Secure IoT Registry

CIRA's IoT Registry
Remote eSIM Provisioning

and more ☺

ICANN | 69, Technical Day

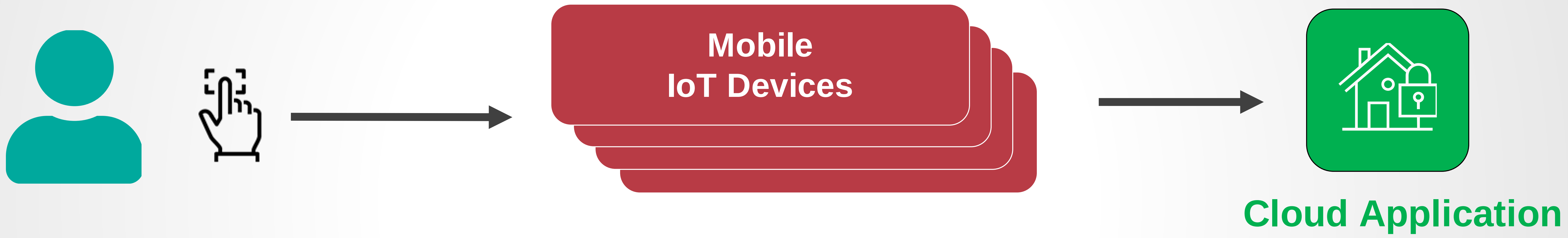
Oct. 19th 2020

Presented By

Natasha D'Souza, Product manager, IoT Security,CIRA Labs

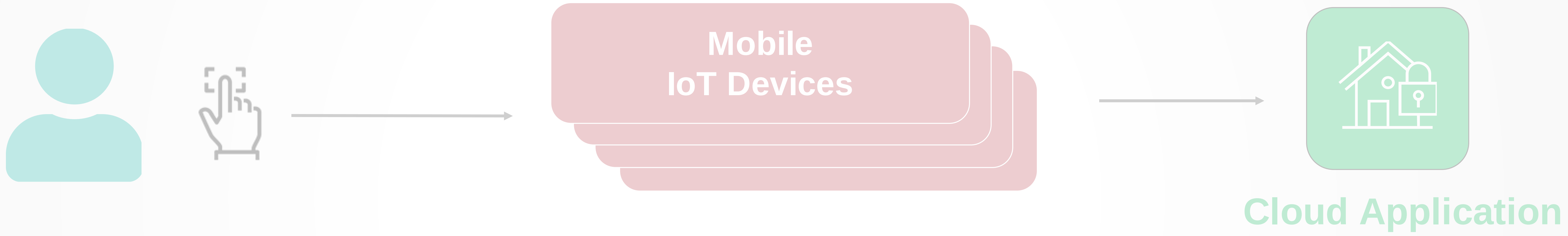
IoT Turning Point: Hardcoded vs. Zero Touch

