Secure trust and information access for the Internet of Things

Kary Främling

The Open Group, Internet of Things Work Group: *Chair*
Aalto University: *Professor, Computer Science*
Umeå University: *Professor, Data Science*
ControlThings Limited: *CEO*

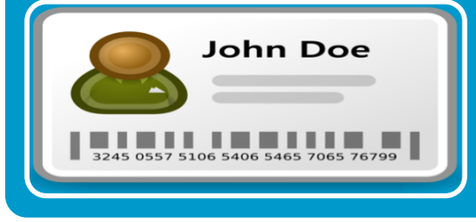
Aalto University
School of Science

ControlThings
Excellence Embedded

THE Open GROUP
Making standards work®

Summary

Security challenges in IoT



Security basics

Access Control based on O-DF and O-MI

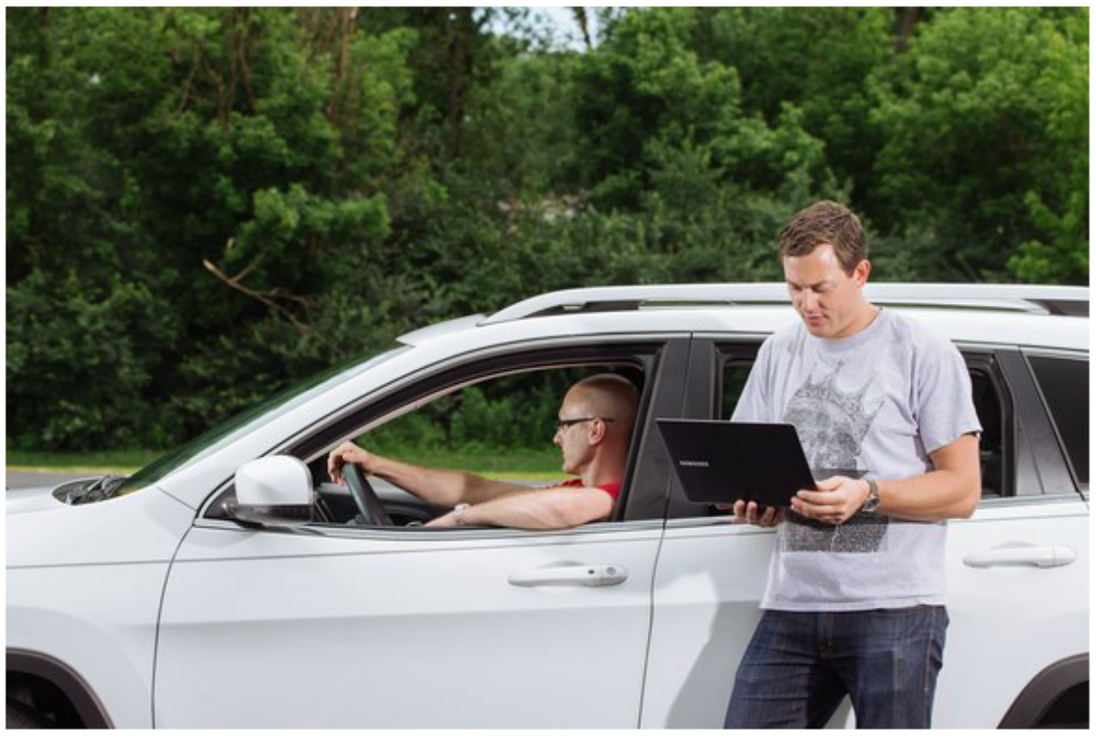
Certificates and Trust

Conclusions

Taking control over car

ANDY GREENBERG SECURITY 08.01.16 03:30 PM

THE JEEP HACKERS ARE BACK TO PROVE CAR HACKING CAN GET MUCH WORSE



Security researchers Charlie Miller and Chris Valasek. WHITNEY CURTIS FOR WIRED

ALMOST EXACTLY A year ago, Chrysler announced a recall for 1.4 million vehicles after a pair of hackers demonstrated to

- Wired January 8th, 2016
- Somehow gained access to internal CAN bus commands
- CAN bus access originally required physical access to connector within car

Aalto University School of Science

ControlThings Excellence Embedded

THE Open GROUP Making standards work®

DoS attack against building automation

Verkkohyökkäys katkaisi kahdesta kerrostalosta lämmöt Lappeenrannassa – ”Laajuus ja voima on aika poikkeuksellinen”

Useat rakennusten automaatiojärjestelmät ovat eri puolilla Suomea ”tiltanneet” palvelunestohyökkäysten vuoksi. Kuinka nettihakkeri voi katkaista kerrostalosta lämmöt?

Palvelunestohyökkäys katkaisi hetkeksi huoneistojen ja veden lämmityksen. (KUVA: MOSTPHOTOS)

Anu-Elina Ervasti HS
Julkaistu: 7.11.2016 19:10

KAHDESSA Lappeenrannassa sijaitsevassa kerrostalossa tapahtui viime viikon torstaina jotain poikkeuksellista: palvelunestohyökkäys katkaisi hetkeksi huoneistojen ja veden lämmityksen.

Luetuimmat

JUURI NYT | PÄIVÄ | VIIK

1. Kuvakooste lukijoiden tulvakuvista kai kukaan halua jäädä pois tässä”, bussikuski ja kaarsi pysäkin ohi
2. Antti Herlin muistelee veljeään rehellisenä ja oikeudenmukaisena ihmisenä
3. Kiusaajat voittivat Niklas Herlinin 18.11.2013 Tilaajille
4. Muistokirjoitus: Niklas Herlin oli hy

- Helsingin Sanomat, Finland, November 7th, 2016
- Attack against heating control of two apartment buildings in Finland
- Insufficient firewall protection
- Lack of prioritization of basic control functionality?

Aalto University School of Science

ControlThings Excellence Embedded

THE Open GROUP Making standards work®

DDoS attack in 2016

Friday morning saw the largest internet blackout in US history. Almost every corner of the web was affected in some way -- streaming services like Spotify, social sites like Twitter and Reddit, and news sites like Wired and Vox appeared offline to vast swathes of the eastern seaboard.

After suffering three separate distributed denial-of-service (DDoS) attacks, Dyn, the domain name system provider for hundreds of major websites, recovered and the web started to spring back to life.

The flooding attack was designed to overload systems and prevent people from accessing the sites they want on a scale never seen before this.

All signs point to a massive botnet utilizing the Internet of Things, powered by malware known as Mirai, which allows the botnet's operator to turn a large number of internet-connected devices -- surveillance cameras, smart home devices, and even baby monitors -- against a single target.

In this case, it was Dyn's servers.

"We're seeing attacks coming from an Internet of Things botnet that we identified called Mirai, also involved in this attack," said Dale Drew, chief security officer at Level 3, in a live stream on Friday, during a time where information about the attack was still scarce.

Dyn later said Saturday in a blog post that the attack was "highly distributed" and involved "tens of millions of IP addresses."

- ZDNet, October 22, 2016
- **WAIT!!**
  - Why blame IoT for this? IoT has nothing to do with it!
  - Gateways, Smart TVs etc would be there anyways, even without IoT

IoT vulnerabilites

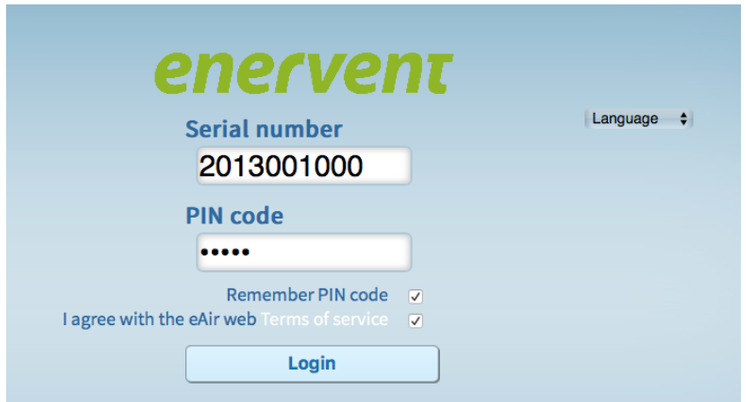
- Devices and buses made for local use are connected directly to the internet
  - Can be attacked by anybody easily
  - Example: Modbus TCP used in Building Automation
    - Port can be found with port scanning
    - If Modbus registry map is known, even direct control may be possible
    - Or just confusing controller by sending random commands
- Firewall configuration is not easy to get right
  - Did you ever try opening only one port on your home gateway?
  - Remains risky even for professionals
- Cryptographical identities are still rare for IoT devices
- Etc etc

