Secure IoT Registry

DNSSEC Based IoT Device Attestation
A new root of trust

Dec. 22nd 2020

Presented By

Natasha D'Souza, Jacques Latour

Agenda

Evolution of SIMs

Built to standards

How does the IoT Registry Work

DNSSEC

Value Proposition of the IoT Registry

cira Secure IoT Registry

WWW.CIRA.CA

eSIMS

SIMS today

Digital eSIMS

IoT SAFE eSIMS

Standards

GSMA

GSMA IoT SAFE

IEFT

DNSSEC

IoT Registry

IoT Registry Ecosystem

Register, Activate, De-activate, Delete

DNS & DNSSEC as the new IoT root of trust

Middleware

Value Proposition

Dev Kit for POC

Opportunities for new innovation

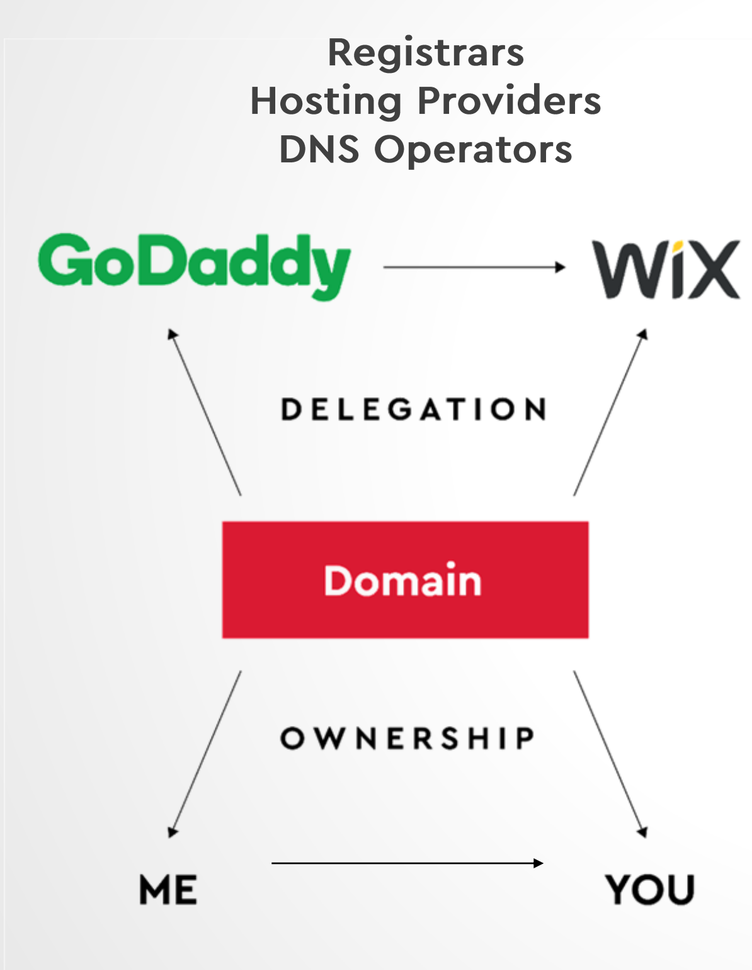
Value to customers

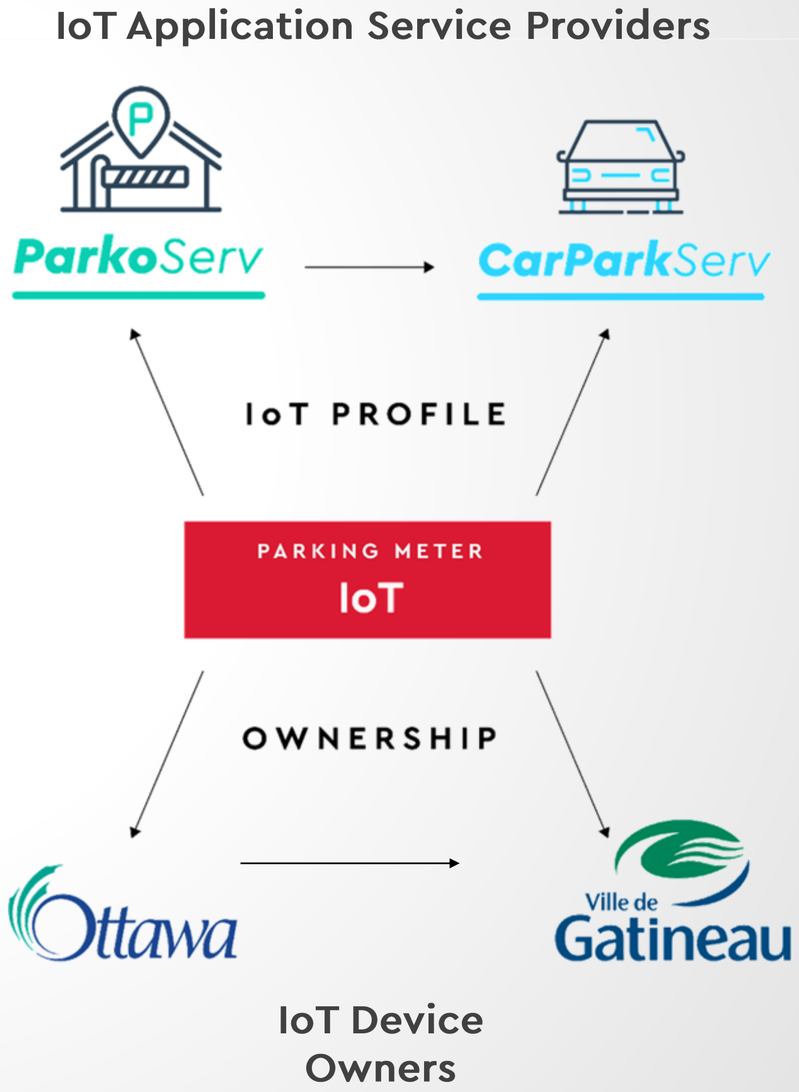
cira

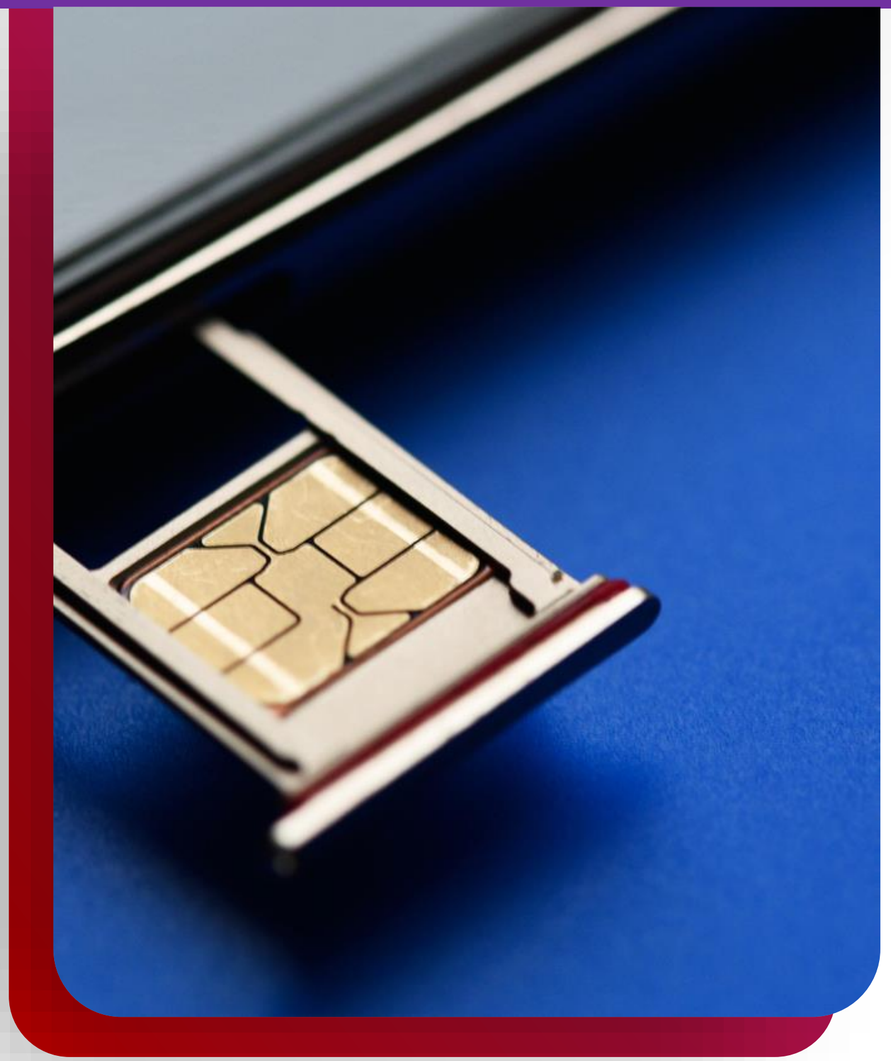
https://github.com/CIRALabs/CIRA-Secure-IoT-Registry