Today - Hardcoded

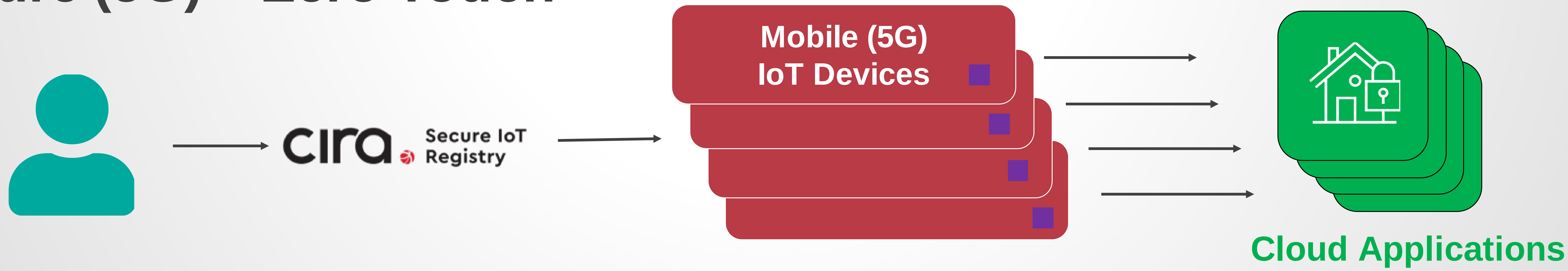


IoT Turning Point: Hardcoded vs. Zero Touch

Today - Hardcoded

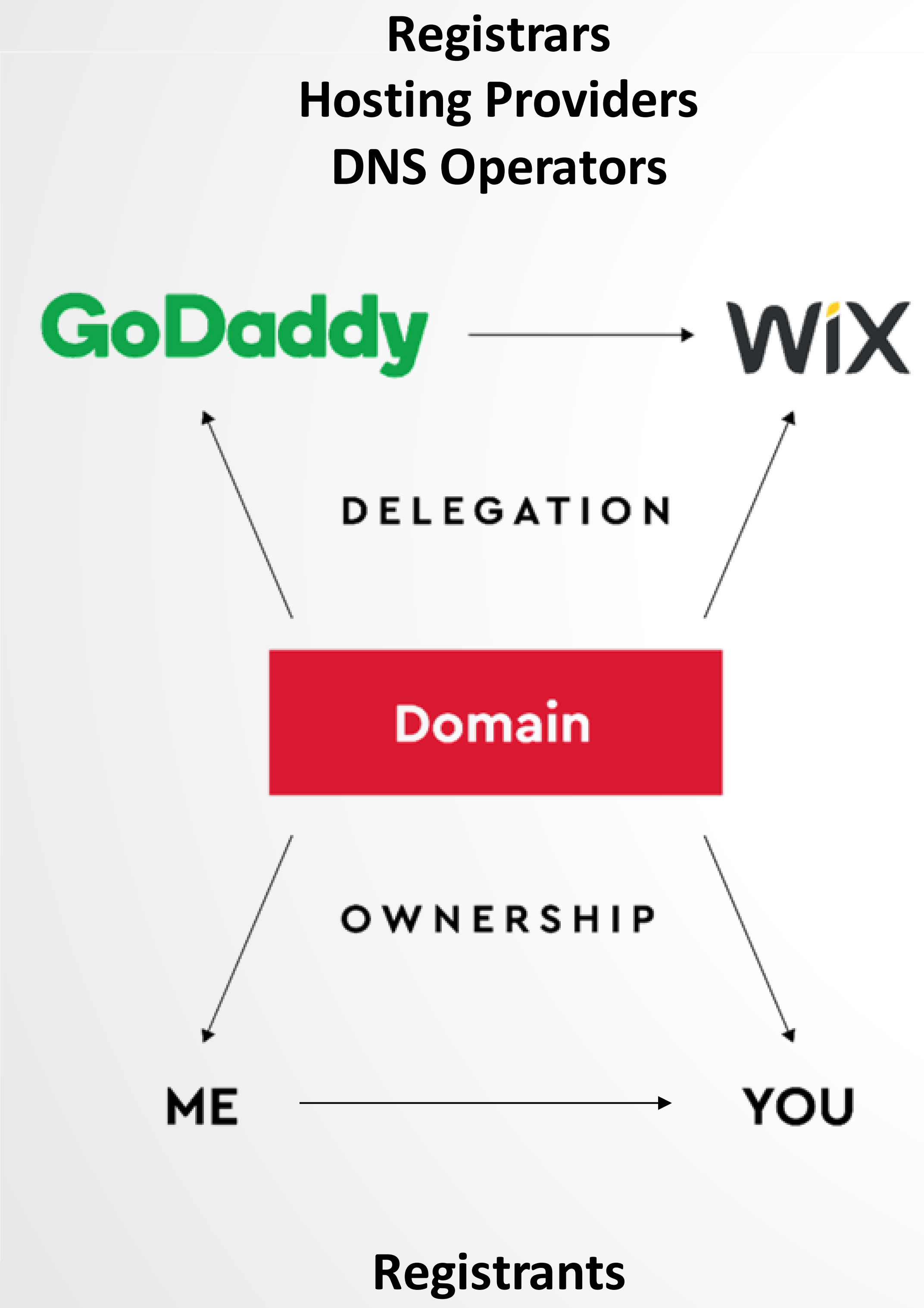


Future (5G) – Zero Touch



🟪 Registry payload

Domain Names & IoT Devices are similar



Registrars
Hosting Providers
DNS Operators

GoDaddy → WiX

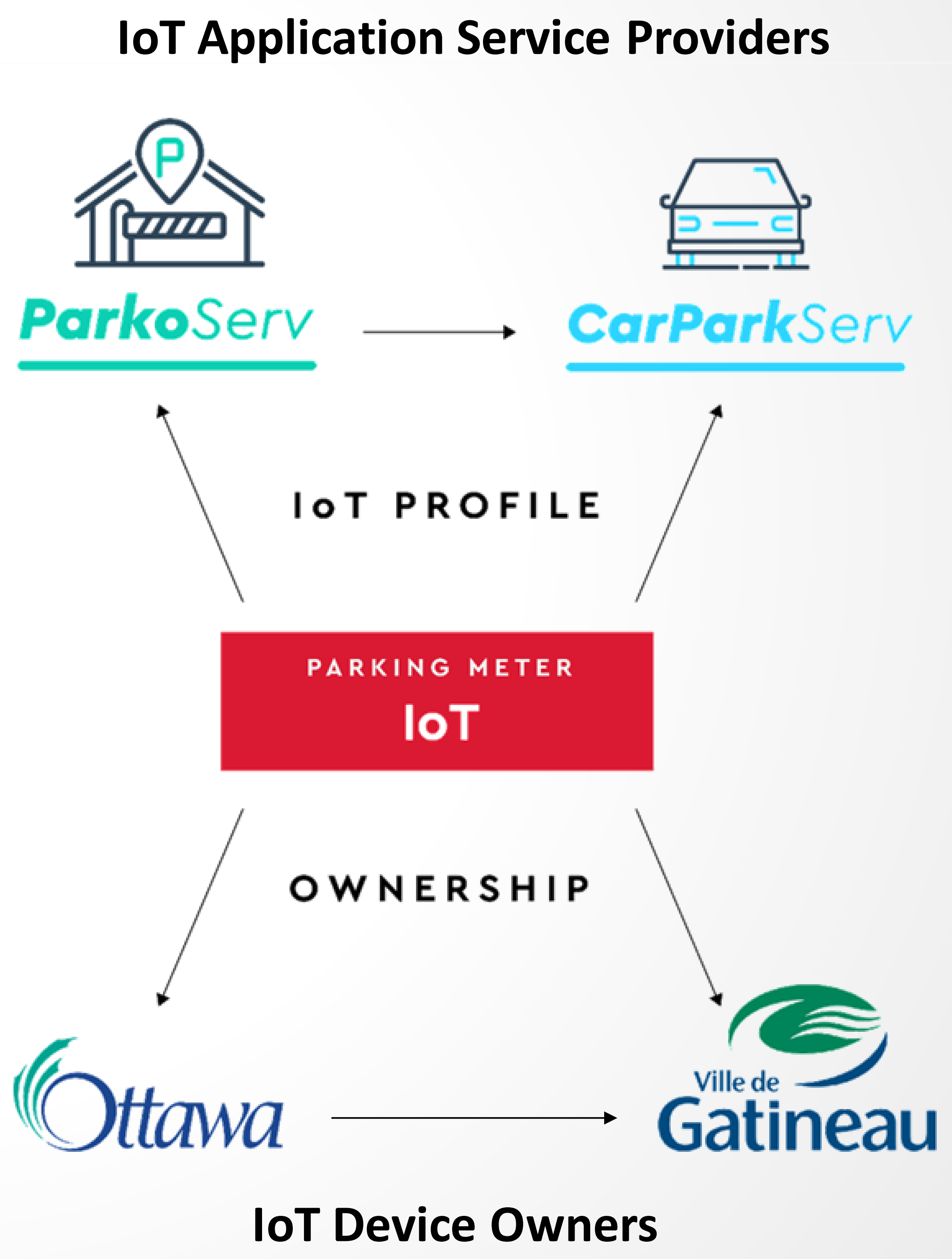
DELEGATION

Domain

OWNERSHIP

ME → YOU

Registrants



IoT Application Service Providers

ParkoServ → CarParkServ

IoT PROFILE

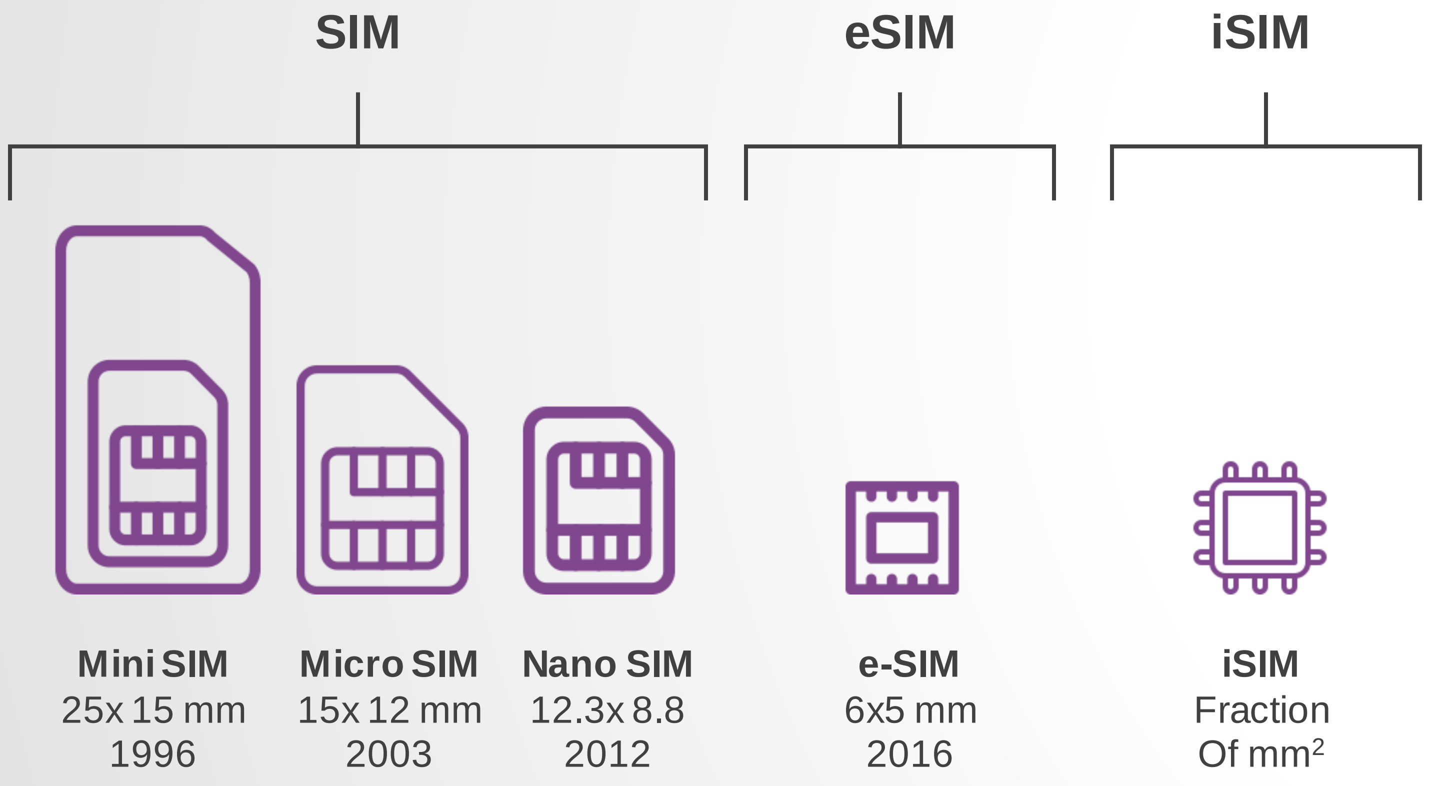
PARKING METER
IoT

OWNERSHIP

Ottawa → Ville de Gatineau

IoT Device Owners

Physical SIM vs eSIM (digital SIM)



SIM

eSIM

iSIM

Mini SIM
25x 15 mm
1996

Micro SIM
15x 12 mm
2003

Nano SIM
12.3x 8.8
2012

e-SIM
6x5 mm
2016

iSIM
Fraction
Of mm^2

SIM

- Have a set of secure credentials stored digitally
- They have to be installed and activated in-store
- **Plastic card - easy to break/lose**
- Needs space for physical installation
- Have to change SIM cards when changing providers

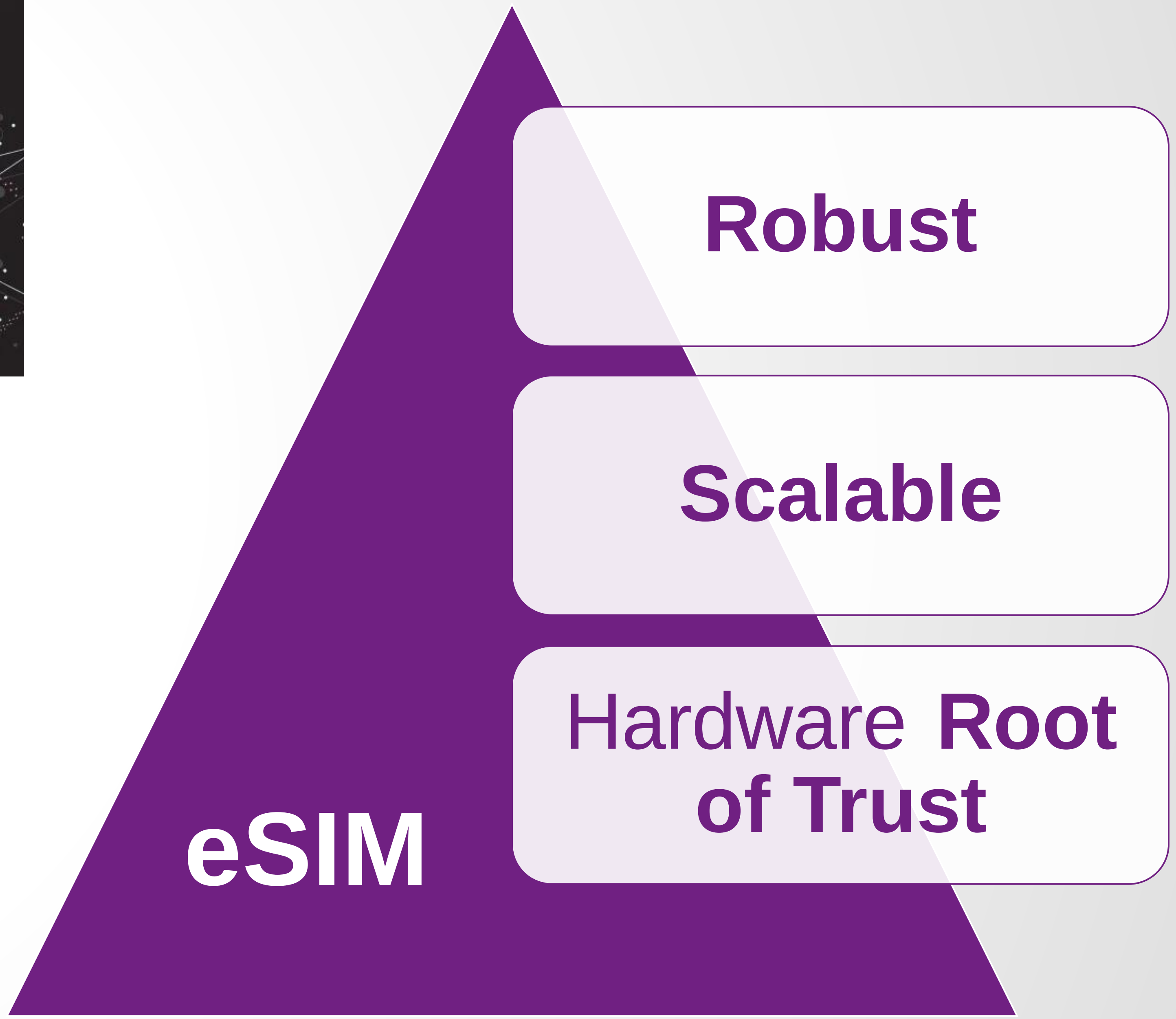
eSIM

- Can be **remotely provisioning over the air**
- Can’t be lost and no in-store visit needed
- Save on space as it’s embedded on the device
- Reduction of mechanical failures
- Change MNO providers remotely
- Multiple profiles on one device

