Secure IoT Registry

Mitigating IoT security threats through device identity management

ICS Security Symposium – Current State of ICS and ICS Security

Jan. 26th 2021

Presented By

Natasha D'Souza

Agenda

cira Secure IoT Registry

Hardware

SIMS today

Digital eSIMS

IoT SAFE eSIMS

Standards

GSMA

GSMA IoT SAFE

IEFT

DNSSEC

IoT Registry

IoT Registry Ecosystem

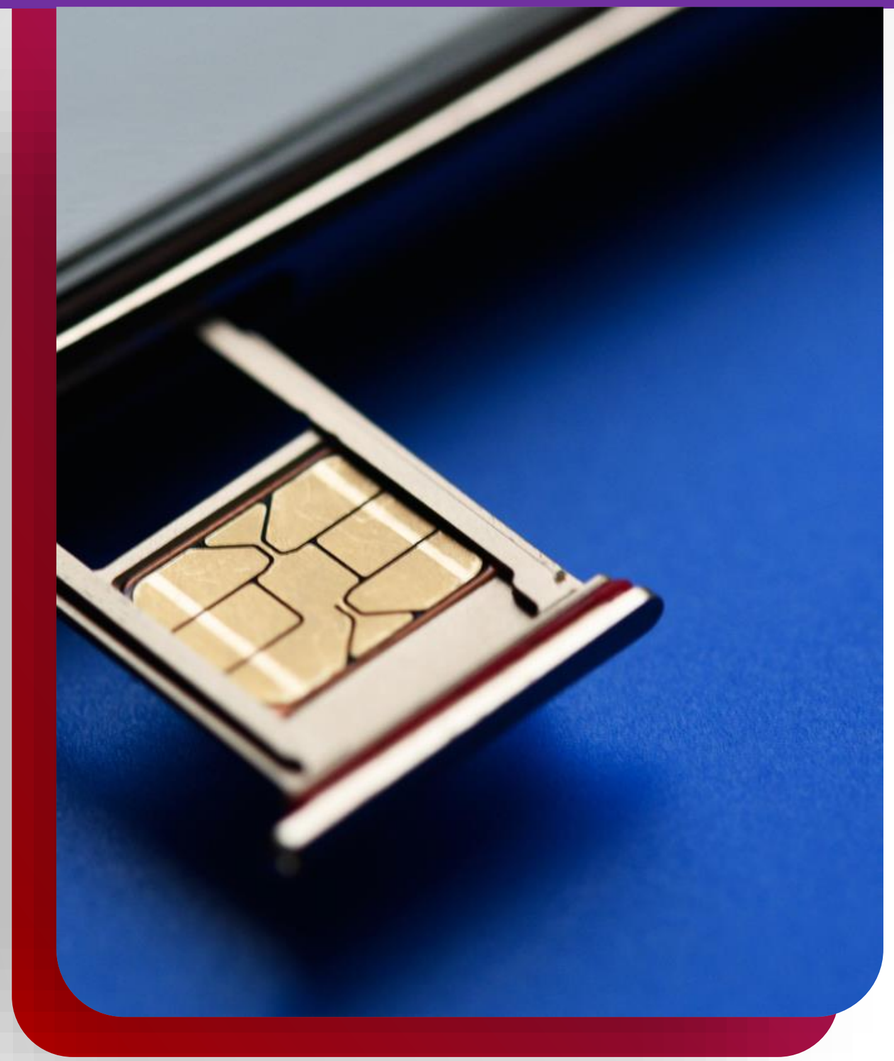
Device Identity Management

DNS & DNSSEC as the new IoT root of trust

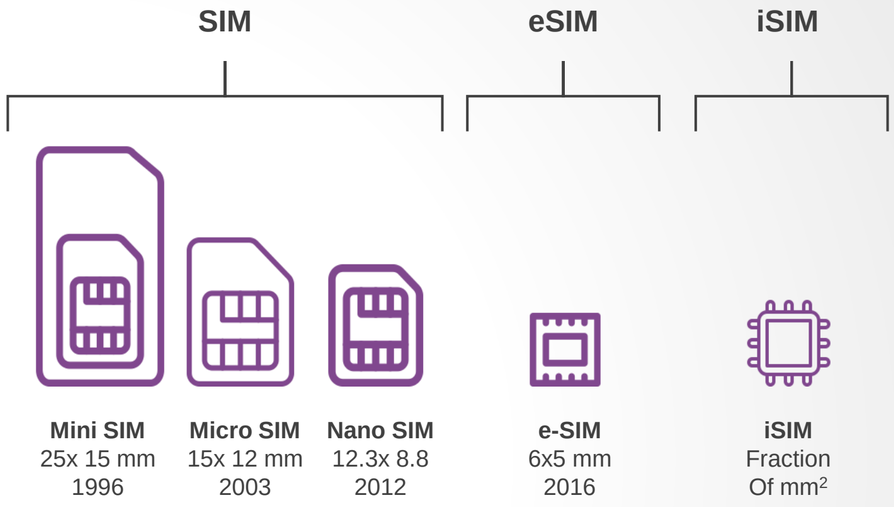
Value Proposition

Use Cases

Value to customers



SUBSCRIBER IDENTITY MODULE - SIM

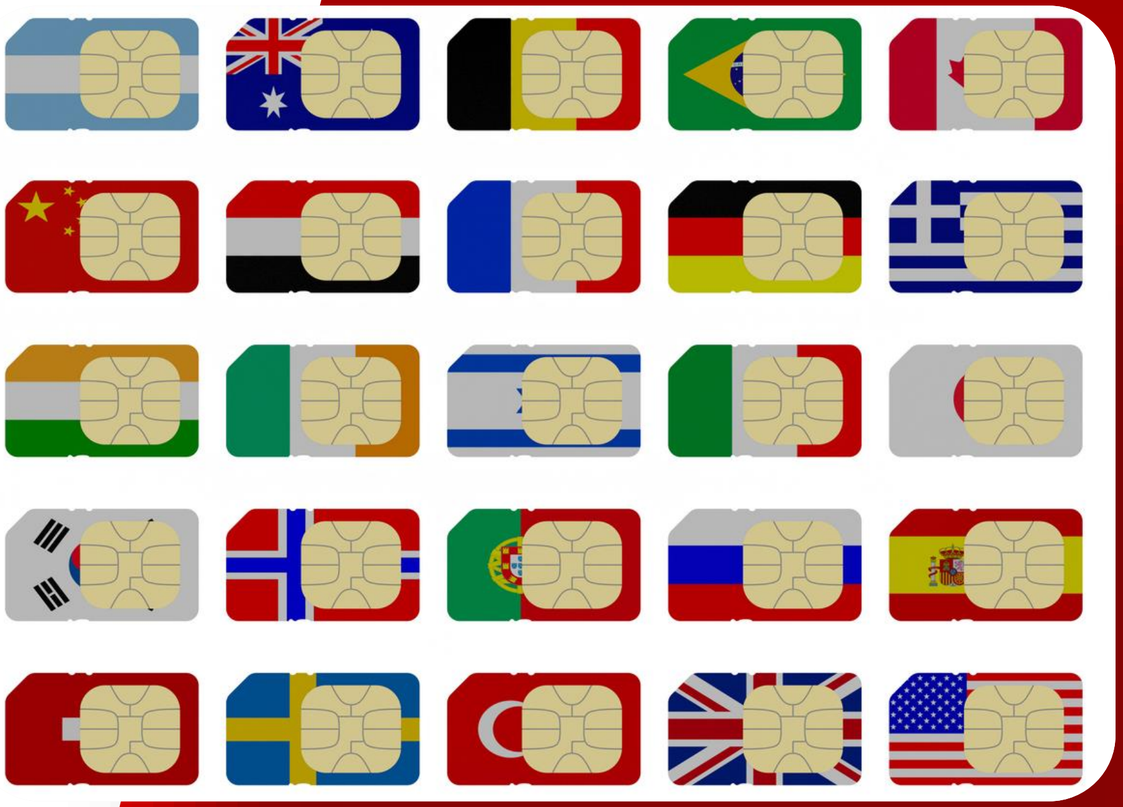


- Tiny, portable memory chip (64k), stores mobile device user info.
- 17 digit code - country code of origin, MNO, unique user ID
- Enables mobile device to connect with a GSM network & GSM networks to track usage

