SECURE IoT HOME GATEWAY & HOME REGISTRY – IDEA & VISION

OPEN STANDARDS DEVELOPMENT

THIS DOCUMENT CHANGES OFTEN

BUILDING A BETTER
ONLINE CANADA

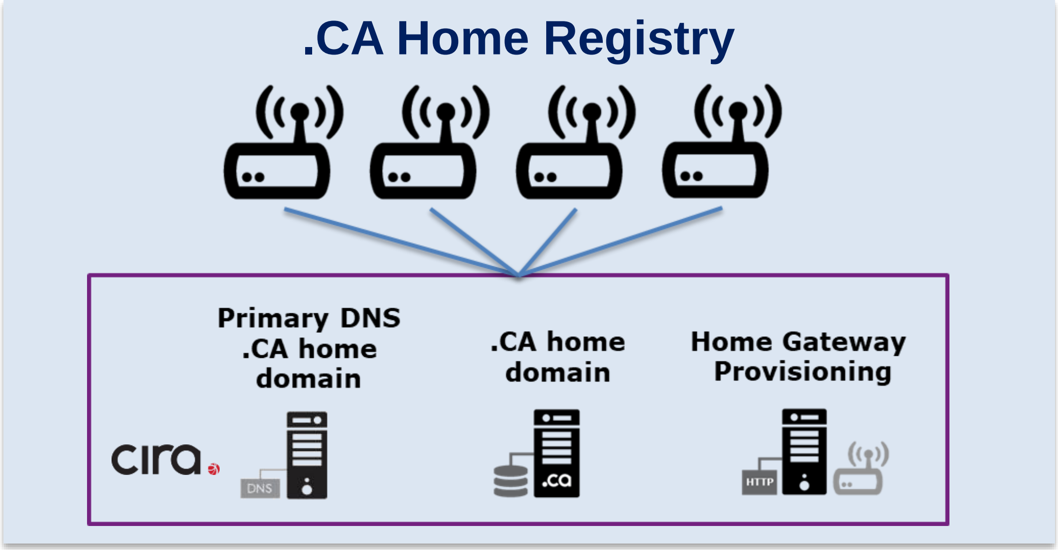
Jacques Latour, CTO
Canadian Internet Registration Authority

May 2018

2 DISTINCT IDEAS INTO ONE SOLUTION

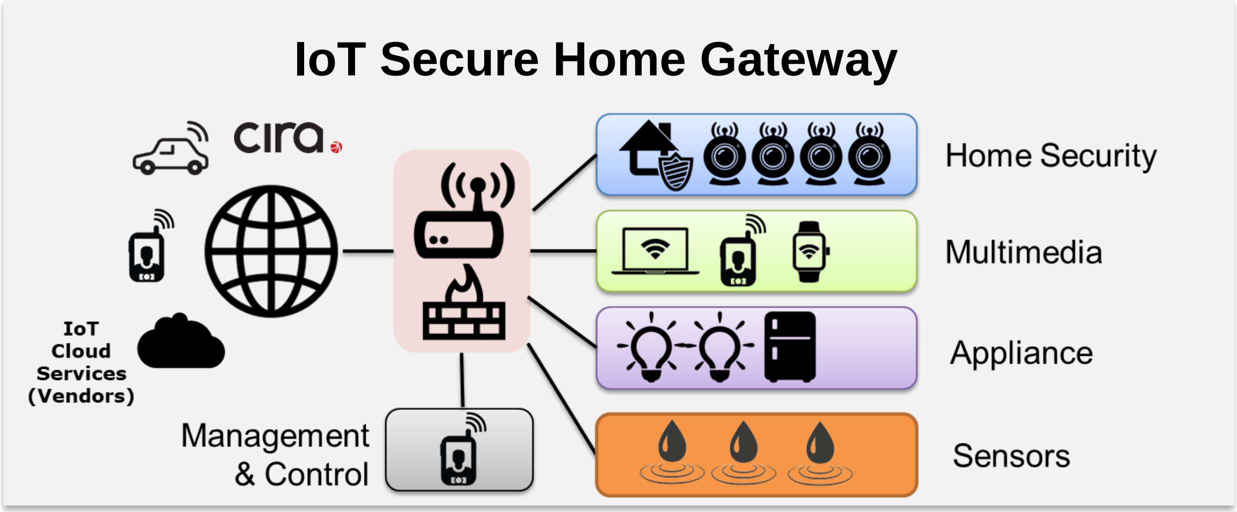
IDEA #1 – ccTLD Home Registry Value Proposition:

- For ccTLD, to have a domain per household
- Leverage the DNSSEC chain of trust by having a registered domain for home use



IDEA #2 – Secure Gateway Value Proposition:

- To create a security framework to protect the Internet from IoT device attacks
- To enhance the home network privacy & security with network access controls



SECURE HOME GATEWAY & REGISTRY IDEA

- For many internet organizations, the #1 risk on their 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
- Protecting IoT devices at the edge is another layer of security that should be further developed
- The security controls would be aimed at protecting the IoT devices from the internet, and to protect the internet from IoT devices.
- The **threat** that **IoT devices** bring is **scale**. The scale of million and billions of IoT device is the threat we need to mitigate.

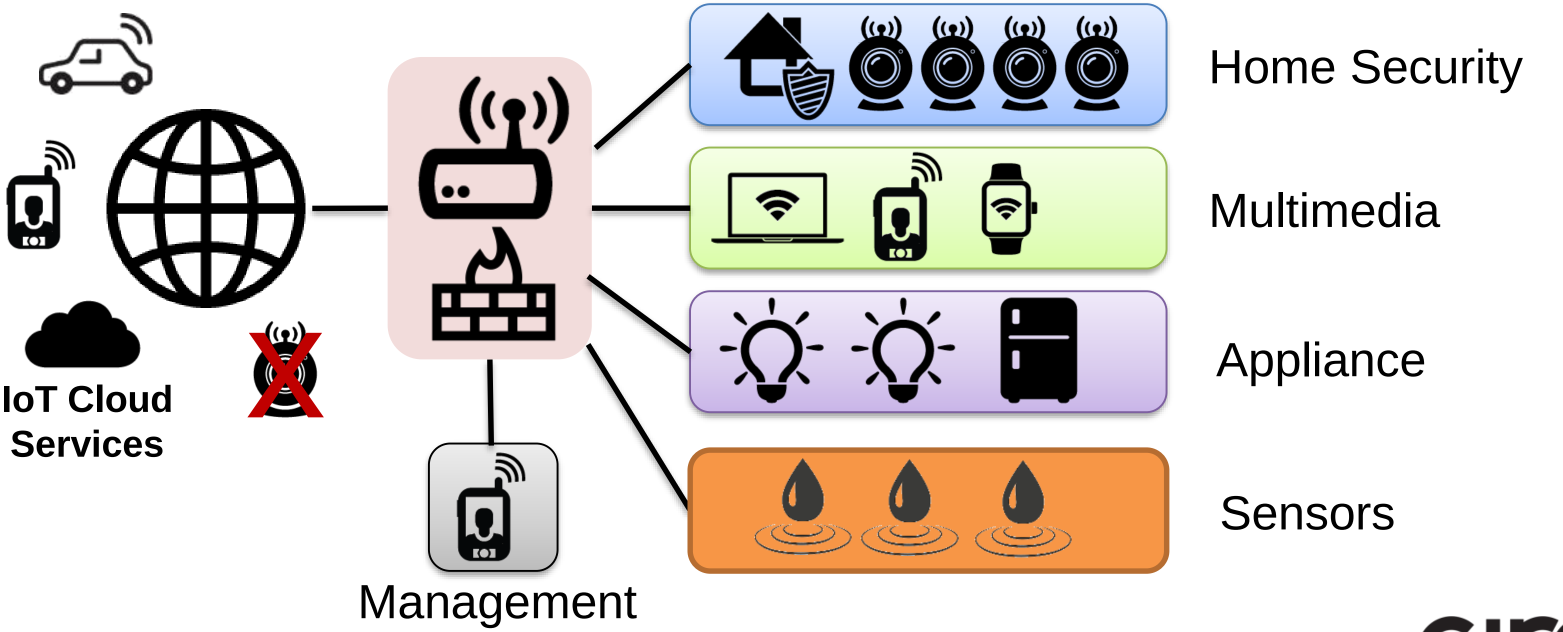
IoT THREAT LANDSCAPE SPECIFIC TO THE INTERNET - **SCALE**