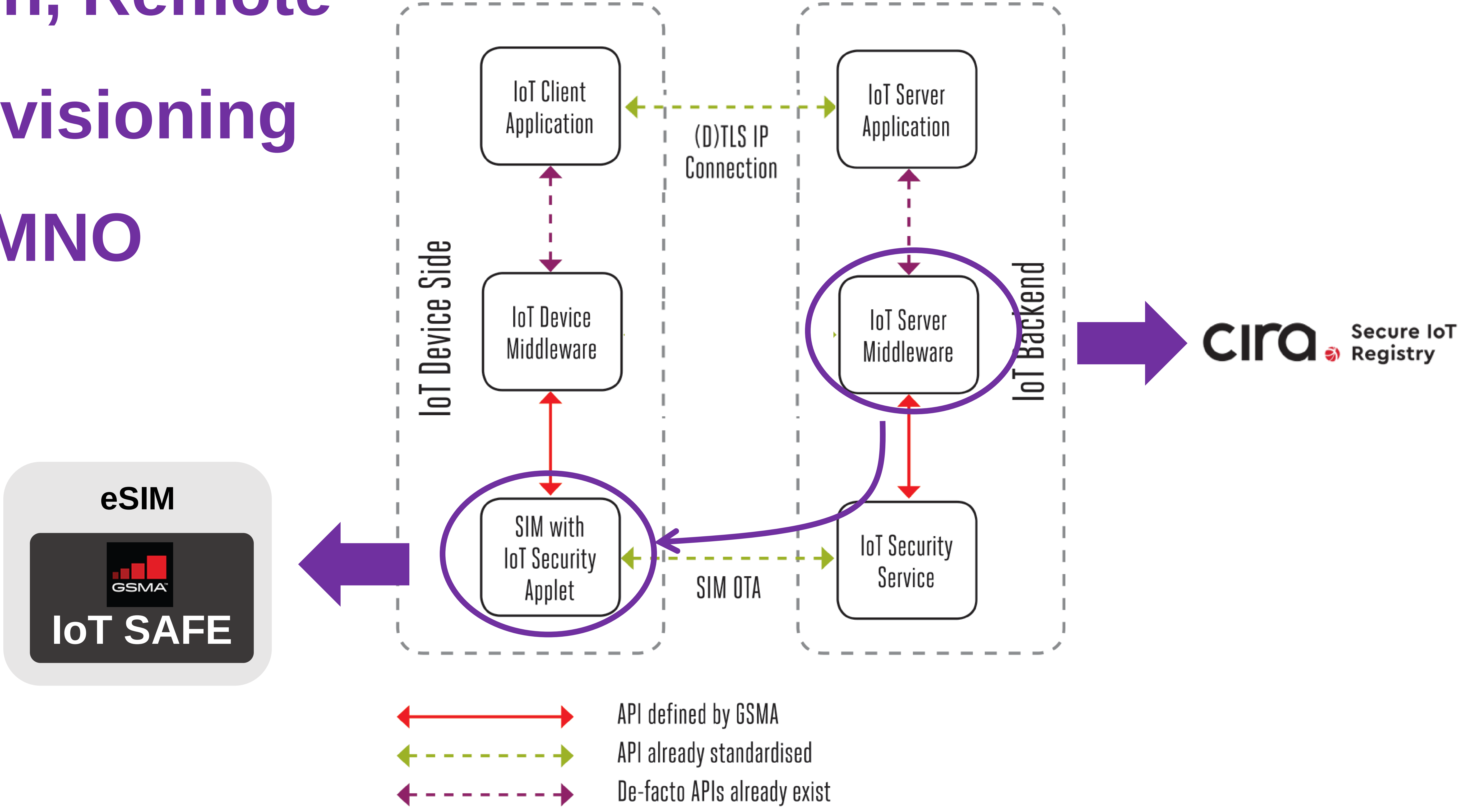
Standards Body to Enable

IoT

- Device manufacturers
- Service providers



Zero Touch, Remote eSIM Provisioning by MNO



IoT Device Side

IoT Client Application

IoT Device Middleware

SIM with IoT Security Applet

(D)TLS IP Connection

SIM OTA

IoT Backend

IoT Server Application

IoT Server Middleware

IoT Security Service

eSIM

GSMA

IoT SAFE

cira Secure IoT Registry

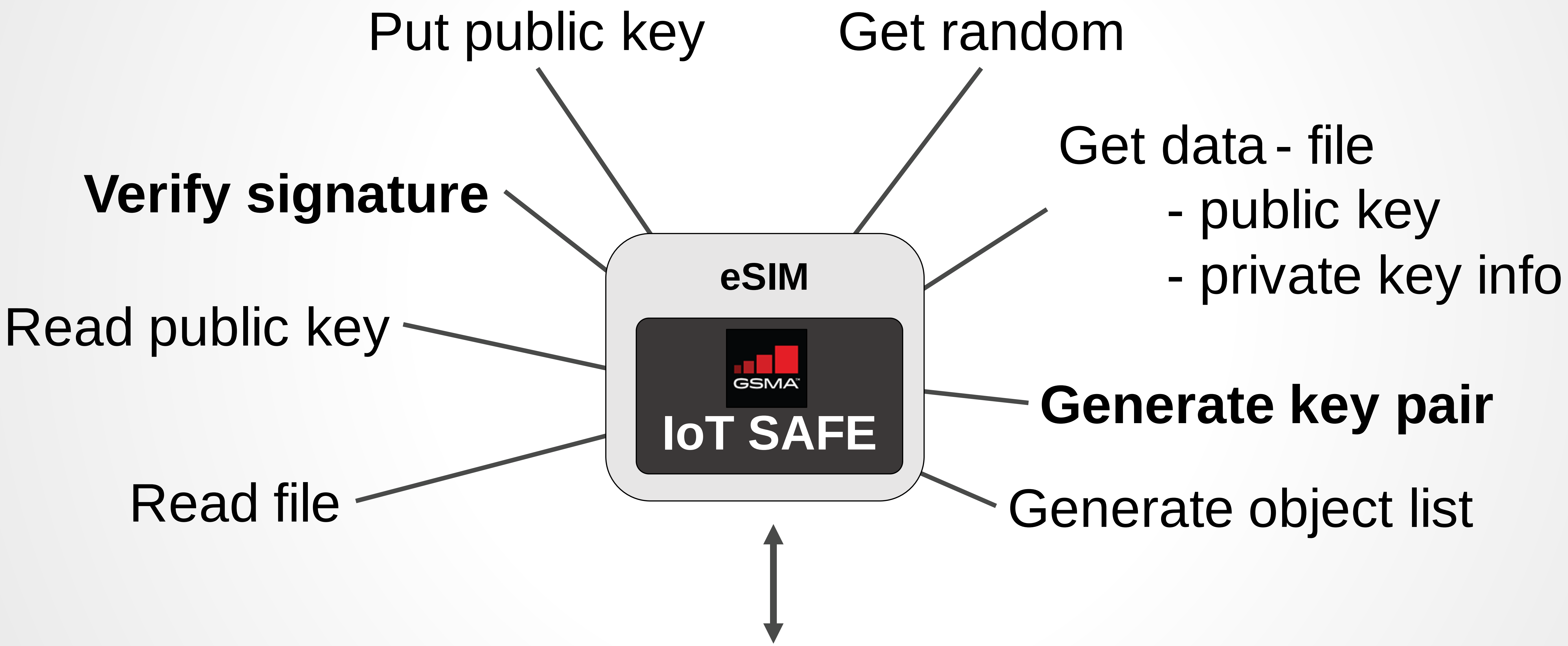
API defined by GSMA

API already standardised

De-facto APIs already exist

The IoT SAFE eSIM can:

eSIM are mini HSM like TPM!