SIMILARITIES BETWEEN

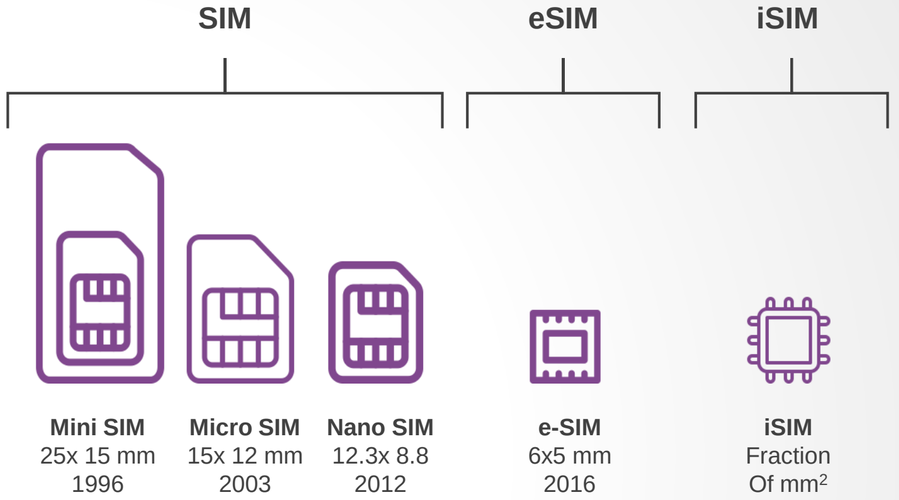
Domain Names & IoT Devices







SUBSCRIBER IDENTITY MODULE - SIM

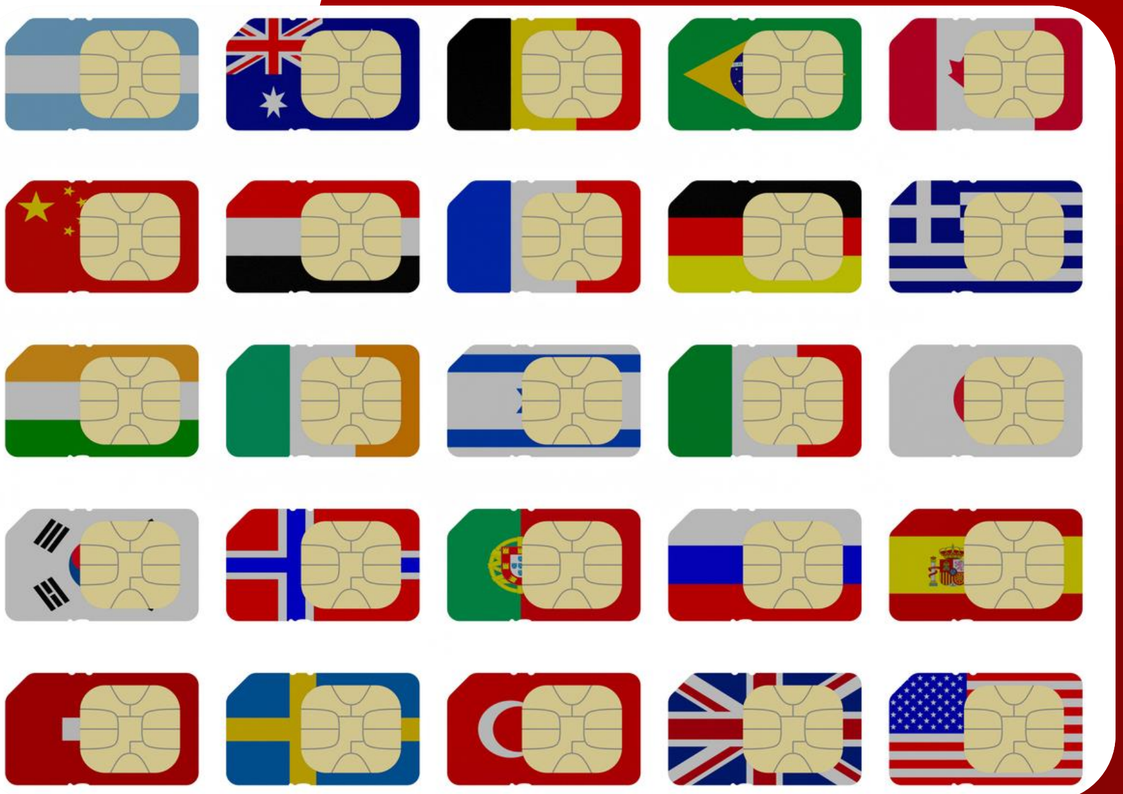


- Tiny, portable memory chip (64k), stores mobile device user info.
- 17 digit code - country code of origin, MNO, carrier, unique user ID
- Enables mobile device to connect with a GSM network & GSM networks to track usage

SIMS TODAY

Physical SIM

- Have a set of stored secure credentials
- Have to change SIM cards when changing providers
- Hackable by having access to a psswd recovery text on the device
- Get damaged easily



eSIM

Embedded SIM (digital)

- Store multiple cellular profiles
- Small it can be fit in small form factor sensors
- Temporary change to another network
- Can’t be physically damaged or lost

“

Internationally harmonized technical standards are key to enhancing IoT security

Internet Society – Final outcomes & Recommendations Report

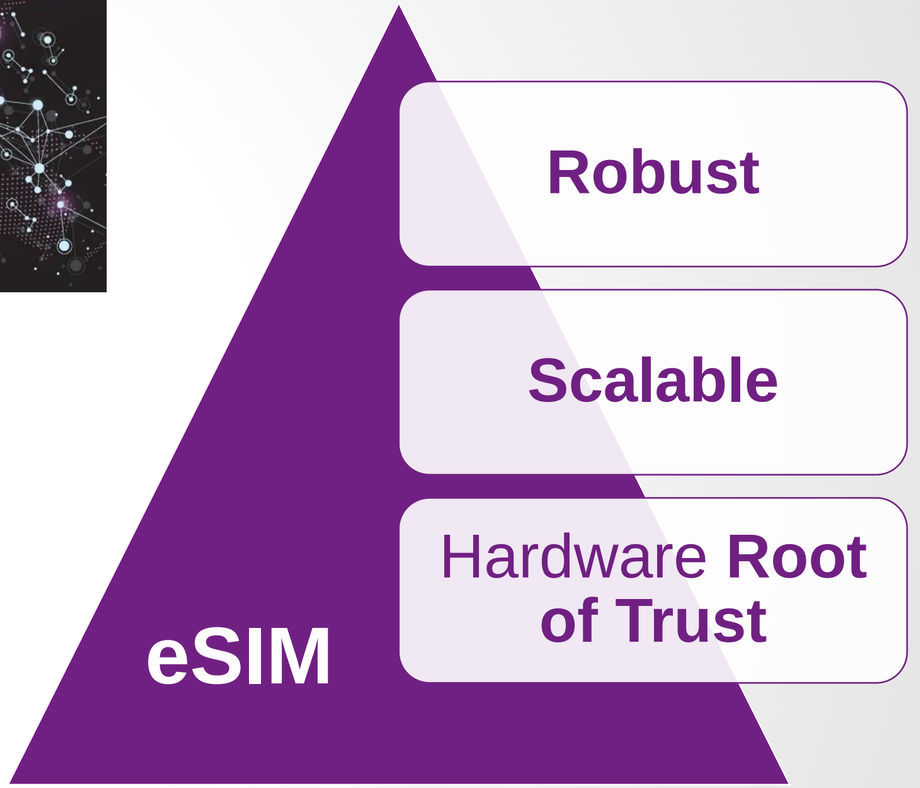
https://www.internetsociety.org/wp-content/uploads/2019/05/Enhancing-IoT-Security-Report-2019_EN.pdf