- IoT device compromises:
  - Used in internet attacks i.e. MIRAI/DYN Attack (DDoS) targeting DNS servers (1.2 Tbs)
- IoT traffic reflection and amplification
  - IoT device used to amplification traffic attack (DDoS) NTP, DNS, SNMP.
- The scale of IoT threat landscape and the breath of exploits is what need to mitigated
  - IoT devices must not have wide open internet access (protected by firewall)
  - Inbound and outbound internet access must be controlled

HOW CAN WE PROTECT IoT DEVICES?

Control inbound and outbound network access

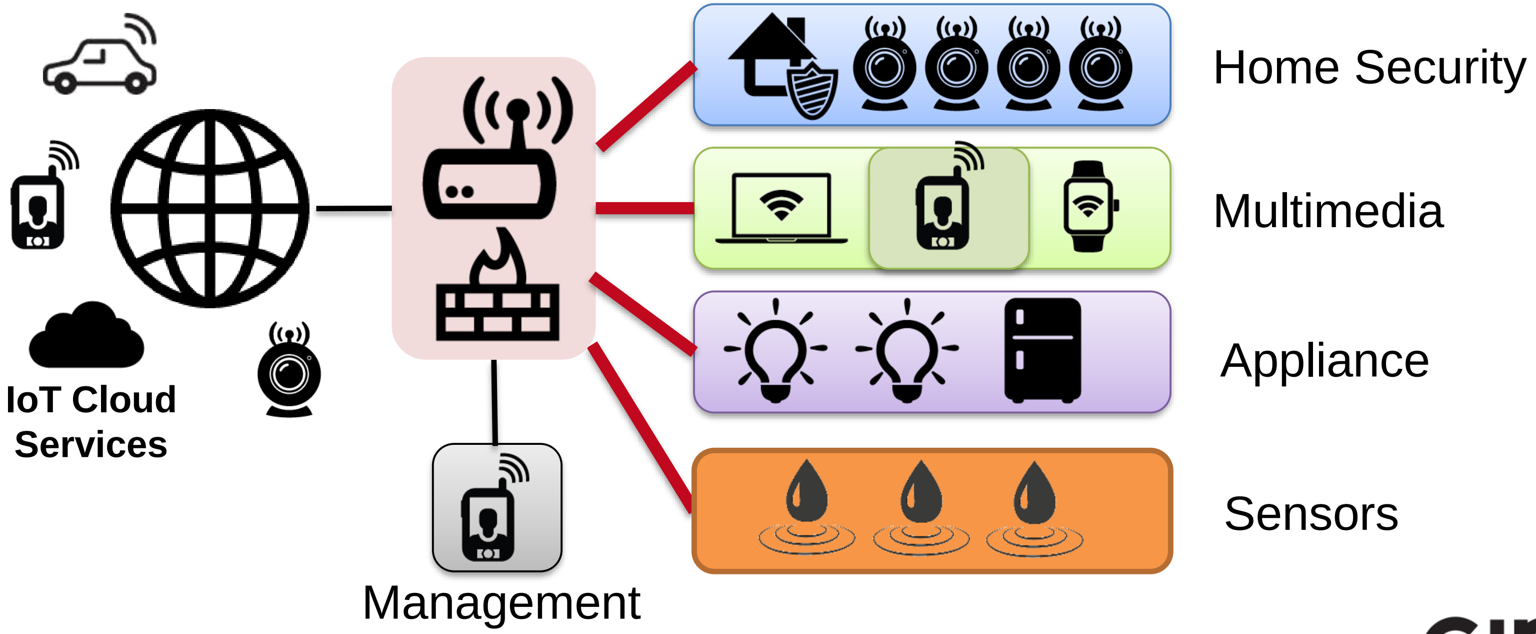
- **Rule 1: Always place IoT behind firewall**
- Rule 2: Segment network by IoT type
- Rule 3: Control access to and from the IoT device



HOW CAN WE PROTECT IoT DEVICES? ONE DEVICE PER VLAN?

Control inbound and outbound network access

- Rule 1: Always place IoT behind firewall
- **Rule 2: Segment network by IoT type**
- Rule 3: Control access to and from the IoT device