Put public key

Get random

Verify signature

Get data - file
- public key
- private key info

Read public key

Generate key pair

Read file

Generate object list

Compute signature → to enable bidirectional TLS Handshake

ENABLING IoT CONNECTIVITY

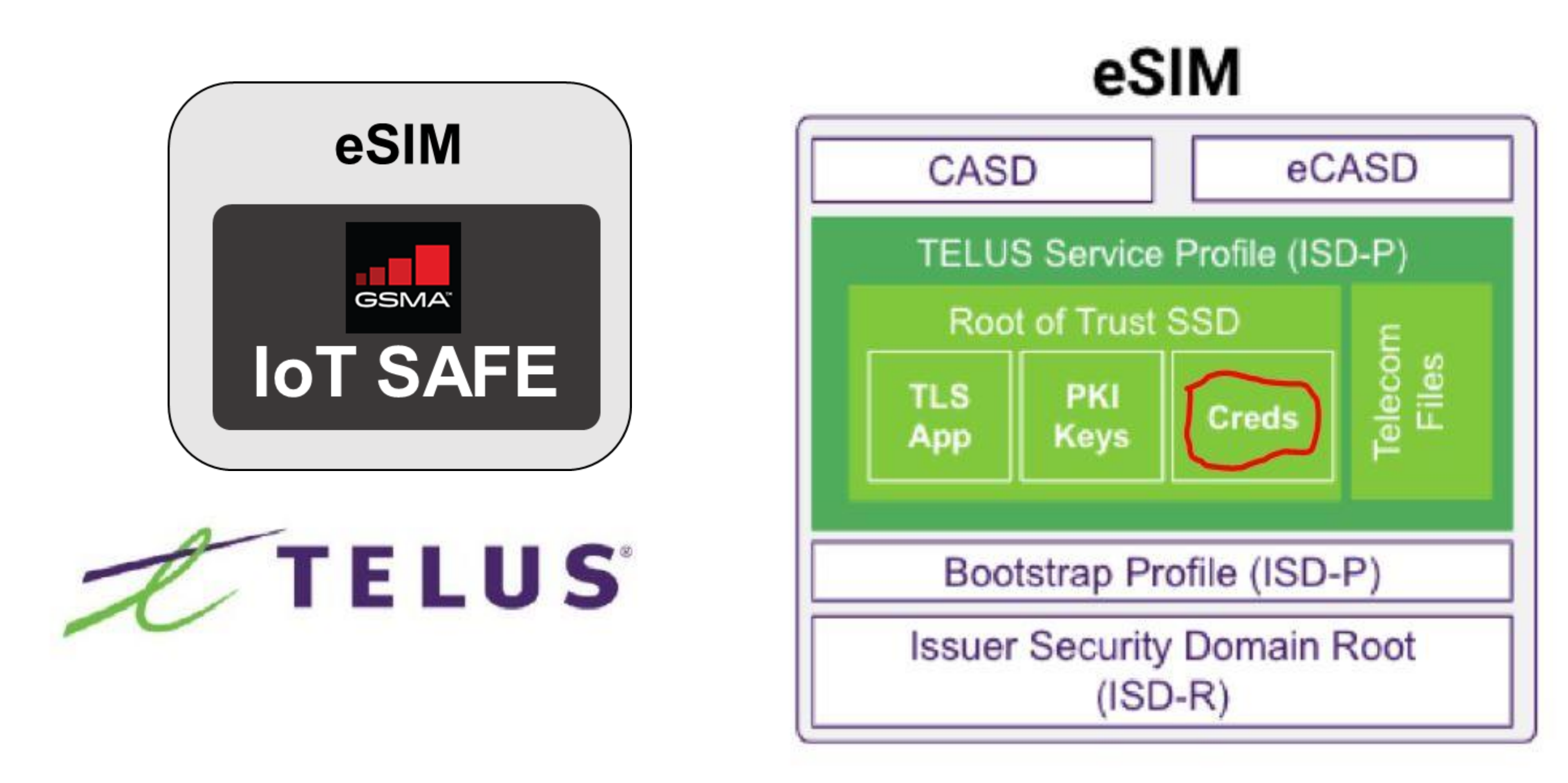
By downloading the Registry Payload to the eSIM

W W W . C I R A . C A

Registry Payload

Application/Cloud Service Provider

- ASP CERTS
- Domain name / URL / FQDN
- Port Number
- IoT, ASP & other Certificates
- SSID credentials

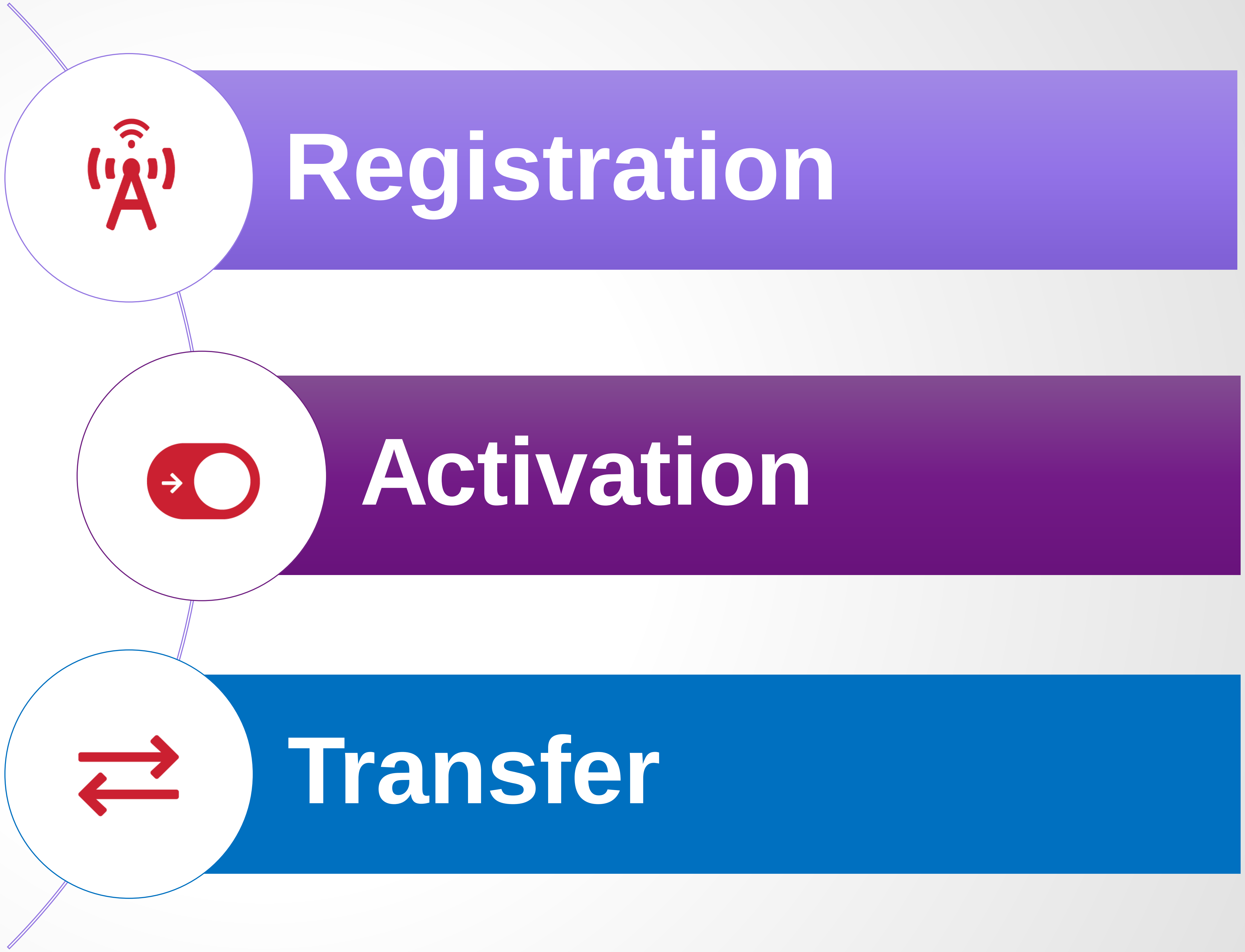

eSIM
GSMA
IoT SAFE
TELUS
eSIM
CASD
eCASD
TELUS Service Profile (ISD-P)
Root of Trust SSD
TLS App
PKI Keys
Creds
Telecom Files
Bootstrap Profile (ISD-P)
Issuer Security Domain Root (ISD-R)