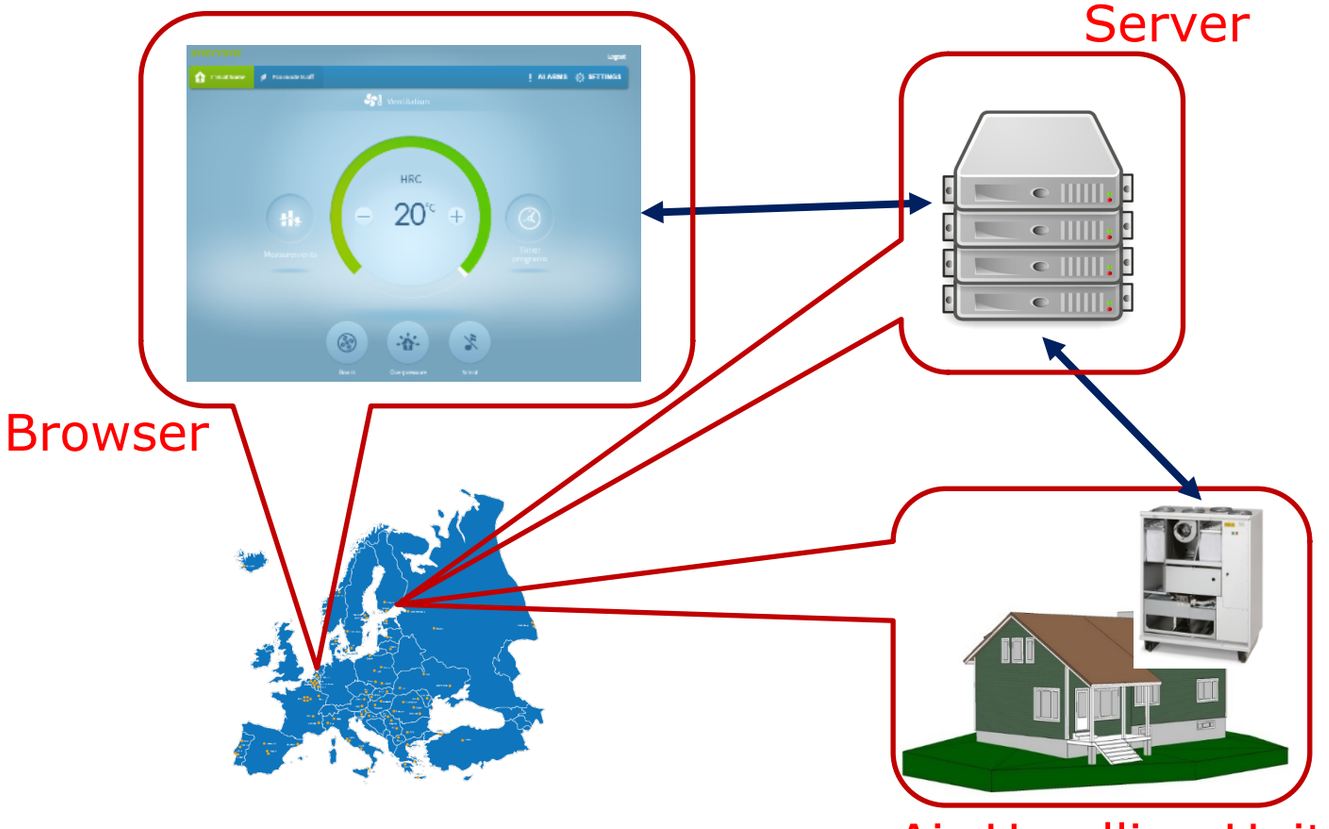
A secure IoT system?

- Unique identities
- Machine authentication by certificate
- User authentication by serial number + PIN

Every machine ships with:

- Serial number
- PIN code
- X.509 certificate





- All communication secured by HTTPS
- Bi-directional control by WebSockets
- Commercially available since 2013
- Why is this not the norm?

Aalto University
School of Science

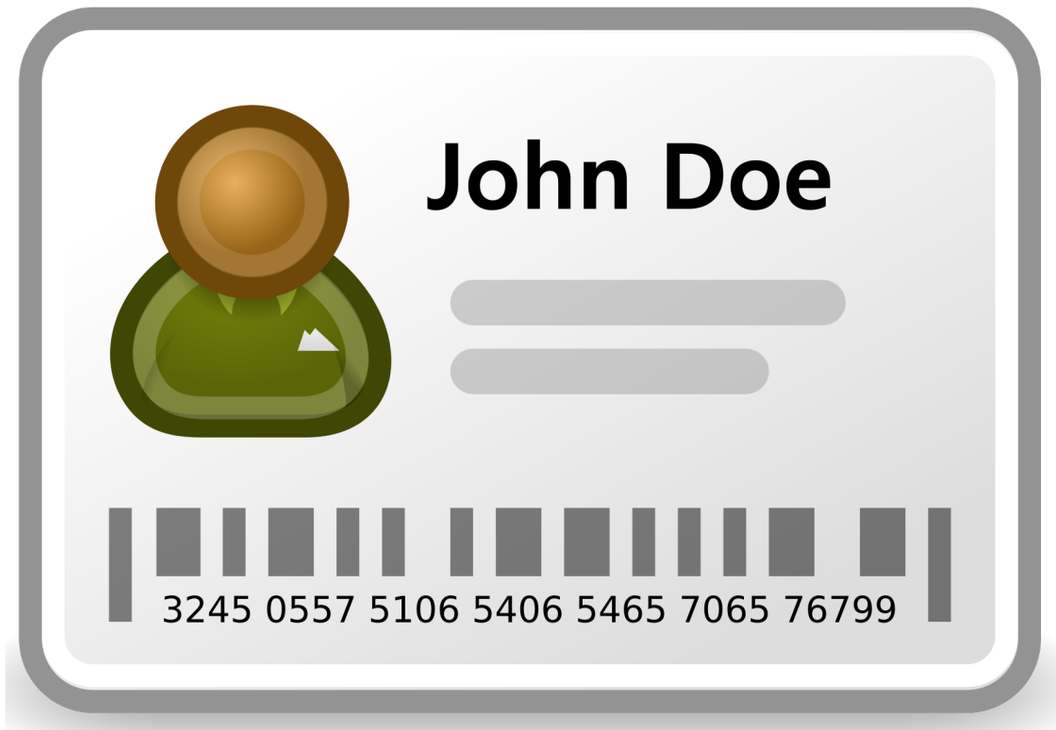
ControlThings
Excellence Embedded

THE Open GROUP
Making standards work®

Security basics

Identity and Identification

- All **entities** need **identity**
  - People, devices, organizations, code, agents, …
- Identity must be **unique** in context of use
  - IoT: usually **globally unique**
  - "Our" approach from 2001: **ID@URI**



- Most things have **more than one identifier**
  - Name, social sec. number, fingerprint, …
  - Licence plate number, VIN number, …
  - Different identifiers in different **roles** and different means of **authentication**

Aalto University School of Science

ControlThings Excellence Embedded

THE Open GROUP Making standards work®

Authentication

- How **validate identity**?
- Needed for determining
  - **Level of trust**
  - **Level of access**
- Authentication depends on **identification support**
  - User name, password (local authentication)
  - Kerberos, Shibboleth, … (network authentication)
  - Oauth, OpenID Connect (delegated trust)
  - Public-private key certificates (PKI)

Also look e.g. at The Open Group Jericho Forum video: https://www.youtube.com/watch?v=ZlG3yZfk9tw&feature=plcp

Authorization / Access control / Entitlement

- **Who** gets access to **what** information?
- **Operations**
  - Read, write, execute, …?
- Different entities may act in different **roles** or **personas** depending on the **context**

- **Access rights** depend on **authenticated role**

Recommended reading and video (The Open Group Jericho Forum): https://blog.opengroup.org/2012/08/07/entities-and-entitlement-the-bigger-picture-of-identity-management/

