

# SECURE IoT HOME GATEWAY & HOME REGISTRY - IDEA



Jacques Latour, CTO  
Canadian Internet Registration  
Authority

Nov 20, 2017

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





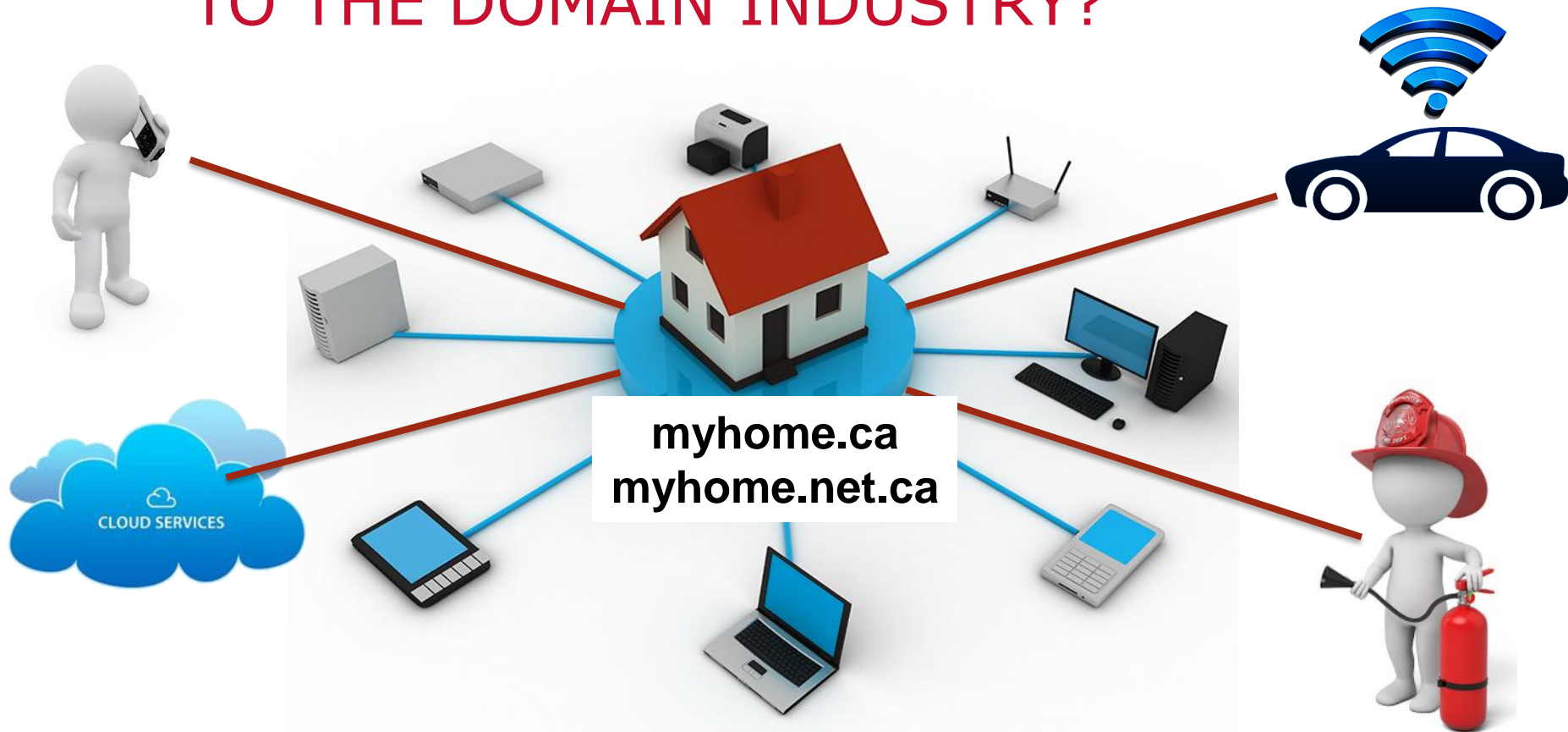
# DO I NEED TO SAY MORE?

