Challenges in **DNSSEC** based IoT Device Identity Management

DNSSEC & Security Workshop

ICANN 2021-06-14

Presented By
Jacques Latour

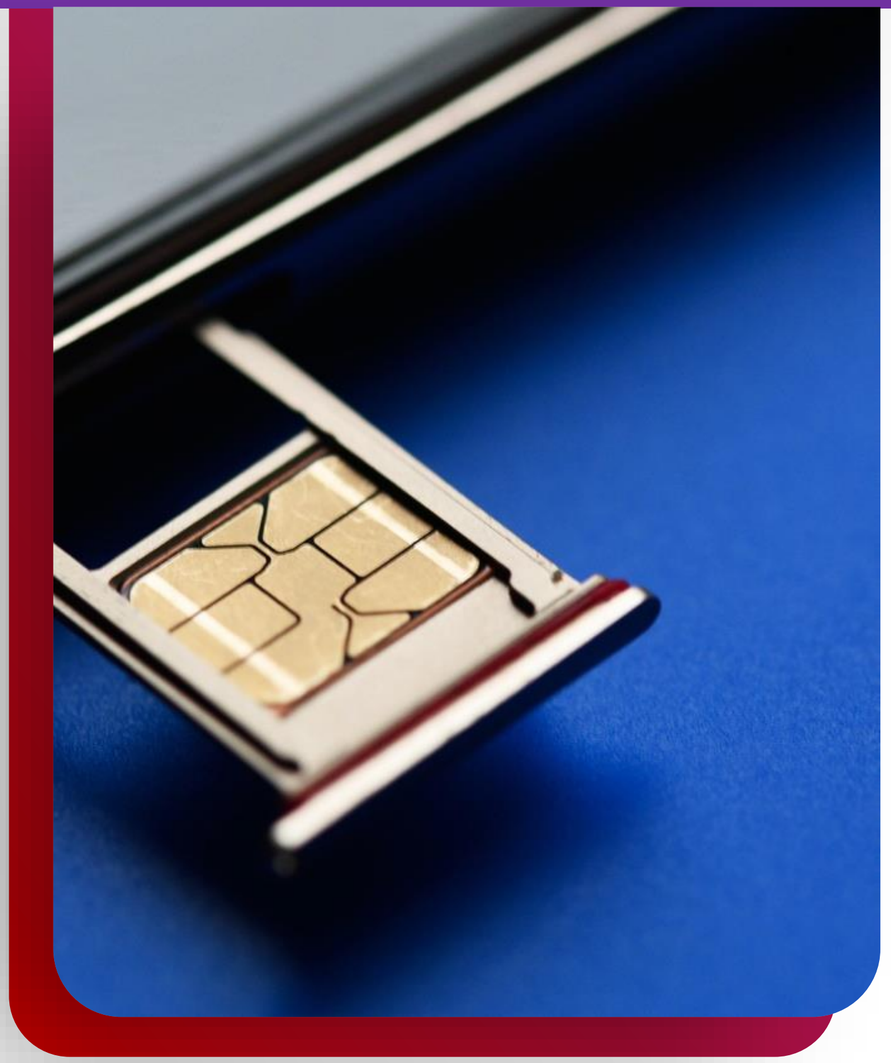
Why did we build an **IoT Registry?**

We saw an opportunity
& took it!