Aalto University School of Science

ControlThings Excellence Embedded

THE Open GROUP Making standards work®

Security specifics for IoT

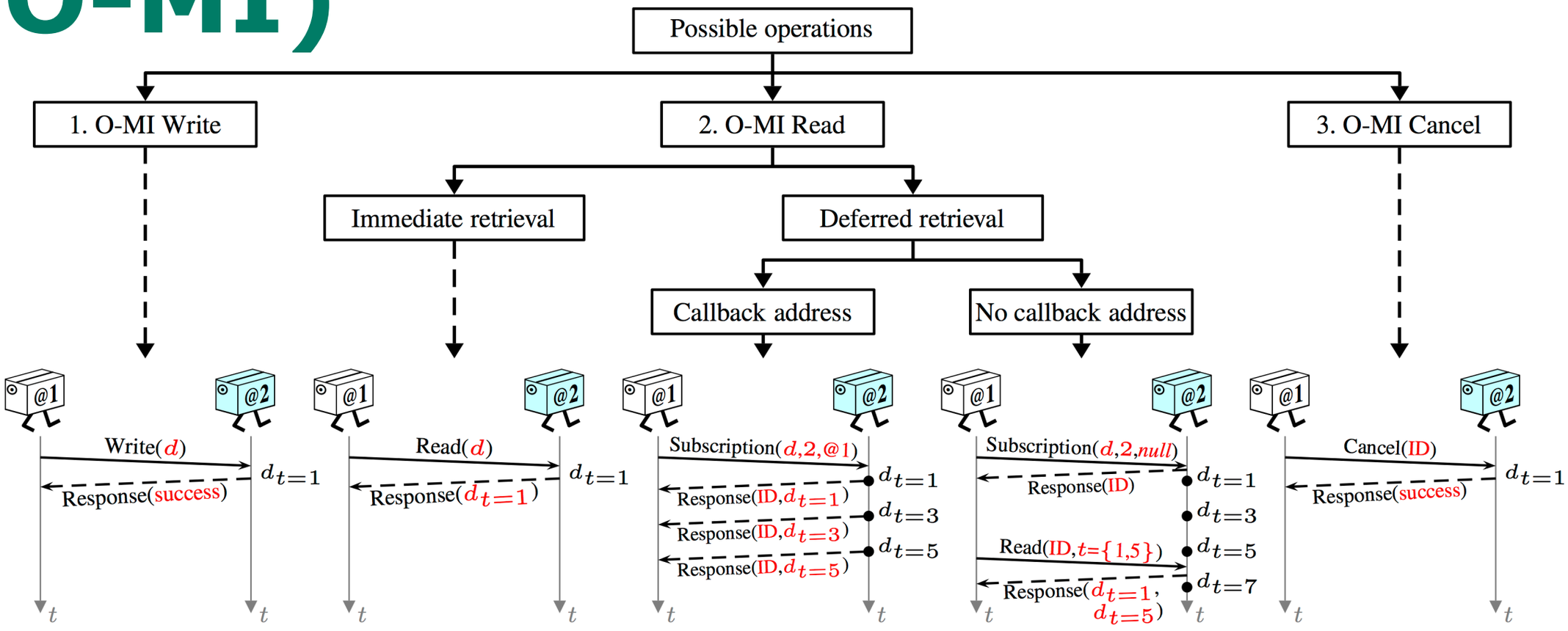
- Most security basics can be applied as such
- Challenges:
  - How identify pieces of information for access rights, as for folders and files in a file system?
  - Distribution of identities (/certificates) to devices, code, …?
  - Device-level, owner-level, organization-level, … certificates?
  - How to update certificates before they expire?
  - How to manage software updates to all those devices behind firewalls etc?

Security in O-MI / O-DF reference implementation

Identification and Authentication

- All Objects in O-DF have identities (compulsory <id> tag)
  - However, these are mainly for annotating information, not for security
- Users identified / authenticated by
  - User name, password
  - Shibboleth
  - Oauth
- Things / gateways /systems identified by
  - Public-private key certificates (PKI)
  - Client Authentication with HTTPS

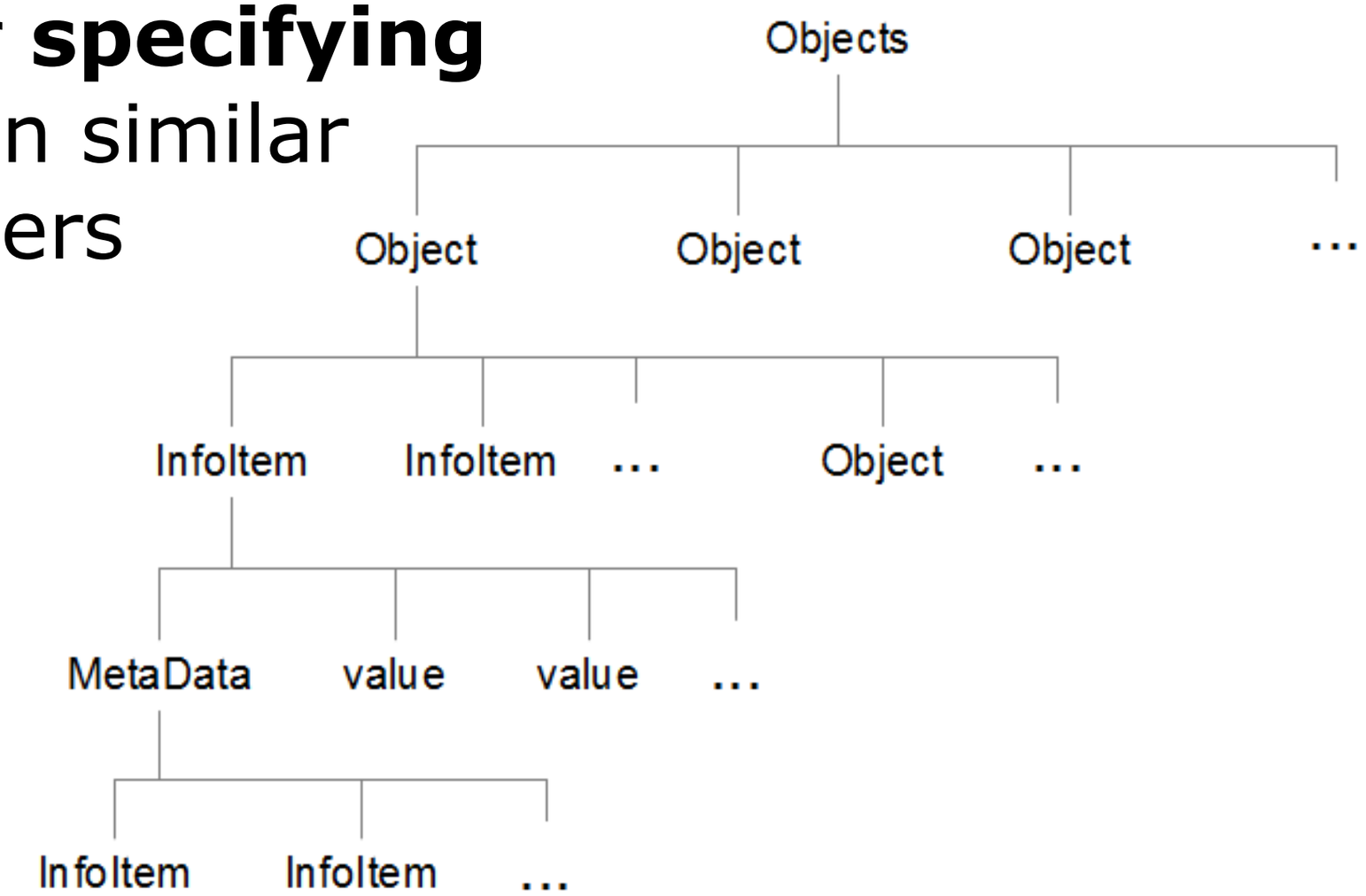
Open Messaging Interface (O-MI)



- Specifies **possible operations**
  - **Read** current and historical information, alerts, other events, …
  - **Write** information, such as sensor values, setpoints, alerts, …
  - **Subscribe** to information with or without callback
  - **Cancel** subscriptions before they expire
  - Upcoming: **call** (execute) methods

Open Data Format (O-DF)

- **Generic object tree** for IoT (or other) data structures
- Can be used for **specifying access rights** in similar ways as for folders and files in a file system

