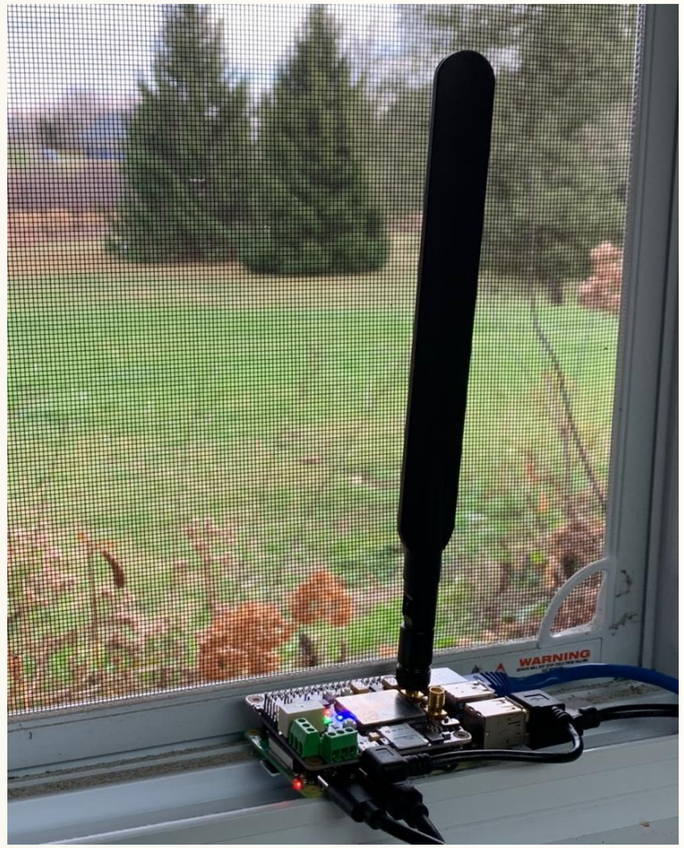
Zero-Touch Universal IoT Device Identity

DNSSEC ICANN Oct 27th, 2021

Presented By
Ash Wilson, Valimail
Jason Blakey, CIRA

PROOF OF CONCEPT



TELUS

Rey Buquid

VALIMAIL

Ash Wilson

cira

Jacques Latour
Natasha D’Souza
Jason Blakey
Jesse Carter

cira

WHAT IDENTITY CHALLENGES GET IN THE WAY OF IOT SECURITY?

What can we do with PKI-Based Device Identity?

E2E Message Security

- Signing/encryption over messaging middleware
- Great way to guard against middleware compromise

Transport authentication

- Device certificate for mutual TLS authentication
- Easier to secure than shared secrets, API tokens

Network Authentication

- Device certificate for EAP-TLS authentication
- Allows granular network access, much better than pre-shared keys

WHAT IDENTITY CHALLENGES GET IN THE WAY OF IOT SECURITY?

Interoperability & cost barriers…

Certification Authority

- Creation, operation, maintenance, protection can be costly
- Unapproachable for small businesses
- Introduces an additional namespace to the application/organization
- Often onboard everything to the same CA to avoid identifier collisions

Message security

Proprietary API integration for certificate discovery

Transport and Network Authentication

- Requires distribution of trust anchors (risk of identifier collisions)
- Revocation requires OCSP or distribution of CRL

WHAT IDENTITY CHALLENGES GET IN THE WAY OF IOT SECURITY?

Focus on Network Authentication

What does the ideal state look like?

User purchases a device or secure element with a pre-provisioned universal identity (CA involvement earlier in the supply chain)

Universal identity enables roaming

- Across different access networks (WiFi, 5G, Ethernet)
- Across network providers (rural, municipal, enterprise, telecom)

Client identifier useful for accounting, charge-back

Revocation simpler than OCSP/CRL

FOUNDATIONAL DECISIONS

How important is the namespace?

CSA, Summary Guidance for Identity and Access Management in the IoT-
Step 1a: Define a common namespace for IoT devices

This first step defines the journey.
Many architects just define an entirely new namespace

What if, instead of creating a new namespace, we just use DNS?

(https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/identity-and-access-management-for-the-iot.pdf)

WHAT IDENTITY CHALLENGES GET IN THE WAY OF IOT SECURITY?

TRUST YOUR EMAIL

Focus on Network Authentication

Two gaps between present state and Universal Identity

1. Absence of a universal namespace for client identities

2. Discoverability of certificates and trust anchors

DANE solves both problems!