Standards Body to Enable

IoT

Device manufacturers

Service providers



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

API In Scope
#2, 4

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

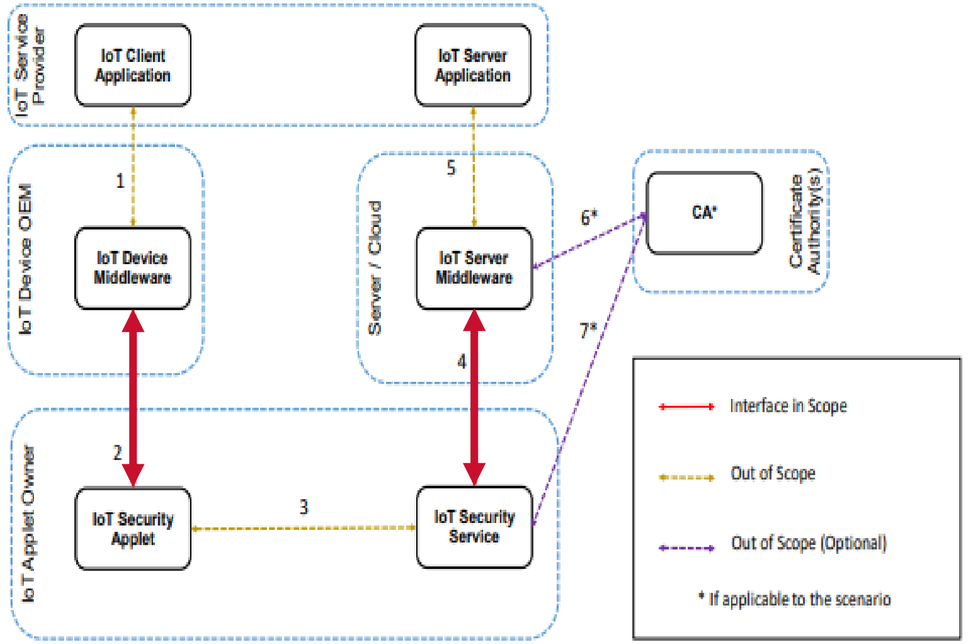
#3
ETSI, 3GPP & Global Platform for OTA SIM management or GSMA for remote SIM provisioning

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

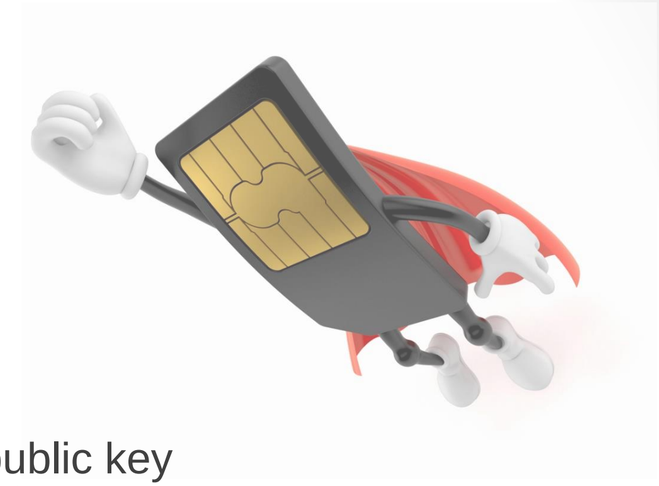
#5
New EPP like IETF standard to be developed

ARCHITECTURE

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



eSIM ARE LIKE SMARTCARDS, MINI HSM OR TPM



Put public key

Get random

Get data file
public/private key info

Read public key

eSIM

GSMA

IoT SAFE

Read file

Generate object list

Verify signature

Generate key pair

Compute signature on eSIM to enable mutual TLS Handshake

IoT SERVER MIDDLEWARE

API #2

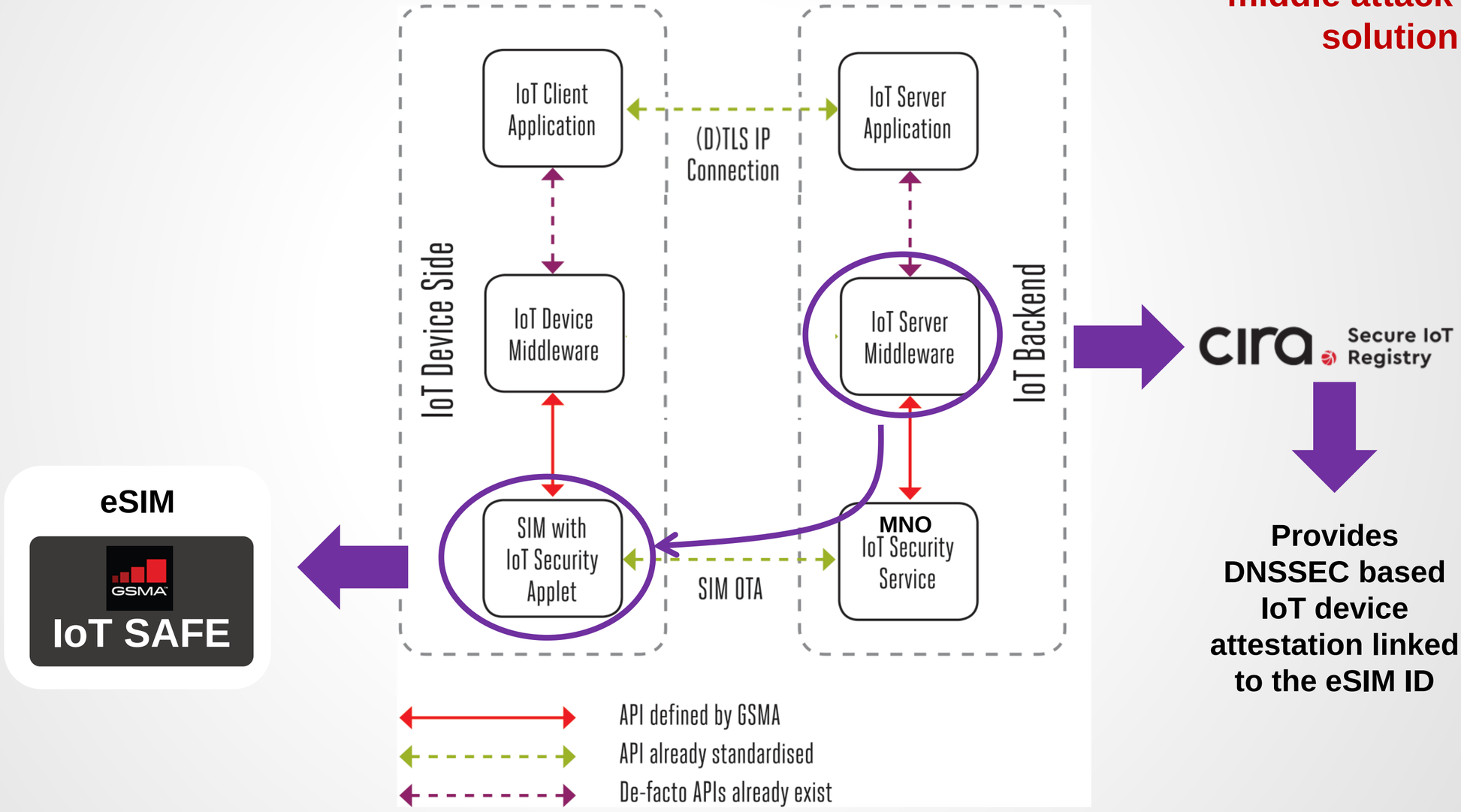
- Card Provisioning Service
- Credential Establishment / Management Service
- Trust Store Service
- CA Certificate Request Service

Functional Requirements	
M1	The IoT server middleware will enable the IoT server application to perform the security procedures defined in section 3.3 of this document (for example performing a (D)TLS connection establishment handshake).
M2	The IoT server middleware will manage the public and private credentials associated with the IoT server application and the public credentials associated with the IoT client application.
M3	The IoT server middleware uses the IoT security service to manage the IoT service provider's credentials within the IoT security applet.
M4	If initiating or renewing PKI credentials the IoT server middleware may use the services of a certificate authority, by acting as a registration authority.
M5	The IoT server middleware has an interface to the IoT security service.
M6	The IoT server middleware may provide an interface to the IoT security service to receive a certificate from a certification authority connected to IoT server middleware.