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



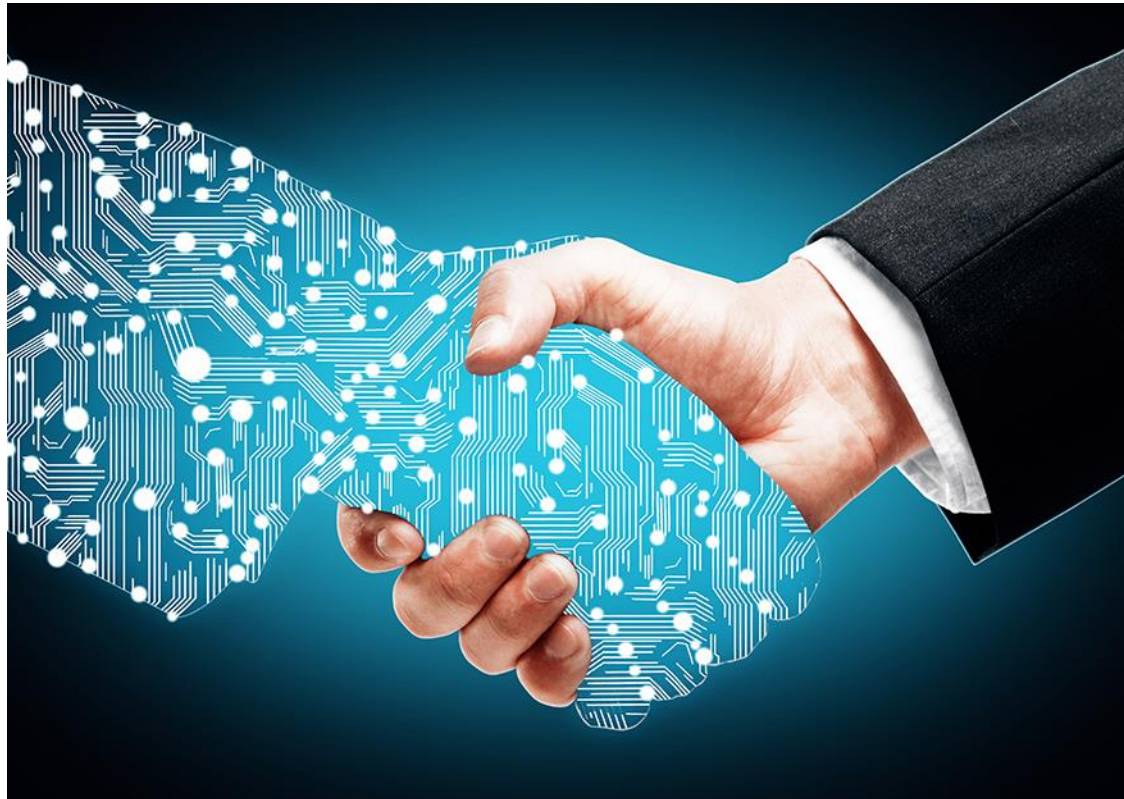


# SERIOUSLY, WHAT DOES THIS BRING TO THE DOMAIN INDUSTRY?



## 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: [yourprinter.][home.arpa](http://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