CAN WE USE DANE TO SUPPORT EXISTING LIBRARIES?

Focus on Network Authentication

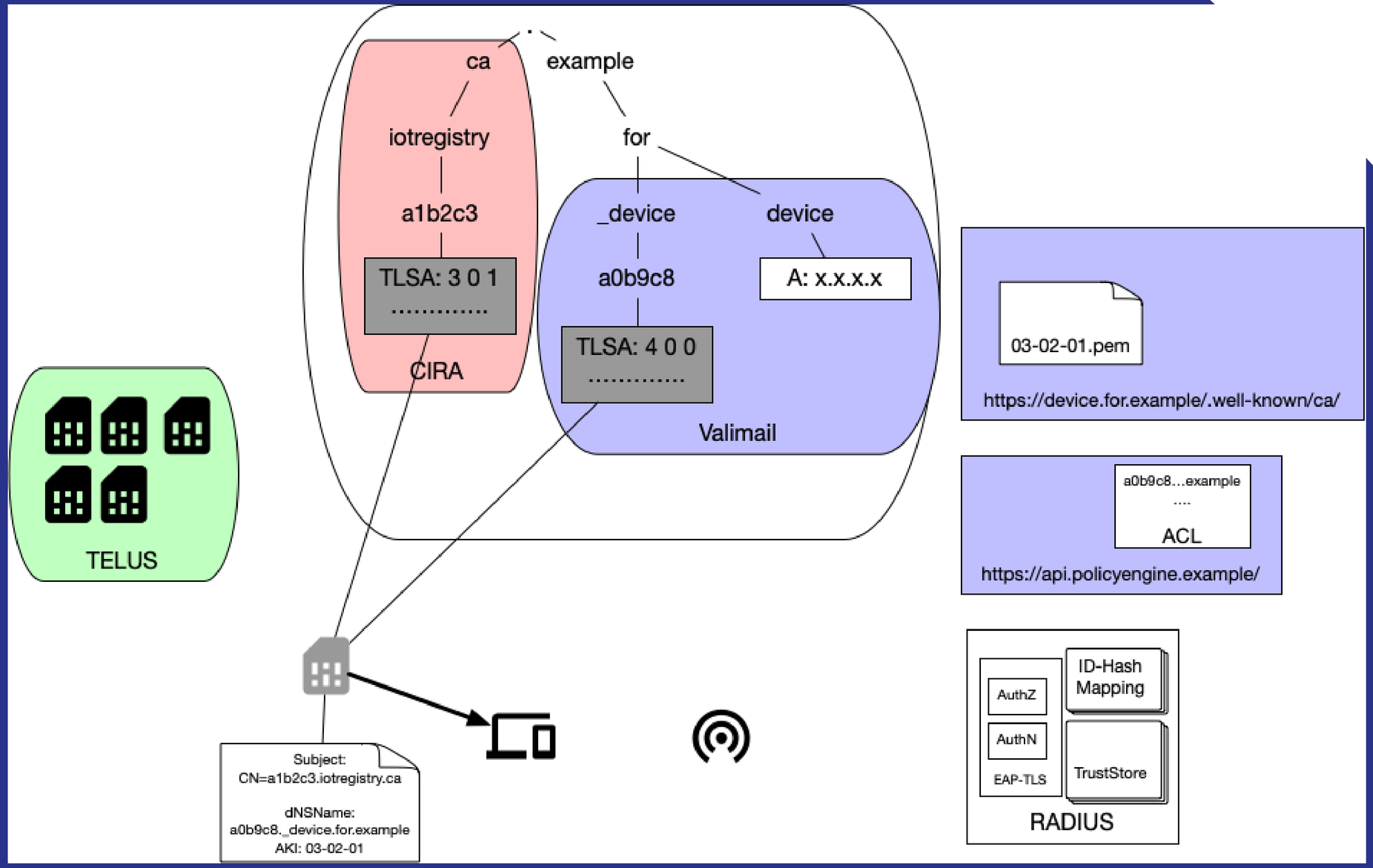
What's a good first step for moving to DNS-bound client identity?