SIMS TODAY

Physical SIM

- Have a set of stored secure credentials
- Locked, mave to change SIM cards when changing providers
- Expensive bill of materials
- Limited control once deployed
- Hackable by having access to a password recovery text on the device
- Get damaged easily



eSIM

Embedded SIM (digital)

- Open ecosystem with multiple profiles
- Smaller power efficient devices
- Reduced cost
- Remote mamagement
- Better at withstanding vibrations and heat, so they can be soldered inside engines and still function

“ Internationally harmonized technical standards are key to enhancing IoT security

Internet Society – Final outcomes & Recommendations Report

https://www.internetsociety.org/wp-content/uploads/2019/05/Enhancing-IoT-Security-Report-2019_EN.pdf

API In Scope
#2, 4

API Out of Scope
1,5,3,6,7

#3
ETSI, 3GPP & Global Platform for OTA SIM management or GSMA for remote SIM provisioning

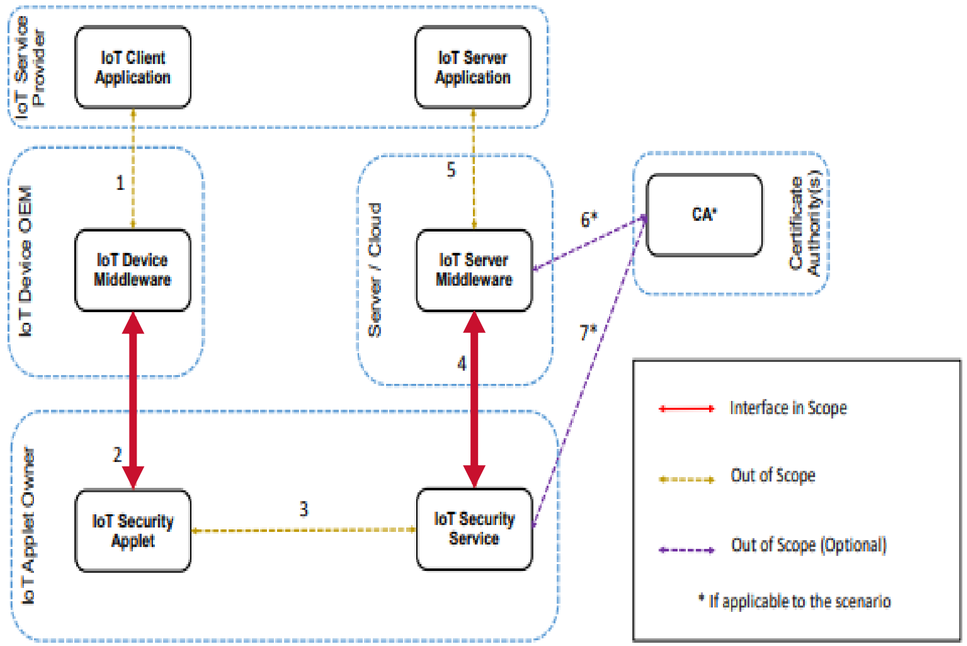
#1, #5
Mozilla IoT Schema, Web of Things

#5
New EPP like IETF standard to be developed

#6,7
Existing CA specs.

ARCHITECTURE

Using the SIM as a 'Root of Trust' to Secure IoT Applications



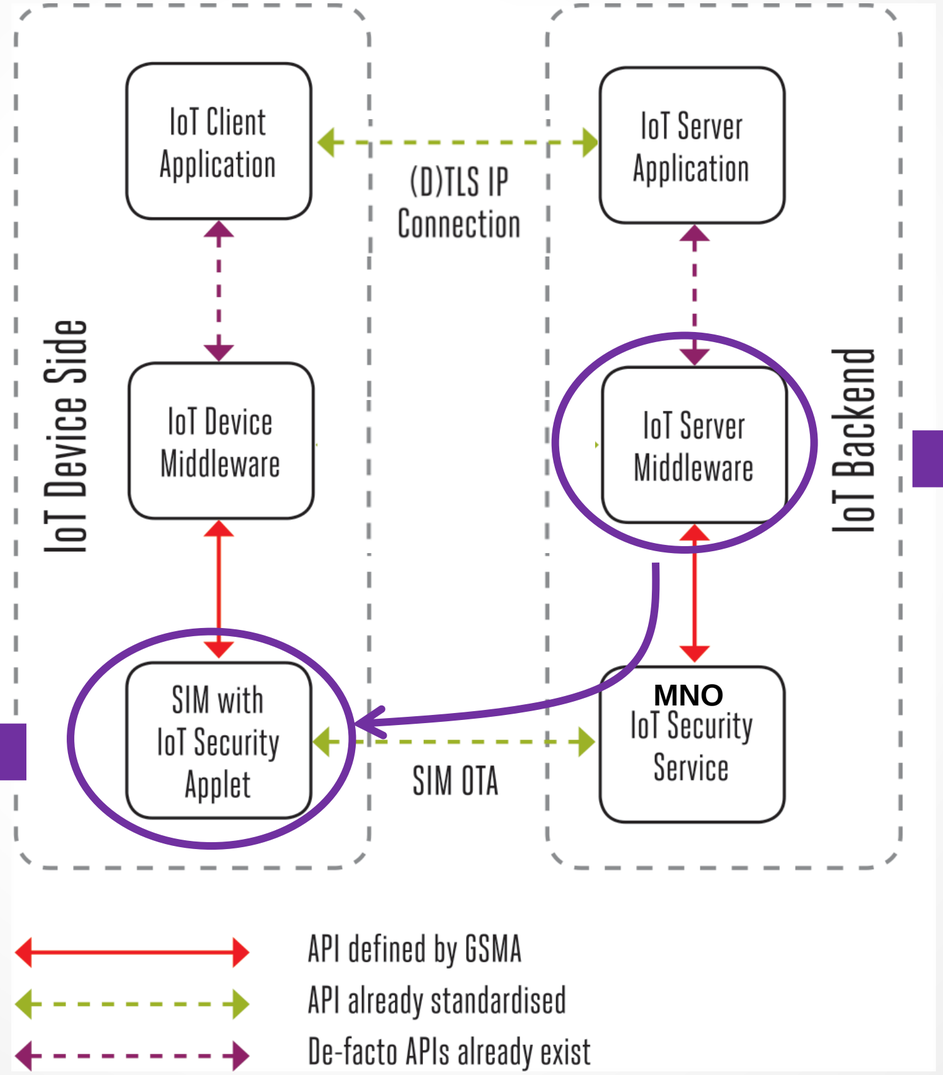
IoT SAFE
IoT SIM Applet For Secure End-to-End Communication