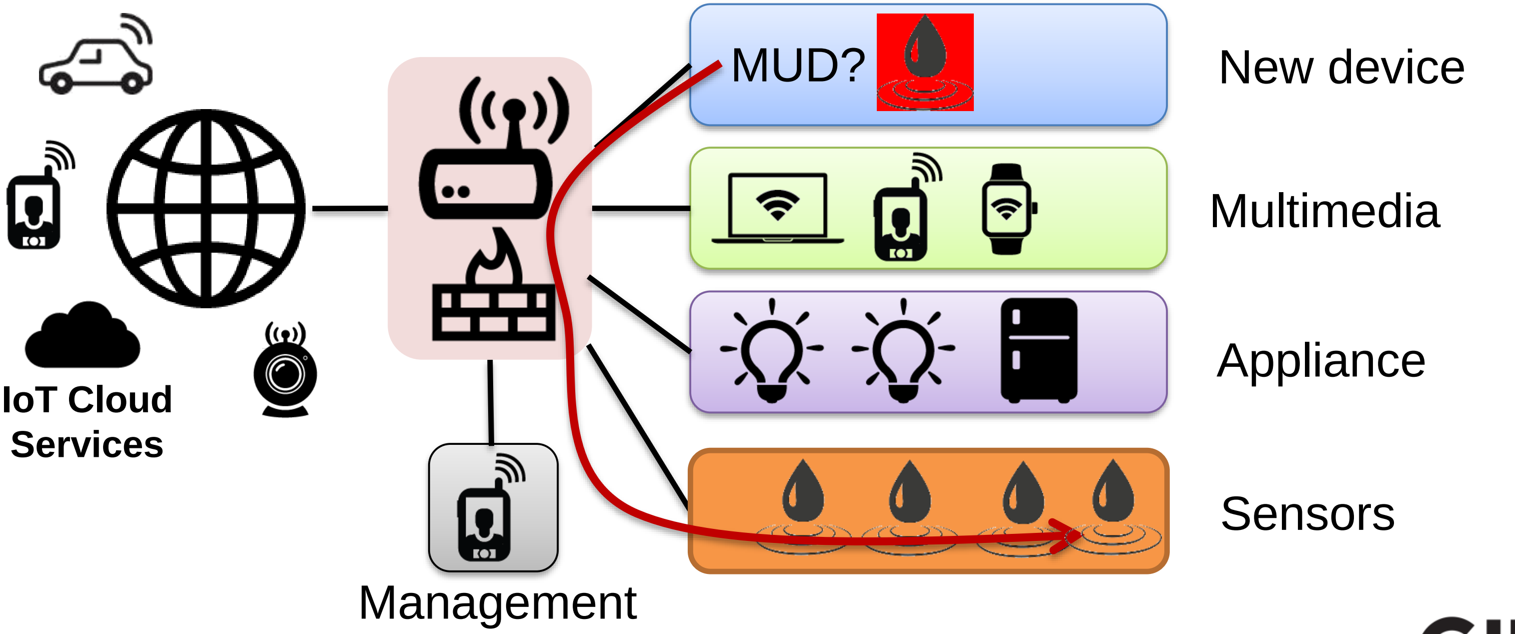


USE MUD TO CLEAN YOUR NETWORK

HTTPS://DATATRACKER.IETF.ORG/DOC/DRAFT-IETF-OPSAWG-MUD/

IETF is working on a Manufacturer Usage Description Specification to help IoT network configuration

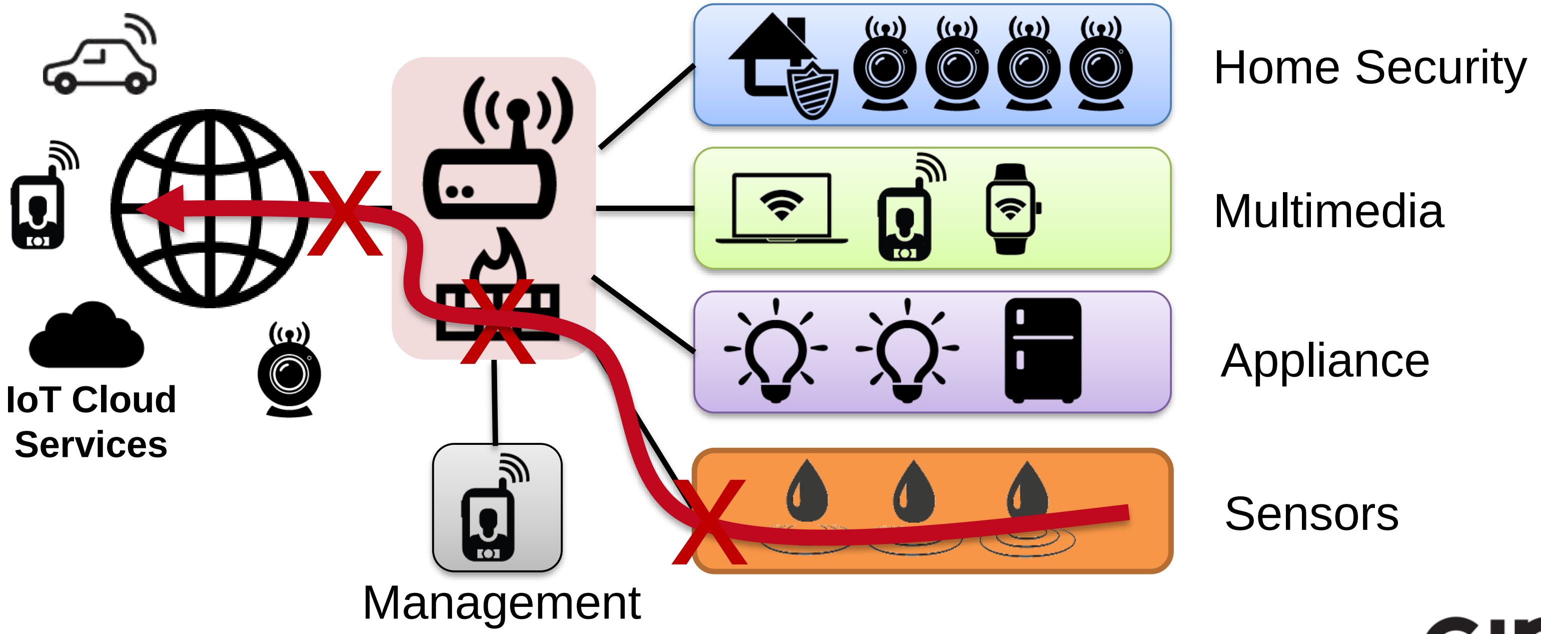
MUD: I'm a water sensor, put me on 'Sensors' LAN



HOW CAN WE PROTECT IoT DEVICES?

Control inbound and outbound network access

- Rule 1: Always place IoT behind firewall
- Rule 2: Segment network by IoT type
- **Rule 3: Control access to and from the IoT device**

