

SECURE IoT HOME GATEWAY & HOME REGISTRY IDEA



cira.

BUILDING A BETTER
ONLINE CANADA

Jacques Latour, CTO
Canadian Internet Registration
Authority

Nov 15, 2017

TODAY'S HOME NETWORK & IOT IMPLEMENTATION ARE DISPARATE, KIND OF SCARY & NEED STRUCTURE!



THE HOME NETWORK OF THE FUTURE SHOULD BE SAFE, SECURE AND SIMPLE TO USE!



THE HOME NETWORK SHOULD BE REACHABLE FROM THE INTERNET SEAMLESSLY AND SECURELY



MAYBE EVEN YOUR CAR SHOULD BE CONNECTED TO YOUR HOME NETWORK



because your home is bigger than your house

AND THE HOME NETWORK GROWS TO INCLUDE PERSONAL AND WEARABLE IOT, INSIDE AND OUTSIDE THE HOME...



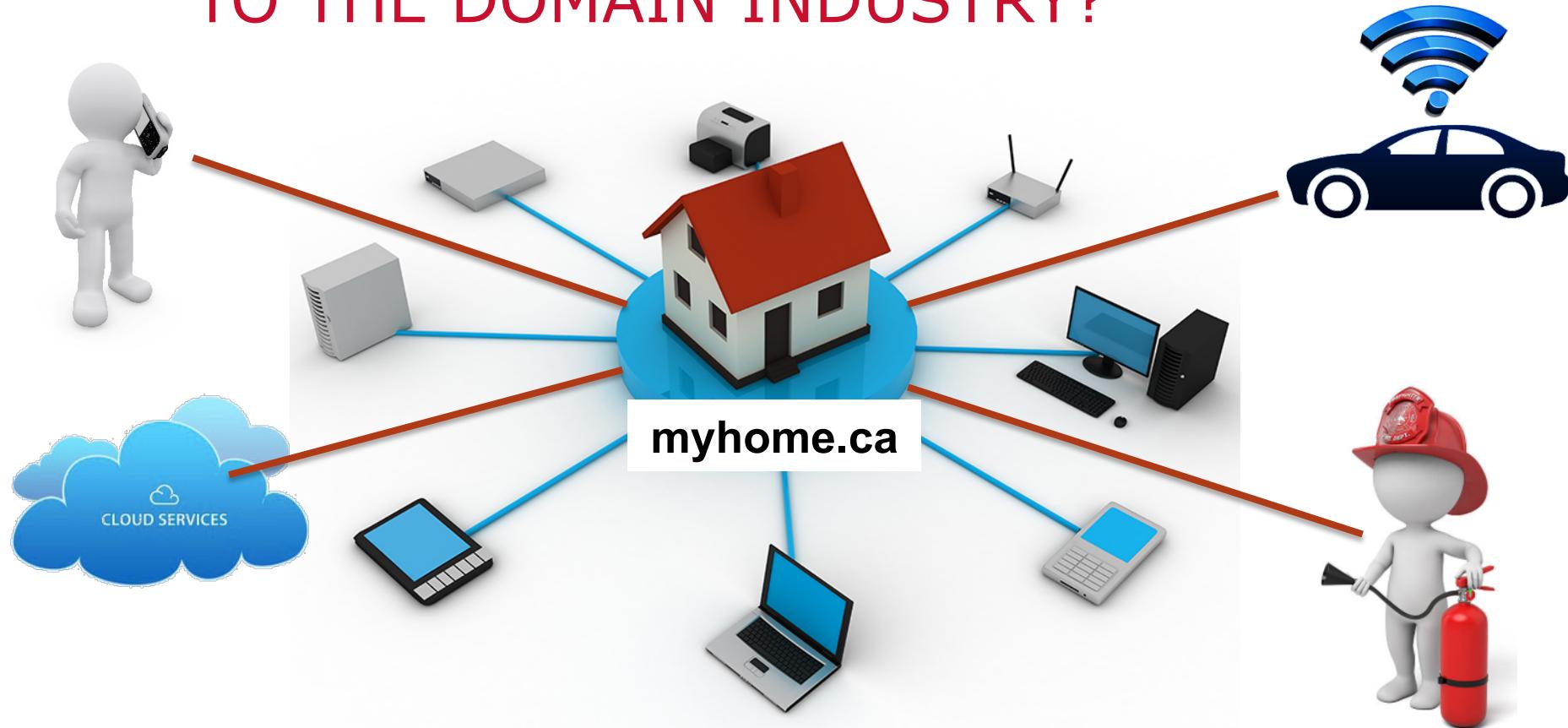
YOUR HOME NETWORK BOTH INTERNAL
AND EXTERNAL TRAFFIC SHOULD BE
SECURED USING A COMMON KEY