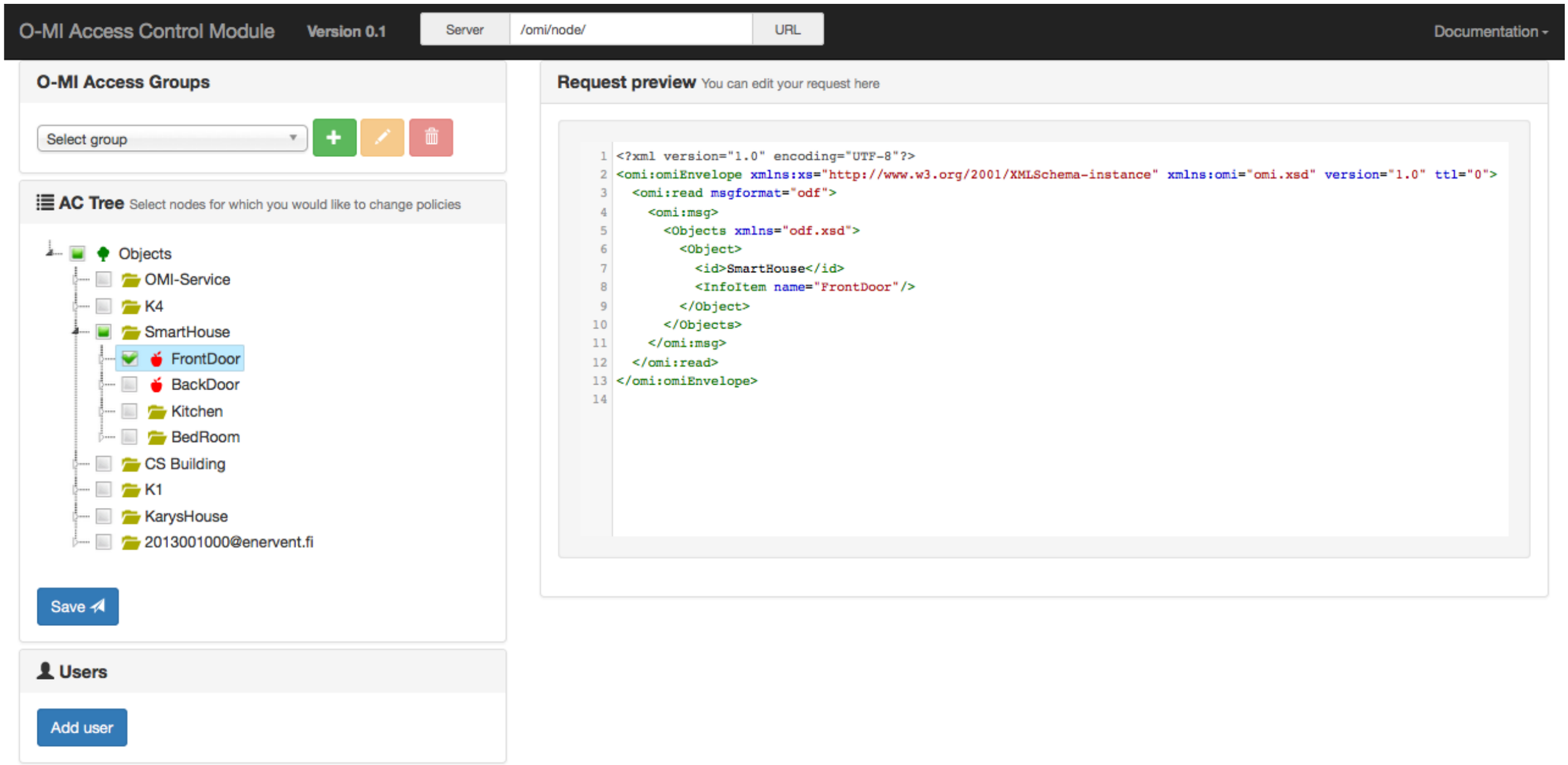


Aalto University
School of Science

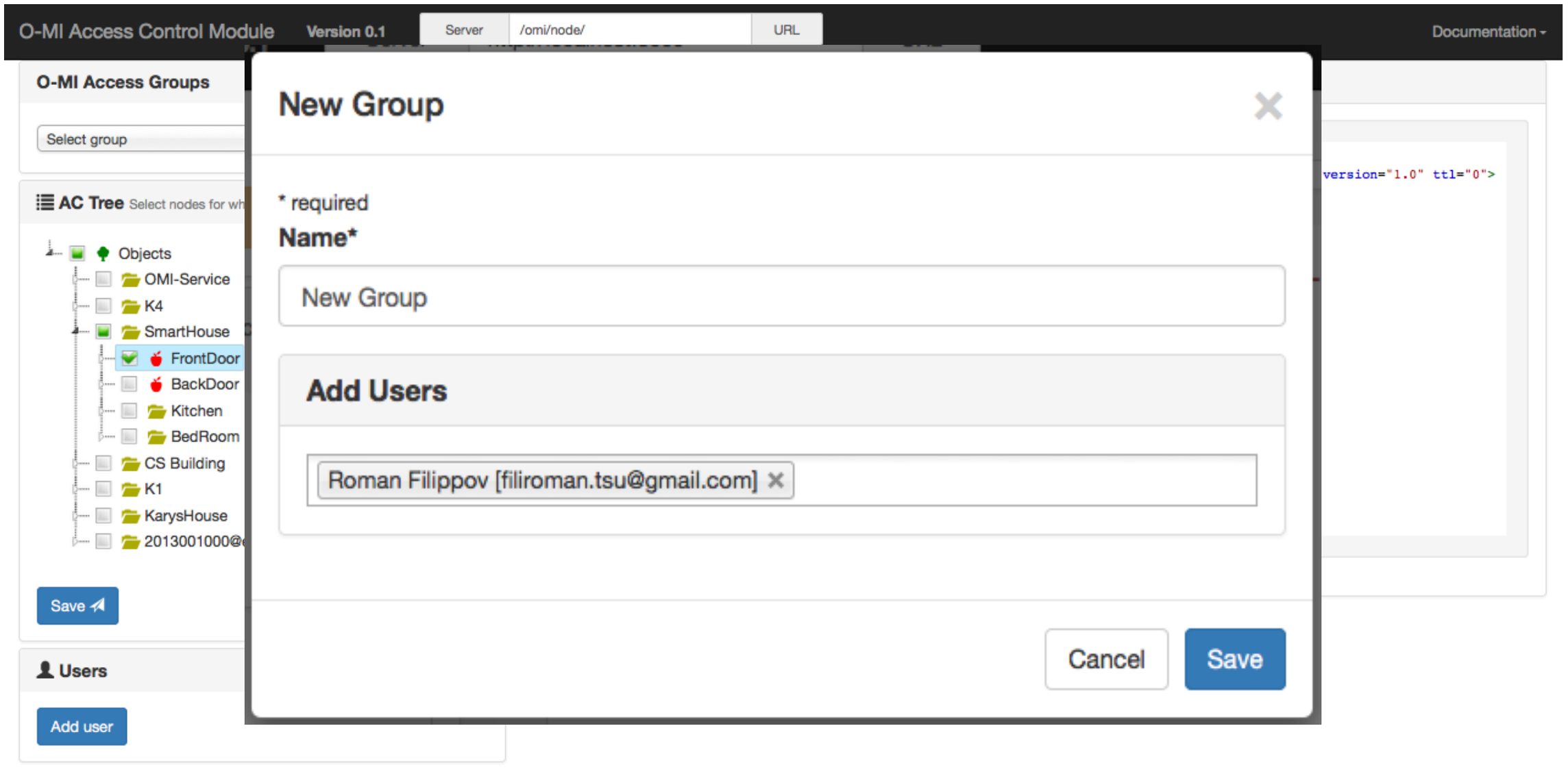
ControlThings
Excellence Embedded

THE Open GROUP
Making standards work®

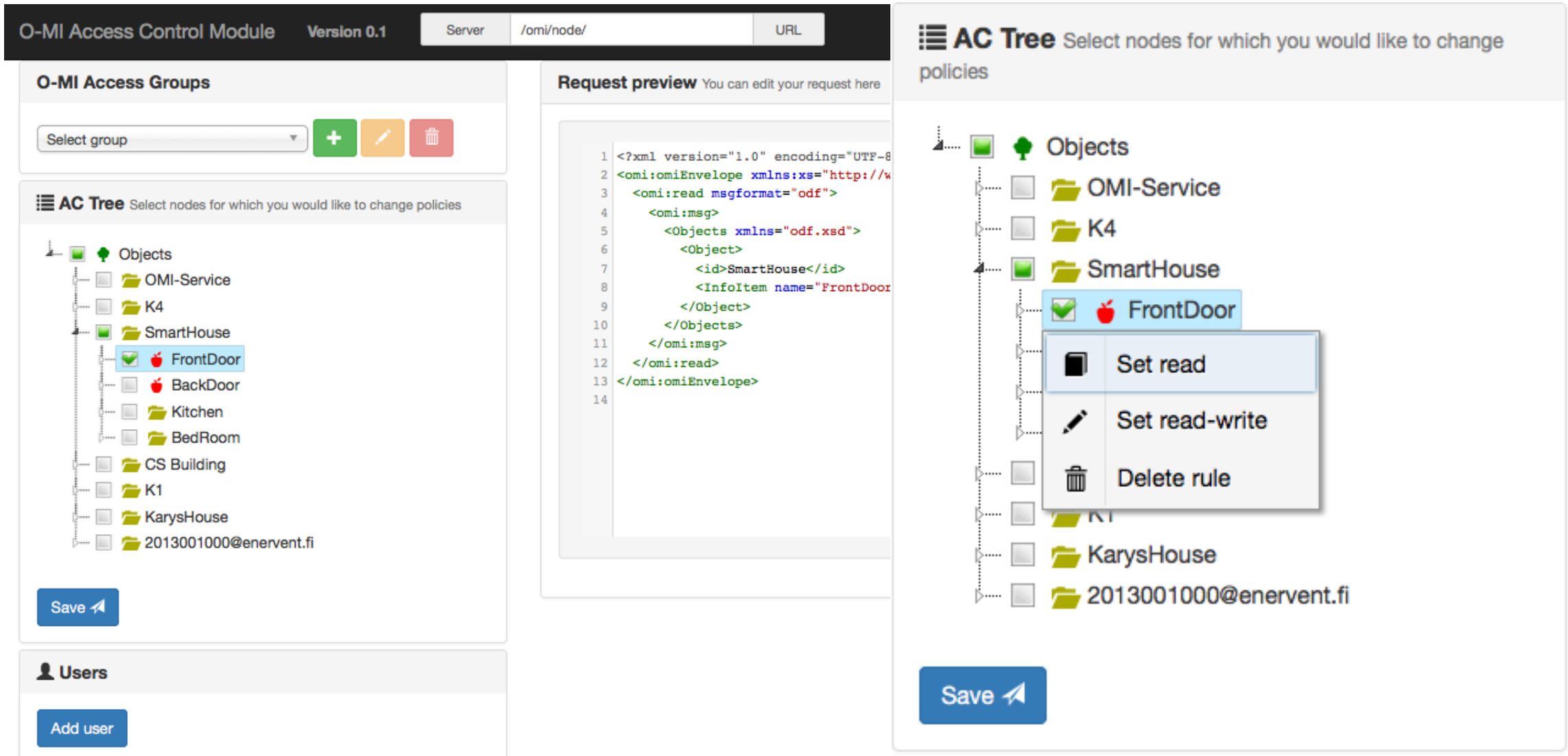
Access Control Management UI



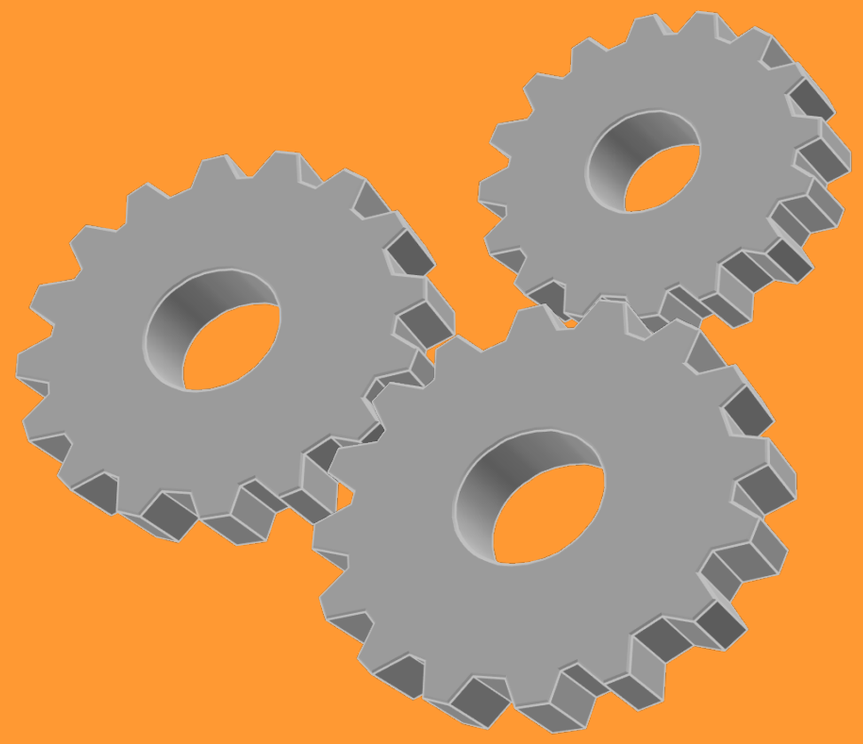
Access Control Management UI



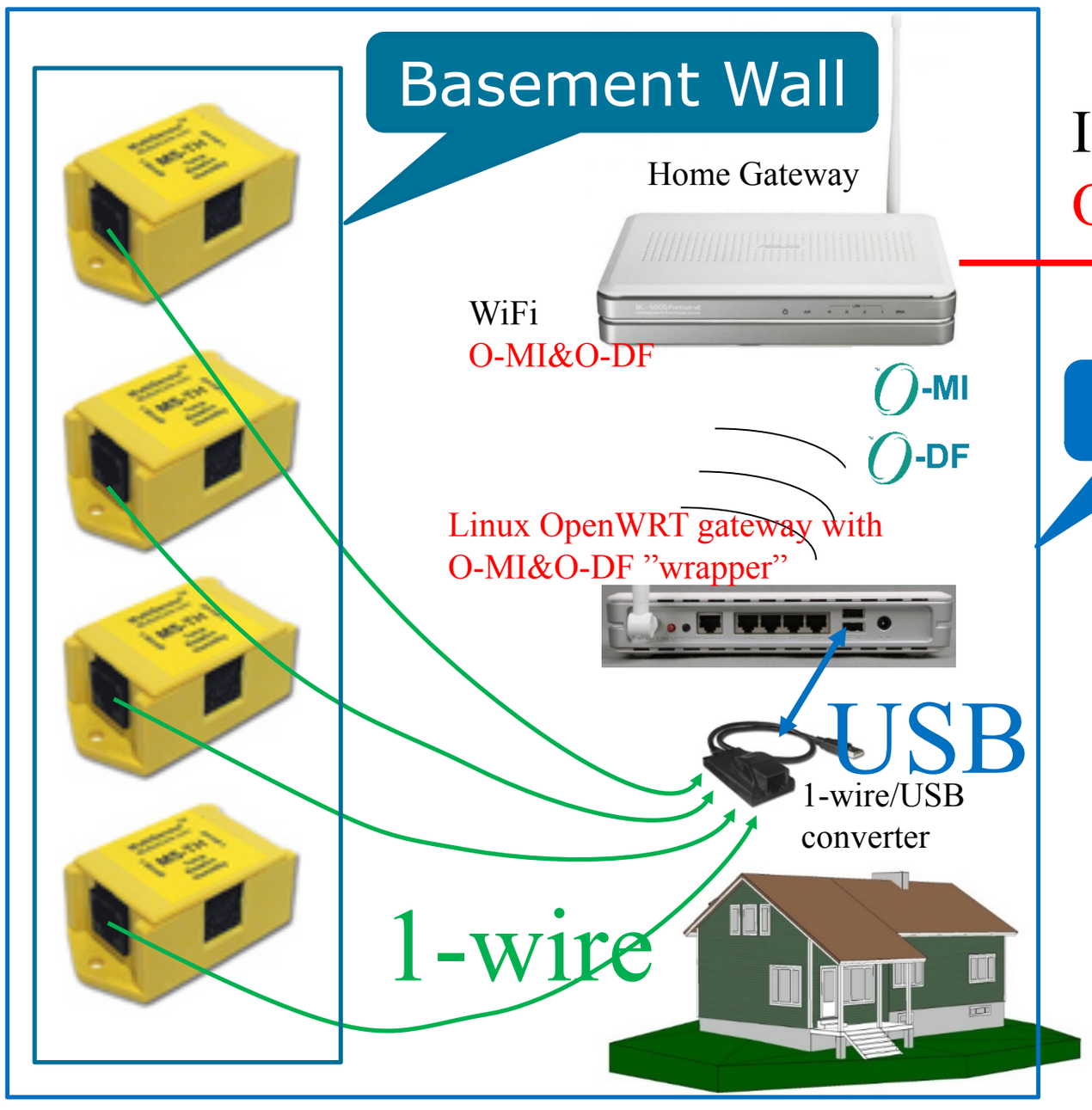
Access Control Management UI