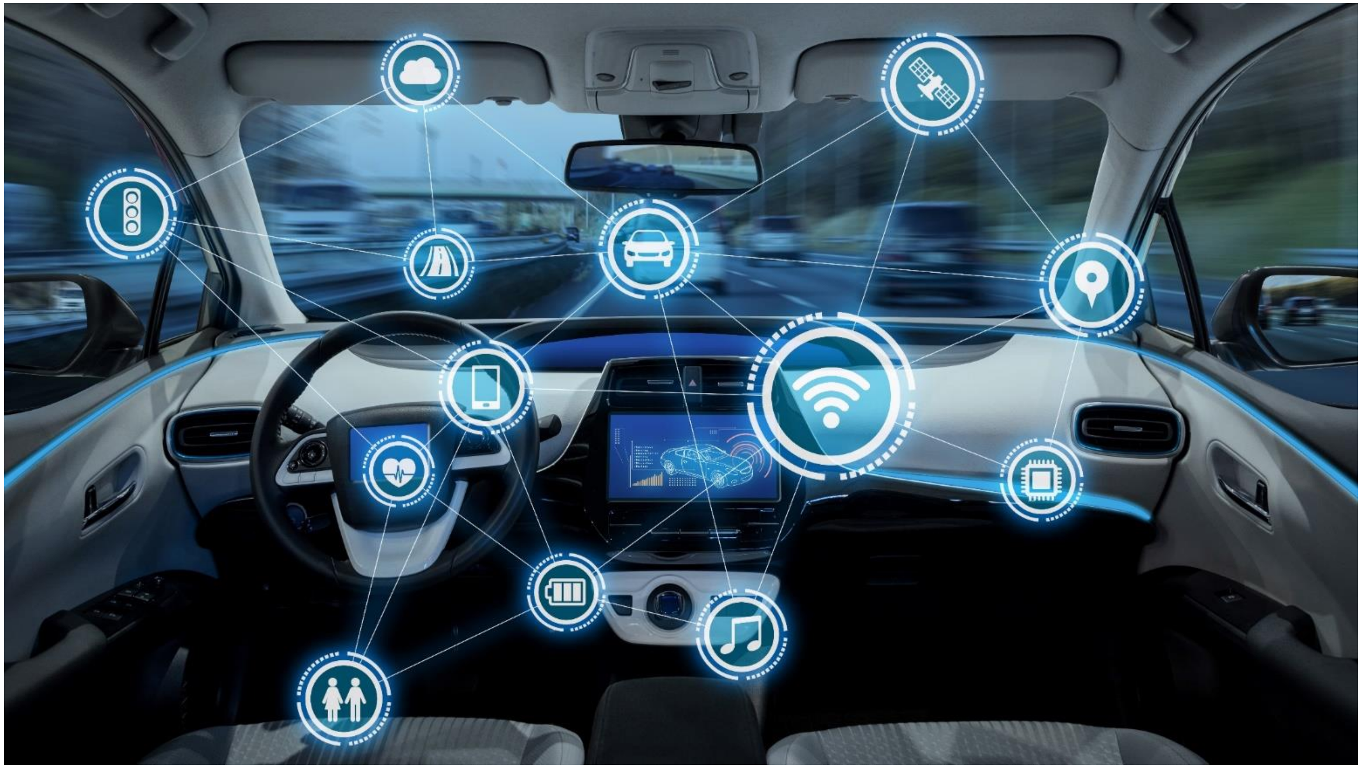


TODAY’S HOME NETWORK & IOT IMPLEMENTATION ARE DISPARATE, KIND OF SCARY & IN NEED OF STRUCTURE!

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

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

EVEN YOUR CAR WILL BE CONNECTED TO YOUR HOME NETWORK



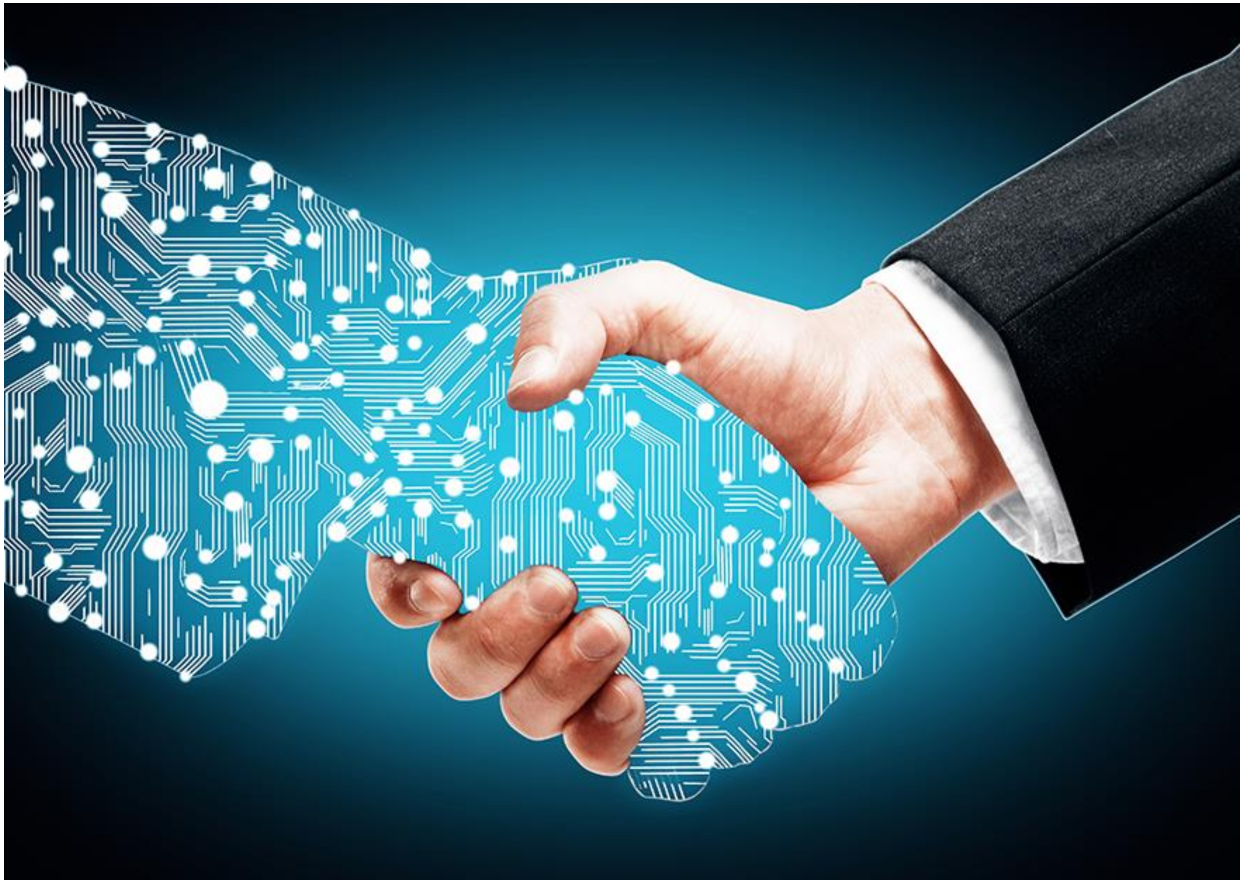
because your home is bigger than your house