DO I NEED TO SAY MORE?

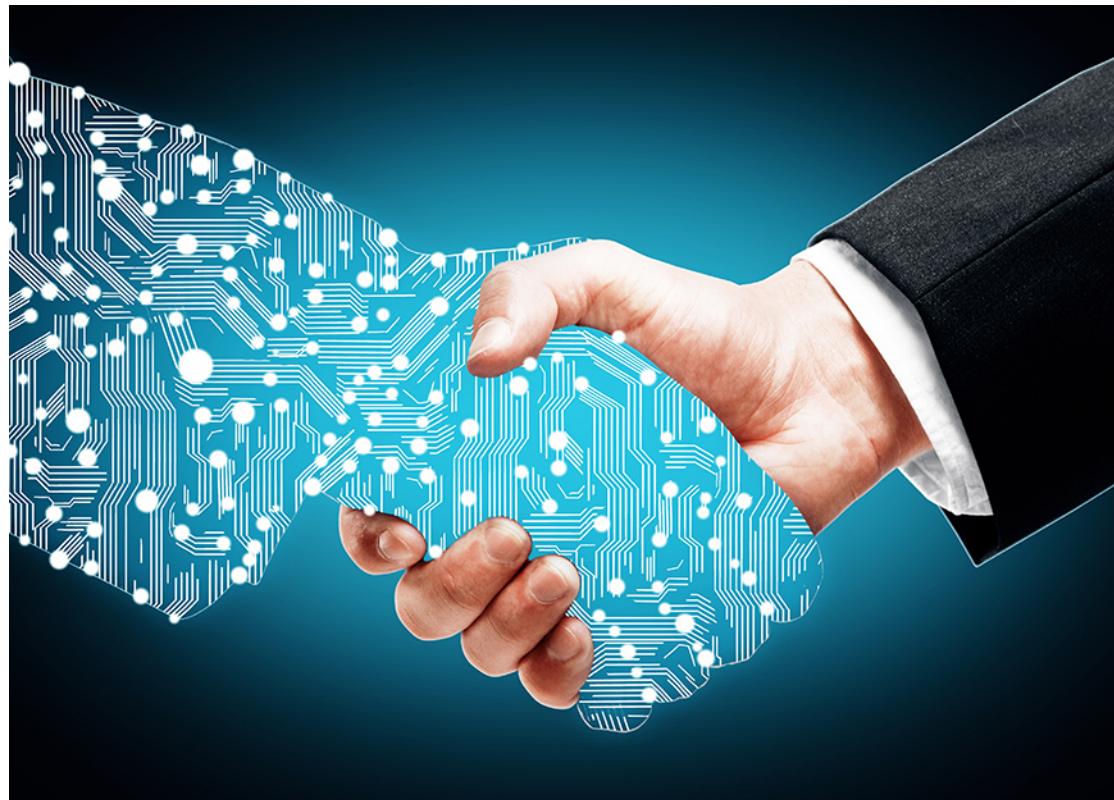


SERIOUSLY, WHAT DOES THIS BRING TO THE DOMAIN INDUSTRY?



A domain name per household!!!

LEVERAGING THE CHAIN OF TRUST IN DNSSEC AND SOME INNOVATION TO CREATE A SECURE HOME NETWORK PLATFORM



HOME.ARPA.

DRAFT-IETF-HOMENET-DOT-14

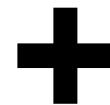
- IETF working on making the default home network address: [home.arpa.](#)

<<The naming mechanism needs to function without configuration from the user. While it may be possible for a name to be delegated by an ISP, homenets must also function in the absence of such a delegation.>>

- Let's make delegated "home" domains function without user configuration!

