

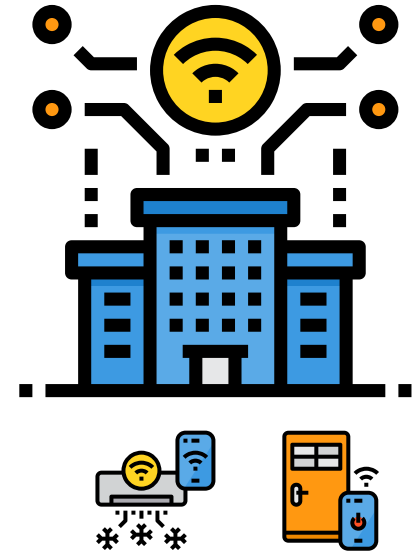
IoT Device Ownership when ownership is complex

Michael Richardson <mcr+ietf@sandelman.ca>
IETF IOTOPS WG

draft-richardson-iotops-iot-iot-01

Door Locks

- Everyone has them.
- Simplest IoT actuator
- What did you do last time you were locked out?
- Does your neighbour have a spare key?
- Do you have your neighbour's spare key?
- How many people have your keys?



Smart Building
Multi-tenant
Many changes

How do you delegate access?

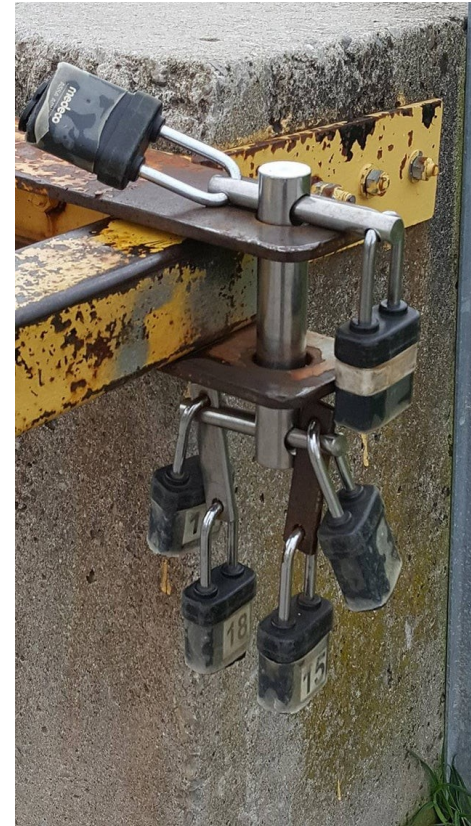
- There is the kerberos-ticket-like way
 - The realtor lock.



What about multiple people?

- This is a 6-way OR gate
 - Unlocking any of the padlocks will allow this gate to open
- It presents an interesting audit problem
- First time I saw this kind of thing, I thought it was some kind of art installation.

https://www.reddit.com/r/ProgrammerHumor/comments/6ehxli/or_gate/



How does the mailman enter?

- In France, with



How do police/emergency get in?

by force if they have to (warrant?!)



How do police/emergency get in?

by force if they have to (warrant?!)



How do police/emergency get in?

by force if they have to (warrant?!)



police-rescue-sex-doll

How do police/emergency get in?

by force if they have to (warrant?!)



How do police/emergency get in?

by force if they have to (warrant?!)



How do police/emergency get in?

by force if they have to (warrant?!)



Intro to Line of Duty show

When you are locked out?

- Locksmith will drill out the lock
- The replace it.
- Then you give out keys
- How does locksmith know you are authorized?



When DNSSEC was drilled

- “some lucky locksmith in Los Angeles is going to have to drill out the safe’s locking mechanism and put in a new one”



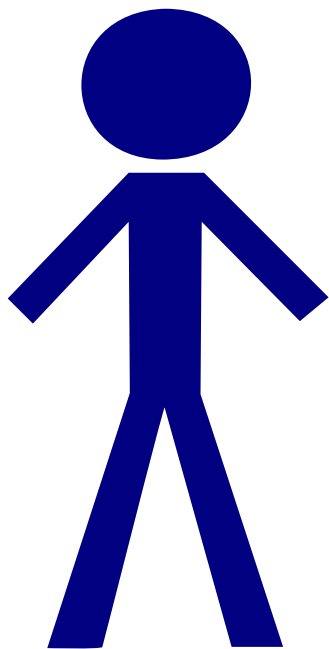
https://www.theregister.com/2020/02/13/iana_dnssec_ksk_delay/