https://www.gsma.com/iot/iot-safe/

ZERO TOUCH REMOTE eSIM PROVISIONING

Building on the existing eSIM → MNO trust model

'Bad Actor' in the middle attack proof solution



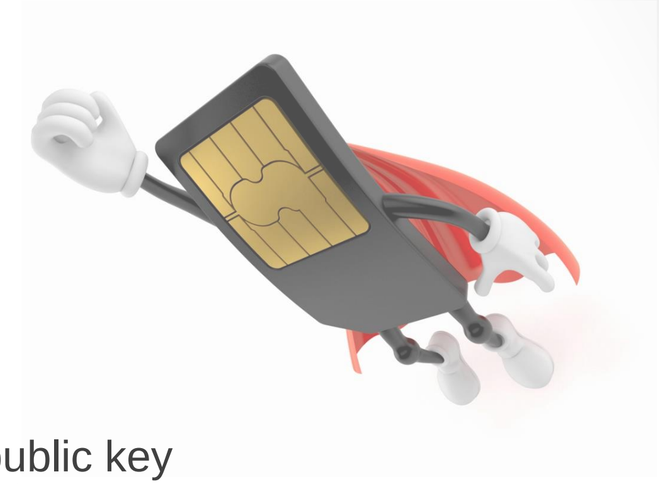
eSIM

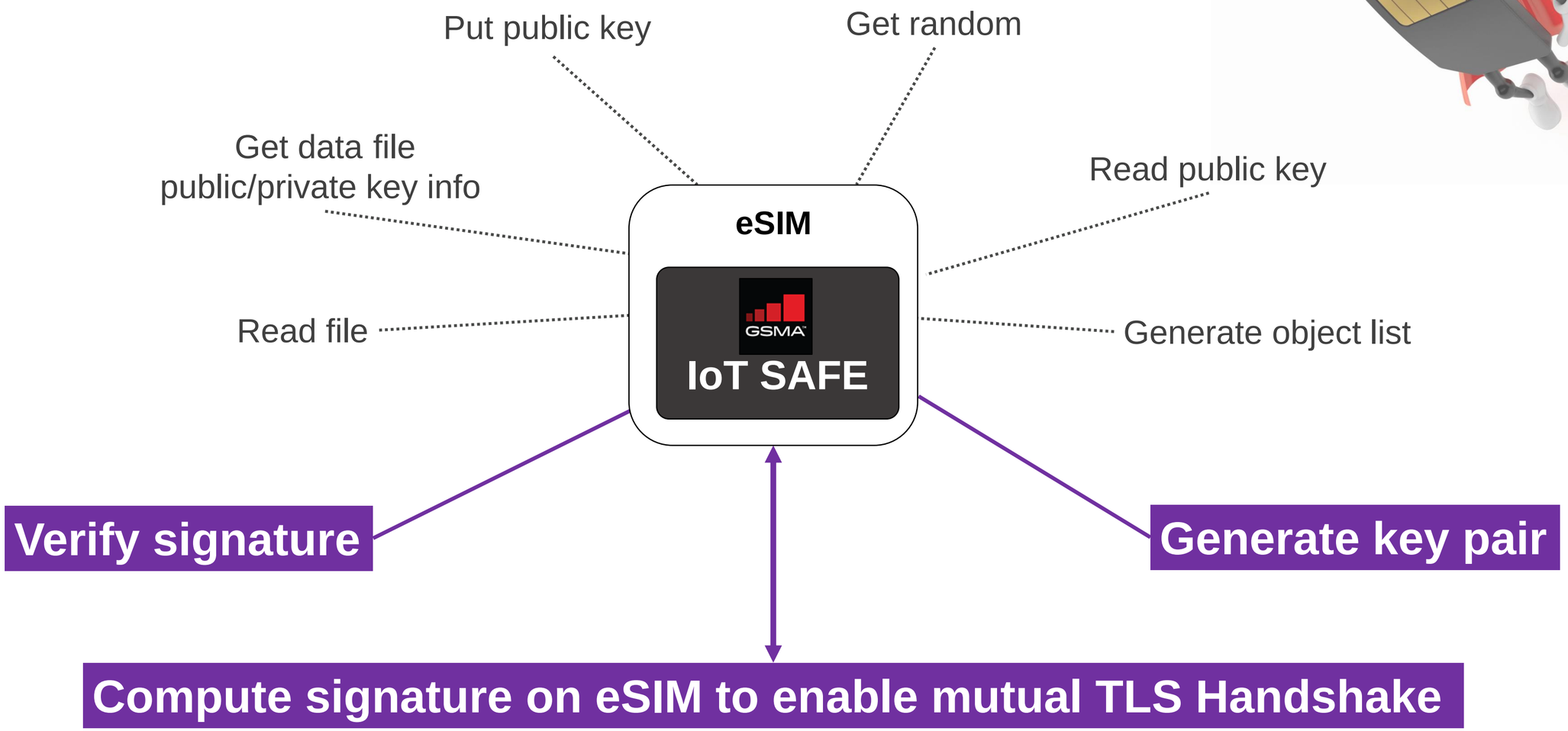
GSMA IoT SAFE

cira Secure IoT Registry

Provides DNSSEC based IoT device attestation linked to the eSIM ID

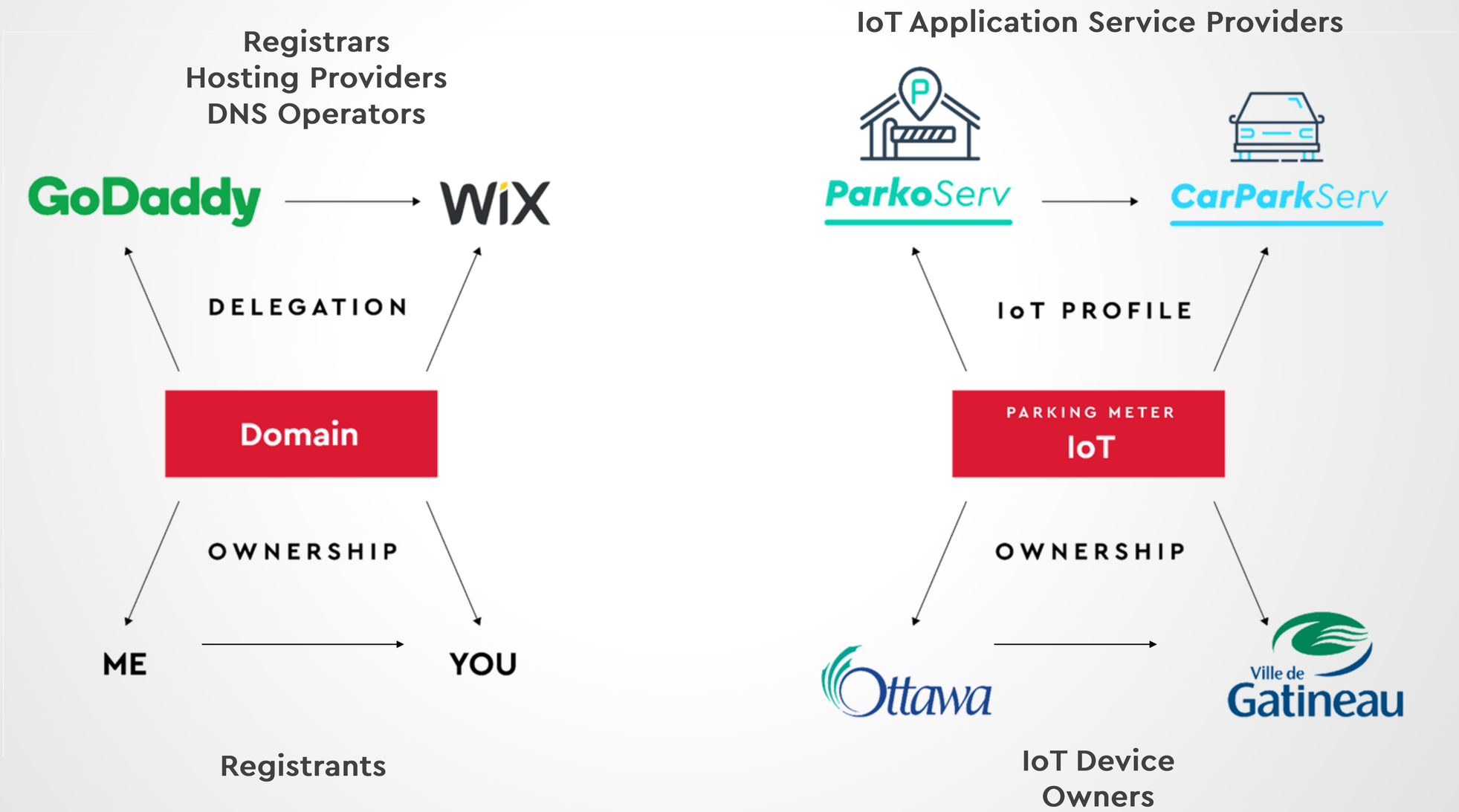
eSIM ARE LIKE SMARTCARDS, MINI HSM OR TPM