THE FOCUS IS ON AUTOMATION

Registry
Automation



Home Network
Automation

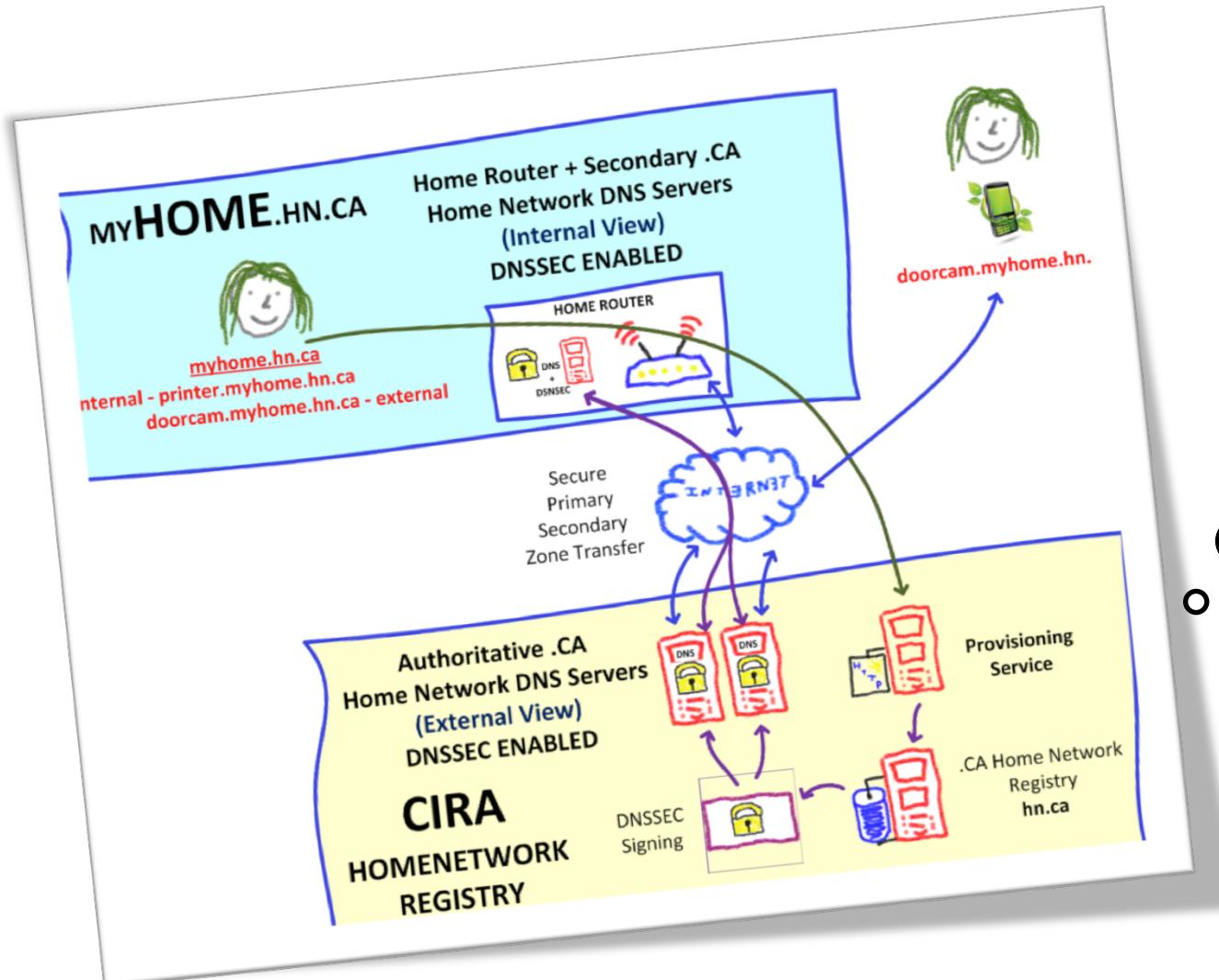


Innovation

YOUR LOCAL CCTLD WILL PROVISION YOUR DOMAIN, SIGN IT WITH DNSSEC AND ESTABLISH A SECURE CHAIN OF TRUST TO YOUR HOME GATEWAY, MAGICALLY SOLVING ALL YOUR WORRIES AND KEEPING YOUR ONLINE FAMILY SAFE ☺