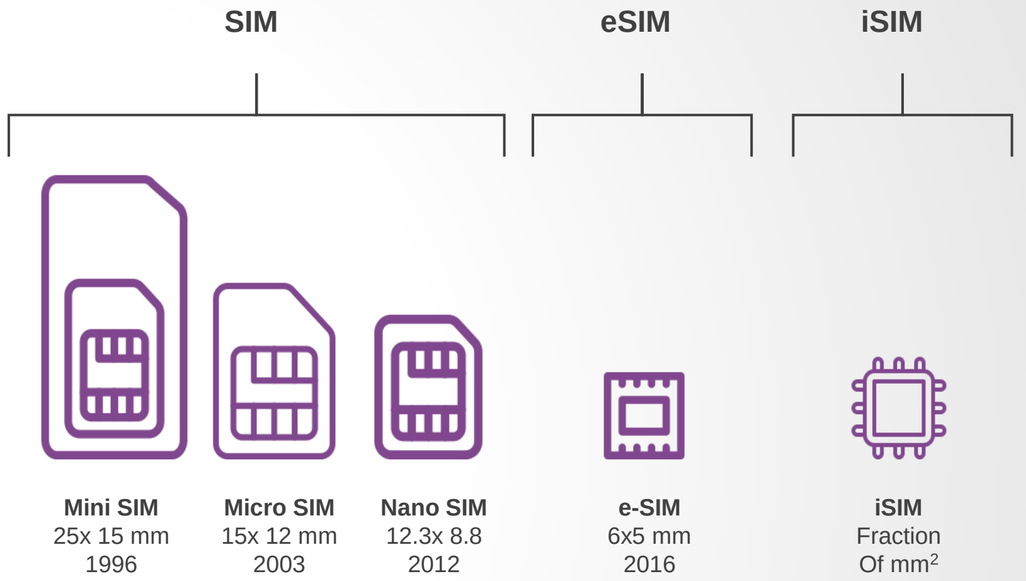
Goal is to have **DNSSEC** integral in the solution for **IoT Device Identity** and **mutual TLS authn**

It’s a major learning curve!!!

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



SUBSCRIBER IDENTITY MODULE - SIM



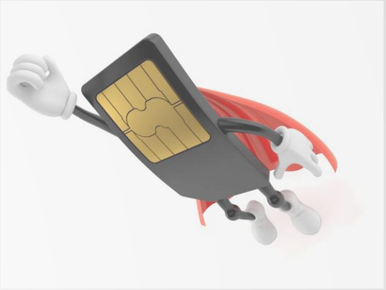
*** A Secure Element (SE) is a tamper-resistant microprocessor-based platform**

The SE securely stores sensitive data such as the application data and IoT device Identity

The embedded SIM is a new secure element compliant with GSMA

* https://www.thalesgroup.com/en/markets/digital-identity-and-security/mobile/secure-elements