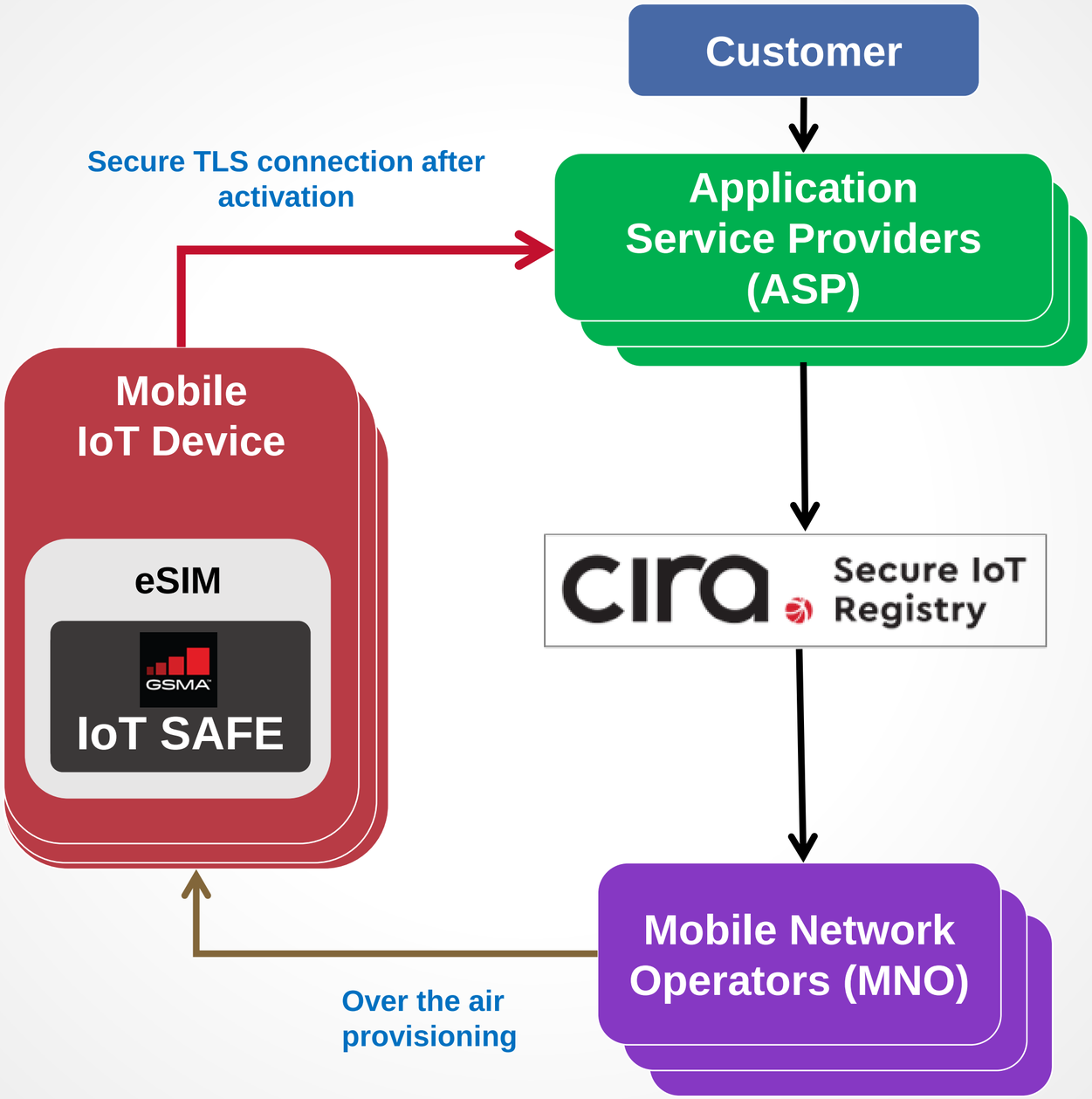
SIMILARITIES BETWEEN

Domain Names & IoT Devices



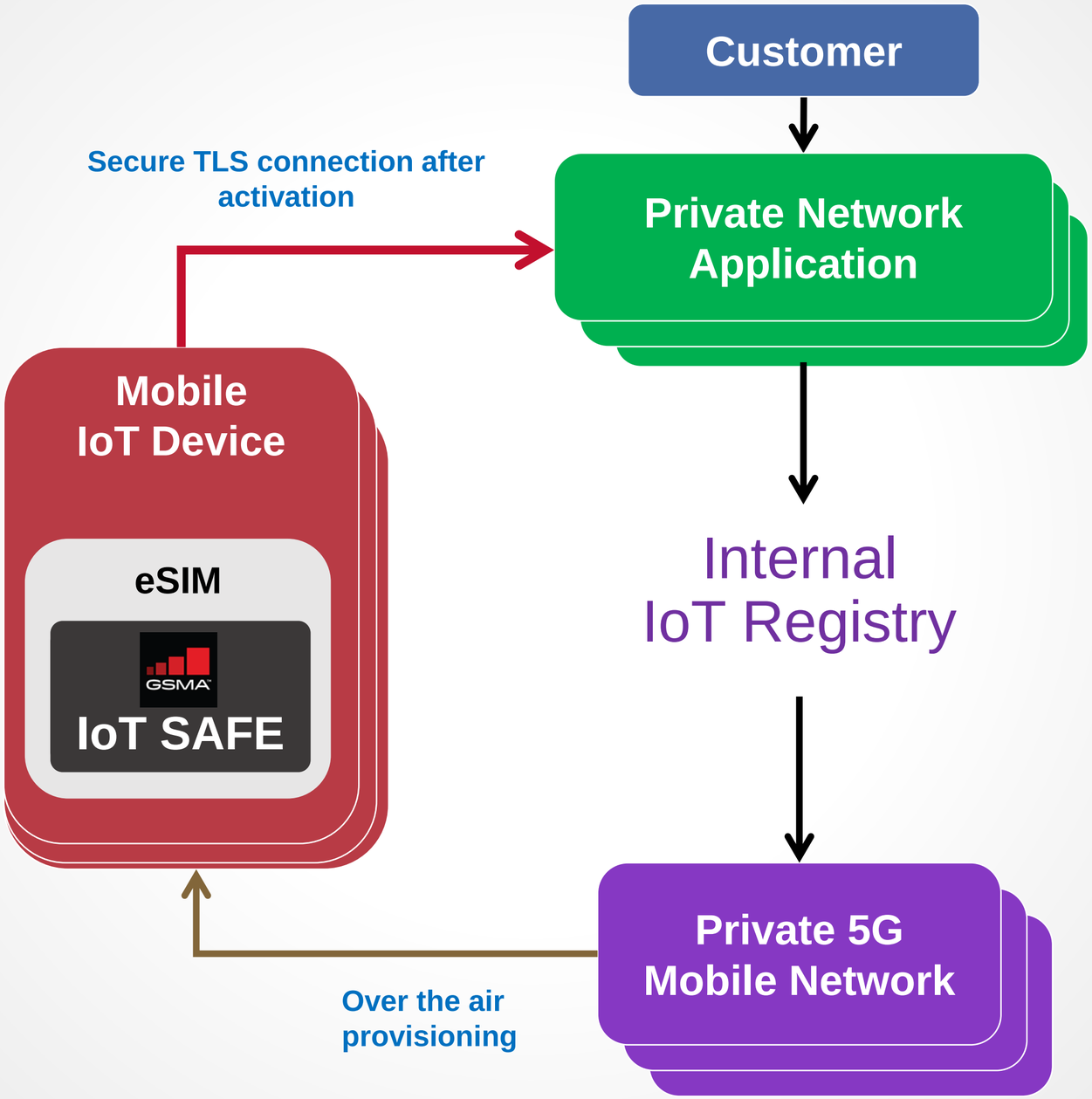
IoT REGISTRY

Public Internet Ecosystem



IoT REGISTRY

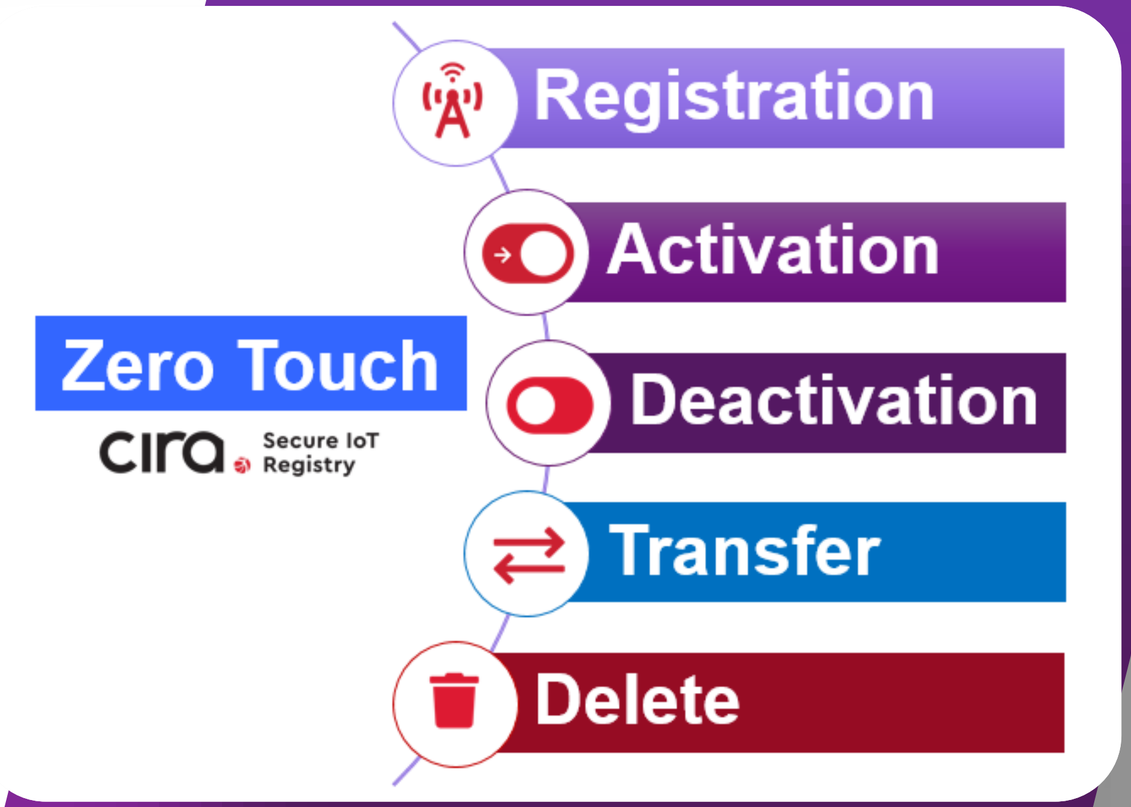
Private Network Ecosystem



CIRA SECURE IoT REGISTRY

Device Identity Management

- Connects to correct MNO
- Pushes configuration / security certificates to the devices
- Provisioning/De-provisioning devices
- Changing MNO/service provider for devices
- Disconnecting from MNO



HARDWARE ROOT OF TRUST

Inherent Trust of a cryptographic system by the ecosystem

- Foundation on which all secure operations of an ecosystem use & depend on
- Provides a trusted execution environment (TEE) for software to run on
- Inherently trusted so must be secure by design
- Critical component of public key infrastructures (PKIs)
- Trust keys & cryptographic information to be authentic & authorized