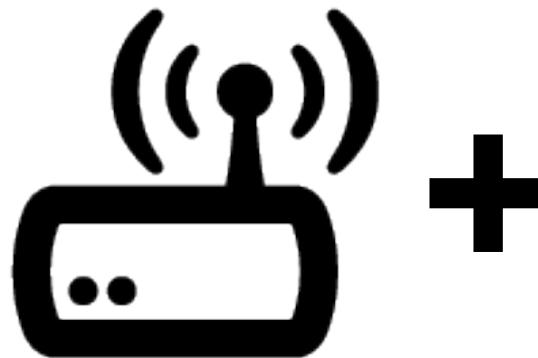
REMEMBER, IT'S AN IDEA. SO FAR IT LOOKS LIKE THIS...



That's
Supposed to be
a napkin
design

STEP 1

- When you buy a home gateway, it comes bundled with a .CA home network domain



A 2nd or 3rd level domain
i.e. myhome.net.ca
i.e. myhome.ca

RFID card
(Code to activate
provisioning and
domain)

STEP 2

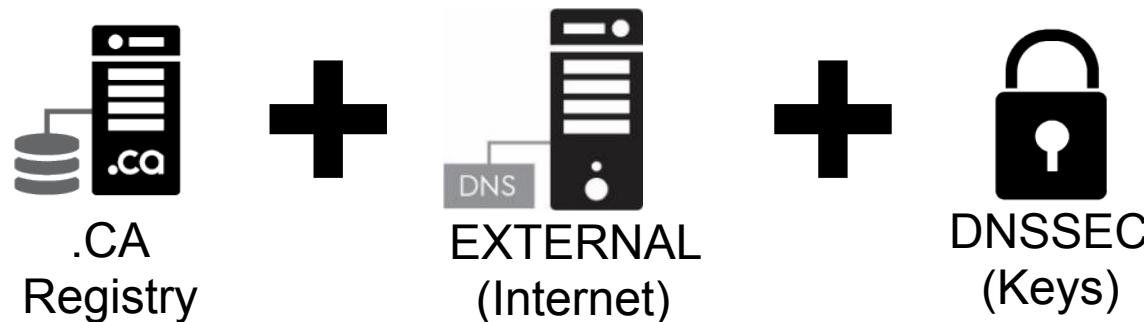
- Then you follow the provisioning instructions
 - Install & open the CIRA Home Gateway app
 - Turn on the Home Gateway
 - “TAP” your mobile to discover the home gateway
 - Pick a domain name, 2nd or 3rd level domain name
 - Enter the secret code (“TAP” RFID card)
 - Home Gateway ready for configuration