Making it work



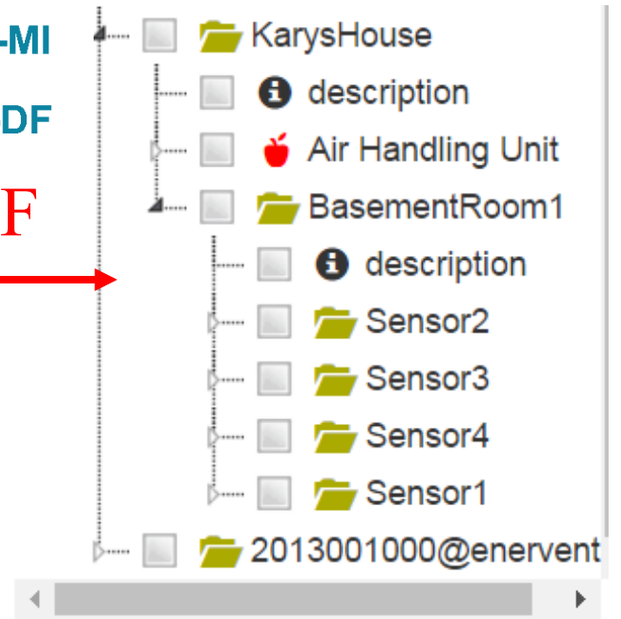
Sensoring using 1-wire sensors



O-MI&O-DF Reference Implementation Sandbox

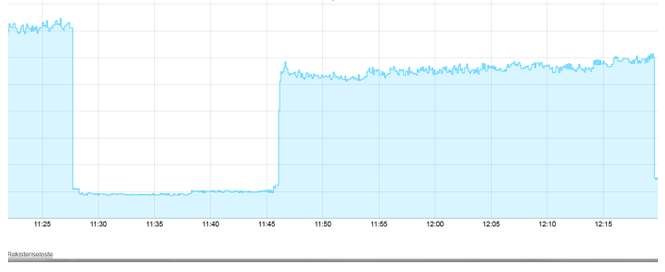
Internet
O-MI&O-DF

O-MI
O-DF



Internet
O-MI&O-DF

O-MI
O-DF



User Interface

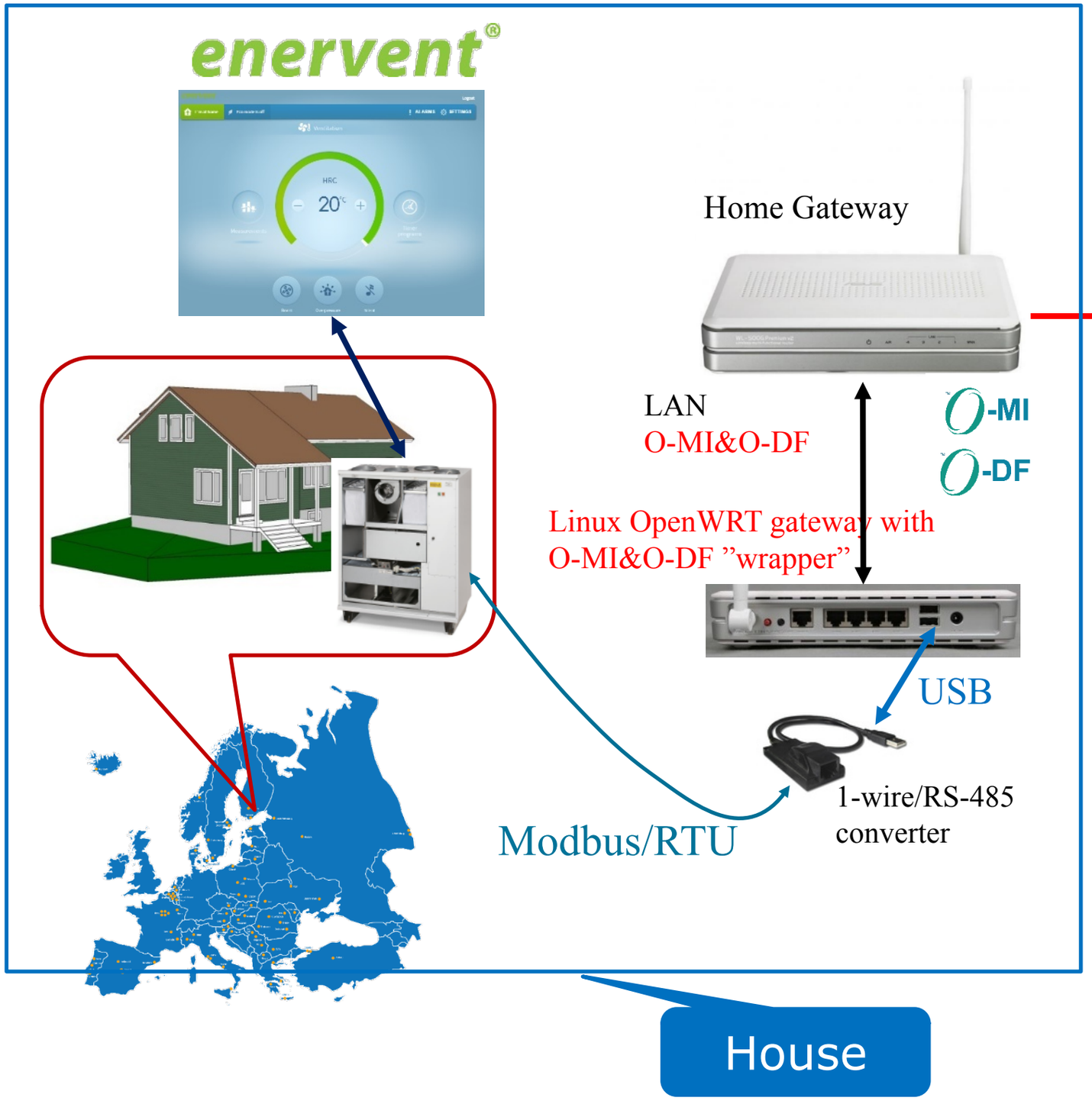
THE Open GROUP
Making standards work®

1-wire sensoring ”under the hood”

- Retrieve sensor values, create O-MI write with O-DF payload