eSIM

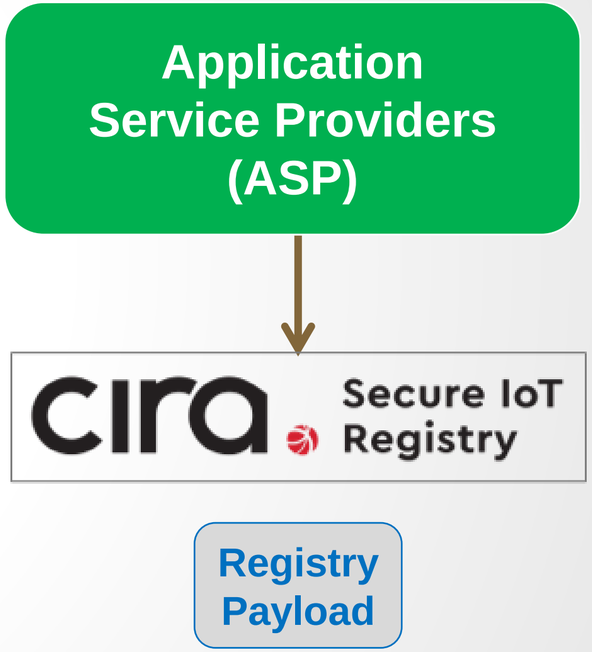
GSMA IoT SAFE

Registration

INFO FOR THE IoT DEVICE TO CONNECT WITH THE ASP

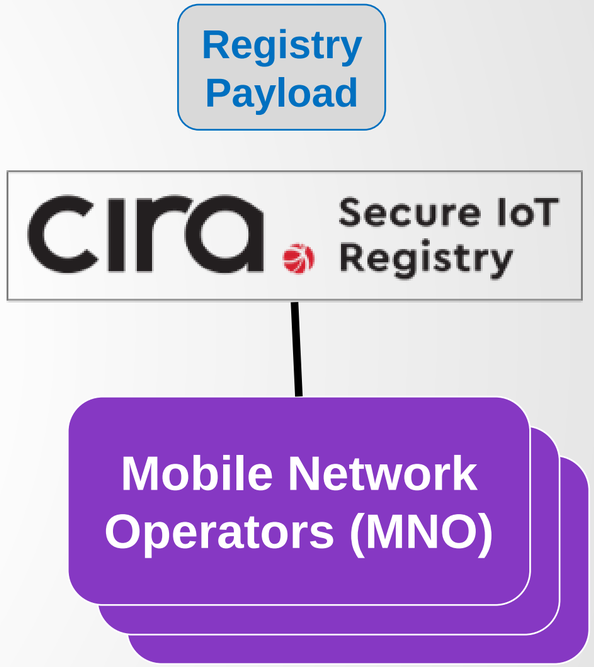
Cloud IoT Application Service Provider Requirements

- Building the Registry Payload content
- Need the IoT device end point info.
  - URL, port,
  - WiFi SSID + Password (encrypted)
  - ASP CERT, etc…
  - ASP FQDN (that's DNS ;-)



Registration

Mobile Network Operator Integration



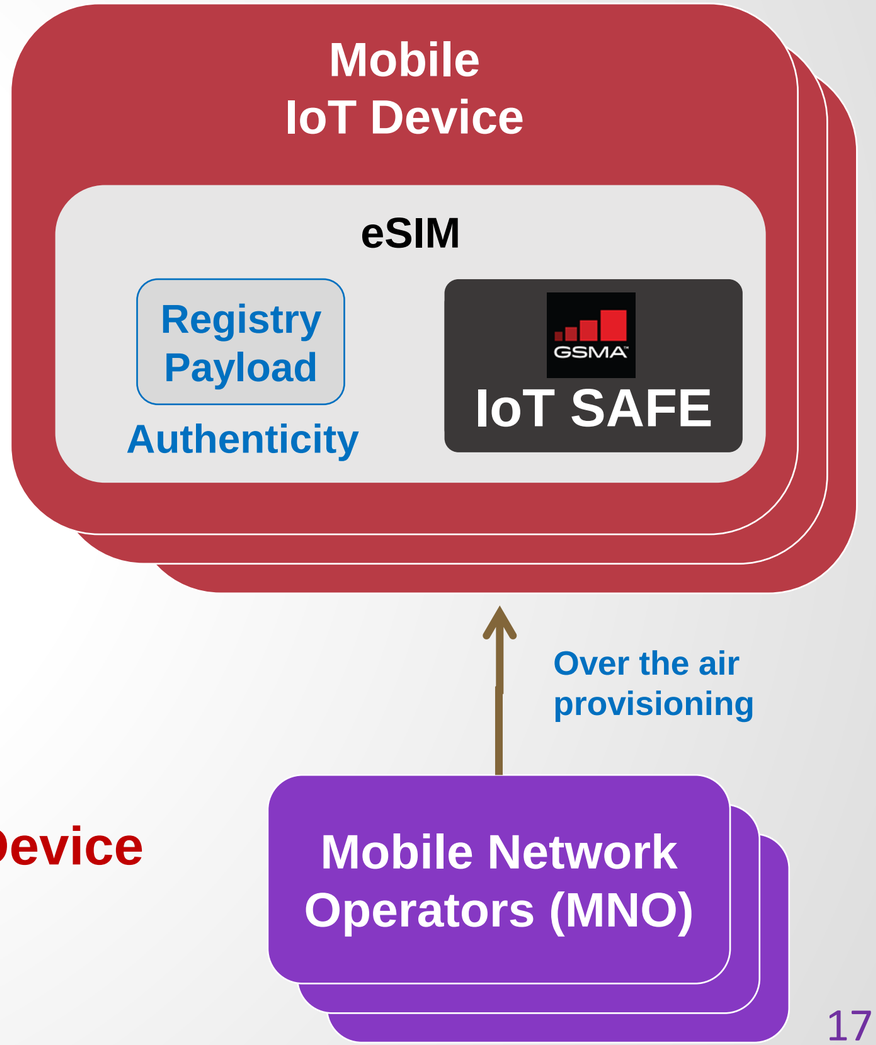
- Setup trusted connection
- Provide CIRA root certs
- Provide CIRA IoT Registry DoT service
- Enough info to send a **Registry Payload to the IoT device**

Enough information for the IoT device to connect with the ASP

Activation

Once IoT device is live on MNO Network

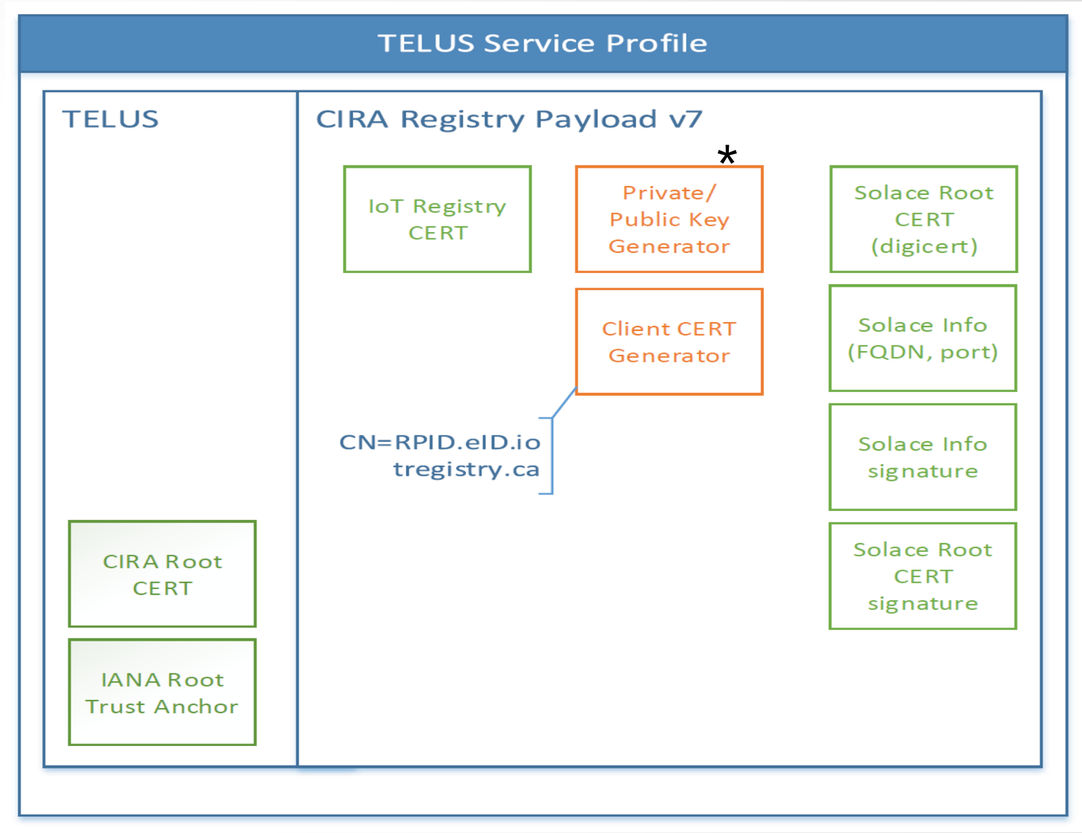
- Ask the IoT device via MNO to create a new key pair (public/private)
- MNO sends the IoT device CSR to the IoT registry to sign
- IoT Registry returns a signed CERT to the MNO & ASP
- MNO sends the signed CERT on the IoT eSIM