ZERO TOUCH REMOTE eSIM PROVISIONING

Building on the existing eSIM → MNO trust model

‘Bad Actor’ in the middle attack proof solution



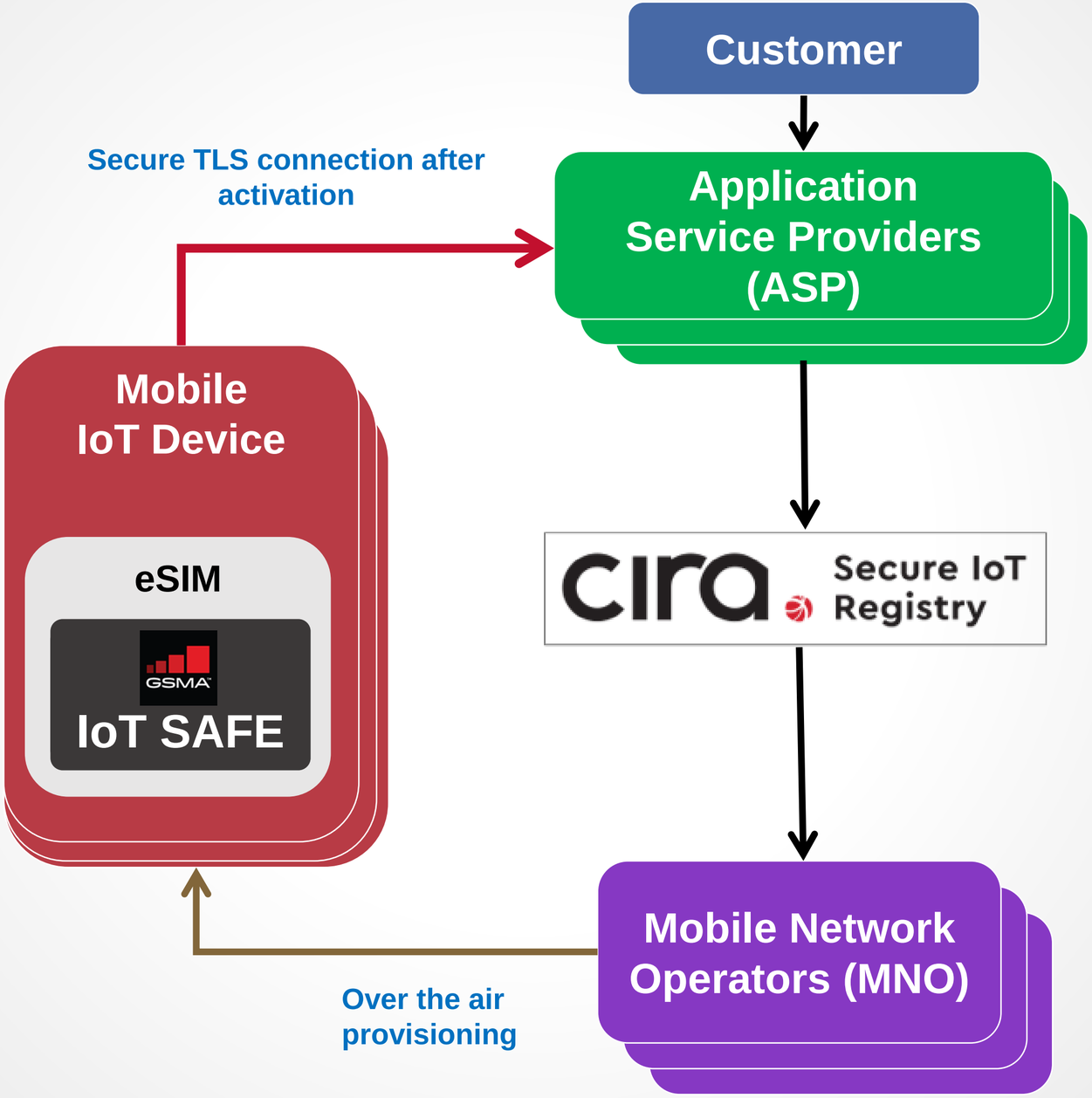
cira Secure IoT Registry

Provides DNSSEC based IoT device attestation linked to the eSIM ID

WWW.CIRA.CA

IoT REGISTRY

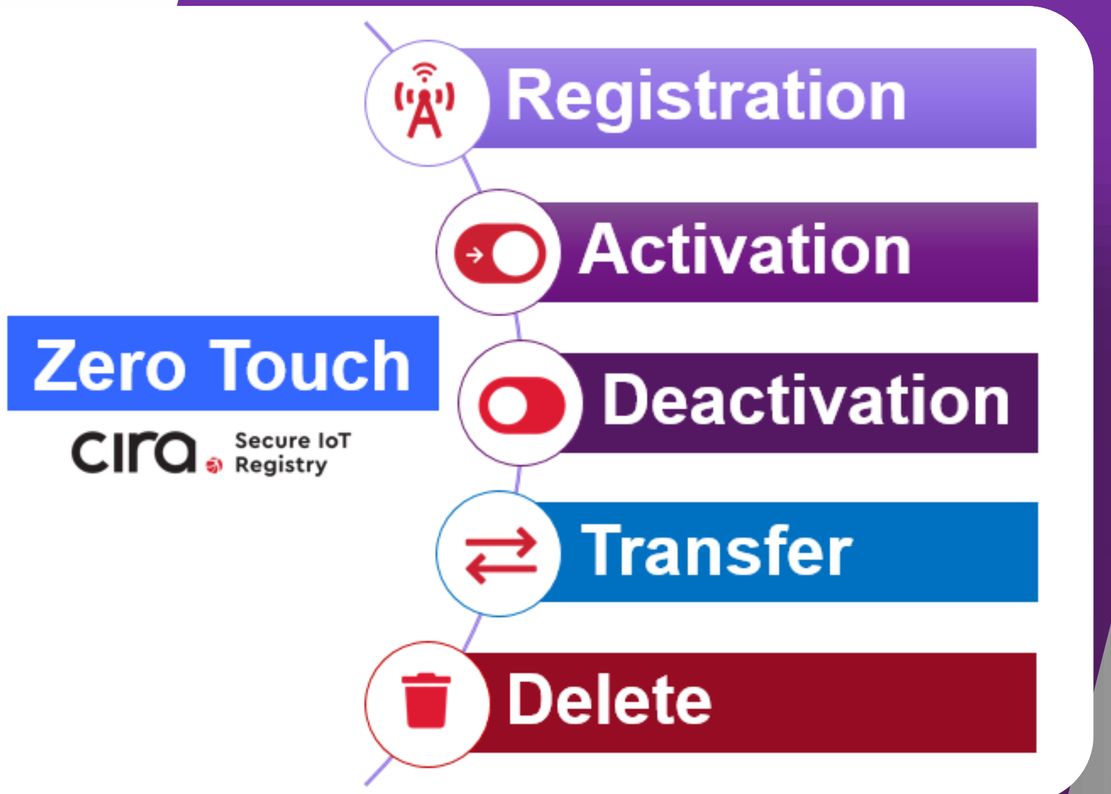
Ecosystem



CIRA SECURE IoT REGISTRY

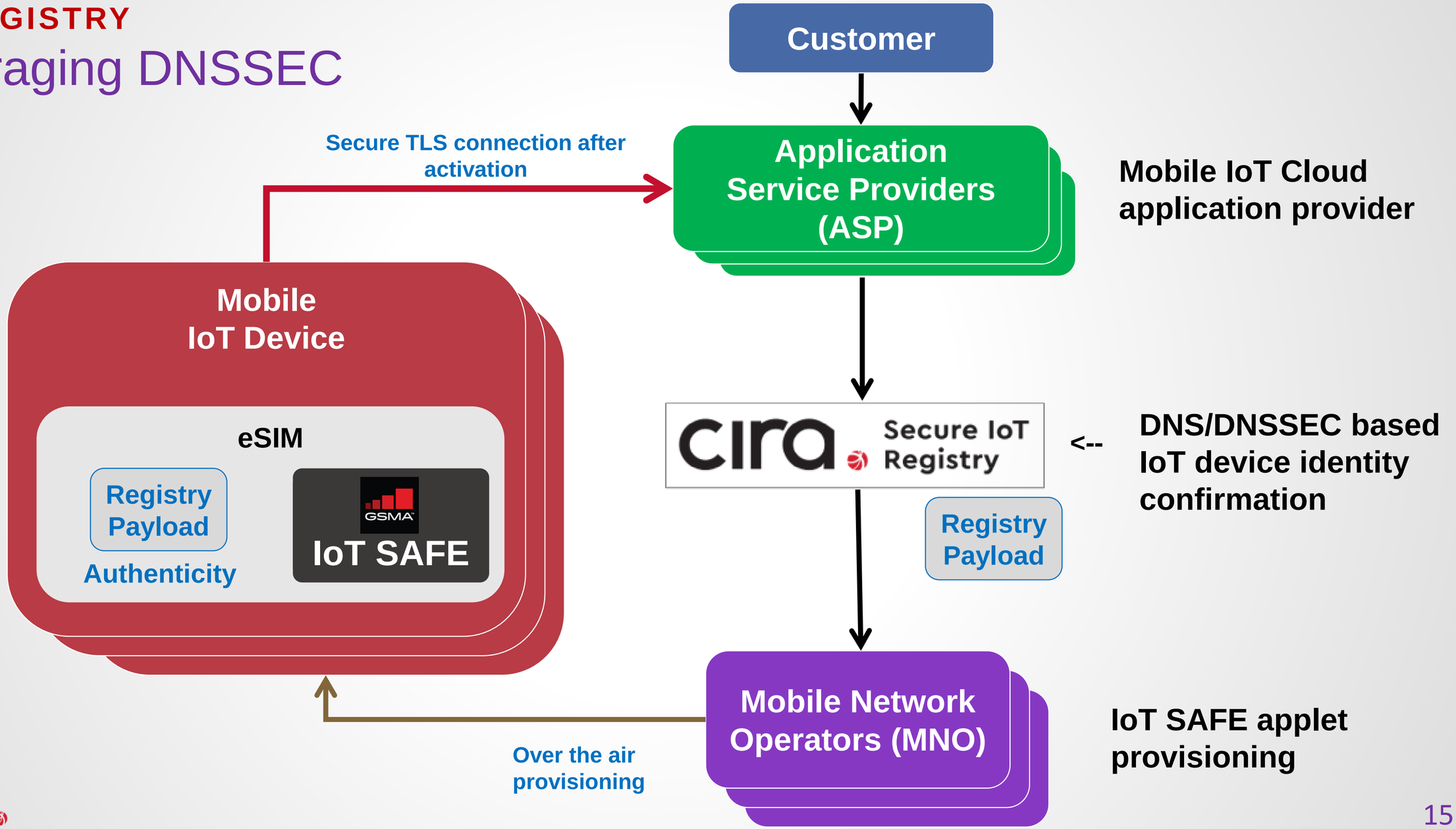
Zero Touch

- Declares device telco stewardship
- Pushes configuration / security certificates to the devices