  - Shell scripts running on OpenWRT Linux, about 20 lines of code
- Send with **curl**:

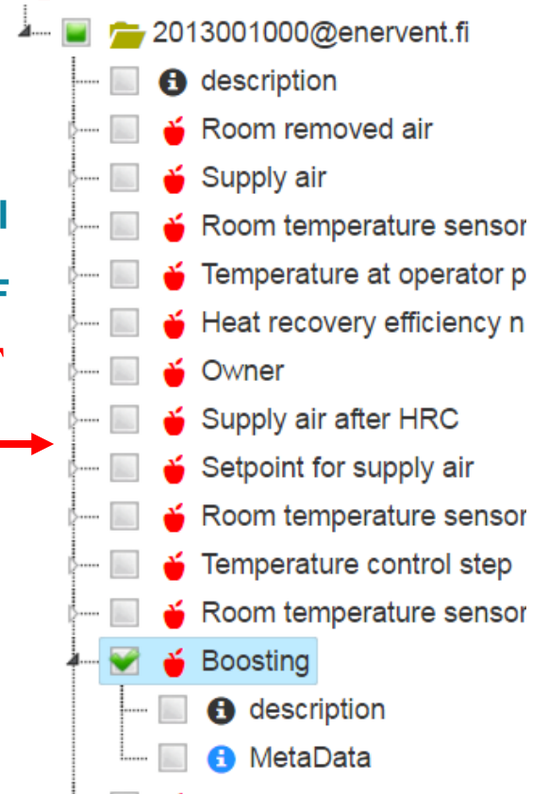
```
*/10 * * * * /usr/bin/curl --header "Content-
Type:text/xml;charset=UTF-8" --cert-type "pem"
--cert "/root/client.pem:xxx_xxx" --cacert
"/root/chain_TERENA_SSL_CA_2.pem" --data
"`/root/test_omi_write.sh`"
"https://otaniemi3d.cs.hut.fi/omi/node/" >
/dev/null
```

