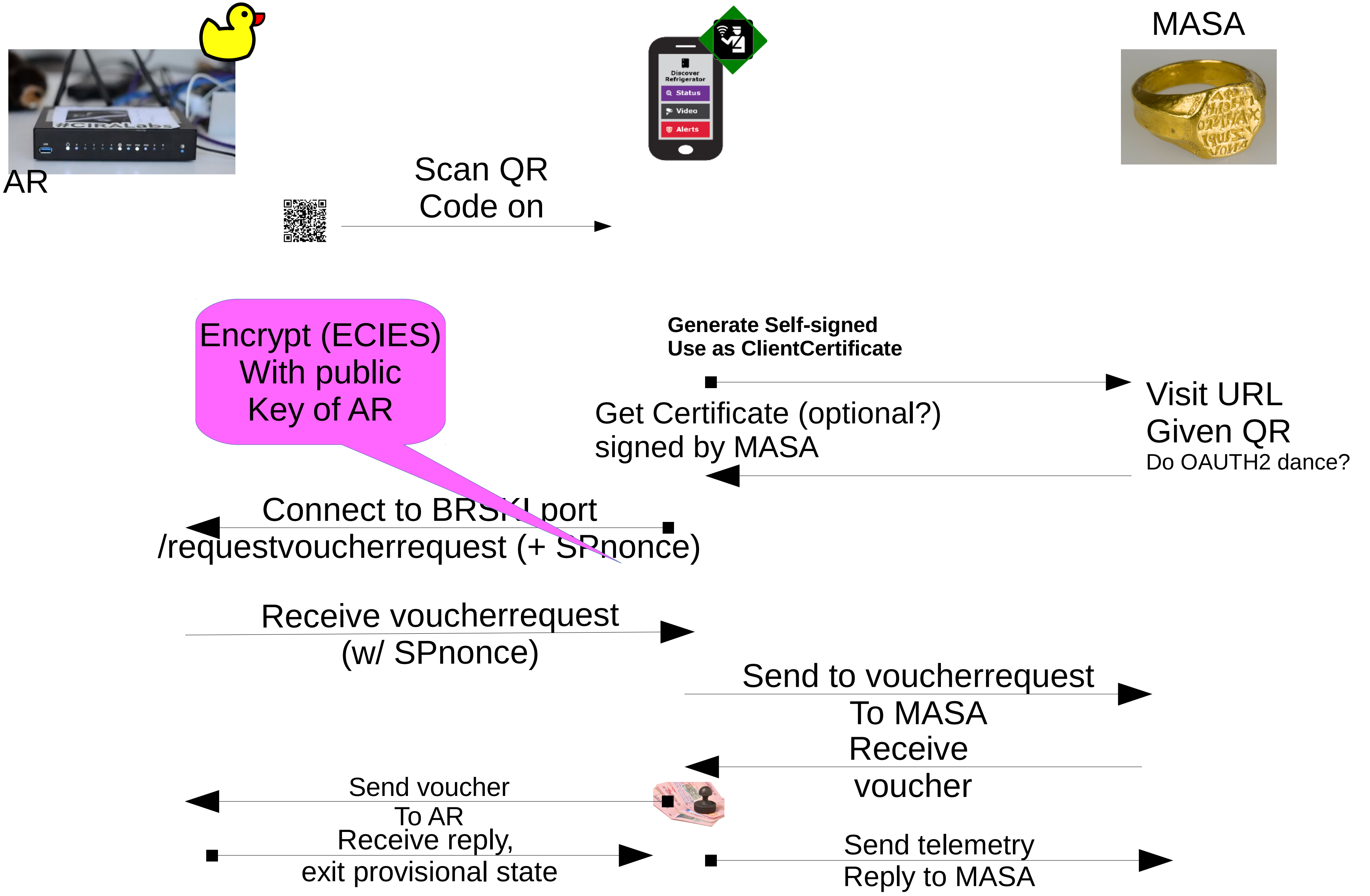
Send to voucherrequest
To MASA

Receive
voucher

Send voucher
To AR

Receive reply,
exit provisional state

Time Sequence Diagram



MASA

AR

Scan QR
Code on

Encrypt (ECIES)
With public
Key of AR

Generate Self-signed
Use as ClientCertificate

Visit URL
Given QR
Do OAUTH2 dance?