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

because eventually they will be IPv6 enabled

YOUR HOME NETWORK SECURITY BOTH INTERNAL AND EXTERNAL MUST BE PROTECTED USING A COMMON KEY

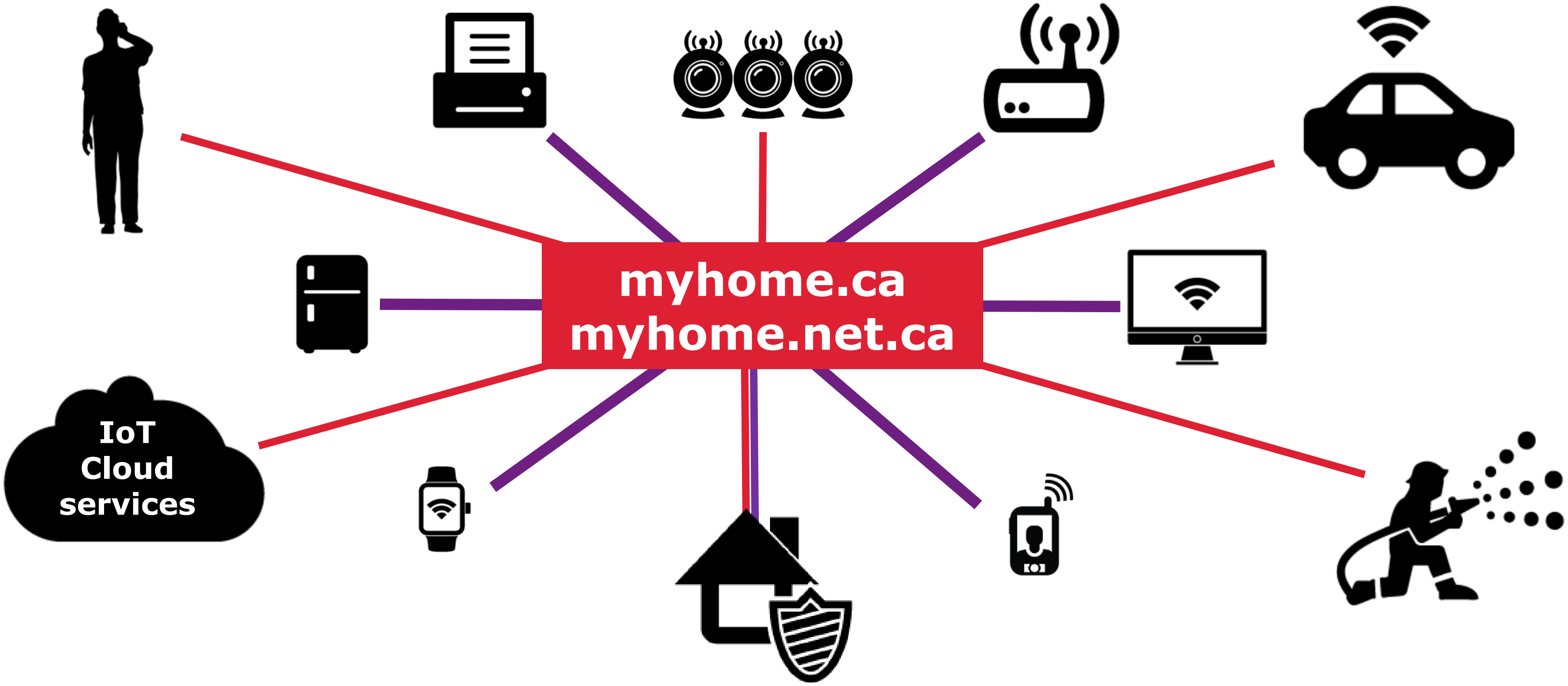
LEVERAGING THE CHAIN OF TRUST IN DNSSEC AND SOME INNOVATION TO CREATE A SECURE HOME NETWORK PLATFORM



DO WE NEED TO SAY MORE?

Public service announcement: We're out of IPv4 addresses !!!

WHAT DOES THIS BRING TO THE ccTLD DOMAIN INDUSTRY?



A domain name per household!!!

THE FOCUS IS ON AUTOMATION

Registry Automation

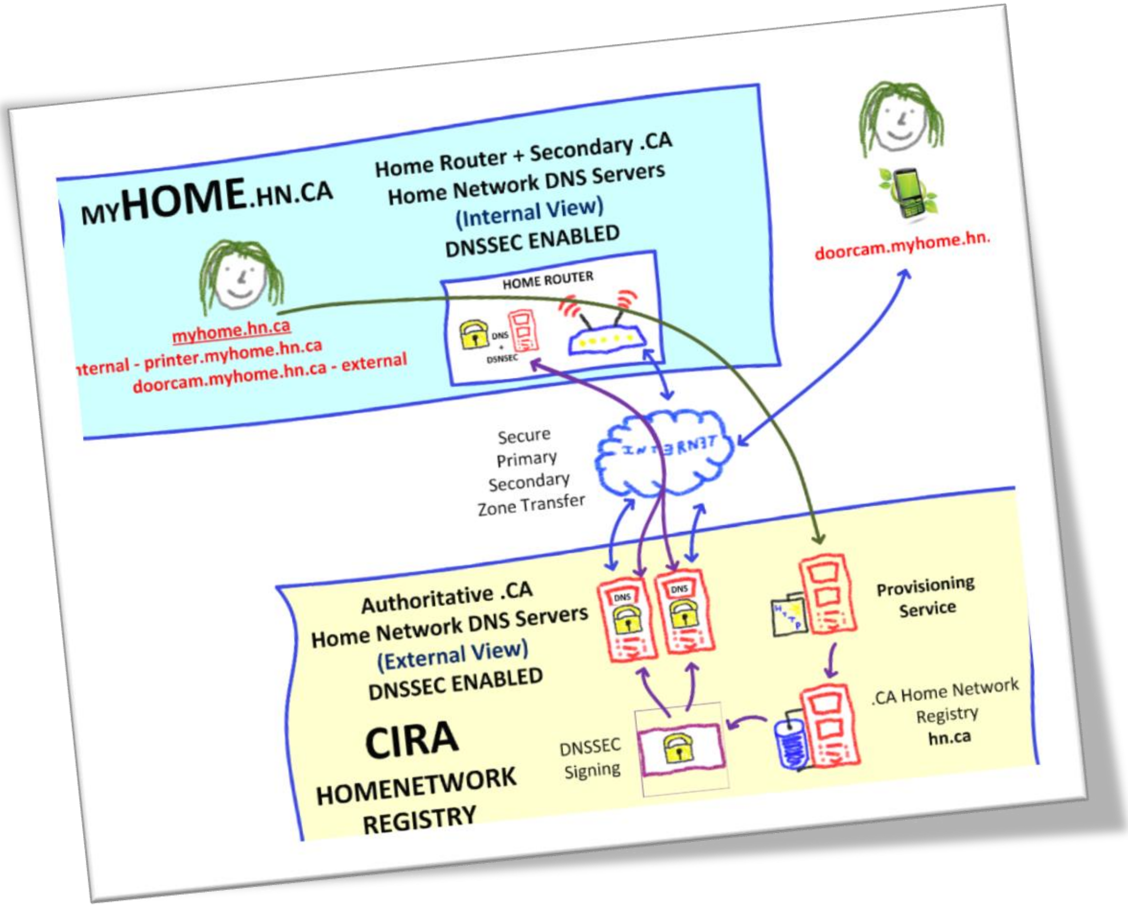
+

Home Network Automation

Innovation

Your local ccTLD will provision your DNSSEC signed domain internally on your gateway and externally on the Internet, and establish a secure chain of trust to your home gateway, magically solving all your worries and keeping your family safe ☺