- Provisioning/De-provisioning devices
- Changing device telco stewardship/service provider for devices
- Removing telco stewardship



IoT REGISTRY

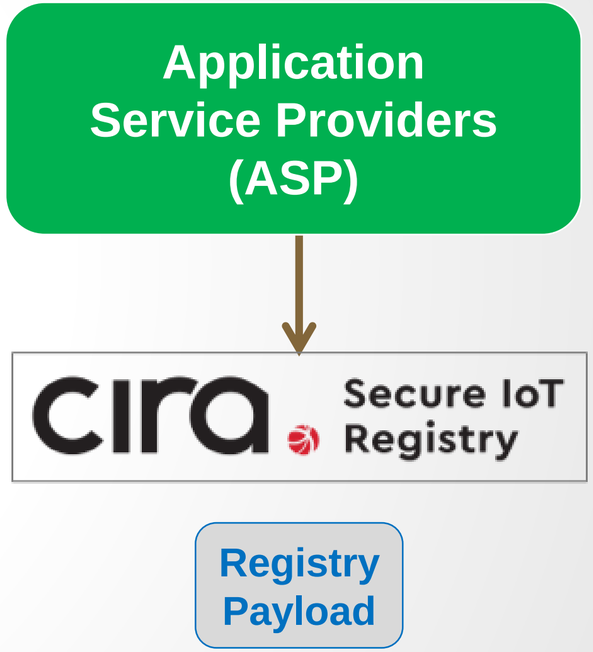
Leveraging DNSSEC



INFO FOR THE IoT DEVICE TO CONNECT WITH THE ASP

Cloud IoT Application Service Provider Requirements

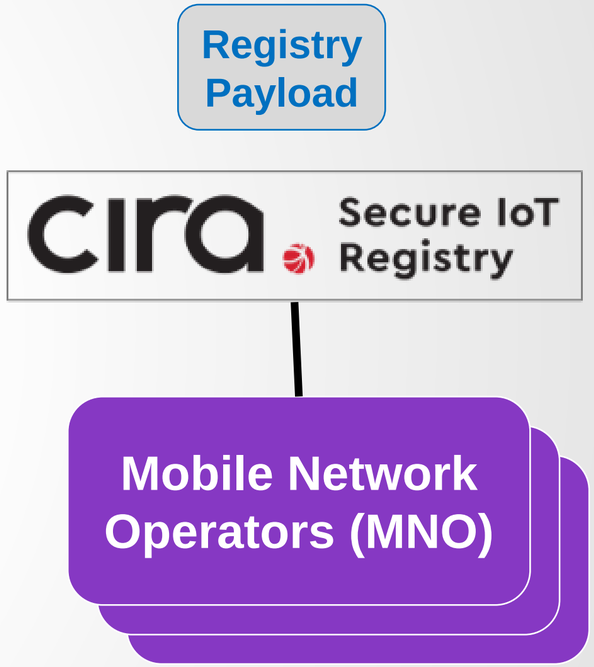
- Building the Registry Payload content
- Need the IoT device end point info.
  - URL, port,
  - WiFi SSID + Password (encrypted)
  - ASP CERT, etc…
  - ASP FQDN (that's DNS ;-)