GSMA IoT SAFE –> Pretty robust IoT Device Identity Solution



Put public key

Get random

Get data file
public/private key info

Read public key

eSIM

GSMA
IoT SAFE

Read file

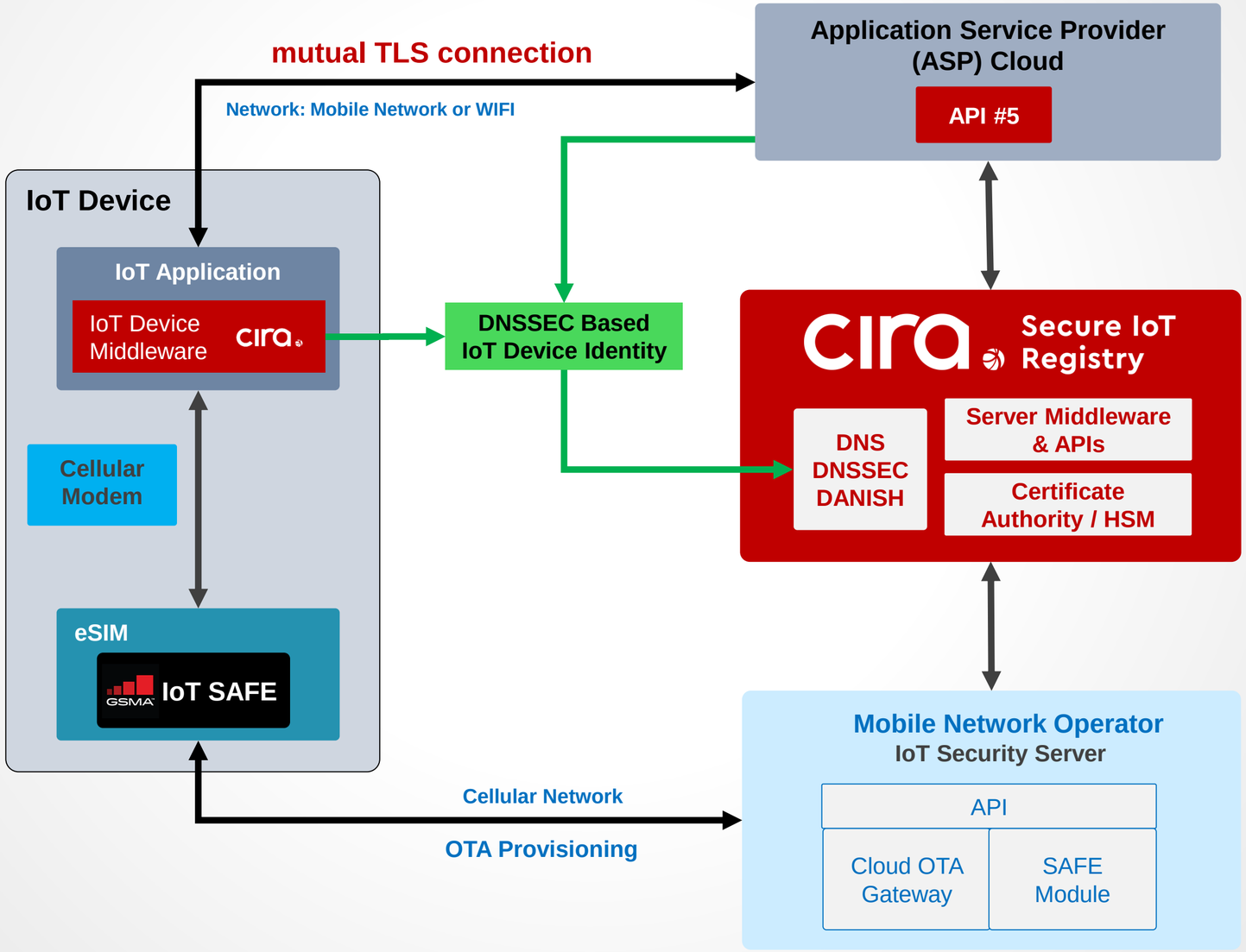
Generate object list

Verify signature

Generate public/private key pair

Compute signature on eSIM to enable mutual TLS Handshake

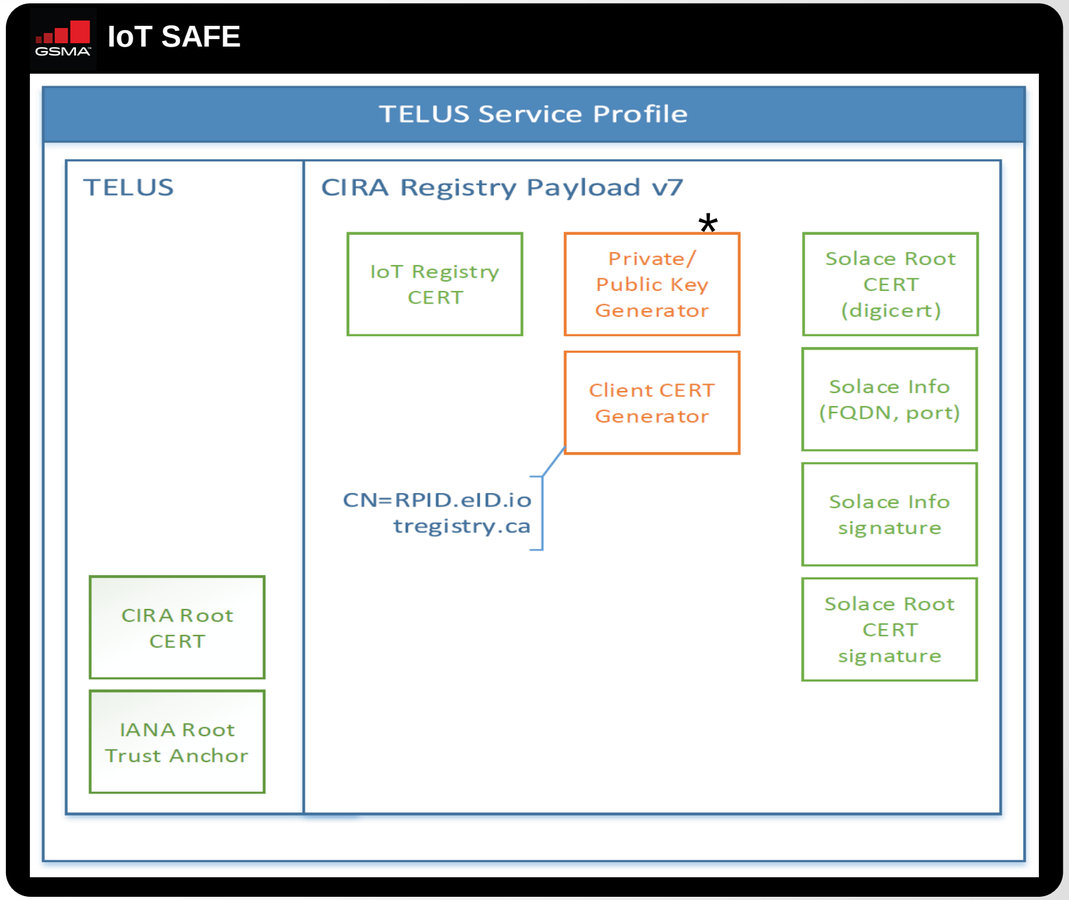
Building on top of the existing GSMA MNO -> eSIM trust model



- IoT SAFE - IoT Device Identity Management

IoT SAFE Applet – IoT Device Identity from CIRA Registry Payload

- **IoT Device Identity:**
  - **Private/Public key pair**
  - **Signed Client CERT (by IoT registry)**
  - **Unique DNS identifier subjectAltName/CN**



Server Side – TLSA – recap - this works now!

RFC 7671 DNS-Based Authentication of Named Entities (DANE) Protocol