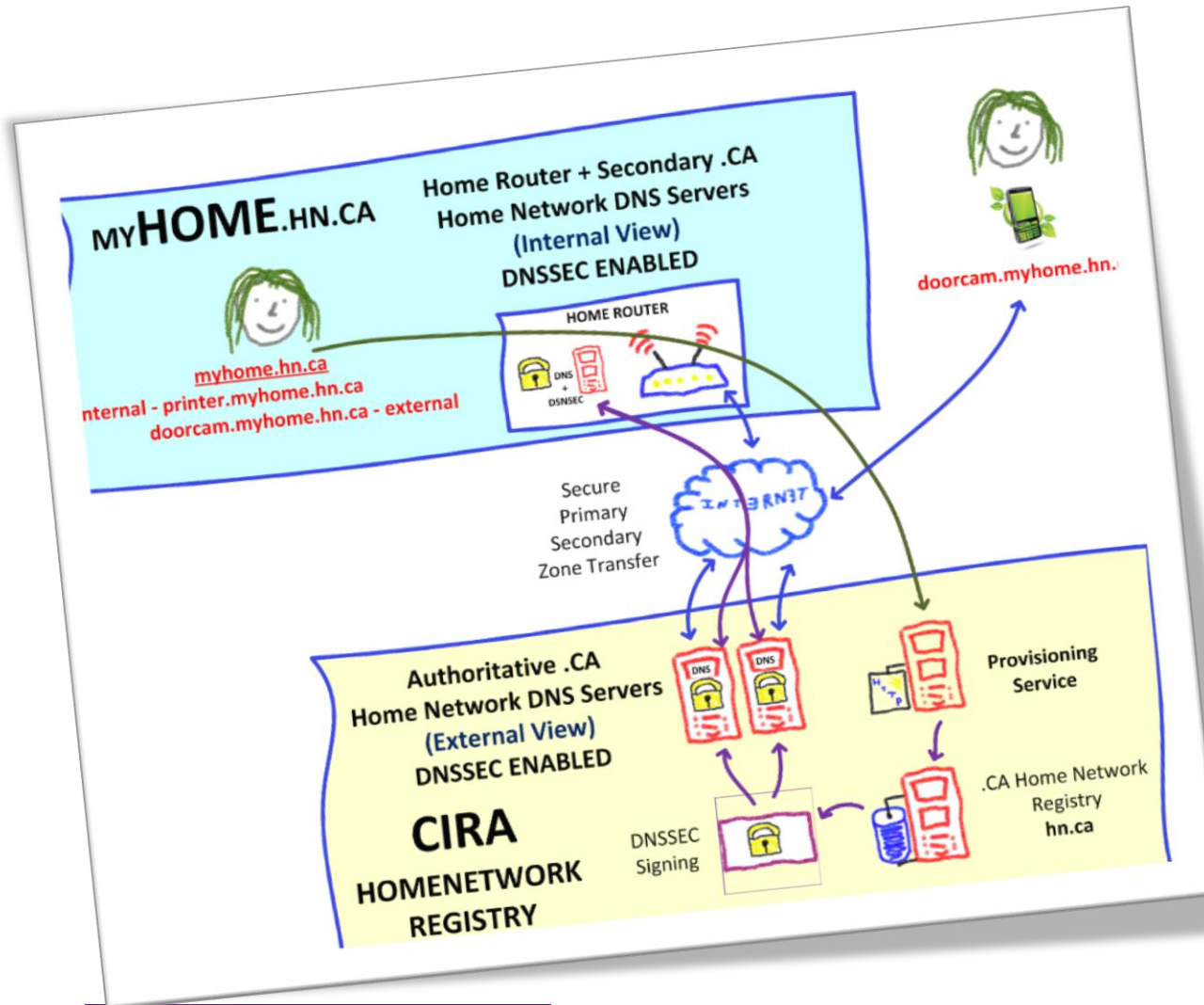
# Innovation





Your local ccTLD will provision your DNSSEC signed domain internally on your gateway and externally as DNS primary, 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...



## STEP 1

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




A 2<sup>nd</sup> or 3<sup>rd</sup> 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, 2<sup>nd</sup> or 3<sup>rd</sup> level domain name
  - Enter the secret code (“TAP” RFID card)
  - Home Gateway ready for configuration