EAP-TLS deployed with CA-issued client IDs

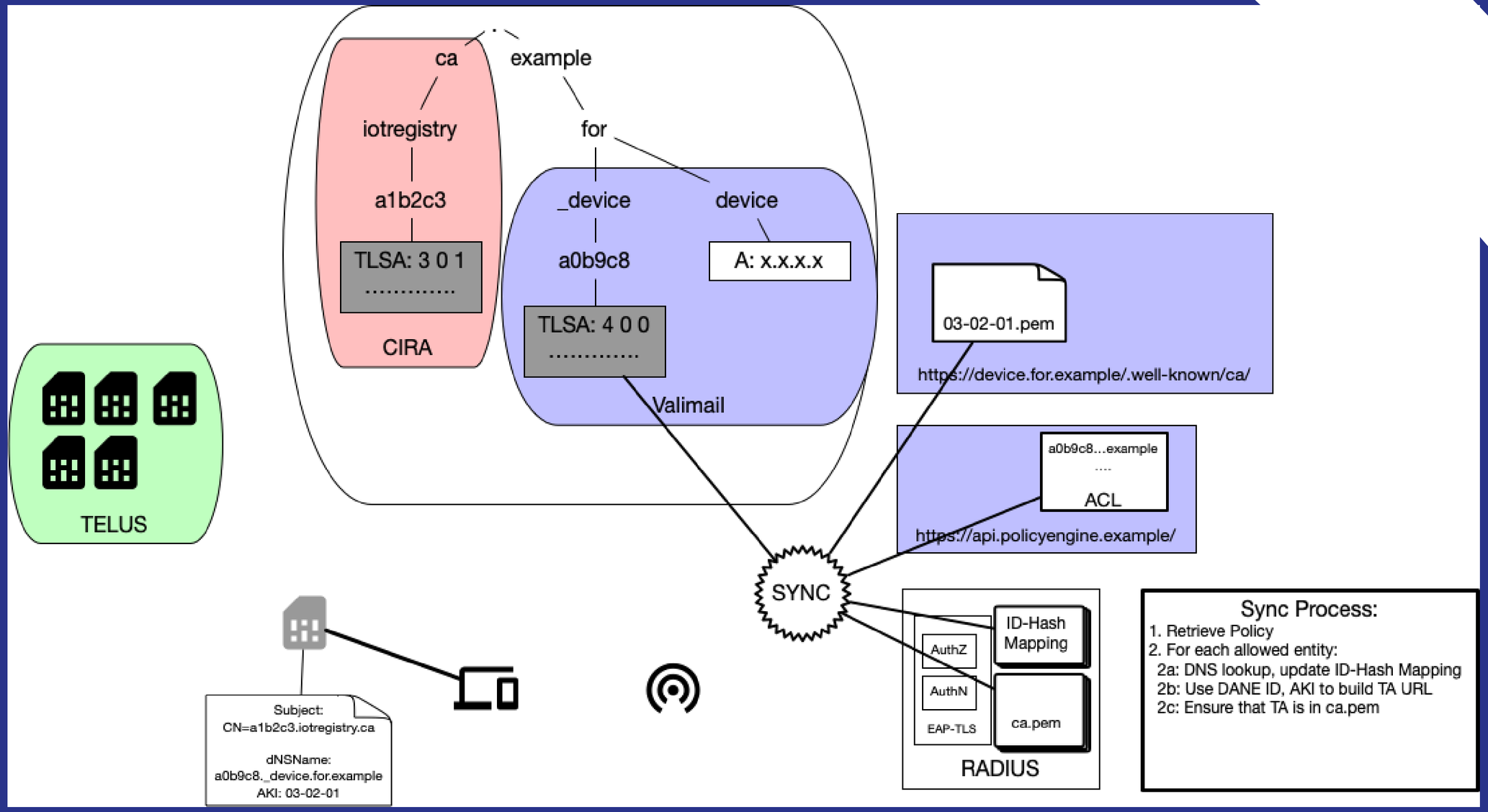
Can we dynamically manage CA certificates in RADIUS

…while enforcing DNS name bindings?