Authorization and Auditing

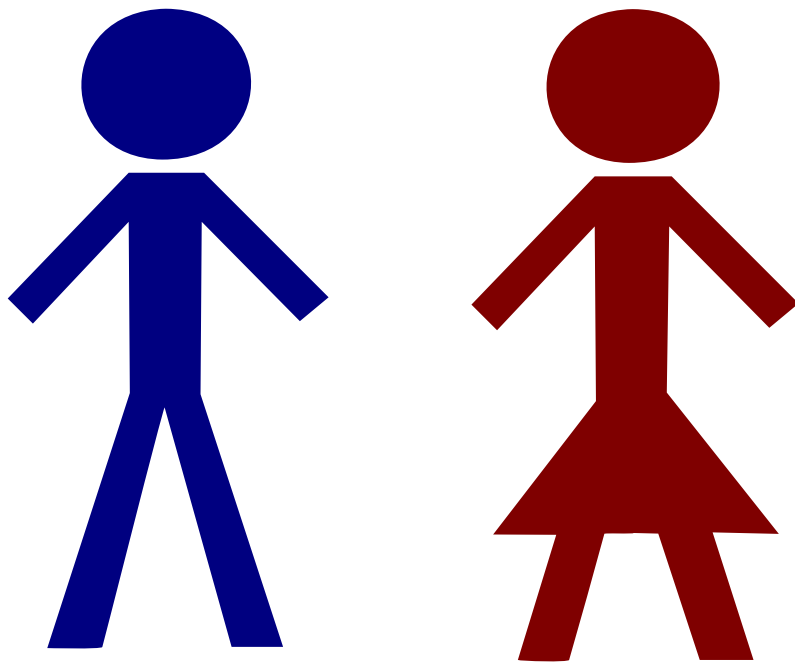
- Who is allowed to open your door?
- Who is allowed to change the list of who can open your door?
- When your door is opened, who gets to know about it?
- It's not just about your door. It's about everything “smart” in your house
- do you want to drill out your furnace?

Authorization for YOU?

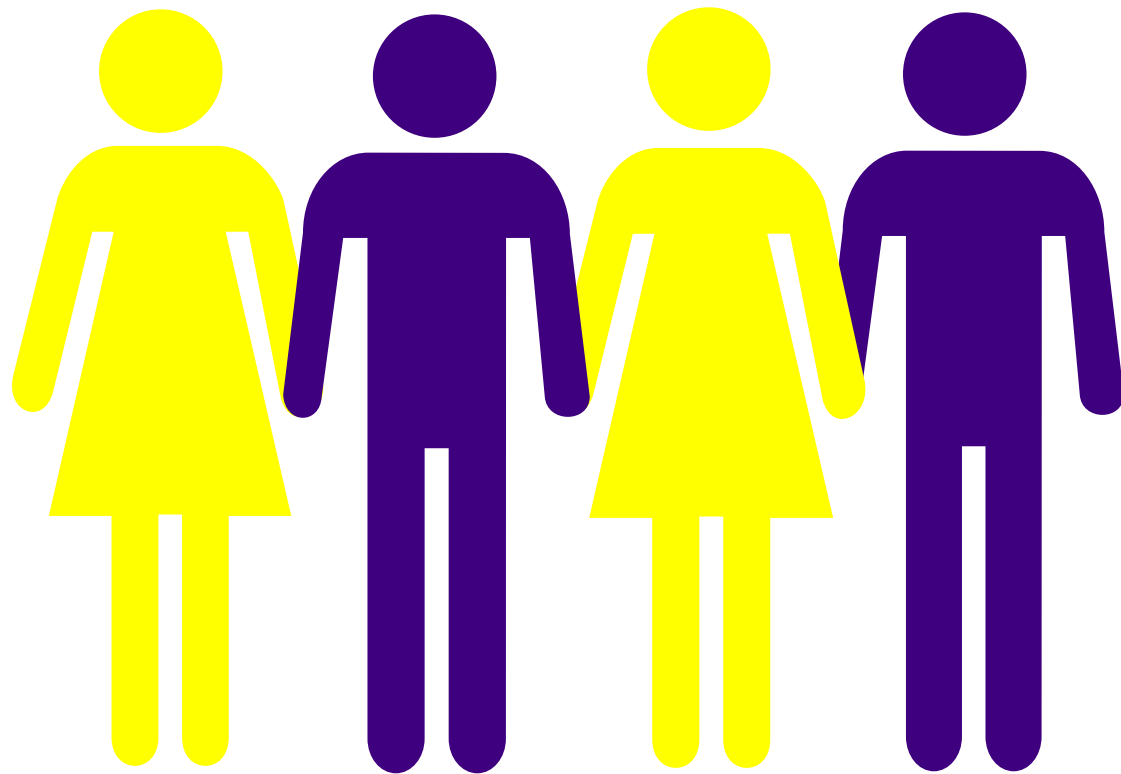
Authorization for YOU?