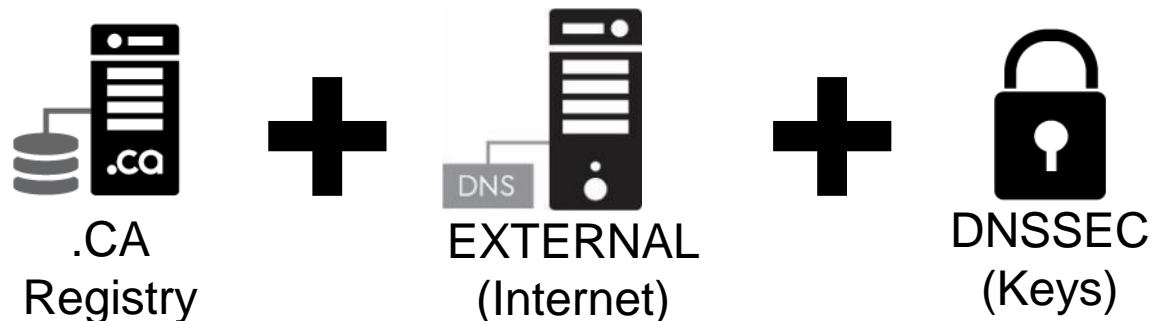


**myhome.ca** +  **code**



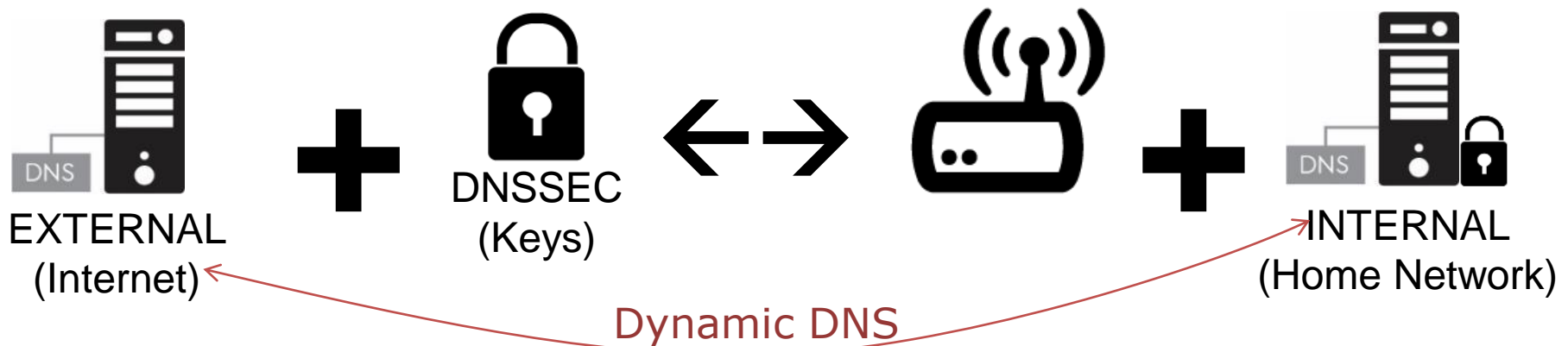
## STEP 3

- 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 NEED WORK

- 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

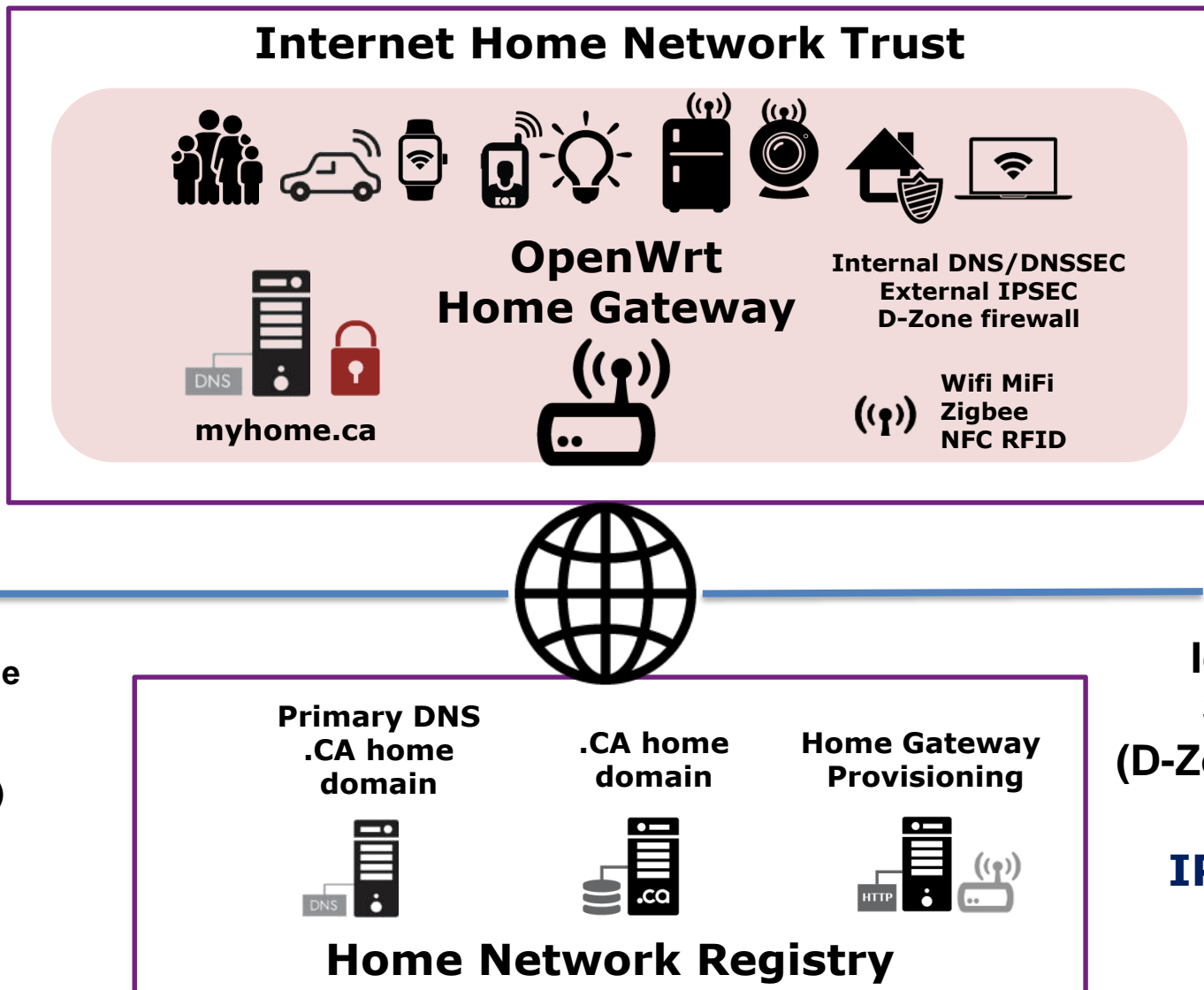


## STEP 5

- 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