myhome.ca +  **code**

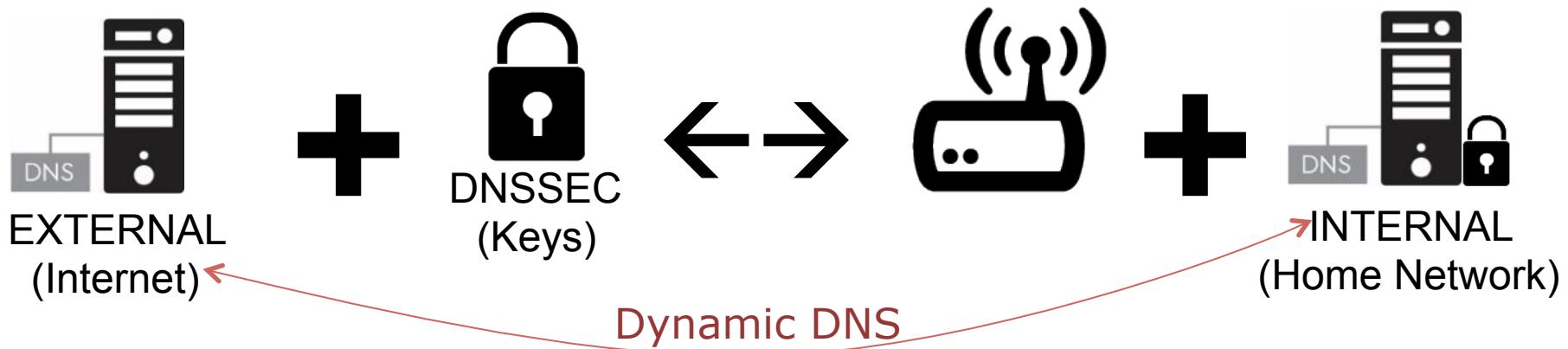
STEP 3

- Automated Backend Provisioning @ CIRA
 - CIRA creates the .CA domain name in the registry
 - CIRA signs the .CA domain with DNSSEC
 - CIRA is primary for the external DNS view of the .CA domain
 - CIRA provides secondary DNS to the .CA domain



STEP 4