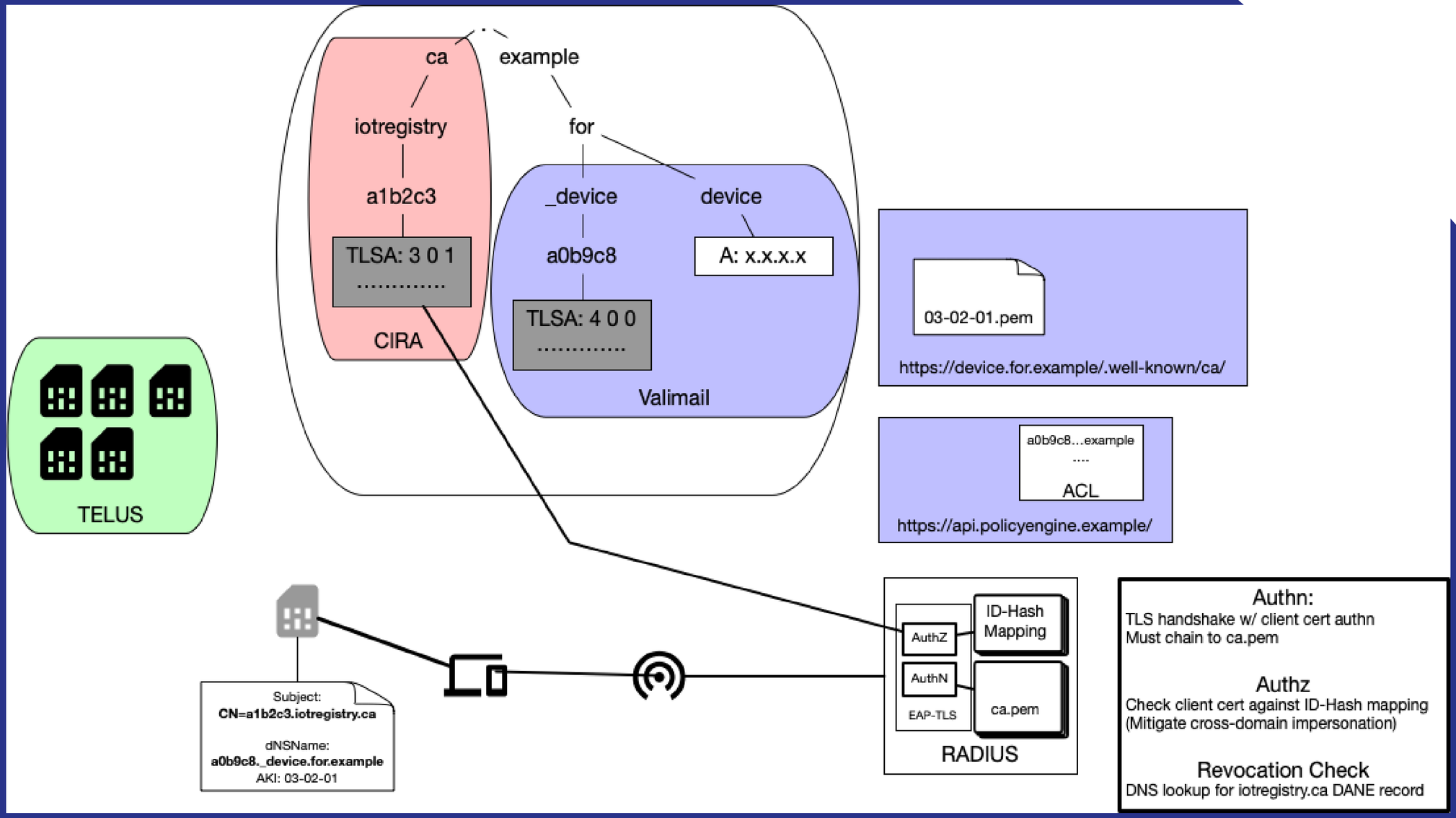
IDENTITY ISSUANCE



TRUST STORE SYNC



AUTHENTICATION / AUTHORIZATION



When vapor gets real ;-)

TRUST YOUR EMAIL

Quick DEMO!

well, kind of ☺, maybe

The CIRA IoT Registry Overview + (Mostly Update)