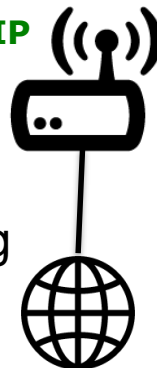


## AT THIS POINT WE HAVE

- 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

Internal domain fully operational  
Secured internally by DNSSEC



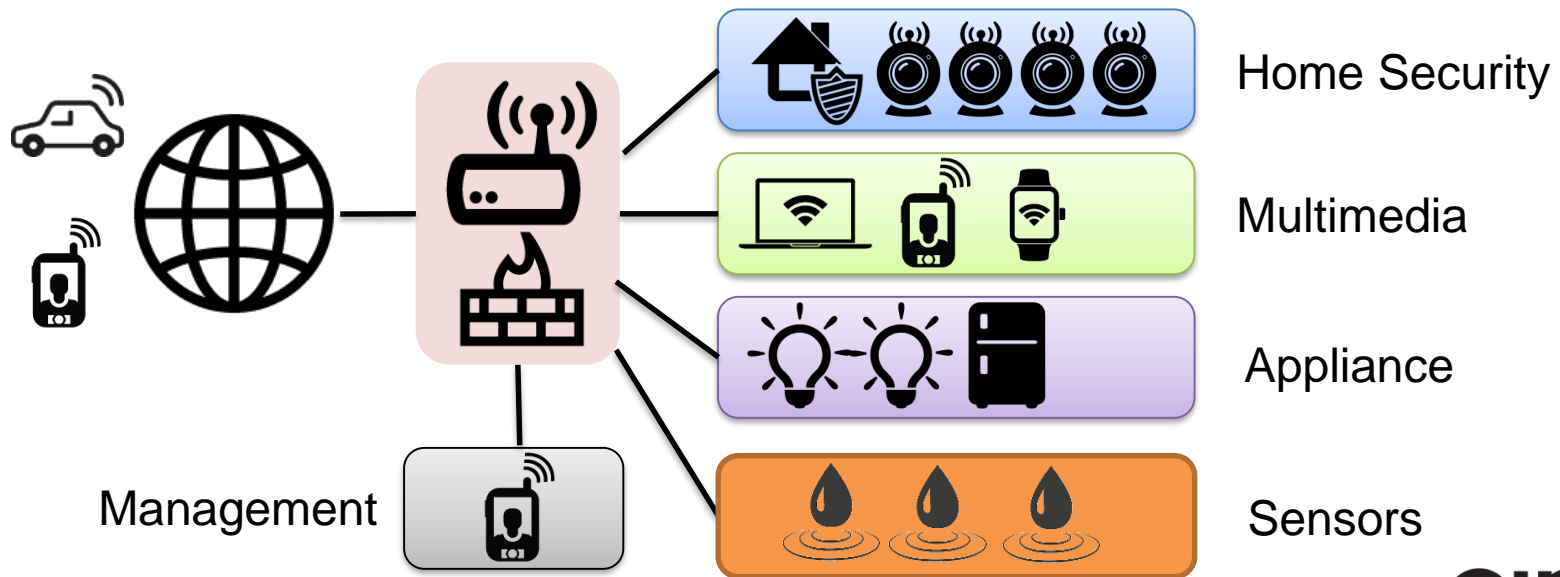
External domain to allow exposing  
internal services and make them  
available externally