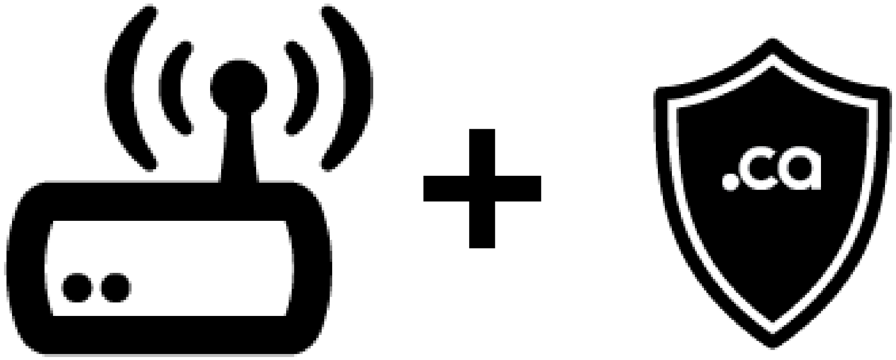
REMEMBER, IT’S AN IDEA & VISION! GET READY FOR THE STORY ☺



That’s
a napkin
design
☺

STEP 1 (THIS IS A STORY ☺)

- 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

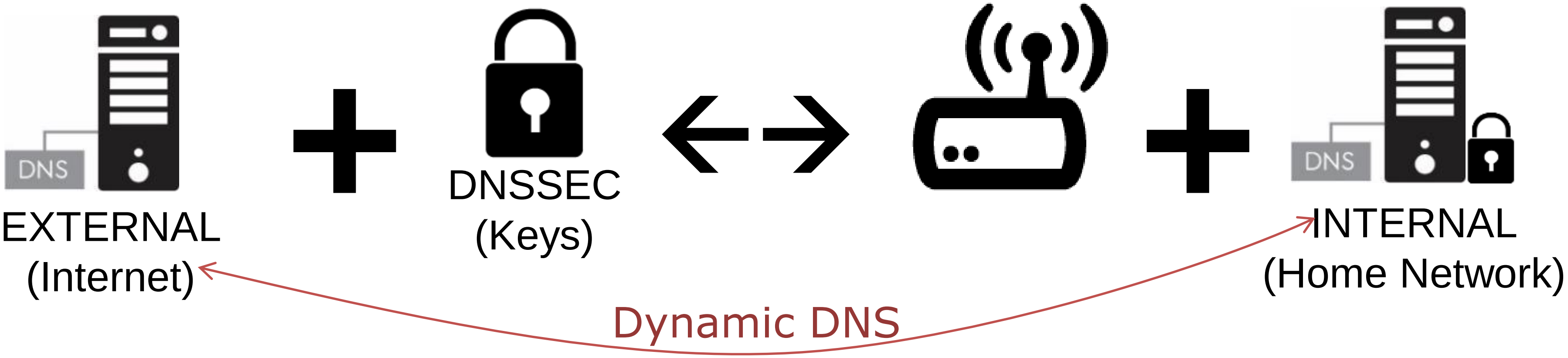
.CA Registry

EXTERNAL (Internet)

DNSSEC (Keys)

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

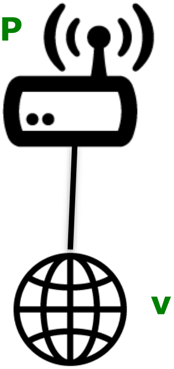


STEP 5

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

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

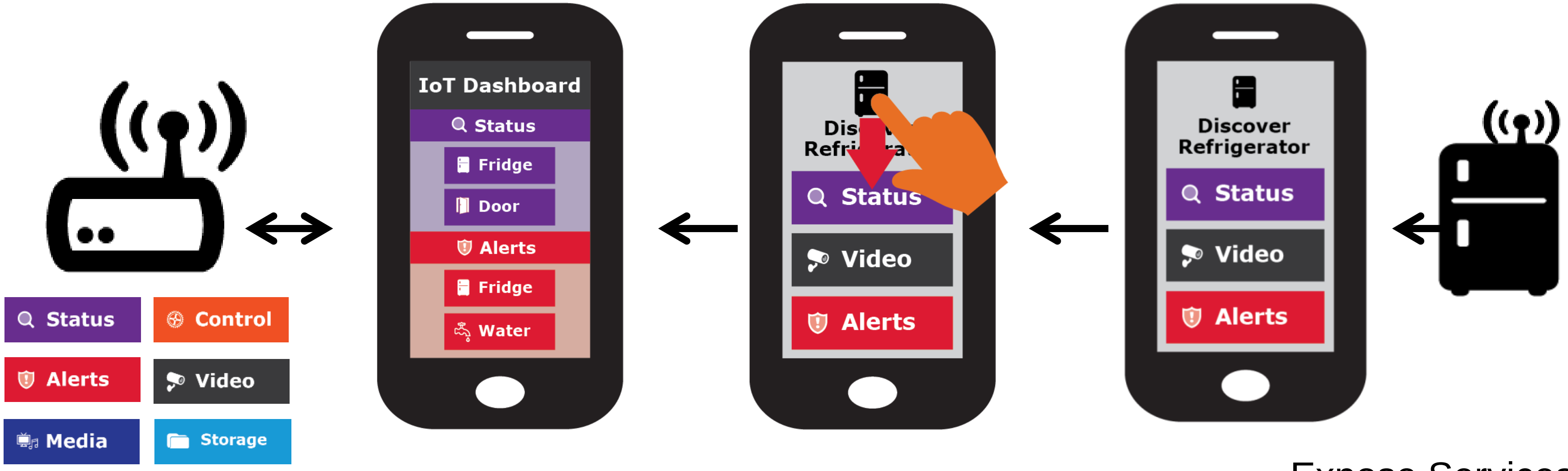
Internal domain fully operational
Secured internally by DNSSEC

