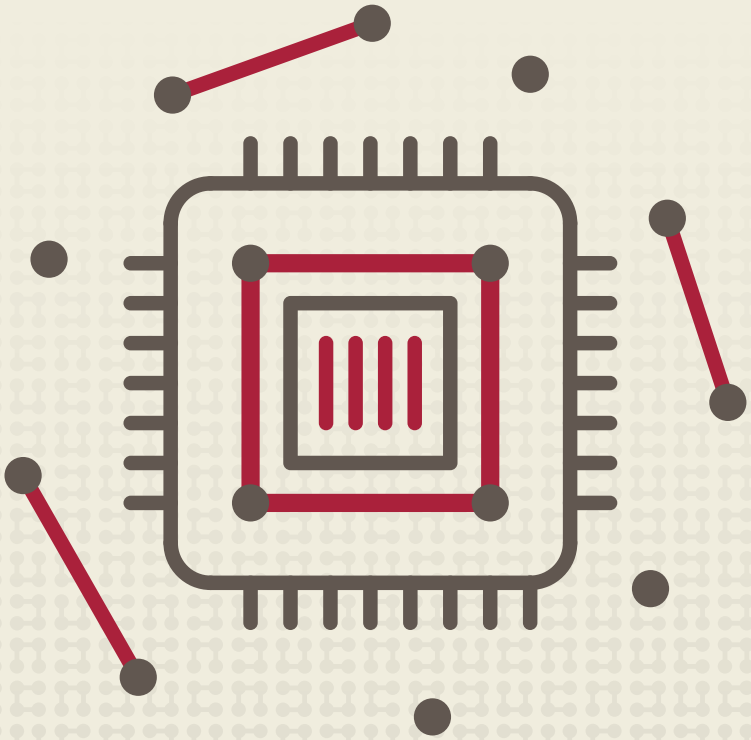
cira Labs

Secure IoT Registry



Zero-touch device identity management for IoT deployments that offers

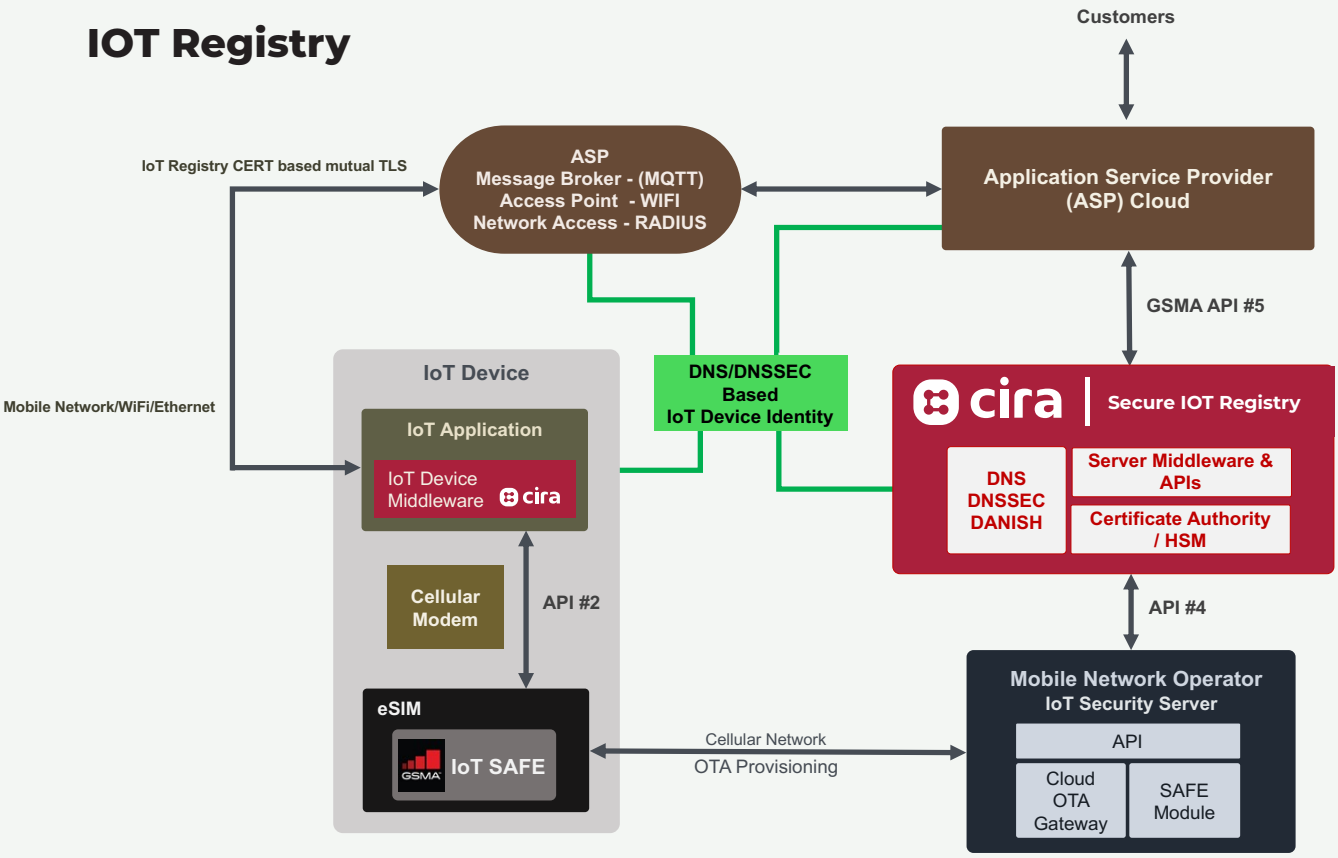
- Inherent/increased security
- Zero-touch provisioning
- Extended certificate lifecycle management