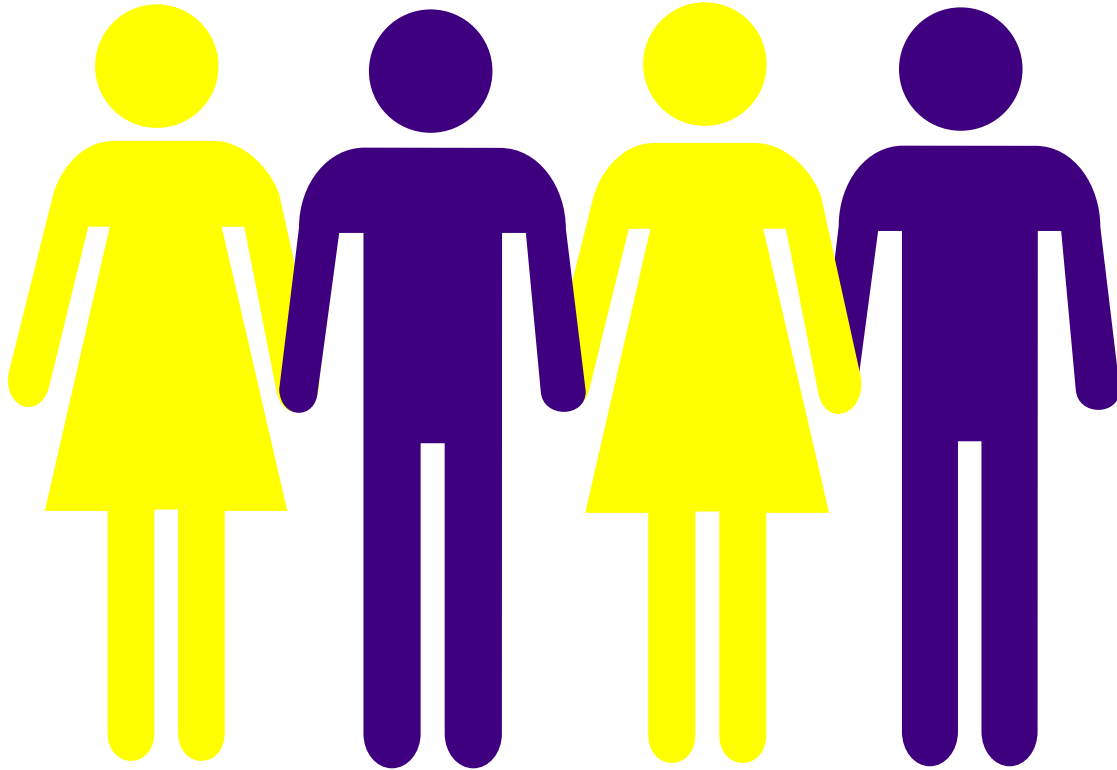
Authorization for YOU?



Authorization for YOU?



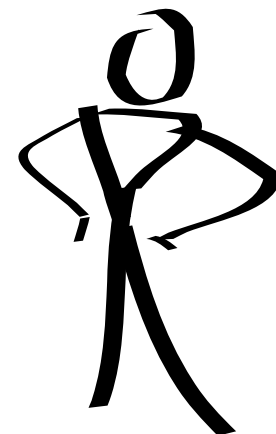
Authorization for YOU?



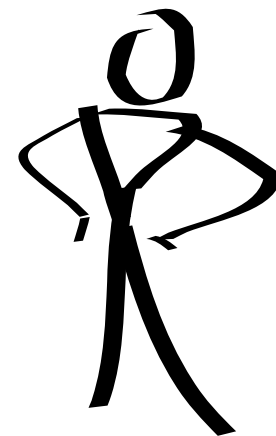
Authorization for YOU?