Air Handling Unit

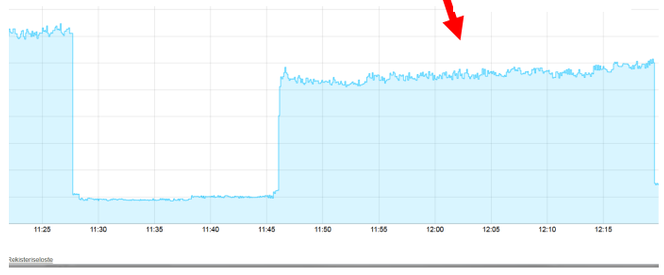


Internet
O-MI&O-DF

O-MI&O-DF Reference Implementation Sandbox



Internet
O-MI&O-DF



User Interface

THE Open GROUP
Making standards work®

Air Handling Unit "under the hood"

- Retrieve sensor values, create O-MI write with O-DF payload
  - Shell script running on OpenWRT Linux, about 3 lines of code per value to retrieve
- Send with **curl**

```
*/10 * * * * /usr/bin/curl --header "Content-
Type:text/xml;charset=UTF-8" --cert-type "pem" --
cert "/root/client.pem:XXX" --cacert
"/root/chain_TERENA_SSL_CA_2.pem" --data
"`/root/test_omi_write.sh`"
"https://otaniemi3d.cs.hut.fi/omi/node/" > /dev/null
```

Recall: Security specifics for IoT

- Most security basics and existing technologies applied as such
- Available operations specified by O-MI
- Access Control specified using O-DF Objects and InfoItems
- Remaining challenges:
  - Certificates are currently signed by the receiving O-MI node
  - Distribution of identities (/certificates)?
  - Device-level, owner-level, organization-level, … certificates?
  - How to update certificates before they expire?
  - How to manage software updates to all those devices behind firewalls etc?
  - Current and Future operations in O-MI: Callback, Execute, Delete
  - Generic requests based on Object type etc: O-DEF (Open Data Element Framework) could help!

Trust-based Identity Overlay model

Example: Car arriving in town

Find parking place close to …

I'm driving in street xxx, location yyy

Street temperature is…

Just drove into hole in the street!

Need to charge my EV battery, N kWh…

ESP system activated, slippery!!

Parking/ EV charging place reserved…

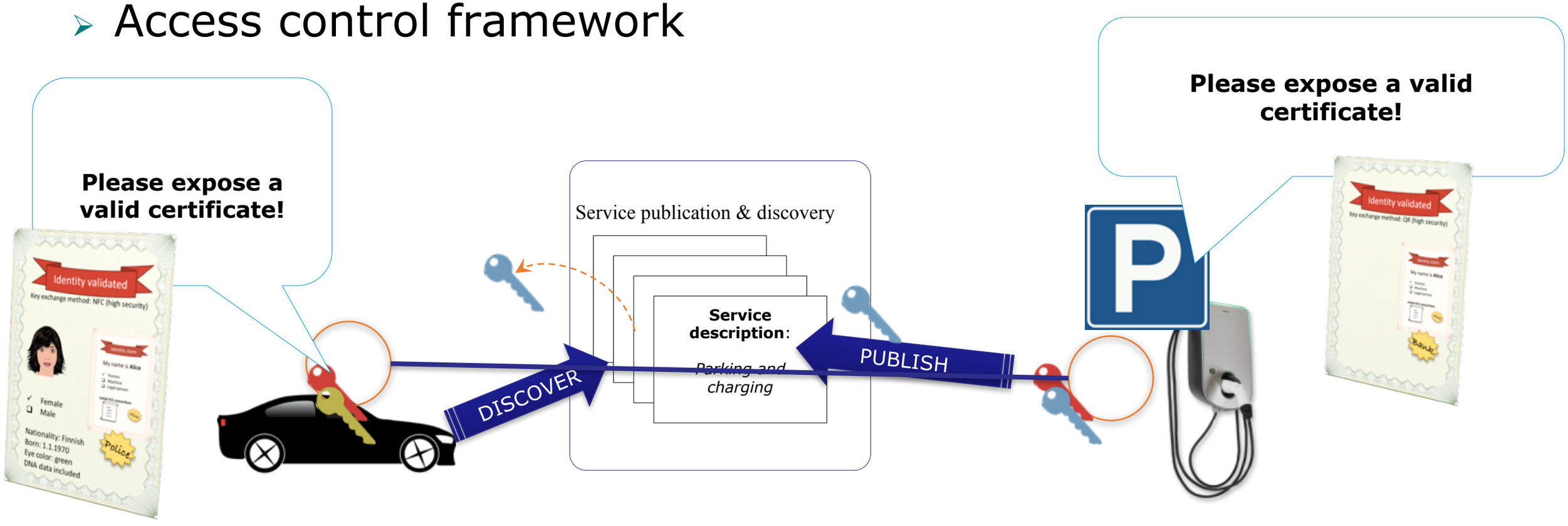
Hole in road 100 meters ahead!

Slippery 100 meters ahead!

School class crossing street in 5 minutes, change route!

Trust framework

- Establish mutual trust, with ad hoc connections, no implicitly trusted third party
- Establish secure inter-service communication, peer-to-peer (authentication, encryption)
- Own identities for each service
- Access control framework



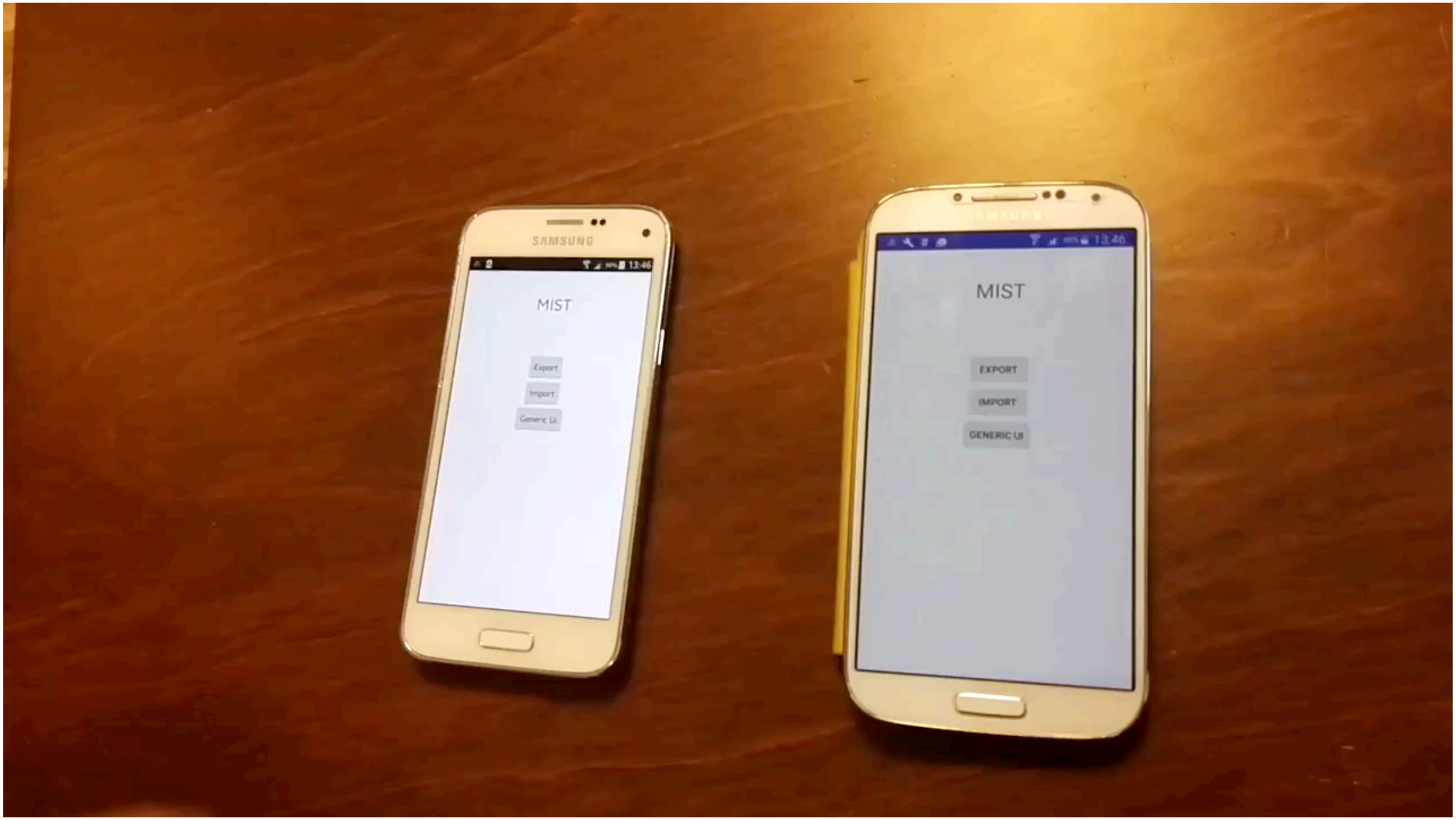
Aalto University
School of Science

ControlThings
Excellence Embedded

THE Open GROUP
Making standards work®

Create trust-relations (visually explained)