*The TLSA RR (Resource Record) for a service is located at a DNS name that specifies certificate constraints should be applied for the services at a certain TCP or UDP port. At least one of the TLSA RRs must provide a validation (path) for the certificate offered by the service at the specified address.

The RR itself has 4 fields of data, describing which level of validation the domain owner provides.

- the certificate usage field
- the selector field
- the matching type field
- the certificate association data

Example of a MQTT Service TLSA Record for above Application Service Provider

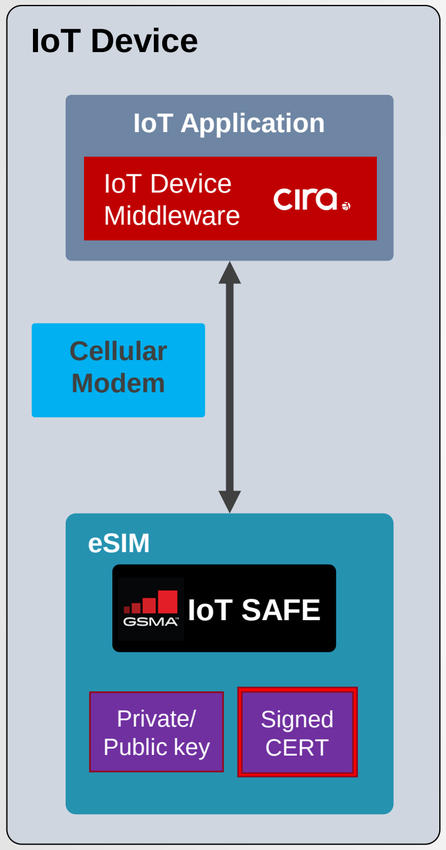
- Port: 8883
- Protocol: TCP
- Certificate Usage: 3 Domain issued certificate
- Selector: 0 (entire certificate)
- Matching Type: 0 entire match (1 or 2 = hash of certificate)
- Certificate: ASP-PKIX-CERT

_8883._tcp.iotasp.ca TLSA 3 0 0 …ASP-PKIX-CERT

*https://en.wikipedia.org/wiki/DNS-based_Authentication_of_Named_Entities

Client Side – TLSA for client identity – couple of internet drafts ☺

Shumon, Viktor & Ash to the rescue !!!