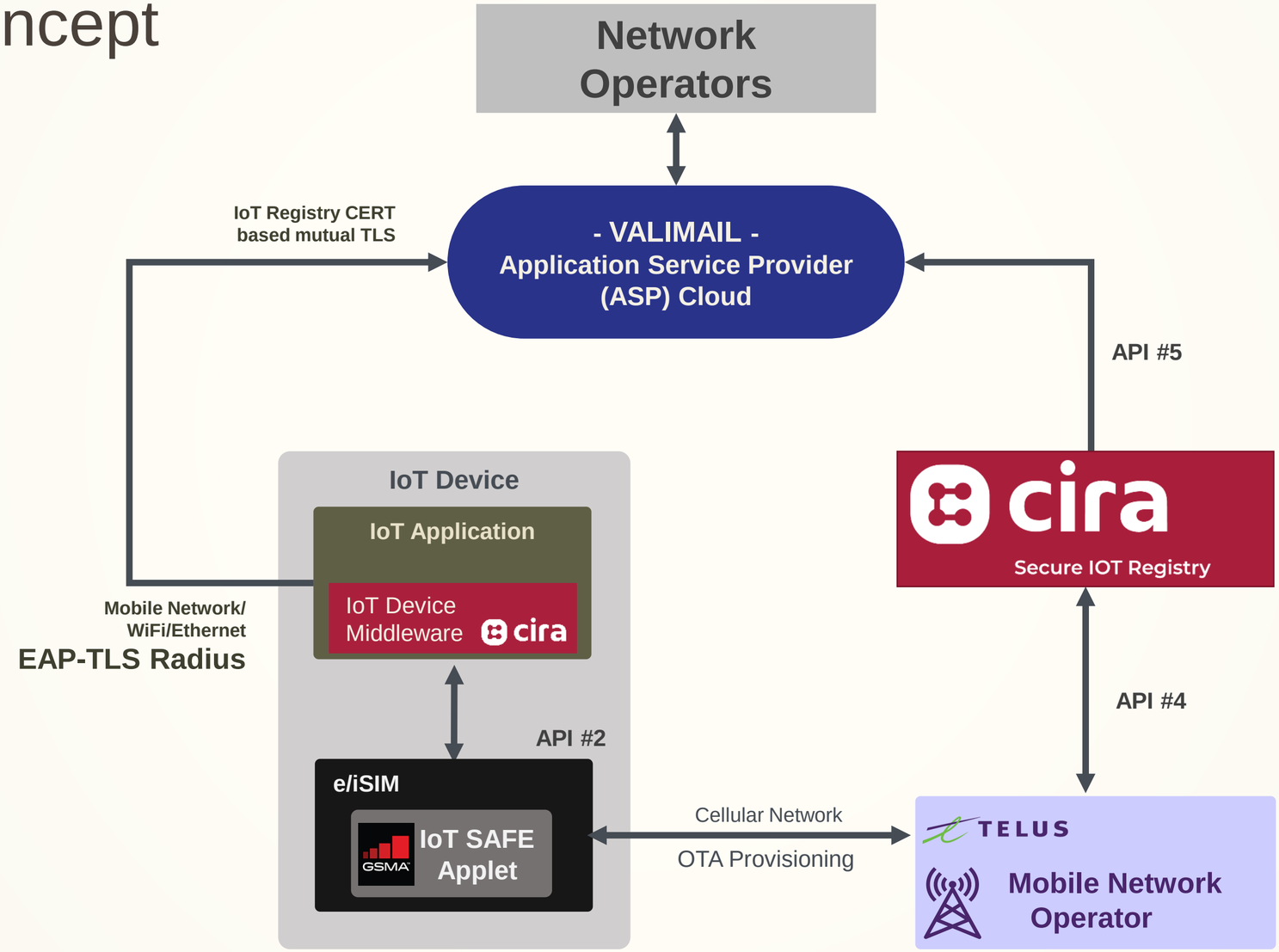
ICANN69 – vTechDay

https://69.schedule.icann.org/meetings/sMAzQxxMpvoRQckC2

ICANN71 – DNSSEC & Security Workshop

https://71.schedule.icann.org/meetings/3q22SHqif9XF5nFqG

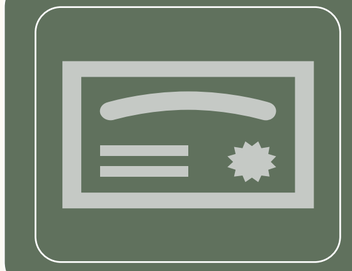
Proof of Concept



IOTSAFE PROVISIONING

After provisioning, the IoT SAFE applet on the eSIM will have

A public/private keypair



A certificate generated and signed by the IoT Registry CA

Credentials: connection data we want to be stored in the IoT SAFE applet

cira

USE CASE

It’s alive!