Length: 0:58



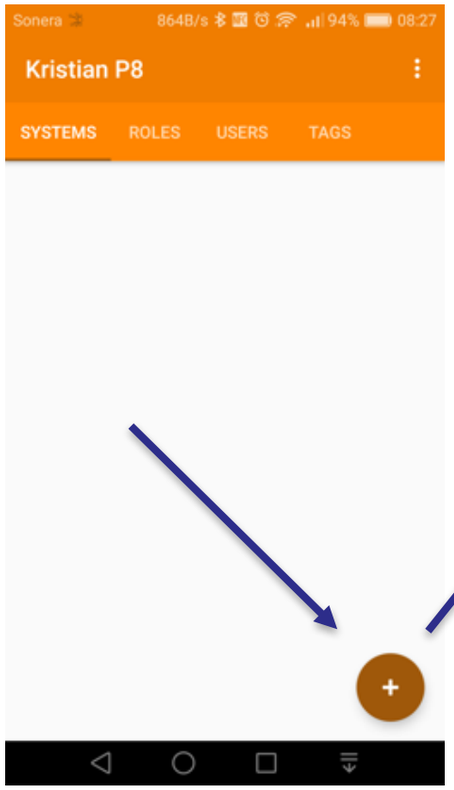
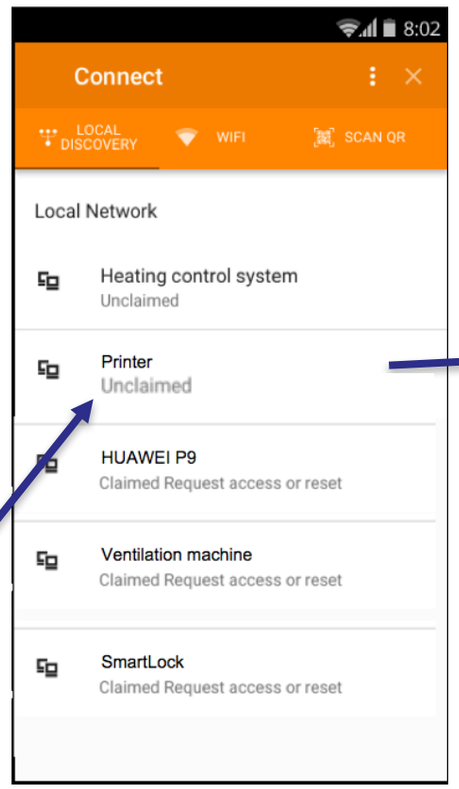
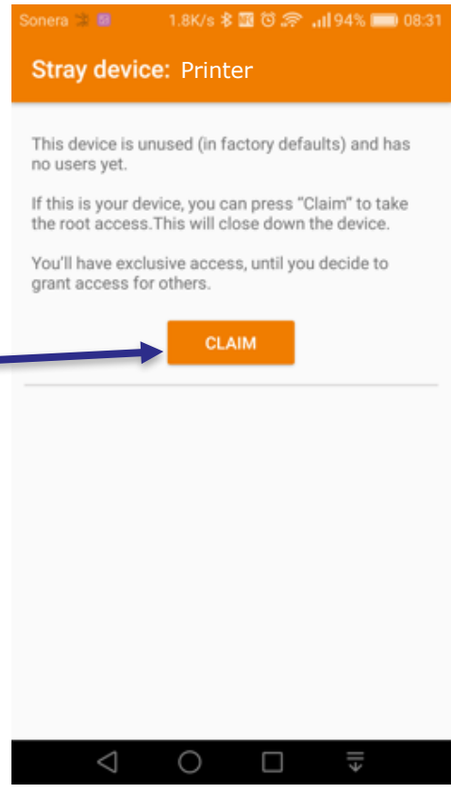
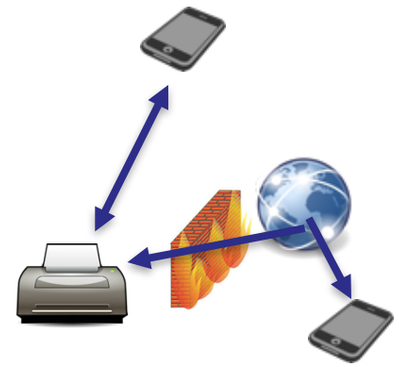
Trust-relations are roaming, even though both are moved to different NAT networks!

Aalto University
School of Science

ControlThings
Excellence Embedded

THE Open GROUP
Making standards work®

Commissioning

1. Power up a new Printer	2. Add a new system in app	3. Use discovery	4. Take the root account	5. Access remotely and locally
				
	The Printer is ready to be accessed from an Android device on the same local subnet.	The trust-based stack will automatically detect available systems	The first user can take the root account (like when setting up a computer). This closes down the bus for future claiming attempts.	Access and control, even without cloud services. No need to configure any firewalls, NAT servers. No need for IP address or hostname hassle

MIST video

- Identity based communication.mp4
- From 4:45

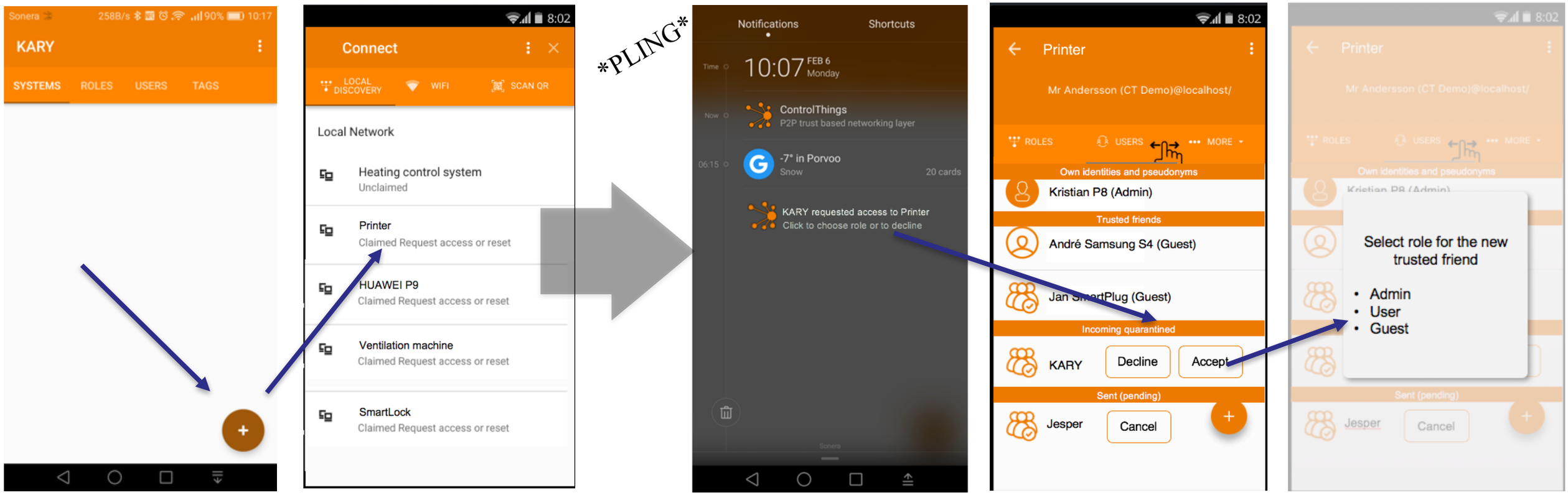
Discovery, access request

Others can discover the Printer

..and request access

The admin will receive the request

…and makes a decision



Several parallel methods for creating trust-relations are supported, this is only an example.
Invitations can be sent over social media, email, etc.

Conclusions

- IoT security basics are same as for any system
- However, IoT also gives many new challenges
- Most ”IoT standards” tend to focus on communication in IoT and tend to neglect security aspects, such as Access Control
- The Open Group IoT standards O-MI and O-DF provide similar Access Control mechanisms as file system based Access Control
- Much remains to do for securing IoT systems on all levels

Thank You!