cira

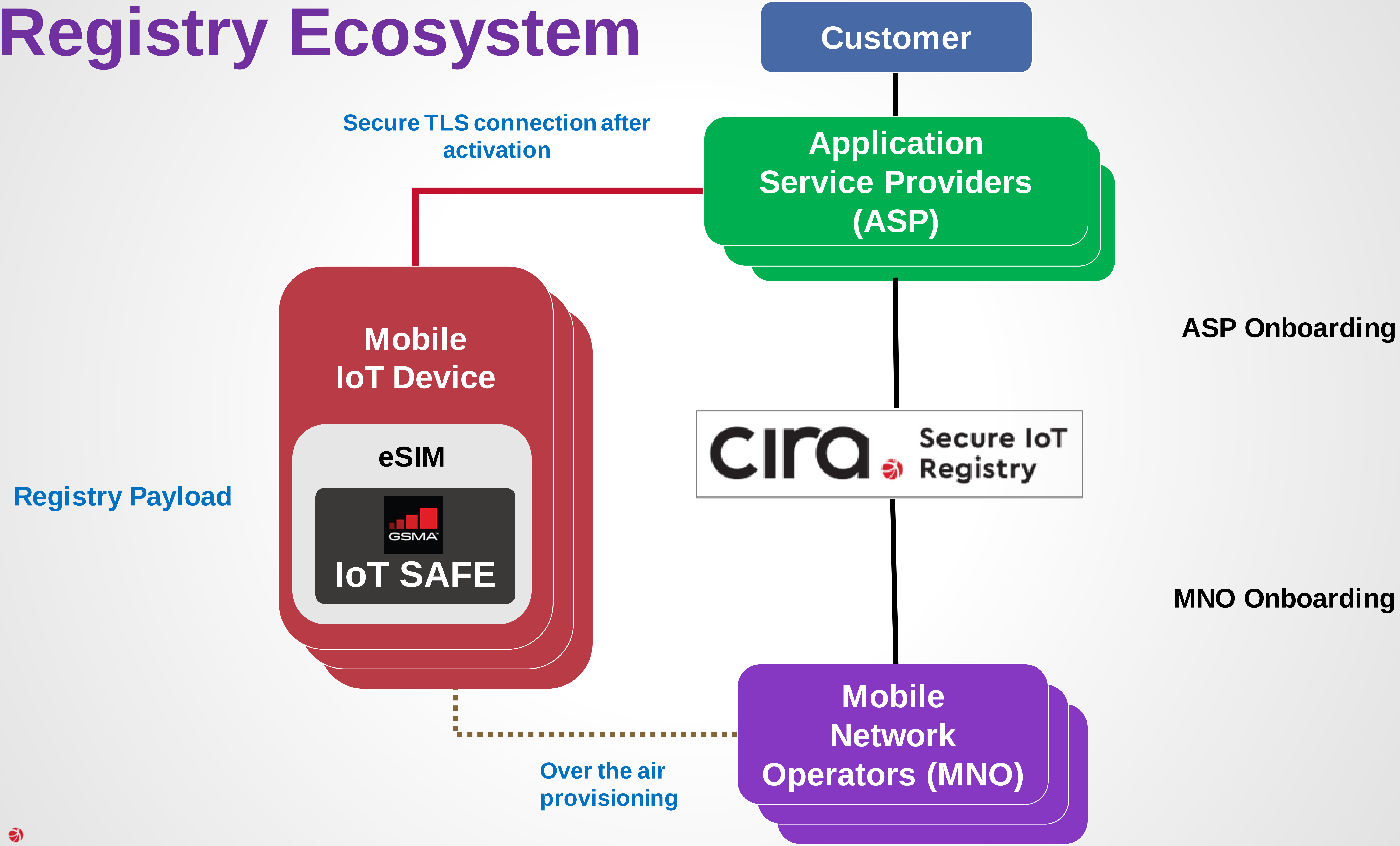
CLASSIFICATION:CONFIDENTIAL

Zero Touch

cira Secure IoT Registry



IoT Registry Ecosystem

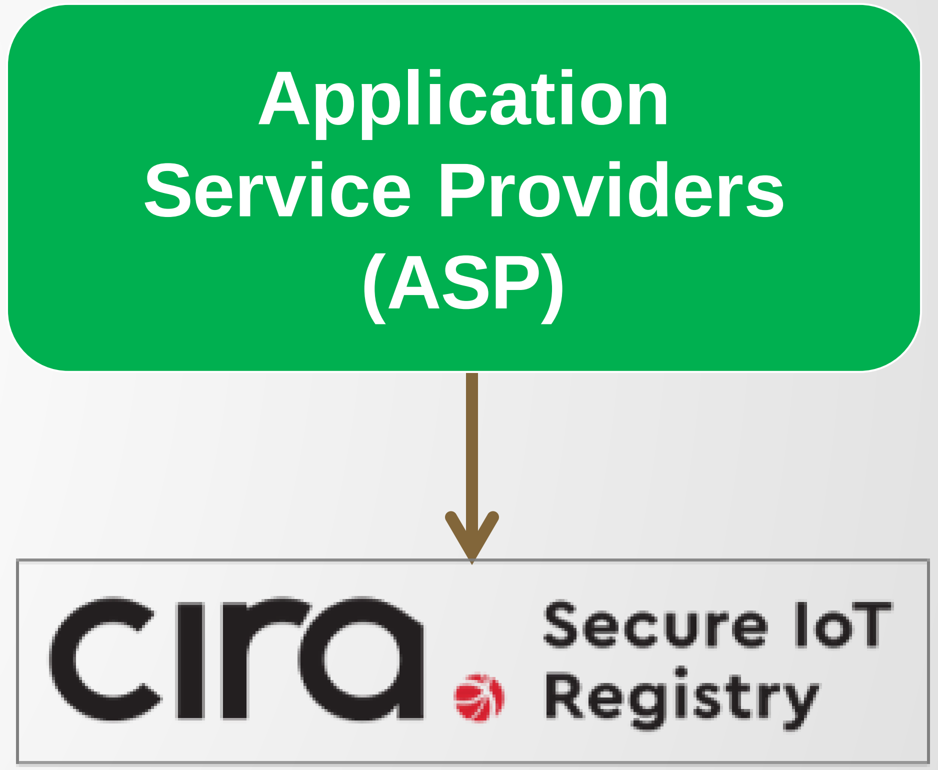


Customer
Secure TLS connection after activation
Application Service Providers (ASP)
ASP Onboarding
Mobile IoT Device
eSIM
GSMA
IoT SAFE
Registry Payload
cira Secure IoT Registry
MNO Onboarding
Mobile Network Operators (MNO)
Over the air provisioning

IoT Registry Onboarding

ASP/Cloud Onboarding (like Registrar onboarding)

- We need to know what their end point config is.
  - URL, port, ASP CERT, etc…
- We provide the IoT Registry root cert, DNS information

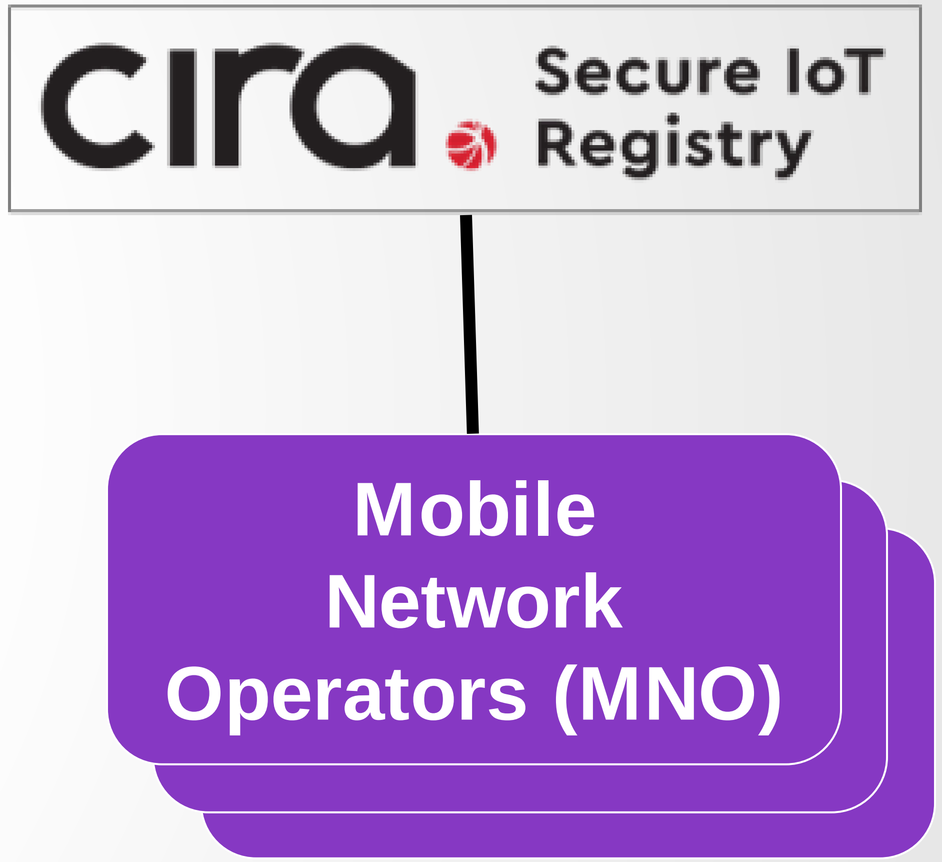


Enough information the IoT device to connect with the ASP

IoT Registry Onboarding

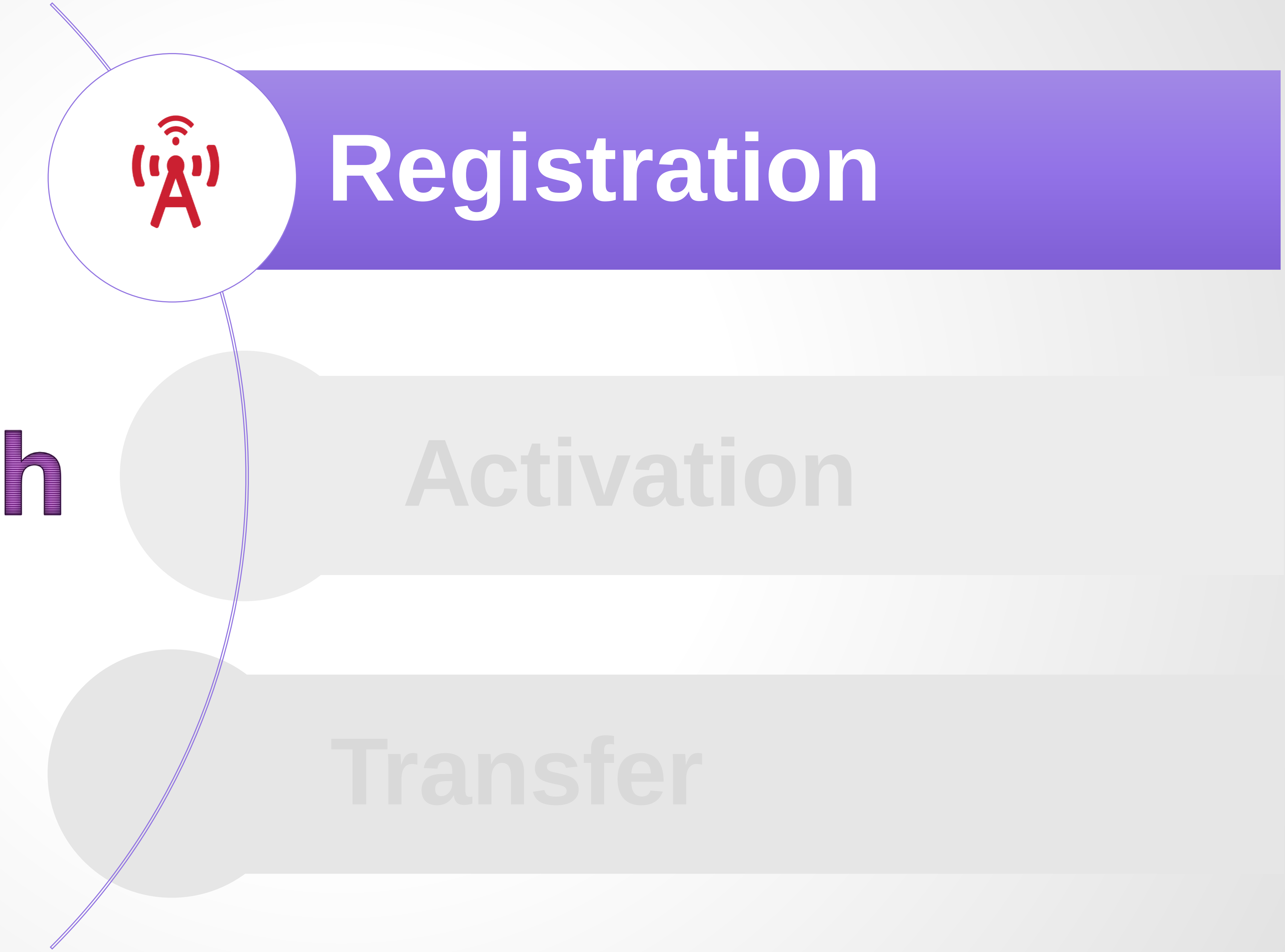
MNO Onboarding (new)