So, at this point, we’ve got a device with a known & verifiable identity, thanks to it’s public key being stored in the Domain Name System

This is called “DANE” – DNS-Based Authentication of Named Entities

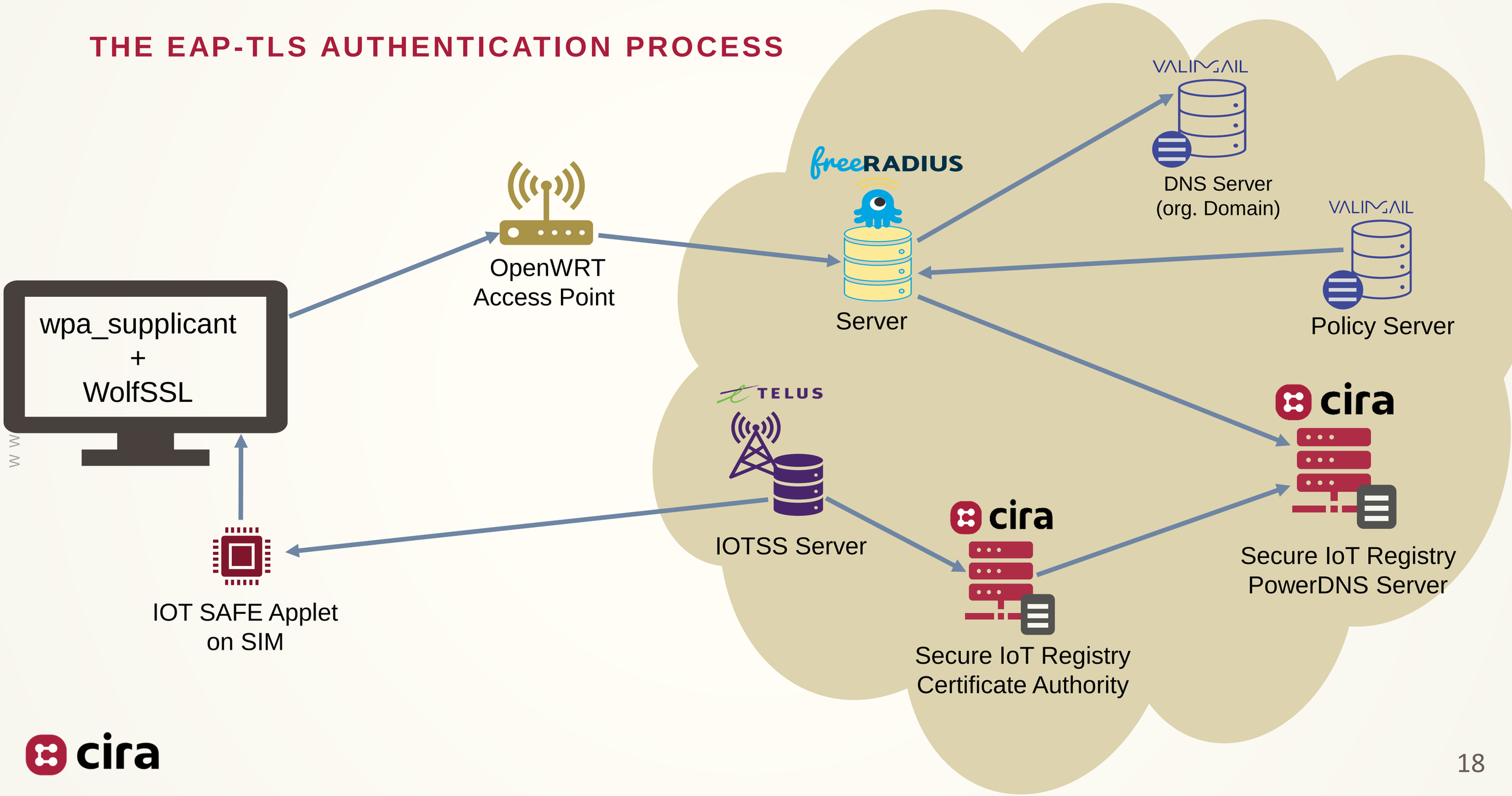
So, what can we do with this system?

A little of this, a little of that...

The secret formula!

The solution we've put together includes
IoT SAFE
CIRA Secure IoT Registry
DNSSEC
DANE
EAP-TLS
wpa_supplicant
WolfSSL
OpenWrt Router
FreeRADIUS
Valimail Custom Policy Server

THE EAP-TLS AUTHENTICATION PROCESS



cira

DANE EVERYWHERE SIMPLIFIES YOUR LIFE ☺

The future with DANE Everywhere
e.g. when EAP-TLS supports DANE, the pattern gets even simpler

DANE & IoT SAFE
a good match

Call to action
join the DANCE (IETF working group)

Q&A

DANCE - DANE Authentication for Network Clients Everywhere

Thank You

ash.wilson@valimail.com

https://www.cira.ca/labs