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

# 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

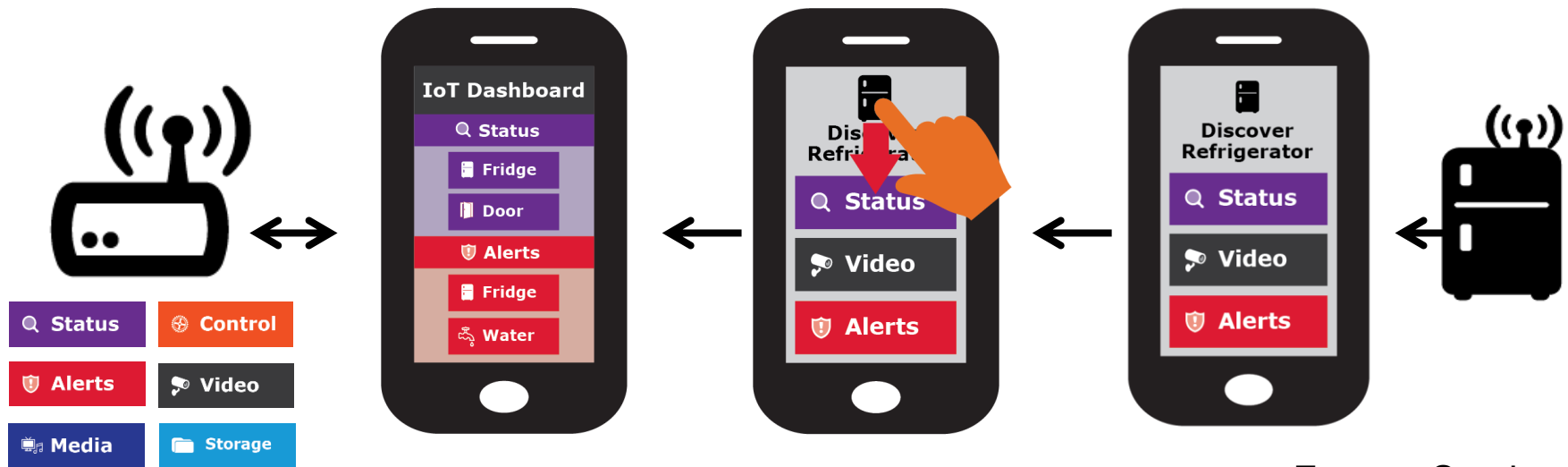


# NETWORK ACCESS CONTROL (NAC) & DEFAULT SECURITY CONTROLS

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



Expose Services  
JSON blob / RFID



# IoT SERVICE / ACTION TYPE

 **Status**

- Status: Up/down, on/off, ok/bad, status variable

 **Video**

- Audio/Video: Camera, video feed

 **Media**

- Media: Audio/Video media feed, TV, music

 **Storage**

- Storage: Data storage, NAS (pictures, files, data)

 **Alerts**

- Alerts: Up/down, on/off, ok/bad, "Water detected"