FEATURING

- Hardware root of trust = end-to-end, chip-to-cloud security
- IoT SAFE eSIM enabled IoT devices = zero touch provisioning/ re-provisioning of credentials
- Next generation DNSSEC-based IoT device identity attestation

The Internet of Things (IoT) has opened a world of possibilities for connectivity and efficiency — but it also introduces a massive security risk. CIRA Labs has leveraged its decades of experience running the .CA Registry to address this risk, by building an innovative new registry for IoT devices. In partnership with TELUS and Thales, CIRA Labs has developed an IoT Registry that offers secure device provisioning and management for IoT device manufacturers, mobile network operators and cloud providers.

IOT Registry



End-to-end, chip to cloud security

CIRA's IoT Registry ensures a hardware root of trust by using TLS-secured communication. It works by validating the identity of the device or server by providing a digital certificate signed by a recognized Certificate Authority (CA). The receiving server or program can then check the authenticity of the certificate.

IoT SAFE eSIM enabled IoT devices

Standards for device identity management are the key to keeping IoT devices secure.

CIRA's IoT Registry uses the IoT SAFE standard, which was developed by the mobile industry to allow IoT device manufacturers and IoT service providers to leverage the IoT device's SIM as a robust, scalable, and standardised hardware Root of Trust to protect IoT data communications.

cira

DNSSEC as a chain of trust

CIRA's IoT Registry uses DNSSEC to take secure communication to the next level. It approaches zero trust security for IoT provisioning by using DNSSEC to allow a client to verify the authenticity of the IoT device. The IoT Registry has a real time publicly available, trusted and verifiable Certificate/Certificate Authority.

The IoT Registry publishes DANE TLSA records signed with a DNSSEC record with a unique identifier for IoT Device Identity, linked to the IoT SAFE root of trust certificate.

MORE BENEFITS

- Connectivity & protocol agnostic
- Secure, seamless on-boarding with enterprise connectivity
- Allows the SIM to be used for application-layer security, as well as mobile network authentication
- IoT security at scale — for hassle free growth

What else does the IoT Registry offer?

- Always on; remote registration, activation & transfer = easy setup and lifecycle management & confirms that it belongs to vendor
- Remote turn-off, wipe-clean IoT device config for granular control of credential provisioning
- IoT security at scale — for hassle free growth

Who can use the IoT Registry?

This registry is being developed for use by the entire IoT community, from mobile network operators to device makers. It is geared towards:

- Cloud providers
- Mobile network operators — to increase adoption
- Device and modem makers — simplify supply chain
- SIM providers
- Network infrastructure providers — simplified and trusted identity management
- Secure IC vendors

PARTNER WITH US! Find out more at: cira.ca/labs/current-projects