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

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

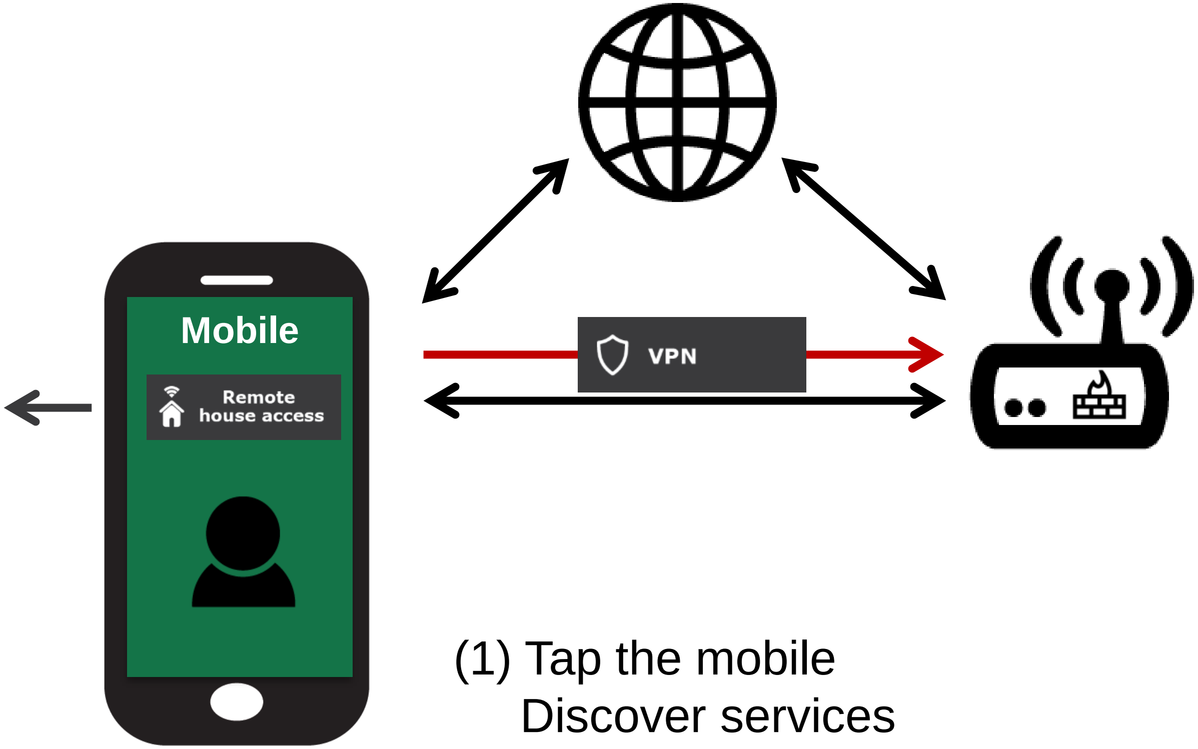
NOW, LET’S SEE HOW WE PROVISION IoT DEVICES IN HOME NETWORK

- Once the IoT device has network access TAP to discover
- IoT device exposes via RFID (or similar) the services available
- Pick relevant IoT services category fro provisioning



Expose Services
JSON blob / RFID

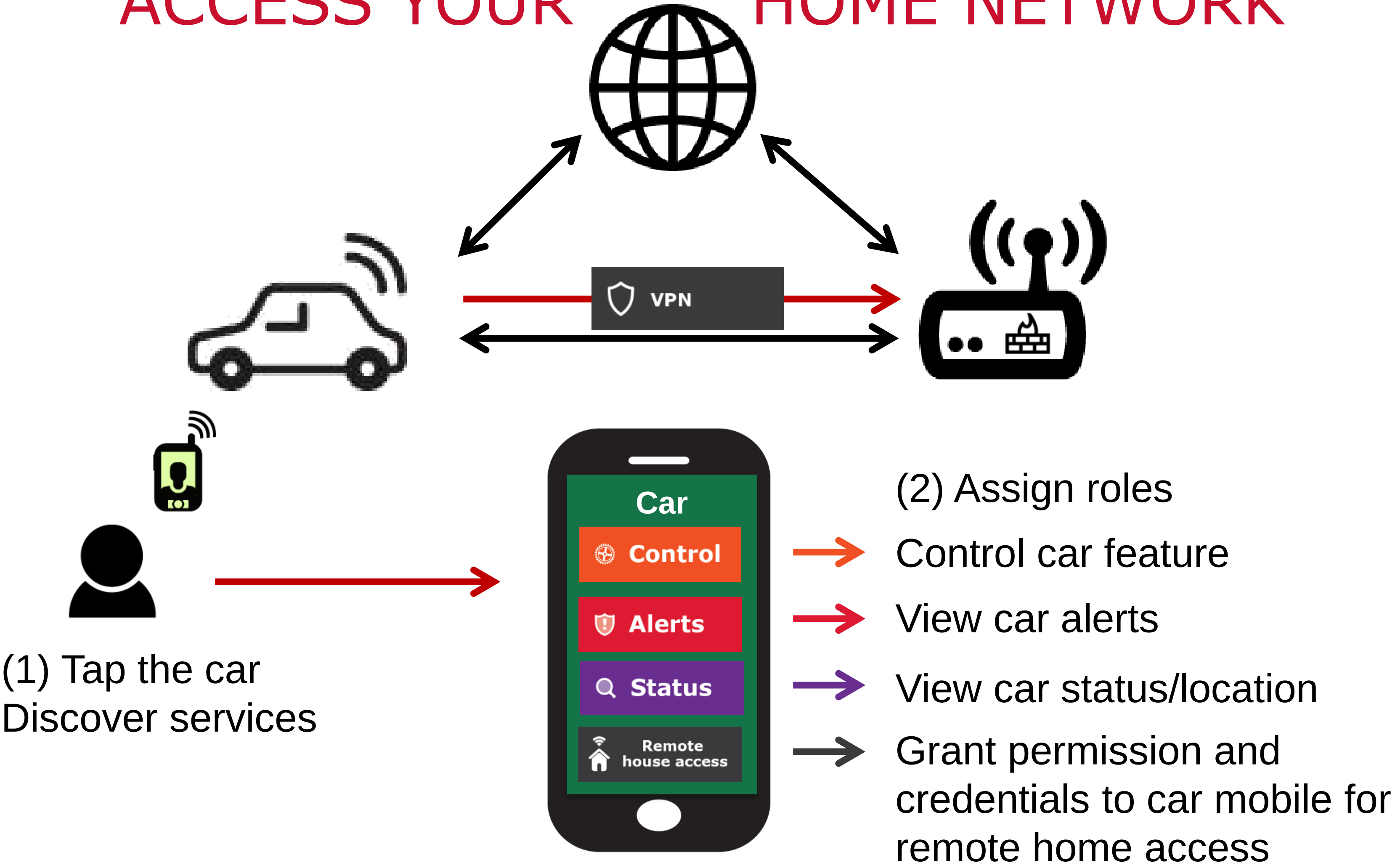
ADDING REMOTE VPN ACCESS TO TRUSTED MOBILE



(2) Grant permission and credentials to mobile for remote home access

(1) Tap the mobile
Discover services

ADDING YOUR CAR TO REMOTE ACCESS YOUR HOME NETWORK



(1) Tap the car
Discover services

(2) Assign roles

- Control car feature
- View car alerts
- View car status/location
- Grant permission and credentials to car mobile for remote home access

IoT SERVICE / ACTION TYPE

- 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?