 **Control**

- Control: Turn up/down, on/off, change device value

 **Cloud Service**

- Cloud Service: IoT vendor, Google, MS, DropBox

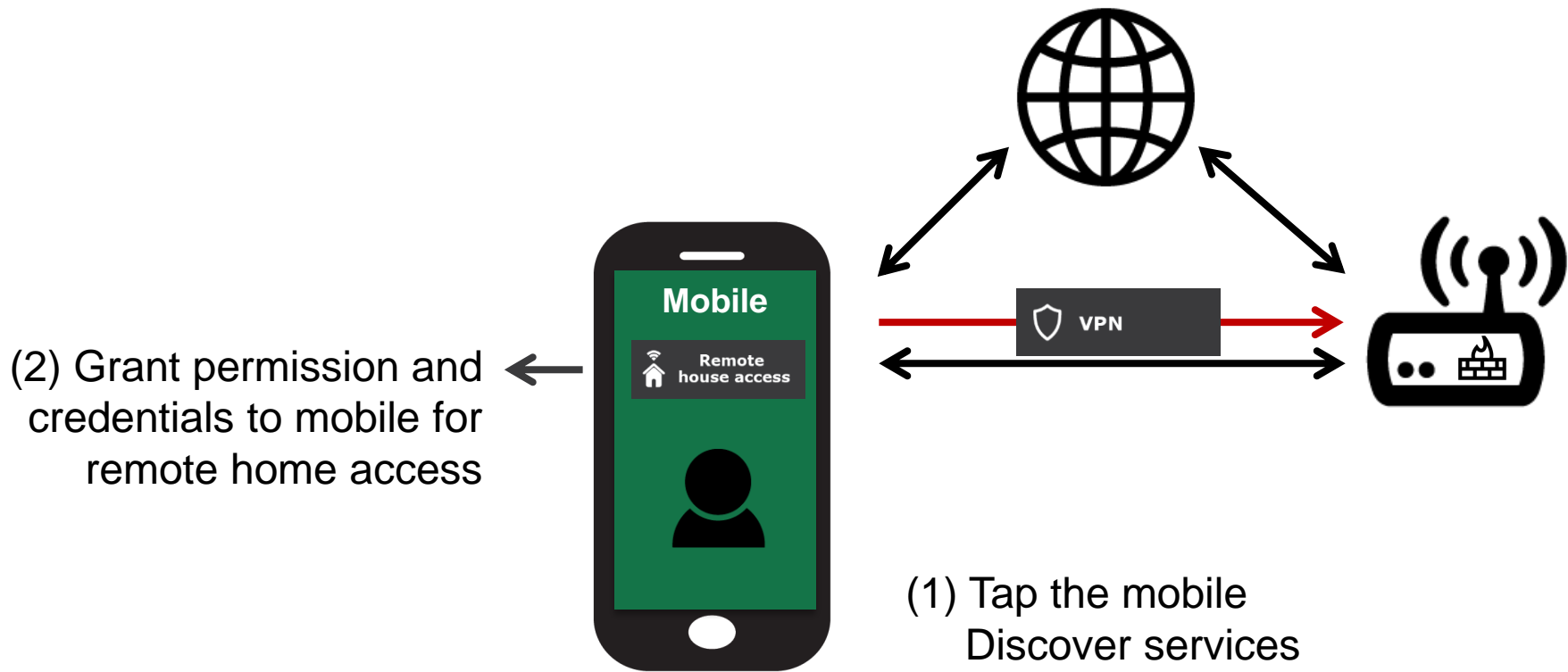
 **VPN**

- VPN (VPN inside myhouse.ca)

 **Remote house access**

- Remote house access
- Other Sensors/ Actuator functions?