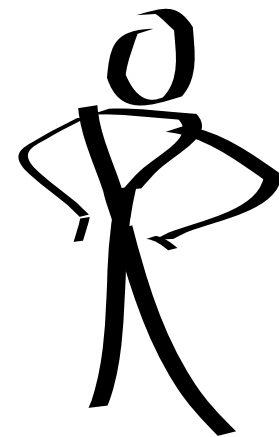
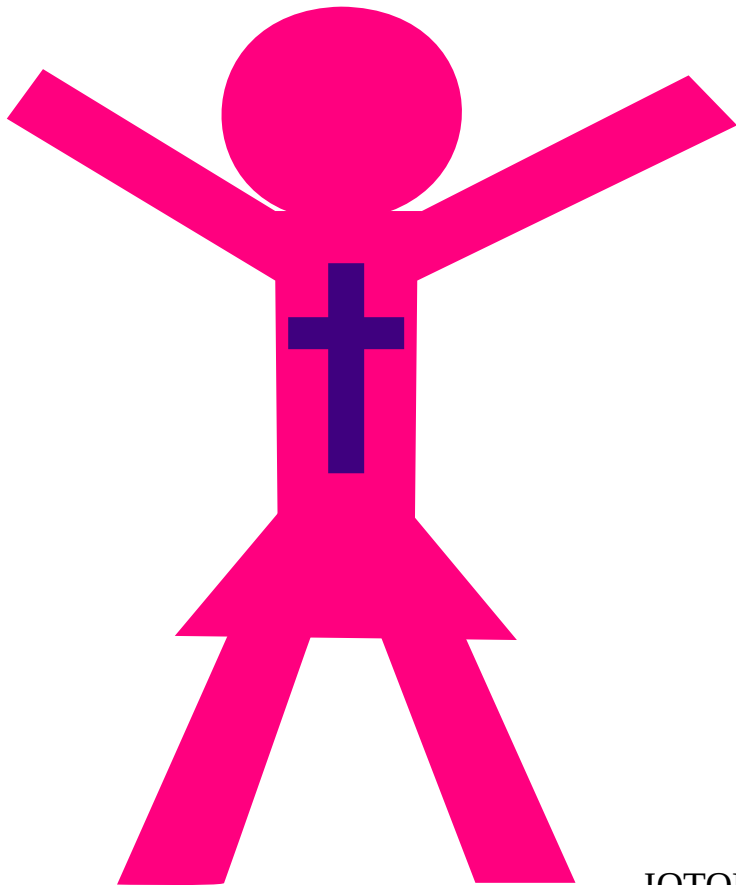
Authorization for YOU?



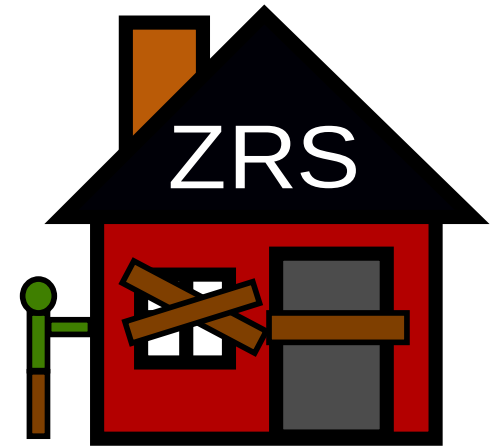
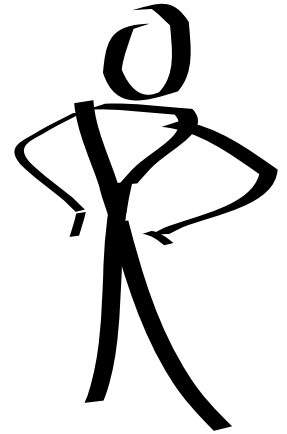
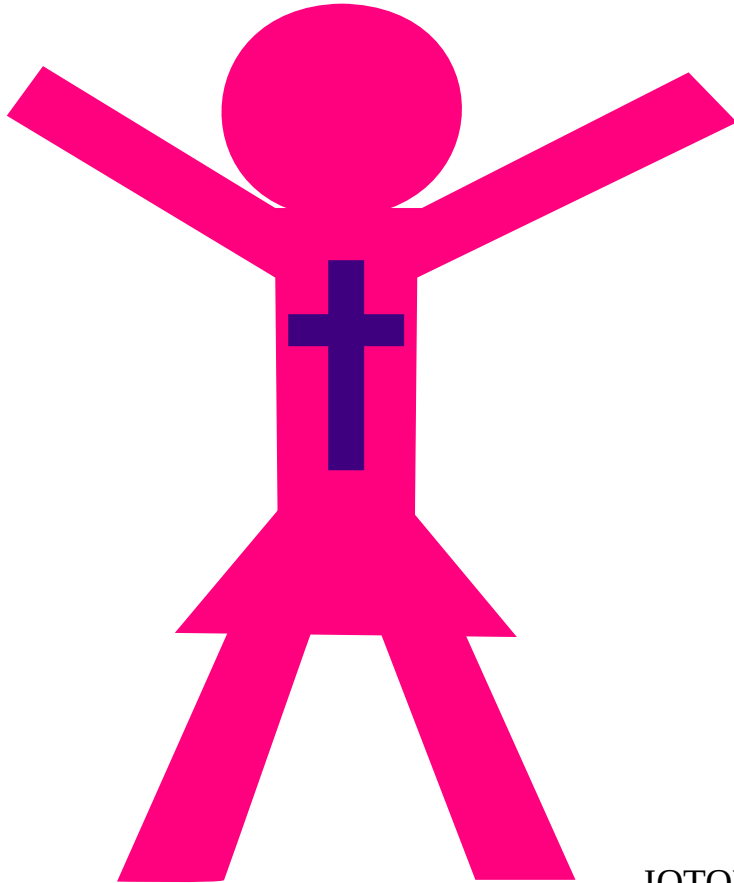
Authorization for YOU?