TODO:
+ ADD SCENARIOS FOR EACH DEVICE TYPE

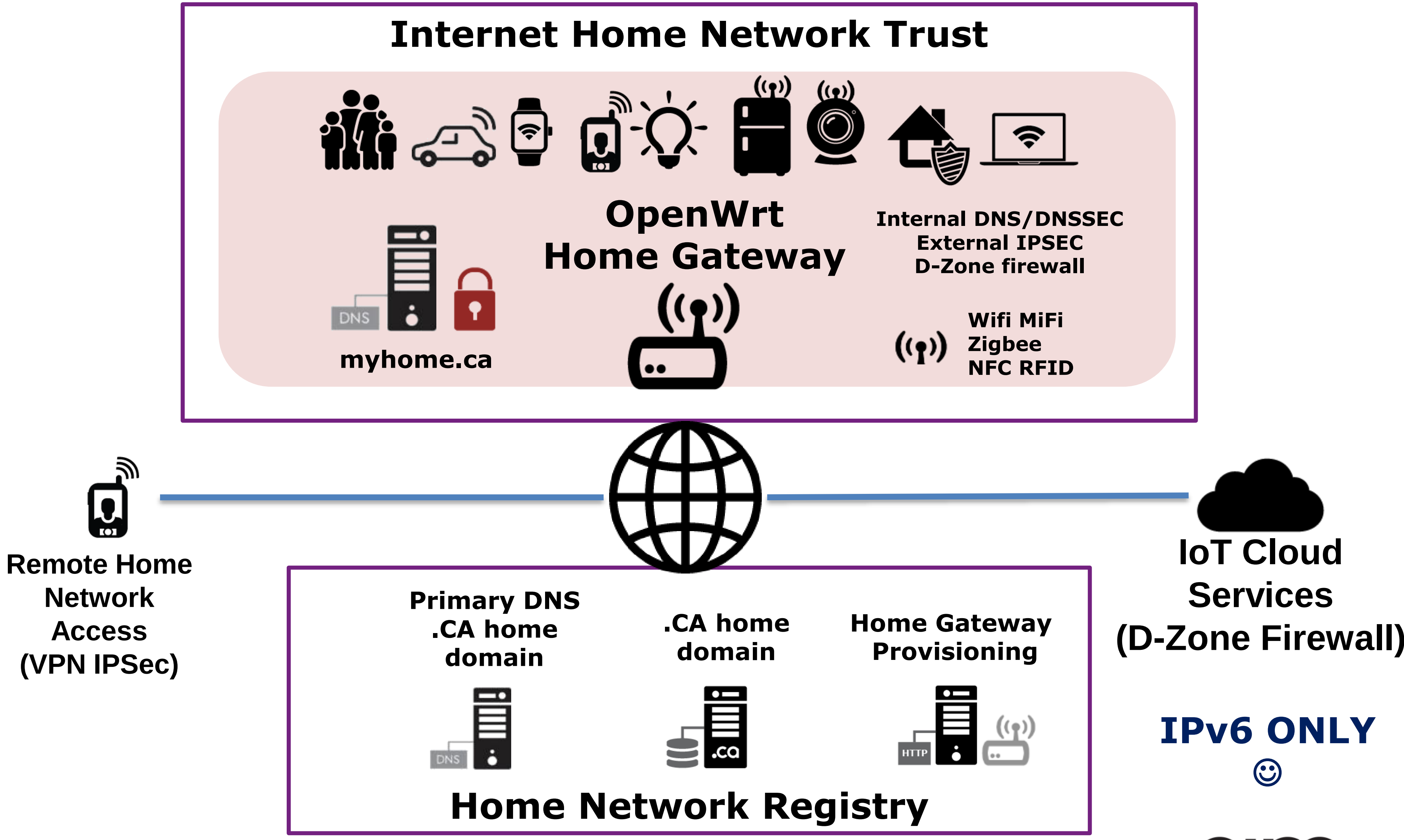
- Example of pushing WIFI to the device
- Show that the fridge is exposing service (MUD profile example)
- No web interface on IoT device
- Focus on cloud / vendor, show they integrate into this solution, can be multi vendor multi cloud provides
- IoT Classification: based on device type, air play could see all camera in the house, the TV could see all camera (security controls)
- Door bell sends to audio device, you car
- Fire alert send to audio receiving device
- Power Utility company allow access to home gateway
  - allow Power Utility to access hot water tank
  - allow Power Utility to adjust thermostats

YOUR HOME NETWORK SECURITY IS COMPROMISED?

- Get the ccTLD to perform an emergency DNSSEC key roll over, externally and on the home gateway
- Will have new keys on home gateway
- This will make all VPN keys & certificate invalid
- A roll over will force the generation of new keys.
  - Trusted "management" home gateway mobile access must be re-established using an out of band token
  - Remote home access trust must be re-established
  - Local network access controls should remain the same

DRAFT

HIGH LEVEL SOLUTION ARCHITECTURE



Internet Home Network Trust

OpenWrt
Home Gateway

myhome.ca

Internal DNS/DNSSEC
External IPSEC
D-Zone firewall

Wifi MiFi
Zigbee
NFC RFID

Remote Home Network Access (VPN IPSec)

IoT Cloud Services (D-Zone Firewall)

Home Network Registry

Primary DNS
.CA home
domain

.CA home
domain

Home Gateway
Provisioning

IPv6 ONLY

☺

WHAT DO YOU THINK?

Want to help?

GOING FORWARD, IT'S A JOURNEY! ccTLD VALUE PROPOSITION

- Motivation
  - Ensure long term ccTLD relevance in the future of IoT
  - To create a secure **<internet home>** IoT environment
- Proposing ccTLD to develop a solution
  - To keep the home network safe and secure
  - 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 – BUILD A PROTOTYPE

- Develop a Proof of Concept and prototype
  - Using .CZ Omnia Home Gateway (openWRT)
  - Home Gateway App (Android/iPhone)
  - Develop some IoT discoverable devices (RFID)
- Use public GitHub to document the functional specification and repo for prototype software
  - Functional specification
  - Software repository

THIS SLIDE DECK IS A VISION
IT’S WHAT WE’LL BE USING IN 5 YEARS

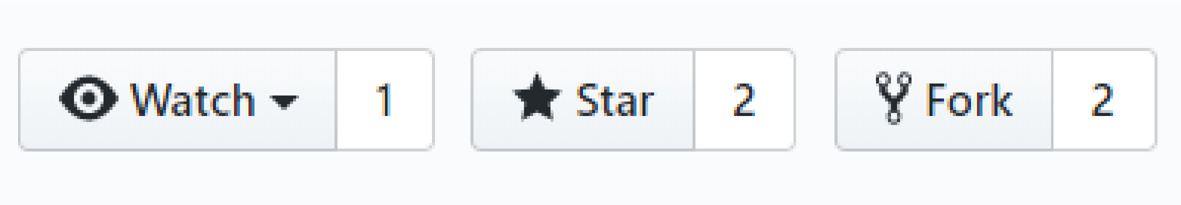
- Is work in progress, presented as a story
  - Story how a home gateway can be IoT friendly and how a ccTLD registry provision a secure domain per household
- Is meant to define a security framework and associated standards
  - IETF, ISO/IEC, others..
- Is tuned around implementation at .CA / CIRA, but not specific just for CIRA
- Is to solicit feedback
- Is another layer of defence in depth to protect the internet

Your new <Internet Home>

https://github.com/CIRALabs/Secure-IoT-Home-Gateway

Watch the github project

to get update notifications



HOME.ARPA. DRAFT-IETF-HOMENET-DOT-14

- IETF working on making the default home network address: [yourprinter.]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!

SOLUTION: 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
  - Sensors -> no access to internet
    - Appliances may have access this zone
  - Appliance -> no access to internet
    - VPN may have access this zone
  - Allow myhome.ca to access myparents.ca
    - Only for Home Security and sensors