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



Enough information the IoT device to connect with the ASP

Zero Touch



Registration

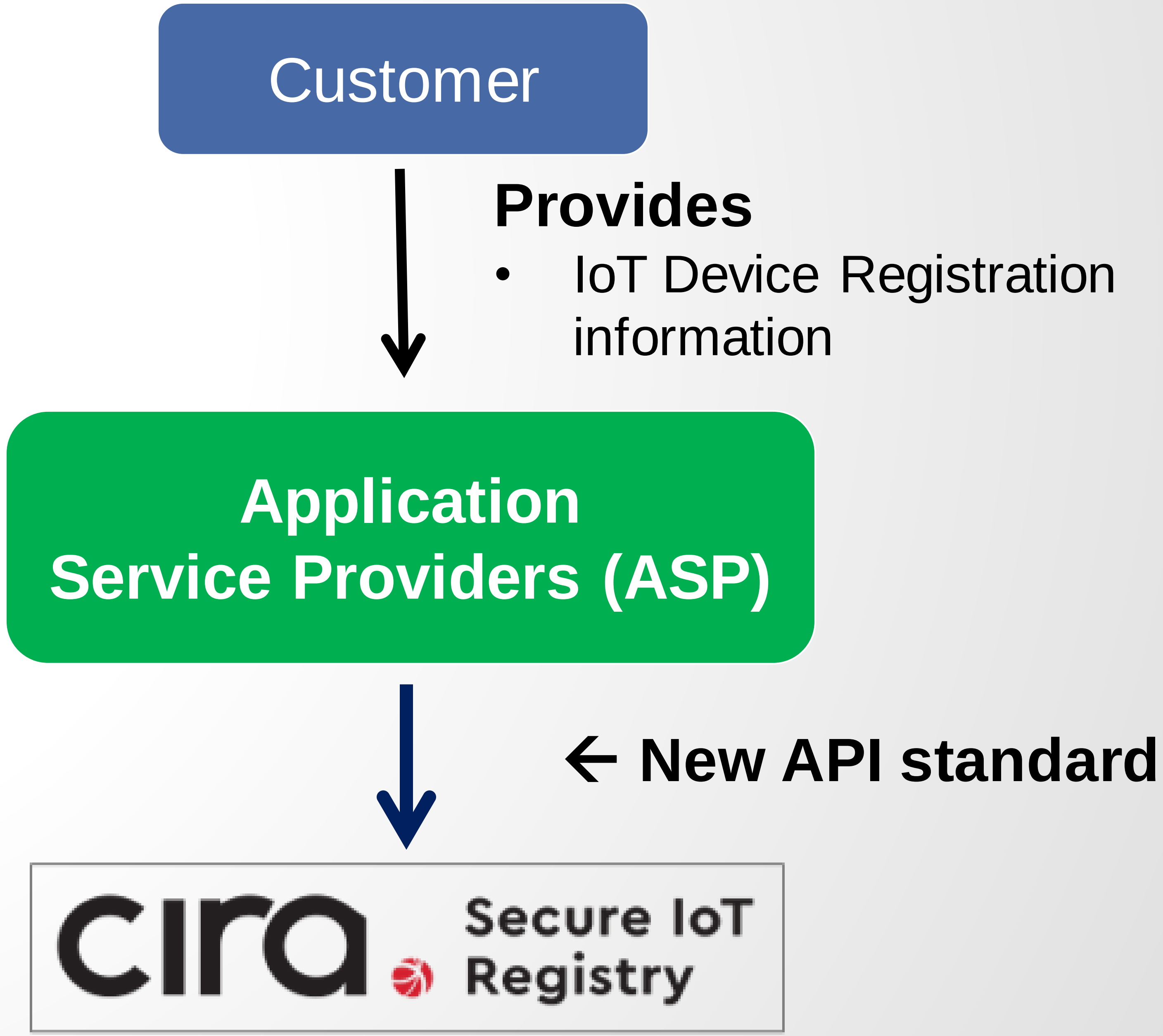
Activation

Transfer

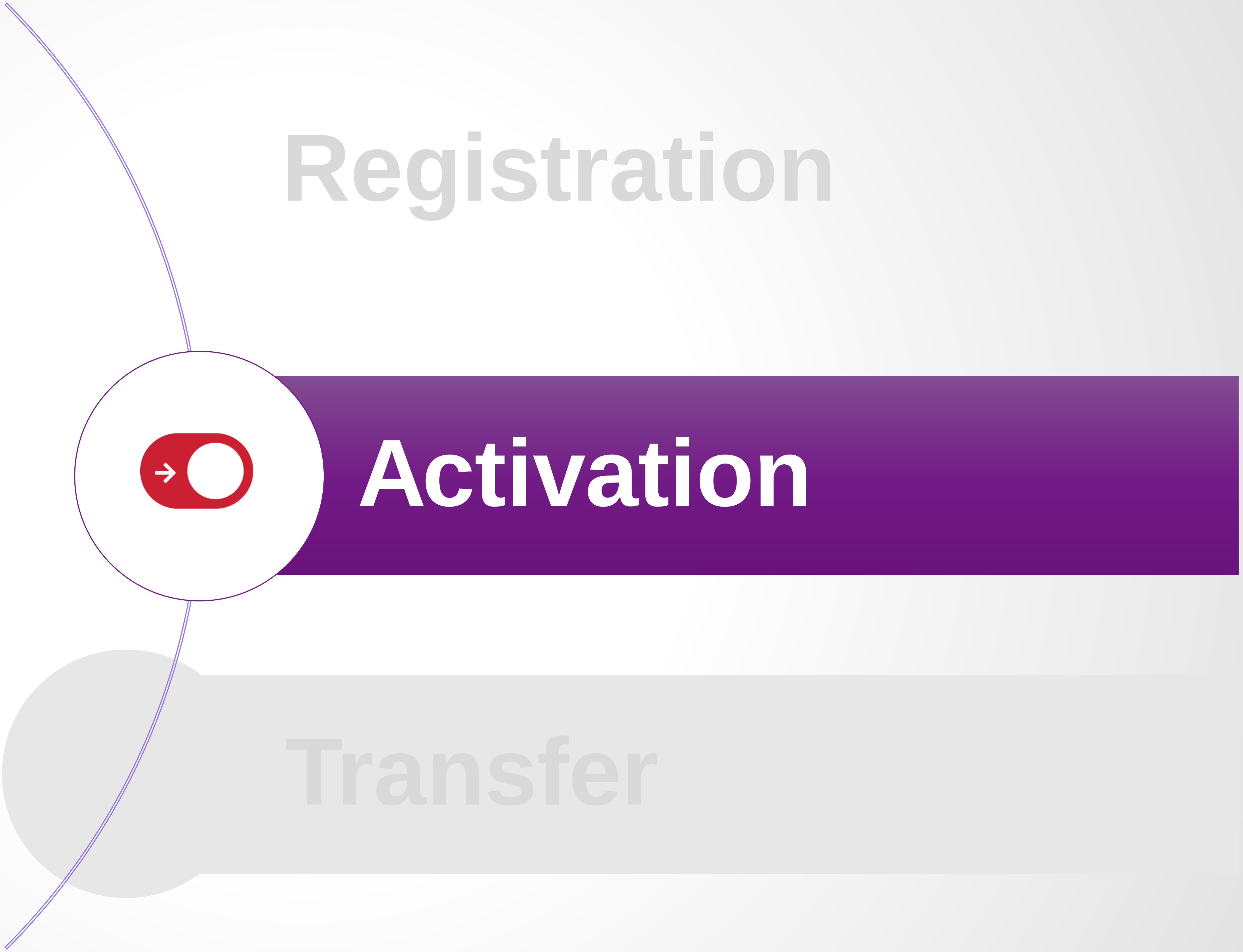
Registration

IoT Device Registration with IoT Registry

- Customer adds a new device with IoT ASP
- EPP like API between ASP and IoT Registry
  - Create, activate IoT device
  - Remove, update IoT device
  - Check status
  - Push IoT public CERT to ASP
  - Etc…
- Need to develop IETF Standard for the API


Customer
Provides
• IoT Device Registration information
Application Service Providers (ASP)
← New API standard
cira Secure IoT Registry