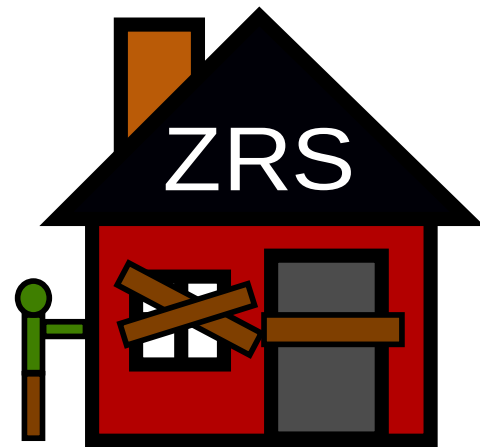
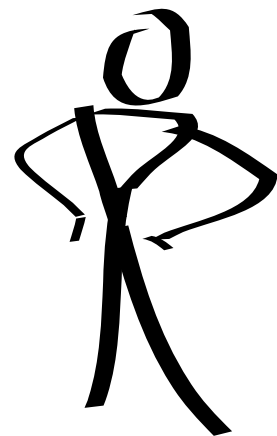
Authorization for YOU?



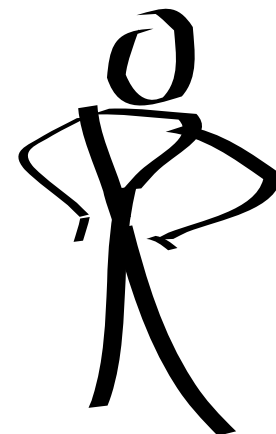
Authorization for YOU?



Authorization for YOU?



Authorization for YOU?



Backdoors?

- Backdoors are things installed without your knowledge.
 - recently associated with malware
 - historically, installed by manufacturer
- Not a backdoor (it's a front door...)
- Visible
- Auditable (when used, and when installed)
- not a secret

Escrow?

- Key Escrow involves turning a copy of private key over to third party
- There are variants for communication security, where the session key is encrypted only
- This is more about a kind of escrow for authorization
- All concerns with attacks on key escrow agents (key holders) would apply, however.

Why standardize?

- a common authorization language will be better understood
- a common system will have better analysis
- all arguments about common libraries and bugs and the like apply
- auditing of rules, and auditing of access log
- third parties need standardized systems
 - with standardized kinds of liability
 - police, banks, lawyers, judicial oversight, oversight of LE

Is this an IETF problem?

- I dunno.
 - maybe? maybe not
 - OASIS also worked on this
- SASL, KeyNote, SPKI, ...
- constrained systems seem to thrive here
- SUIT and TEEP are here, and there are profound authorization issues in who can run what software, or perform updates

Discussion