- Automated Home Gateway provisioning
 - Establish secure connection to Home Gateway
 - Securely send private DNSSEC key to Home Gateway, setup internal DNS and DNSSEC
 - Configure Home Gateway for DNS integration with registry (à la dynamic DNS) for external services

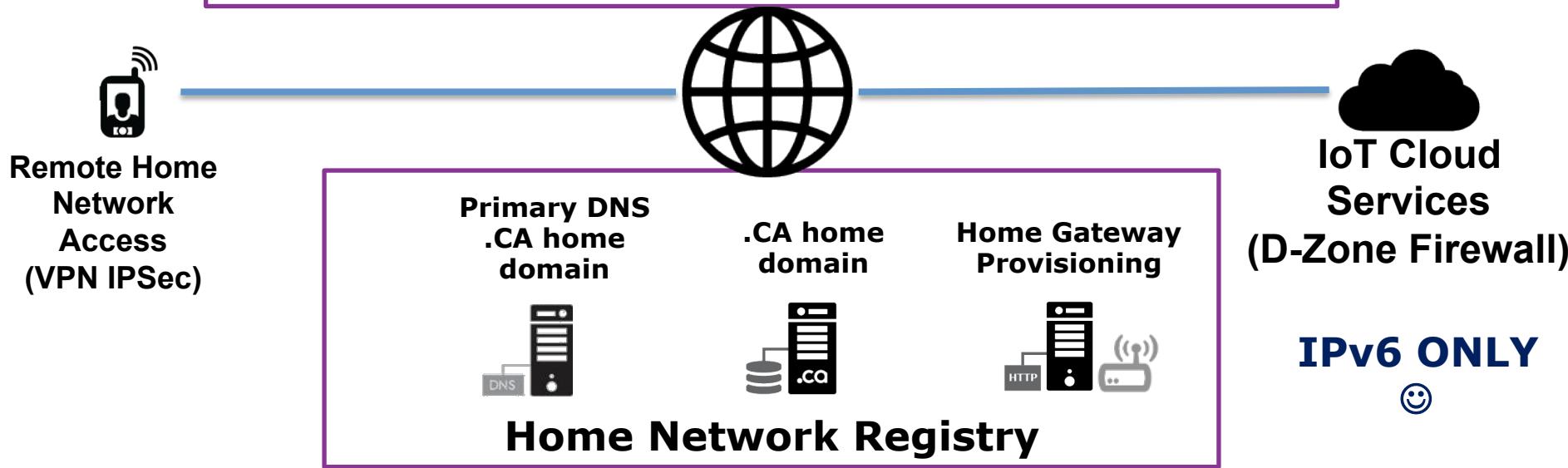
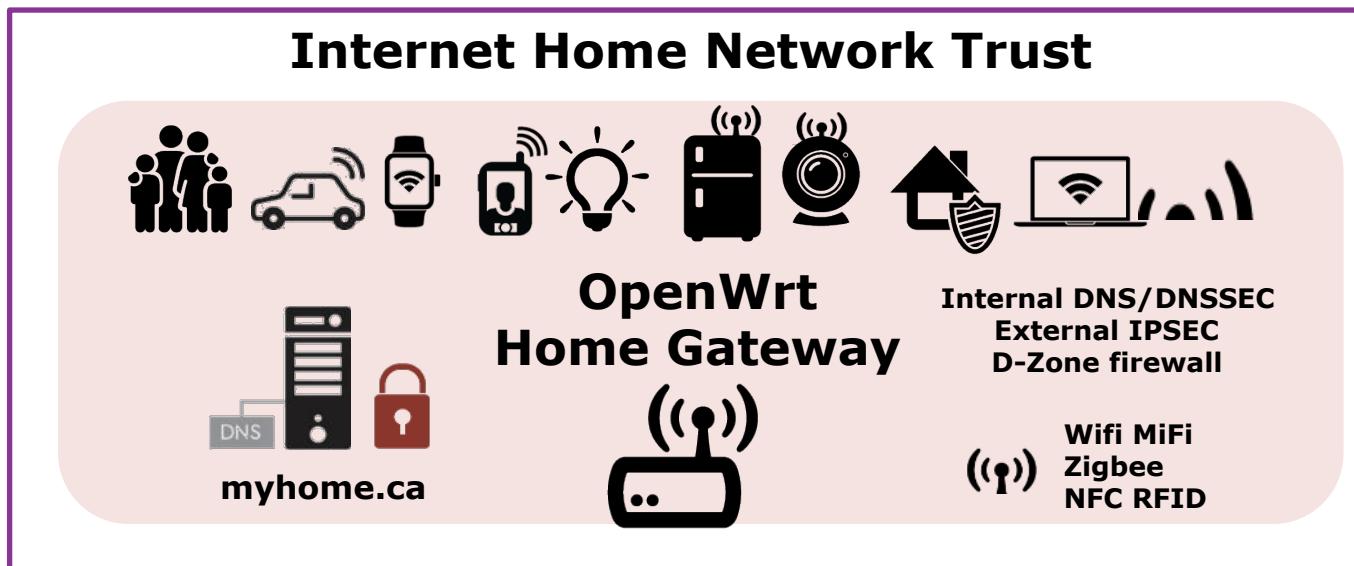