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**

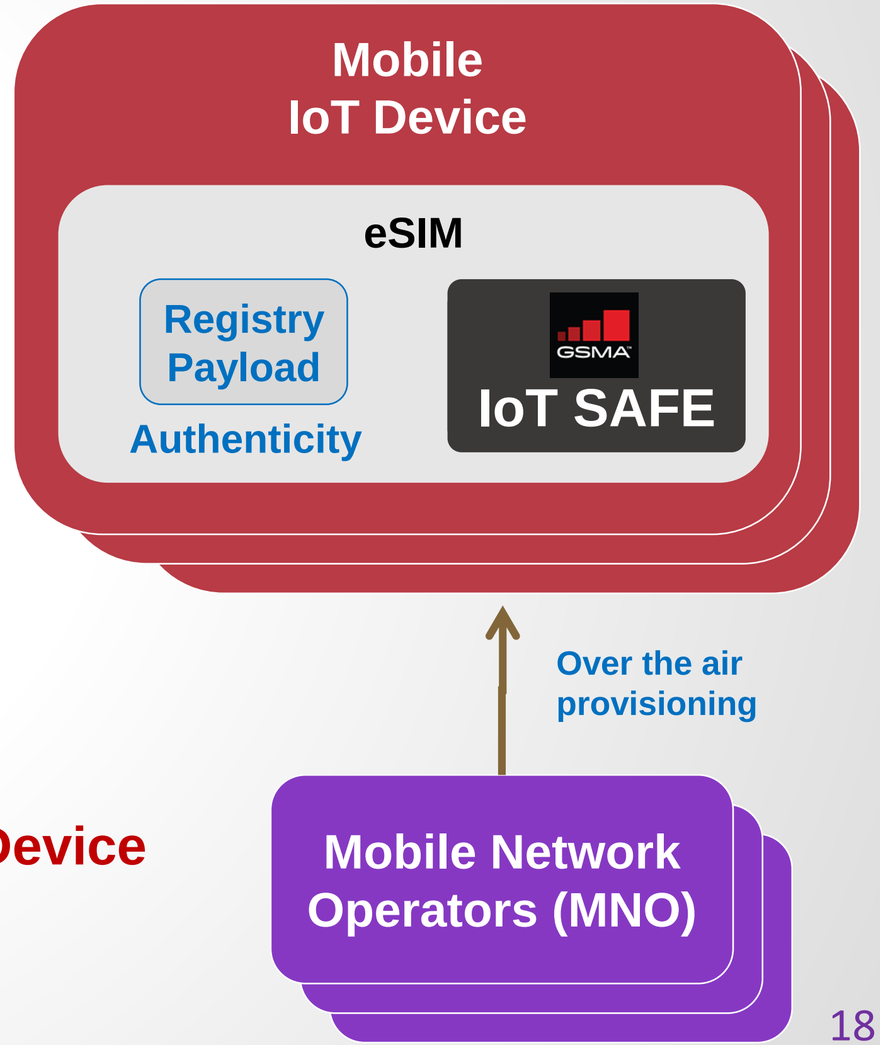


Enough information for the IoT device to connect with the ASP

Activation

Once IoT device is live on MNO Network

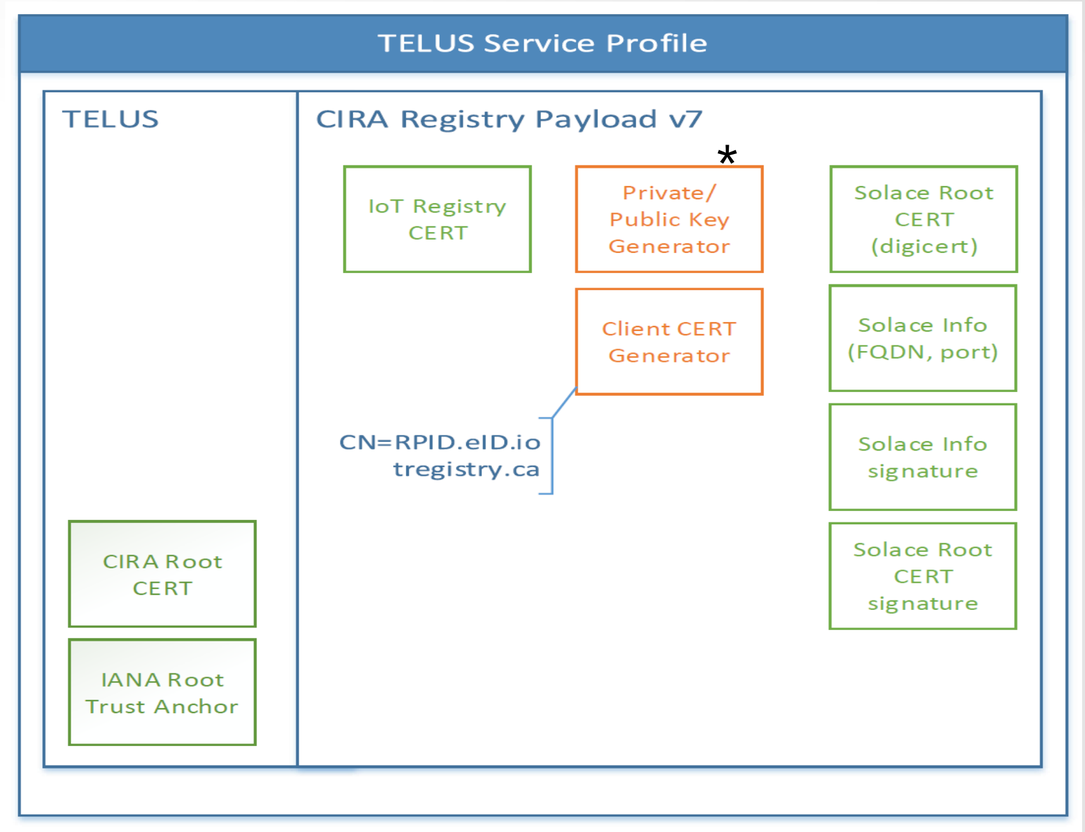
- Ask the IoT device via MNO to create a new key pair (public/private)
- MNO sends the IoT device CSR to the IoT registry to sign
- IoT Registry returns a signed CERT to the MNO & ASP
- MNO sends the signed CERT on the IoT eSIM



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)



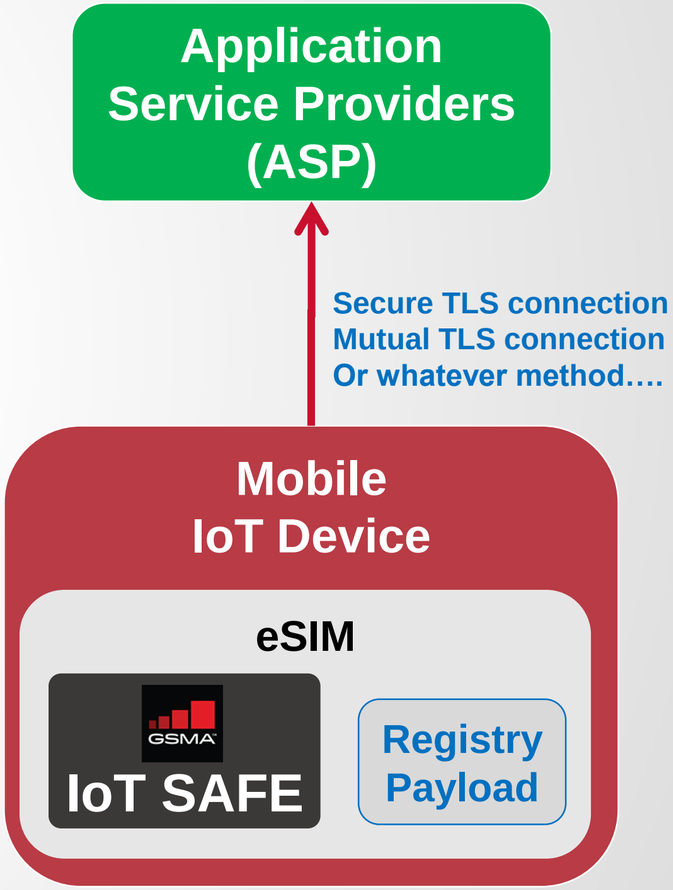
Enabling a new root of trust leveraging DNSSEC

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!)



ANOTHER LAYER OF SECURITY

Why DNSSEC?

- Established & trusted global root of trust with IANA
  https://www.iana.org/dnssec
- DNSSEC signature proves the authenticity of DNS answers

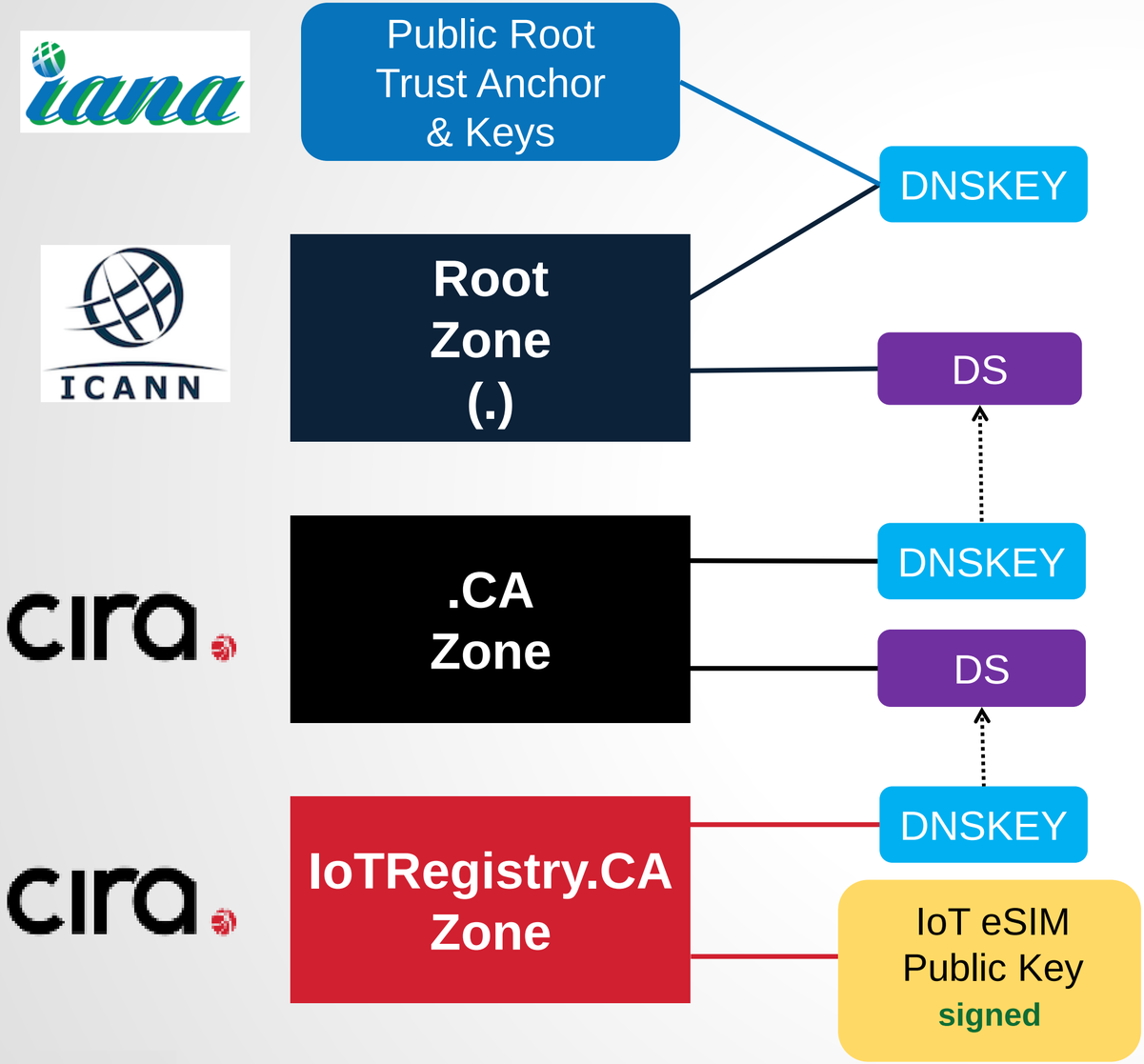
Registry publishes a fingerprint of the signed device certificate in the DNS signed with DNSSEC