Get Certificate (optional?)
signed by MASA

Connect to BRSKI port
/requestvoucherrequest (+ SPnonce)

Receive voucherrequest
(w/ SPnonce)

Send to voucherrequest
To MASA

Receive
voucher

Send voucher
To AR

Receive reply,
exit provisional state

Send telemetry
Reply to MASA

Time Sequence Diagram

Registrar

MASA

EST7030
/simpleenroll

PKIX cert
Specific to this router

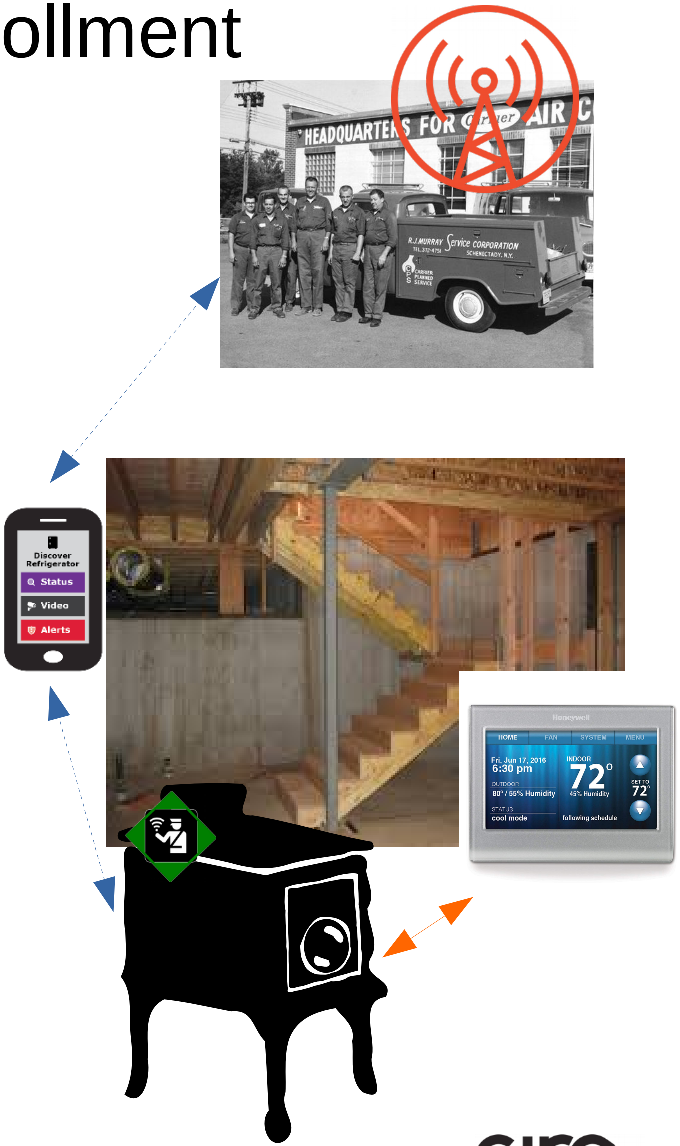
SHG specific
APIs

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

- WiFi Alliance DPP
  - Released in summer 2019
  - Uses Public Key printed on QR code
  - *Runs over new management frames in 802.11*,
    - **presently** inaccessible on current smartphone Oses
      - *latest* Android 10, on some phones works
      - no known iOS code
    - we are writing code today.
- Designed system to transform into DPP in the future

Opportunities: asynchronous enrollment

- new installations/ buildings where there is no network
- LTE from install truck is not reachable from basement
- draft-richardson-anima-smarkaklink
- draft-fries-anima-brski-async-enroll (Siemens-BT)



Questions