Zero Touch



Registration

Activation

Transfer

Activation

IoT Device Activation when “live” on MNO mobile network

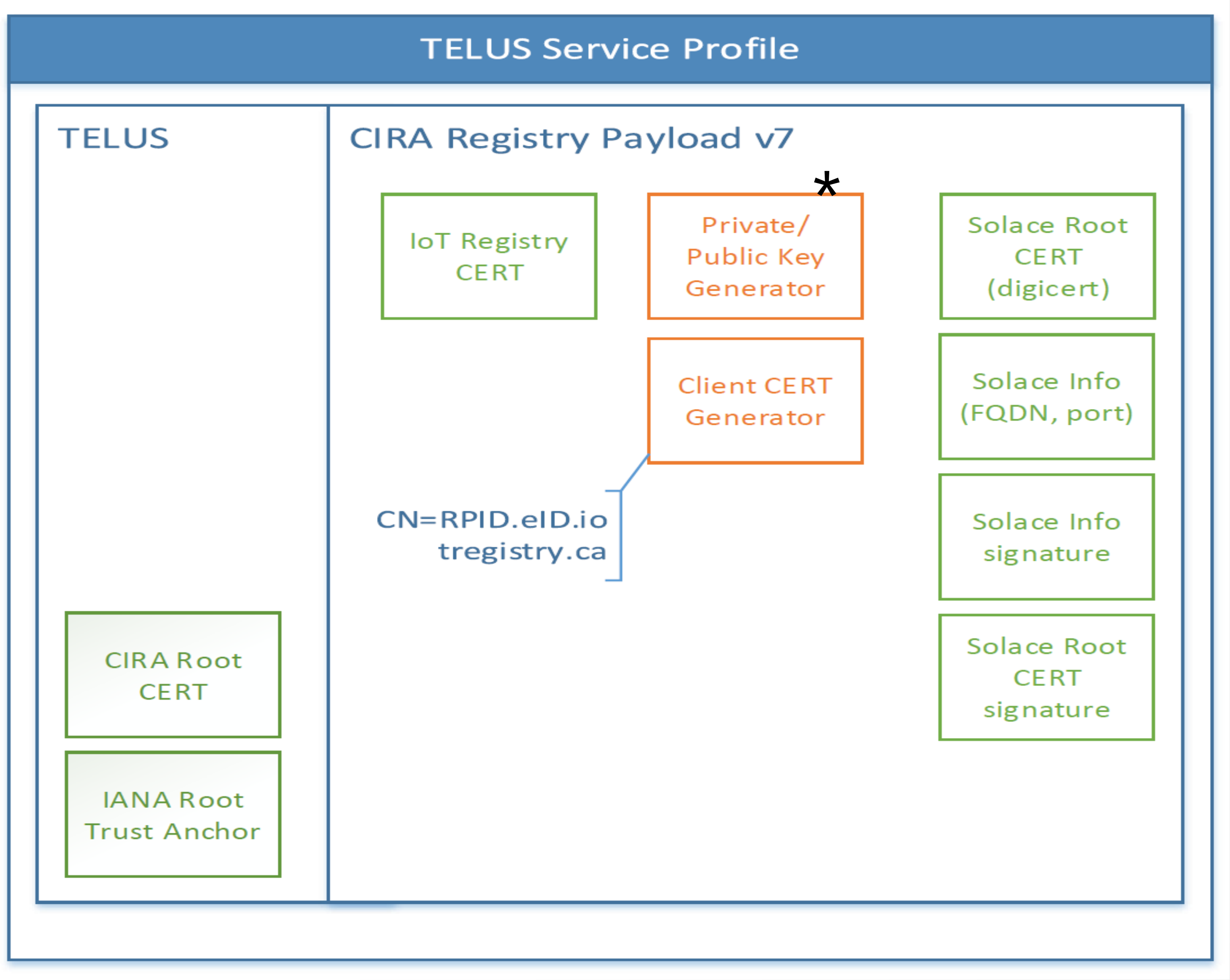
- Once IoT device is live on MNO Network
  - we ask the IoT device via MNO to create a new key pair (public/private)
  - the MNO sends the IoT device CSR the IoT registry to sign
  - The IoT Registry returns a signed CERT to the MNO and ASP
  - The MNO sends the signed CERT on the IoT eSIM
  - The IoT Registry published a hash of the CERT in DNS w/DNSSEC
- The authenticity/identification of the IoT device can be verified with the signed CERT and via DNSSEC

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

Activation

Registry Payload – enabling a new root of trust leveraging DNSSEC

- 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)



TELUS Service Profile

TELUS

CIRA Root CERT

IANA Root Trust Anchor

CIRA Registry Payload v7

IoT Registry CERT

Private/ Public Key Generator *

Client CERT Generator

CN=RPID.eID.io
tregistry.ca

Solace Root CERT (digicert)

Solace Info (FQDN, port)

Solace Info signature

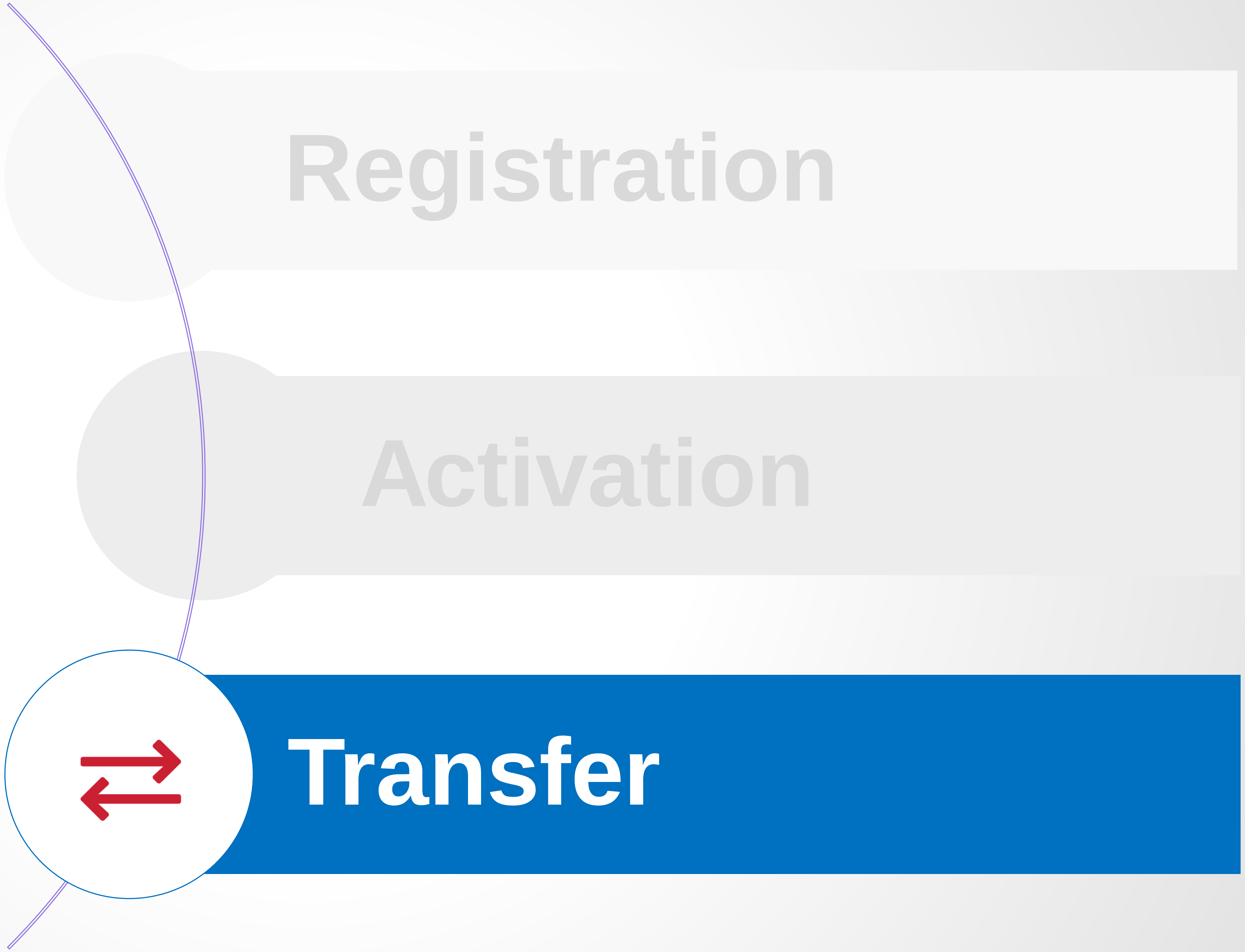
Solace Root CERT signature

🟩 Pre-provisioned at SIM activation

🟧 Downloaded over-the-air

* Private / Public Key pair generated on-board

Zero Touch

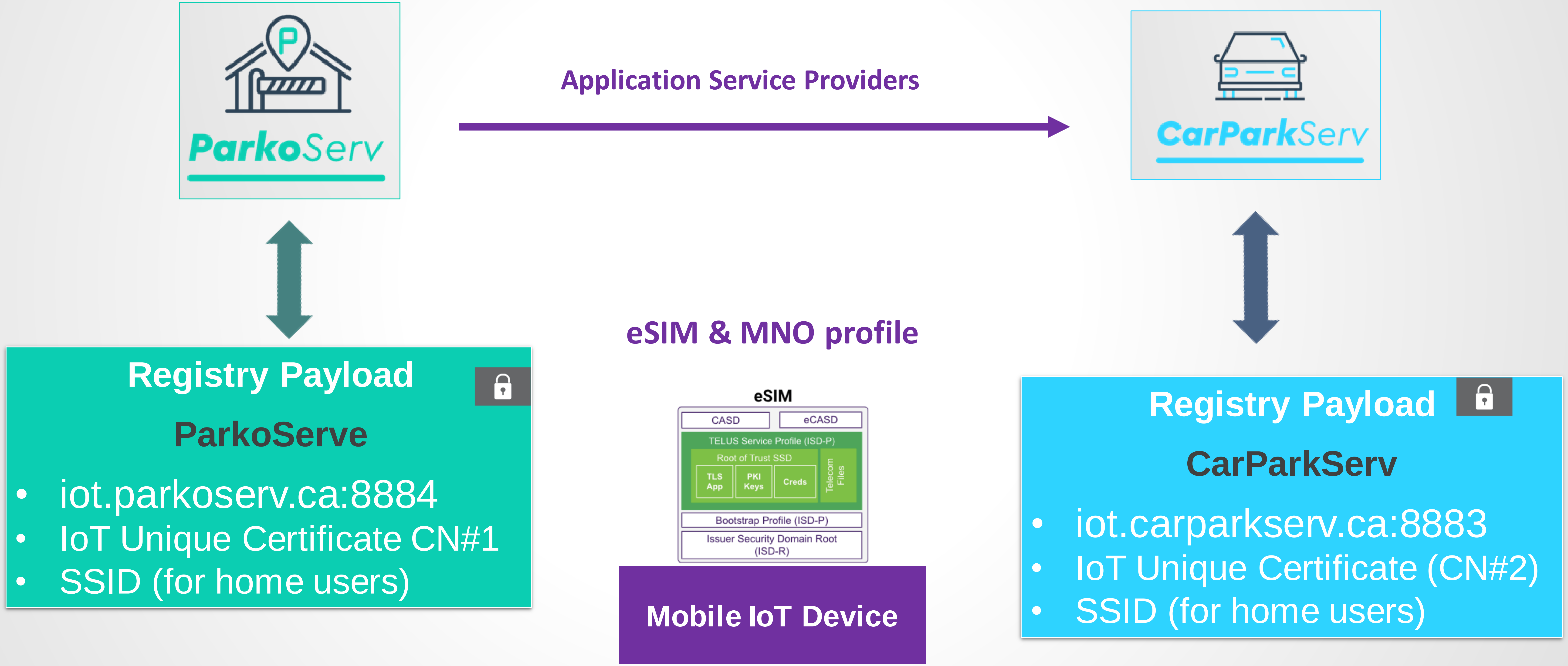


Registration

Activation

Transfer

Transfer between entities



ParkoServ
Application Service Providers
CarParkServ
eSIM & MNO profile
eSIM
CASD
eCASD
TELUS Service Profile (ISD-P)
Root of Trust SSD
TLS App
PKI Keys
Creds
Telecom Files
Bootstrap Profile (ISD-P)
Issuer Security Domain Root (ISD-R)
Mobile IoT Device