This is when we push the Registry Payload to the IoT Device

Registry Payload

- IoT registry CIRA profile
- IoT Registry related CERTs
- CIRA DoT Trusted Recursive CERT
- IANA root trust anchor
- CN – Unique value per SIM linked with eUICCID (unique eSIM ID)



Pre-provisioned at SIM activation

Downloaded over-the-air

* Private / Public Key pair generated on-board

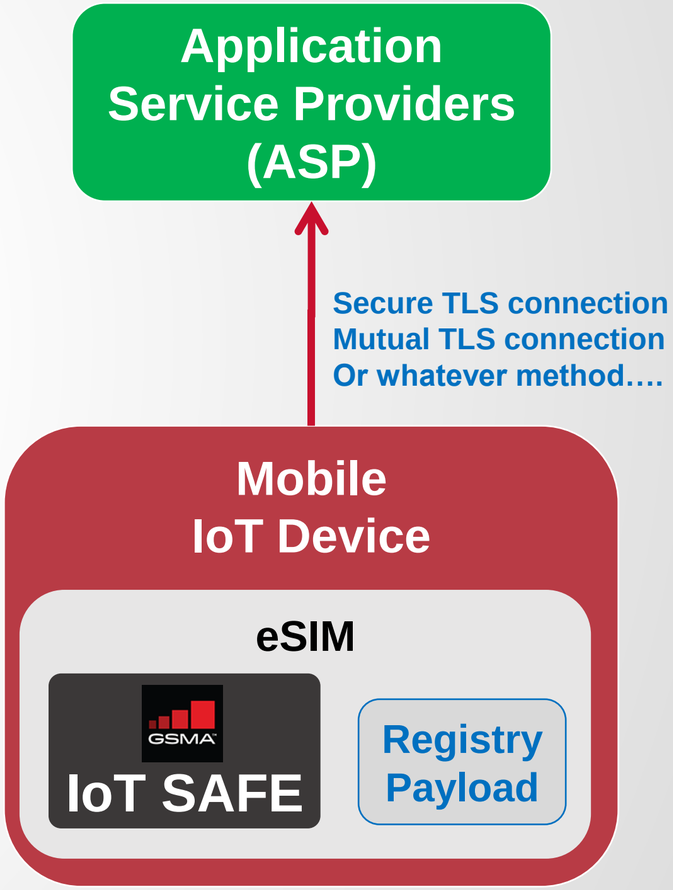
Enabling a new root of trust leveraging DNSSEC

Activation

Connect securely to the cloud/ASP

- Verify authenticity of Registry Payload with the unique IoT device 'IoT SAFE' private keys
- IoT Registry published a hash of the CERT in DNS w/DNSSEC
- Authenticity/identification of the IoT device can be verified with the signed CERT & via DNSSEC
- The IoT device can establish a connection to the ASP

Use Registry Payload information to connect to ASP (IoT device middleware must support this function!)