The ASP can validate the attestation and status of an IoT device with a single DNS CERT query

Makes this fingerprint public to everyone

The IoT device can verify their own attestation by comparing their local CERT and the DNS

Status of revoked & invalid CERTs can be queried real time in the DNS, no need for CRL



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 ✓

IoT Device attestation using DNSSEC – Example

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

- **kdig +tls 1.89122302000310100 8f.iotregistry.ca cert @dot.ciralabs.ca +dnssec**

```
jacques@CIRA-20180025:~$ kdig +tls 1.89122302000310100 8f.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 (denial of existence record)**
  - **kdig +tls 2.89122302000310100 8f.iotregistry.ca cert @dot.ciralabs.ca +dnssec**

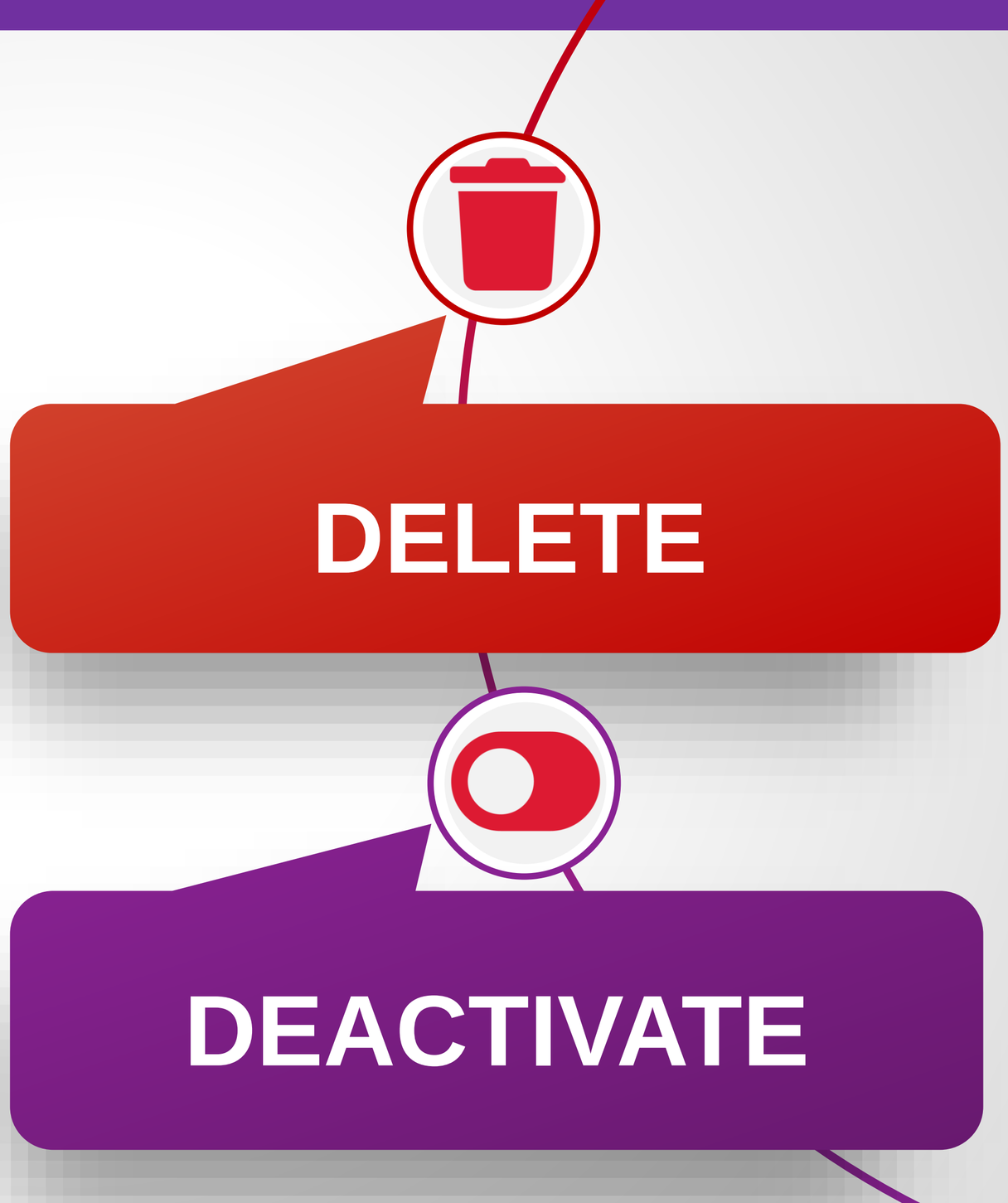
```
;; AUTHORITY SECTION:
iotregistry.ca.          3447    IN      SOA     ns01.iotregistry.ca. host
1.8912230200031010008f.iotregistry.ca. 3447     IN      NSEC    1.8912230
1.1.iotregistry.ca.      3447    IN      NSEC    1.8912230200031010008f.io
iotregistry.ca.          3447    IN      RRSIG   SOA 13 2 3600 2020102200
zU7g==
1.8912230200031010008f.iotregistry.ca. 3447     IN      RRSIG   NSEC 13 4
```

DEACTIVATION & DELETE

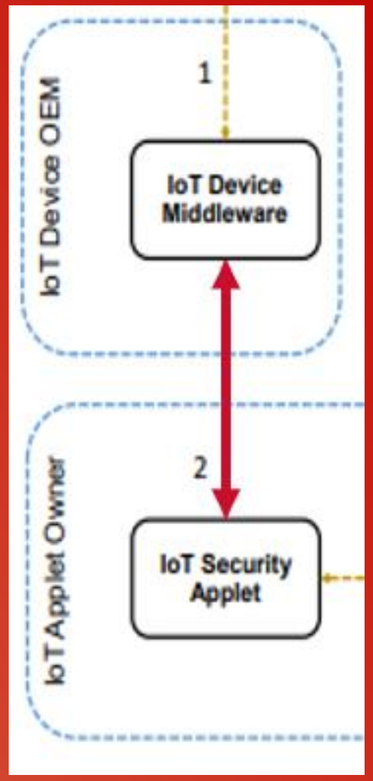
Very Important in Device Management

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

Delete - Delete from the IoT Registry



IoT DEVICE MIDDLEWARE



Functional Requirements	
B1	The IoT device middleware shall be able to mutually authenticate with the IoT server middleware using the flows described in this document.
B2	The IoT device middleware shall implement a (D)TLS stack.
B3	The IoT device middleware provides an API to the IoT client application to establish (D)TLS connection(s) using the IoT security applet.
B4	The IoT device middleware shall implement the (D)TLS functions which are not mandatory within the IoT security applet to establish a successful (D)TLS session. .
B5	The IoT device middleware shall send commands to the IoT security applet.
B6	The IoT device middleware shall support an interface to the IoT security applet on the UICC. This interface shall use the APDU based protocol defined in section 3.3.1 of this document.
B7	The IoT device middleware shall support at least one cryptographic hash operation.
B8	The IoT device middleware shall be able to generate (D)TLS session keys
B9	The IoT device middleware shall be able to verify server certificates.

CIRA MIDDLEWARE

API #2