Registry Payload

ParkoServe

- iot.parkoserv.ca:8884
- IoT Unique Certificate CN#1
- SSID (for home users)

Registry Payload

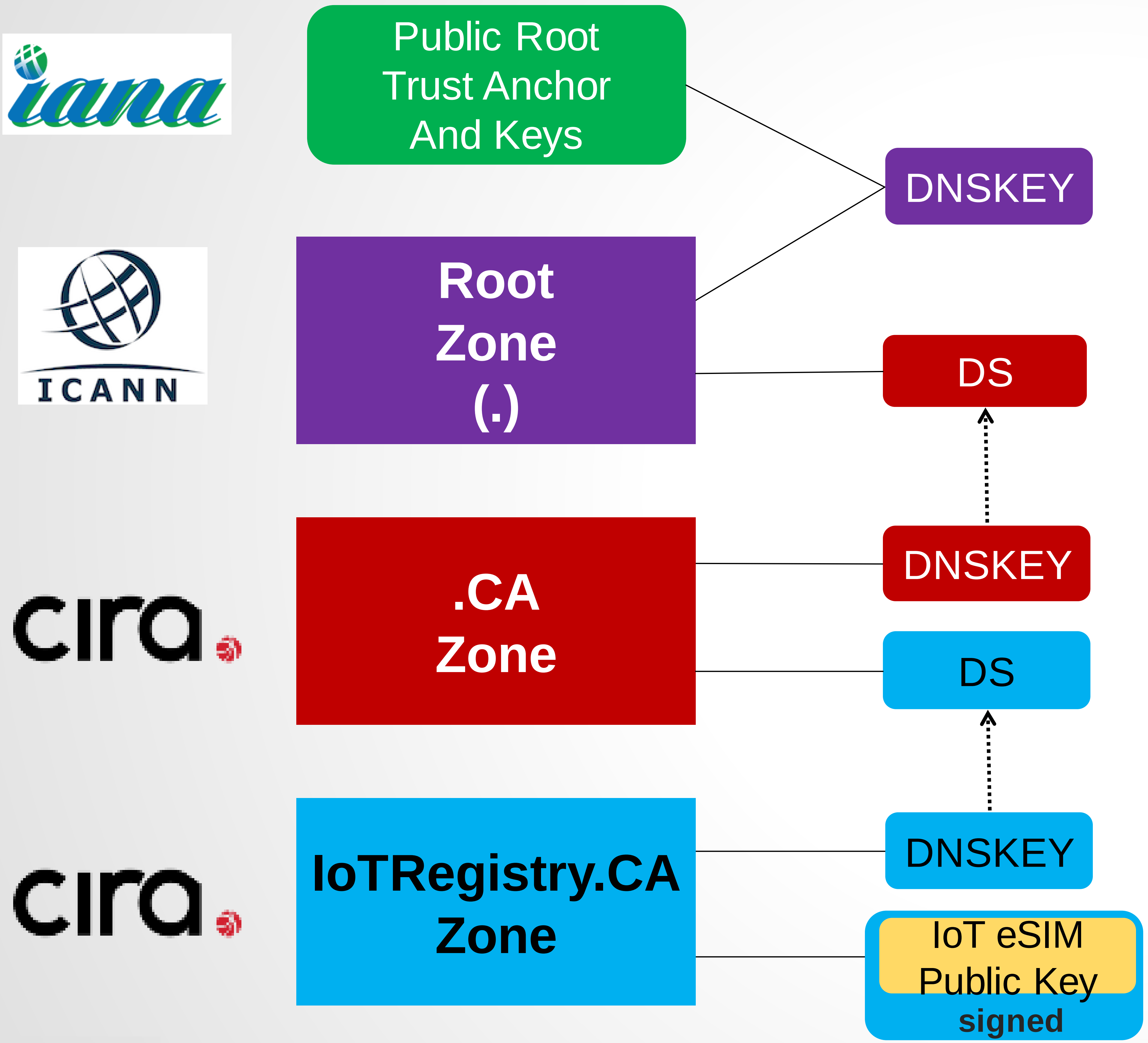
CarParkServ

- iot.carparkserv.ca:8883
- IoT Unique Certificate (CN#2)
- SSID (for home users)

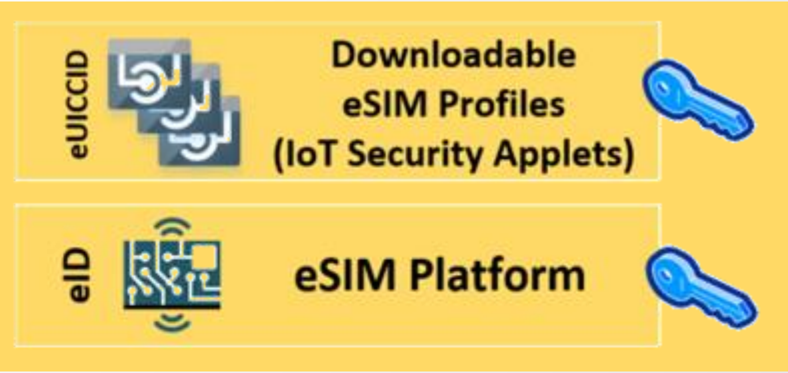
A New Root of Trust – DNSSEC

Leveraging the public DNS & DNSSEC to validate the authenticity of

- eSIM
- IoT security applets
- cloud service providers public keys



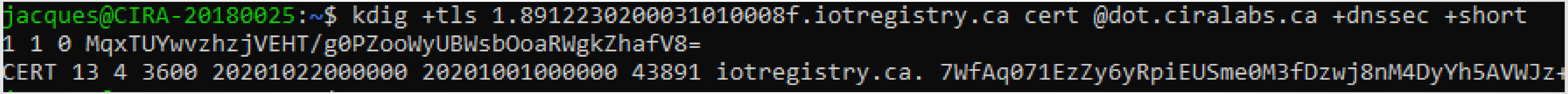
✓ DNS ✓



A few digs ☺

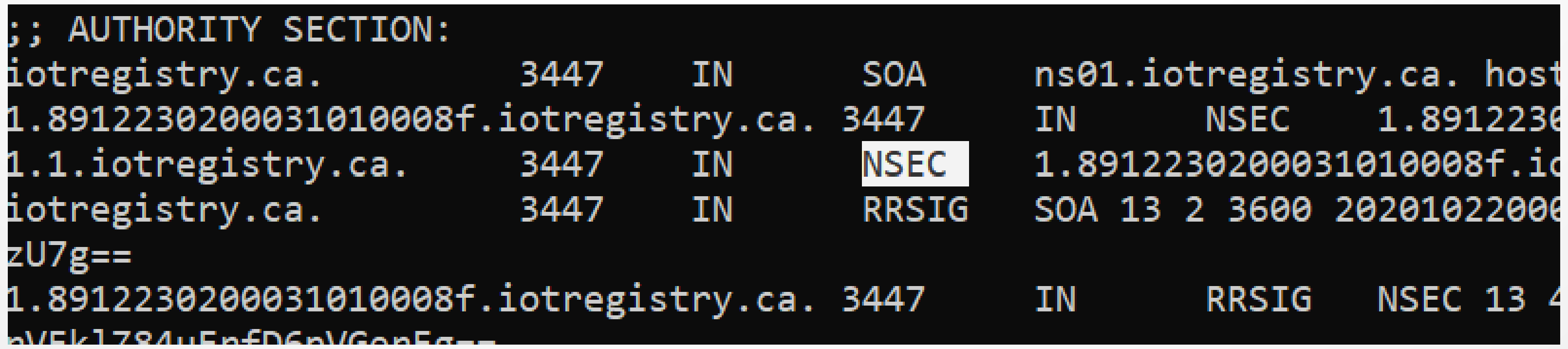
DNSSEC as the new root of trust for IoT devices and it works!

- **kdig +tls 1.891223020003101008f.iotregistry.ca cert @dot.ciralabs.ca +dnssec**



```
jacques@CIRA-20180025:~$ kdig +tls 1.891223020003101008f.iotregistry.ca cert @dot.ciralabs.ca +dnssec +short
1 1 0 MqxTUYwvzhzjVEHT/g0PZooWyUBWsbOoaRWgkZhafV8=
CERT 13 4 3600 20201022000000 20201001000000 43891 iotregistry.ca. 7WfAq071EzZy6yRpiEUSme0M3fDzwj8nM4DyYh5AVWJz+
```

- **The IoT Registry has a real time publicly available, trusted and verifiable Certificate Revoke List (CRL) function in the DNS with NSEC**
  - **kdig +tls 2.891223020003101008f.iotregistry.ca cert @dot.ciralabs.ca +dnssec**



```
;; AUTHORITY SECTION:
iotregistry.ca.         3447    IN      SOA     ns01.iotregistry.ca. host
1.891223020003101008f.iotregistry.ca. 3447     IN      NSEC    1.8912230
1.1.iotregistry.ca.     3447    IN      NSEC    1.891223020003101008f.io
iotregistry.ca.         3447    IN      RRSIG   SOA 13 2 3600 2020102200
zU7g==
1.891223020003101008f.iotregistry.ca. 3447     IN      RRSIG   NSEC 13 4
```

cira

One IoT Registry per country, per ccTLD ?!?!?!

- We need your help to take this concept to the next level
- We tried to fast fail this concept for the last year & it's growing
  - https://github.com/CIRALabs/CIRA-Secure-IoT-Registry
  - https://cira.ca/IoT
- CIRA implementing and contributing to GSMA IoT SAFE standard development

Thank You

Questions?