STEP 5

- Setup secure home network infrastructure
 - Using your trusted mobile & the app, “TAP” the Home Gateway to:
 - Learn the WIFI password
 - Get the IPSec password and keys to VPN in your home network
 - Use your mobile and “TAP” all your IoT devices to add on your home WIFI network, easy peasy ☺



HIGH LEVEL BACKEND ARCHITECTURE

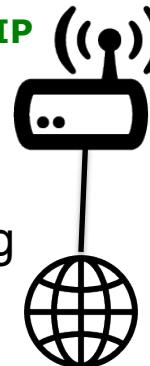


AT THIS POINT WE HAVE

- A home gateway fully provisioned with a .CA domain name, with both internal and external domain name resolution, signed with DNSSEC.
 - WIFI and other networks securely provisioned and setup
- Now we're ready to provision the IoT devices

fridge.la-house-a-latour.ca Internal IP
printer.la-house-a-latour.ca Internal IP

External domain to allow exposing
internal services and make them
available externally

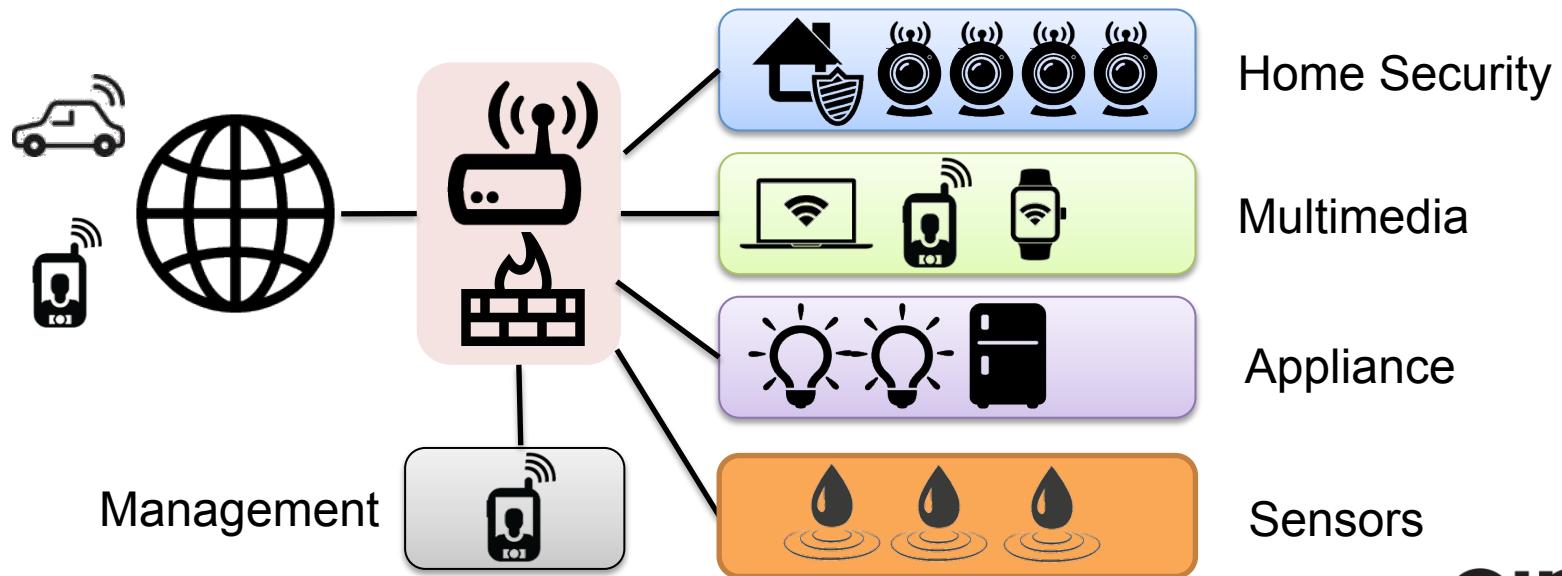


Internal domain fully operational
Secured internally by DNSSEC

vpn.la-house-a-latour.ca External IP

WHAT ABOUT IoT SECURITY? WHAT ABOUT THE HOME NETWORK?

- Protect IoT device
- Rule 1: Place behind firewall
- Rule 2: Segment network by IoT type (NAC)
- Rule 3: Control access to and from the IoT device