TLS Extension for DANE Client Identity
draft-huque-tls-dane-clientid-04
"TLS and DTLS extension to convey a DNS-Based Authentication of Named Entities (DANE) Client Identity to a TLS or DTLS server"

DANE Client Identity Extension "dane_clientid"

- In TLS 1.2, the empty extension is sent in the ServerHello message.
- In TLS 1.3, it is sent in the CertificateRequest message.

DANE CLIENT IDENTITY: use of the _device label in TLSA RR
draft-huque-dane-client-cert-06
"how to publish Transport Layer Security (TLS) server certificates or public keys in the DNS. "

Certificate:

- eID._device.iotregistry.ca TLSA 3 0 0 …SIGNED-CERT

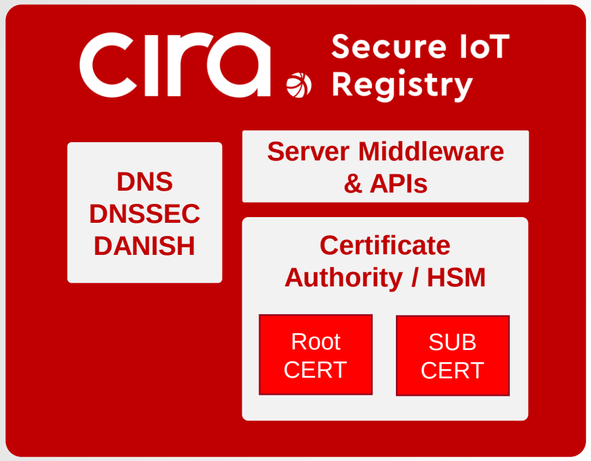
or

Public Key:

- eID._device.iotregistry.ca TLSA 3 1 1 …PUBLIC-KEY-SHA-256

https://datatracker.ietf.org/doc/html/draft-huque-dane-client-cert-06
https://datatracker.ietf.org/doc/html/draft-huque-tls-dane-clientid

Making some progress – a step in the right direction



PKI-Authenticated Certificate Discovery Using DANE TLSA records
draft-wilson-dane-pkix-cd-01
"how to use the TLSA record to enable entity and CA certificate discovery for object security and trust chain discovery use cases, and how to use PKIX validation for TLSA records queried without the benefit of DNSSEC."

Finding CA root cert from IoT device client ID:

- TLSA Client ID: eID._**device.iotregistry.ca**

to

- WebPKI link: https://**device.iotregistry.ca**/.well-known/ca/AKI.pem
  (where AKI is the authorityKeyID extracted from the entity certificate)

But it would be nice to get something like from a TLSA point of view with a new label: _rootcert

Finding CA root cert TLSA from IoT device client ID TLSA:

- TLSA Client ID: eID._**device.iotregistry.ca**

to

- TLSA Root CERT: _rootcert.**device.iotregistry.ca** TLSA 0 0 0 …ROOT-CERT-PUBLICKEY

https://datatracker.ietf.org/doc/draft-wilson-dane-pkix-cd/

Conclusion

DNSSEC should be a standard in opensource apps

To support adoption,

enable DNSSEC by default,

fund the open-source development

Still have many gaps in middleware to support TLSA and DNSSEC by defaults
OpenSSL to support client and server side mutual TLS connection with full DNSSEC TLSA identity authentication
On client to use eSIM to TLS authentication
On client to validate server with TLSA
On Server to use CERT to validate IoT device identity (attestation)

cira

Thank You

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