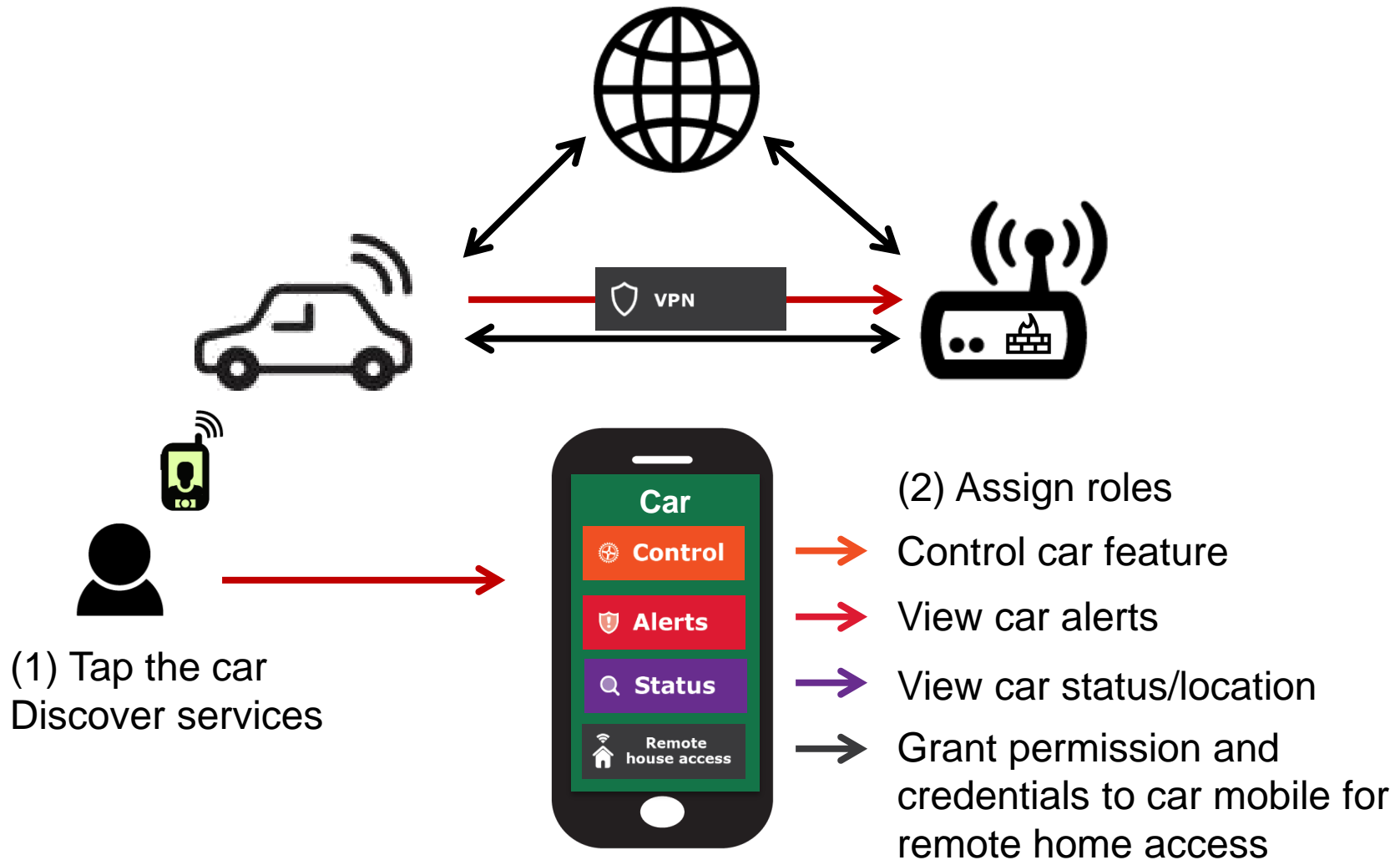
## SCENARIO: ADDING REMOTE VPN ACCESS TO TRUSTED MOBILE



# YOUR HOME NETWORK SECURITY IS COMPROMISED?

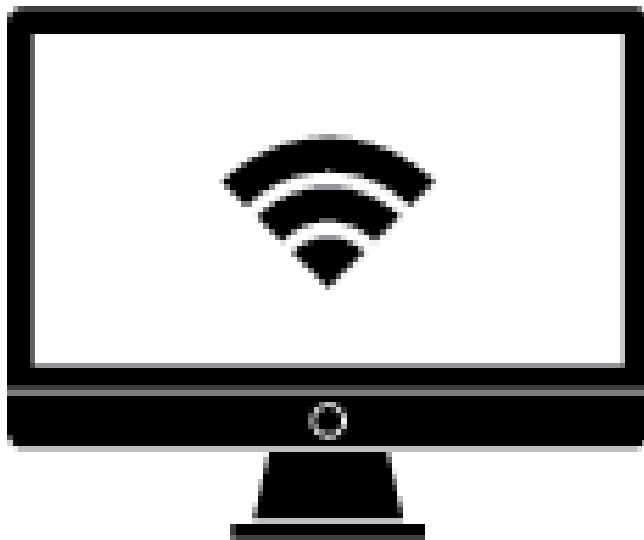
- Get the ccTLD to perform an emergency DNSSEC key roll over, externally and on the home gateway
- Will have new keys on home gateway
- This will make all VPN keys & certificate invalid
- A roll over will force the generation of new keys.
  - Trusted “management” home gateway mobile access must be re-established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

# SCENARIO: ADDING YOUR CAR



**TODO:**

SCENARIO: ADDING A SMART TV



**TODO:**

**+ ADD SCENARIOS FOR EACH DEVICE TYPE**





# WHAT DO YOU THINK?



## Want to help?

# GOING FORWARD, IT'S A JOURNEY!

- 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

- 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

# The new <Internet Home>

**<https://github.com/CIRALabs/Home-Network-Registry-Gateway>**