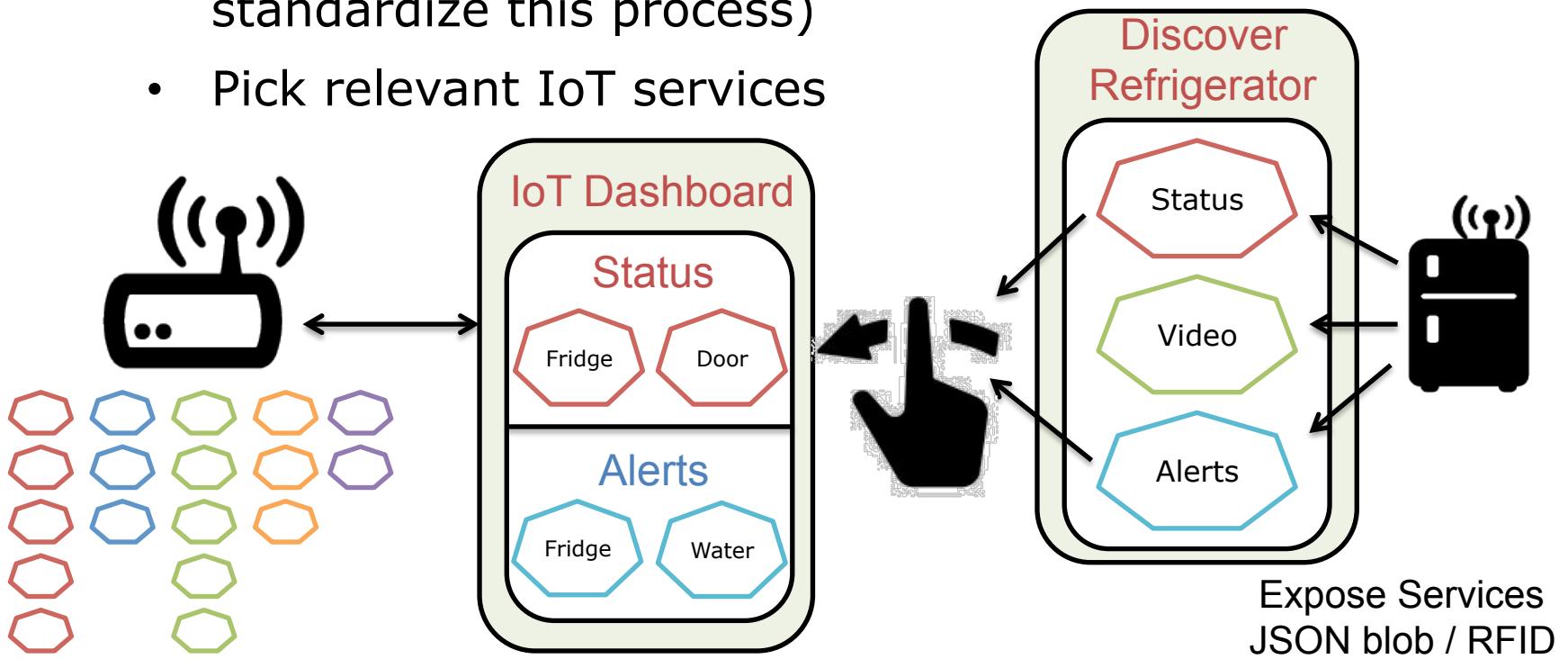


NETWORK ACCESS CONTROL (NAC) & DEFAULT SECURITY CONTROLS

- Something like ; packetfence on openwrt
- Example of default zone security controls / policies
 - Home Security -> may have access to cloud
 - Emergency services may have access
 - Multimedia -> no access to internet
 - VPN may have access this zone
 - Appliance -> no access to internet
 - VPN may have access this zone
 - Allow mydaughter.ca to access
 - my Home Security and my Fridge

NOW, LET'S SEE HOW WE PROVISION IoT DEVICES IN HOME NETWORK

- Once the IoT device has network access, TAP and
- IoT device expose the services available (need to standardize this process)
- Pick relevant IoT services



IoT SERVICE / ACTION TYPE



Status



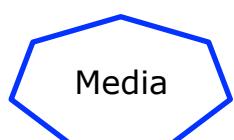
Video



Alerts



Control



Media



Cloud Service

- Status: Up/down, on/off, ok/bad, status variable
- Audio/Video: Camera, video feed
- Media: Audio/Video media feed, TV, music
- Storage: Data storage, NAS (pictures, files, data)
- Alerts: Up/down, on/off, ok/bad, "Water detected"
- Control: Turn up/down, on/off, change device value
- Cloud Service: IoT vendor, Google, MS, DropBox
- VPN (VPN inside myhouse.ca)
- Remote house access
- Other Sensors/ Actuator functions?

WHAT DO YOU THINK?



Want to help?

GOING FORWARD, IT'S A JOURNEY!

- Motivation
 - Ensure long term ccTLD relevance in the future of IoT
- Proposing ccTLD to develop a solution
 - To keep the home network safe and secure
 - To create a secure <**internet home**> IoT environment
 - To leverage DNSSEC as an innovation platform to create a hub for “home trust”
 - That leverages the ccTLD registry expertise
 - To enhance OpenWRT with this functionality

NEXT STEPS

- Develop a Proof of Concept and prototype using .CZ Omnia
- Use public GitHub with functional specification and prototype software
- Research IETF Homenet DNS related drafts/RFC
- Opportunity:
 - Put .CA domains in the forefront as a trusted homenet domain name for personal _HOME_ usage when end to end security is required
 - Sell CIRA Home Gateways

OBSERVATION

- Allocate domains under net.ca, no whois issues
-

The new <Internet Home>

**[https://github.com/CIRALabs/
Home-Network-Registry-Gateway](https://github.com/CIRALabs/Home-Network-Registry-Gateway)**