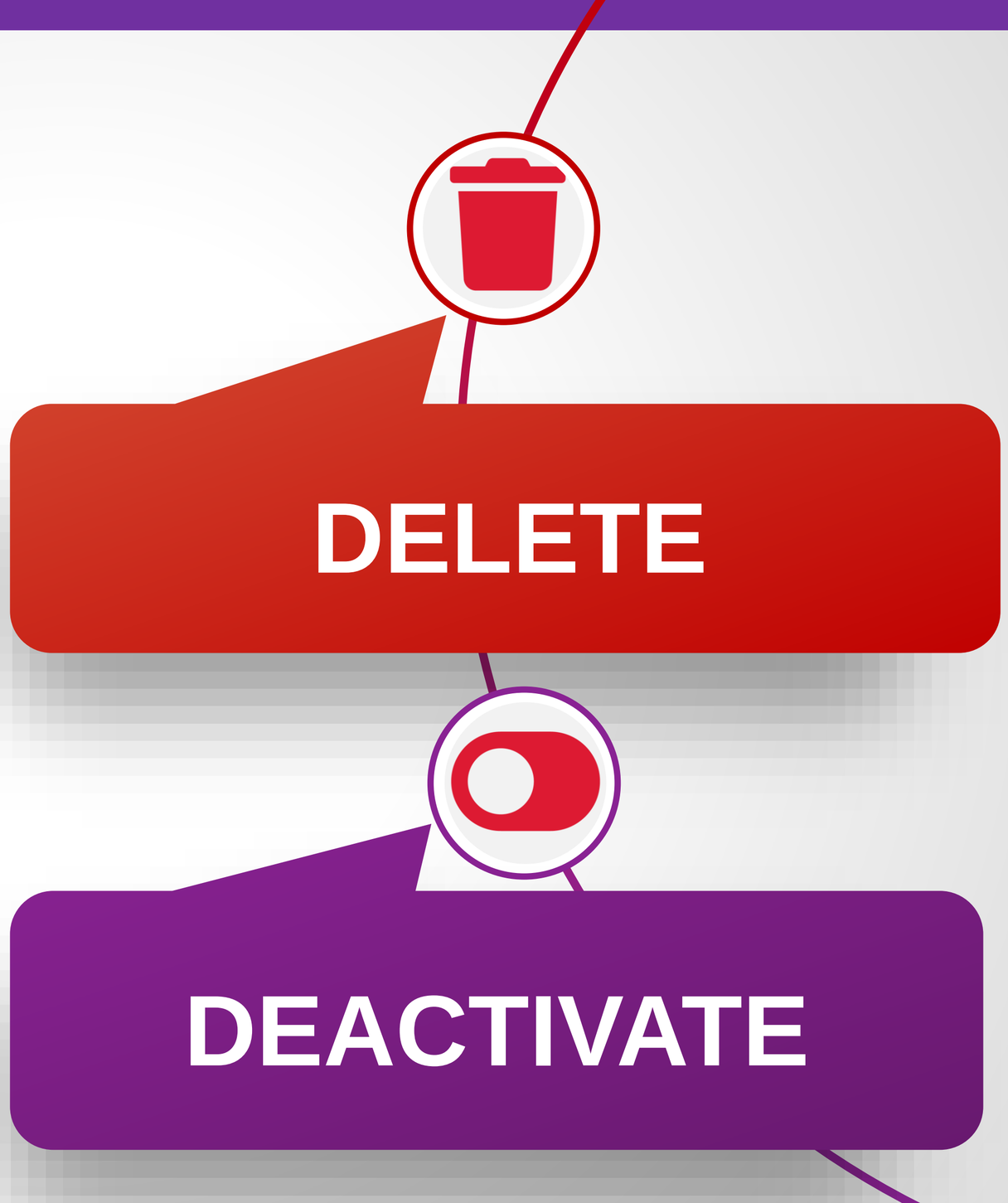


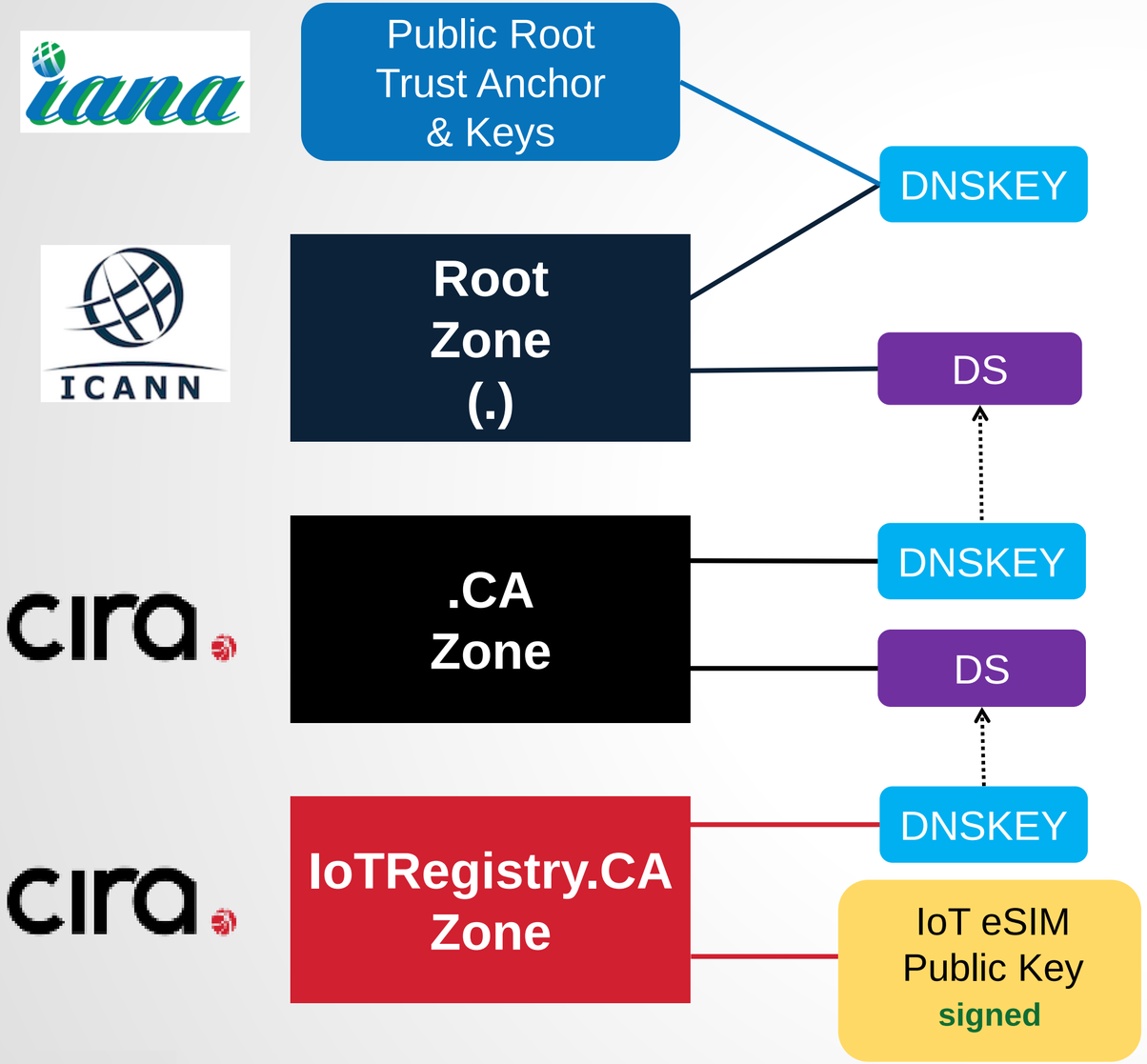
DEACTIVATION & DELETE

Very Important in Device Management

Deactivate - De-provisioned but still listed in the IoT Registry

Delete - Delete from the IoT Registry





A NEW ROOT OF TRUST - DNSSEC

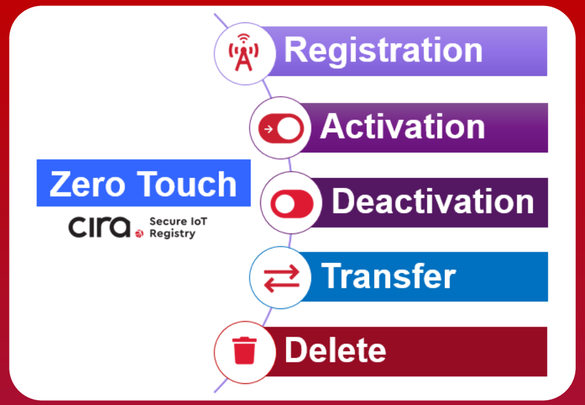
Leveraging the public DNS & DNSSEC to validate

- Authentication of IoT SAFE Applet by eSIM ID
- Authenticity Registry Payload using IoT SAFE crypto functions
- TLSA – DNSSEC based TLS Certificate authentication (ASP authentication)

✓DNS ✓

VALUE PROPOSITION

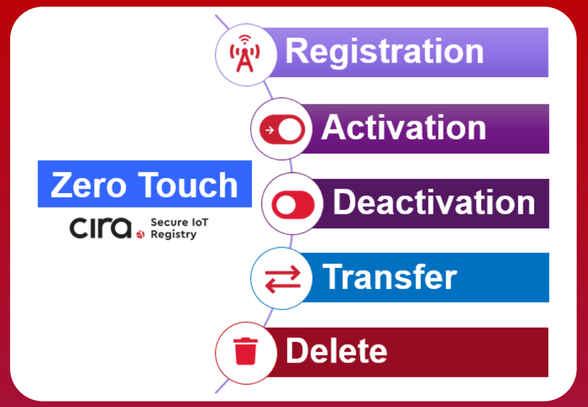
Features vs Benefits



Feature	IoT Device Manufacturer/Cloud Provider	Customers, 3rd Party Installers
Hardware Root of Trust	End-to-end, chip-to-cloud security	Peace of mind
IoT SAFE eSIM enabled IoT devices	Zero touch provisioning/ re-provisioning of credentials	Enhanced, inherent security
Always ON remote registration, activation & transfer	• Easy setup & lifecycle management • Confirmed to belong to vendor	Plug & play installation & setup
Remote turn off / wipe clean IoT device config	Granular control of credential provisioning	Effortless management of broken or stolen IoT devices

VALUE PROPOSITION

Features vs Benefits



Feature	IoT Device Manufacturer/Cloud Provider	Customers, 3rd Party Installers
IoT Security at scale	Hassle free quick scaling	Unlimited options for products
Interoperability across different service providers	New business model	Leverage best value for service
Multiple profiles on one device	Competitive differentiator	Straightforward management

Thank You

Contact Us

ciralabs@cira.ca