- Built on Thales existing middleware

  https://github.com/ThalesGroup/iot-safe-middleware

- Works with Cinterion & Quectel BG96
- C++ sends APDUs to the SIM card & parses the responses
- Python - middleware app loads C++ library to interact with the SIM card & perform basic cryptographic functions
- Golang: To establish a two-way authenticated TLS session

cira

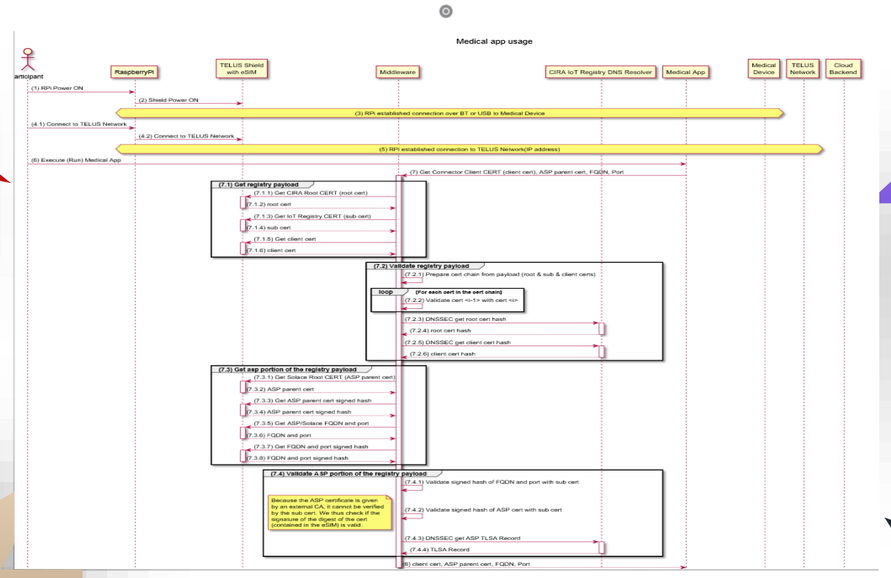
https://github.com/CIRALabs/iot-safe-middleware

CIRA MIDDLEWARE

Demo Kit Middleware

Python App

- Runs demo
- Orchestrates



Python Package

- Provides interface to eSIM data
- Uses C++ Library

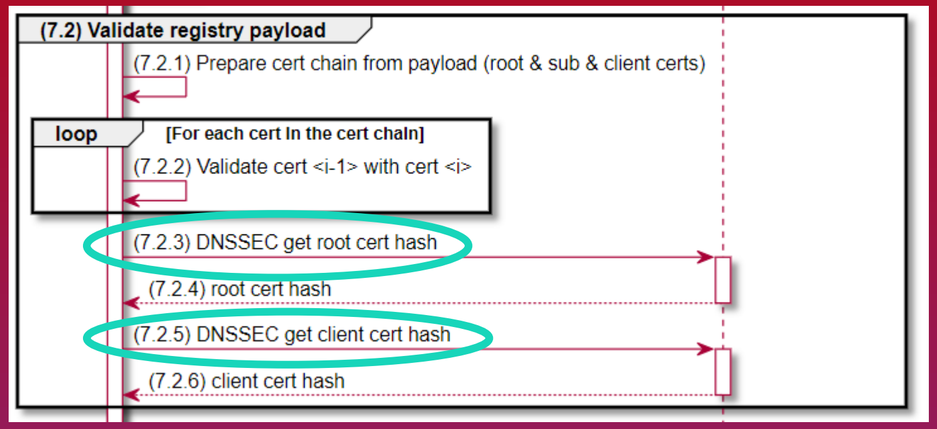
Go App

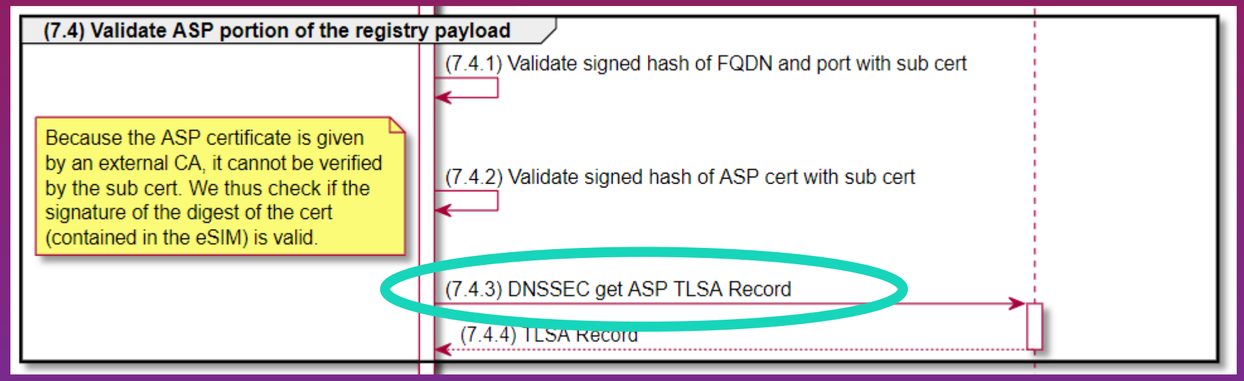
- Opens TLS Tunnel
- Pushes MQTT Events

C++ Library

- Interfaces with the eSIM SAFE eSIM
- Reads/writes configuration in SAFE

Key part of Registry Validation

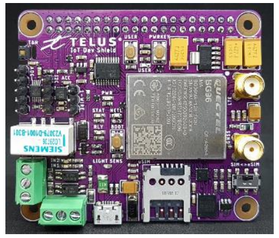




DEVELOPMENT KIT

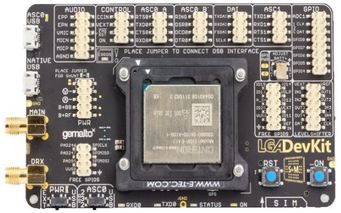
Proof of Concept & L-SPARK Accelerator

- TELUS BG96 Shield with sensors
- Thales Cinterion
- Raspberry Pi 4 or 3B+
- Thales IoT SAFE eSIM



TELUS BG96 Shield

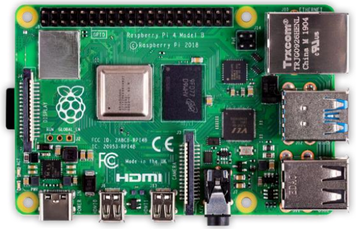
/



Thales Cinterion Devkit

Thales eSIM

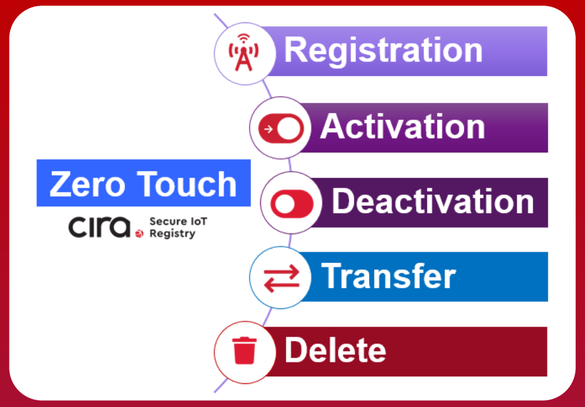
+



Raspberry Pi 4 / 3B+

VALUE PROPOSITION

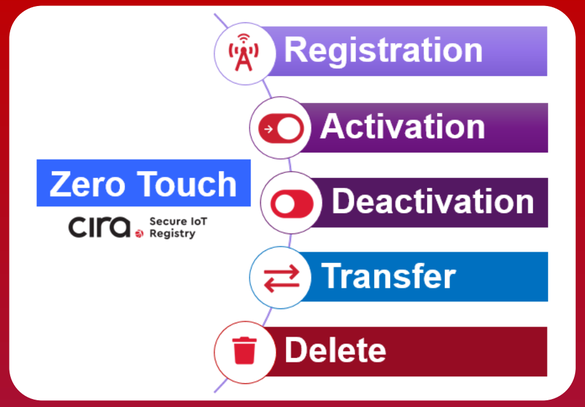
IoT Device Manufacturer/Cloud Provider



Feature	Benefits
Hardware Root of Trust	End-to-end, chip-to-cloud security
IoT SAFE eSIM enabled IoT devices	Zero touch provisioning/ re-provisioning of credentials
Always ON remote registration, activation & transfer	• Easy setup & lifecycle management • Confirmed to belong to vendor
Remote turn off / wipe clean IoT device config	Granular control of credential provisioning
IoT Security at scale	Hassle free quick scaling
Interoperability across different service providers	New business model
Multiple profiles on one device	Competitive differentiator

VALUE PROPOSITION

Customers, 3rd Party Installers



Feature	Benefits
Hardware Root of Trust	Peace of mind
IoT SAFE eSIM enabled IoT devices	Enhanced, inherent security
Always ON remote registration, activation & transfer	Plug & play installation & setup
Remote turn off / wipe clean IoT device config	Effortless management of broken or stolen IoT devices
IoT Security at scale	Unlimited options for products
Interoperability across different service providers	Leverage best value for service
Multiple profiles on one device	Straightforward management

Thank You

https://github.com/CIRALabs/CIRA-Secure-IoT-Registry