Webinar: IoT SAFE Solution for Cellular Device Security

Zero-touch provisioning and encrypted data connectivity for server-hosted apps

Kigen

ZARIOT

CRYPTO QUANTIQUE

© 2024 Kigen

We'll be starting soon, but in the meantime, let us and your network know you're here.

@Kigen

@Kigen_Ltd

Use the chat panel for questions

© 2024 Kigen

Agenda

- Latest developments shaping Zero Touch Provisioning
- Introduction to Kigen IoT SAFE
- ZARIOT's connectivity and wider use cases
- Crypto Quantique's implementation
- Live demo of the joint solution
- Your questions!

© 2024 Kigen

Kigen

Meet our expert panel

Paul Bradley
VP Solutions Sales
at Kigen

Jimmy Jones
Head of Security
at ZARIOT

Chris Jones
Director of Applications
at Crypto Quantique

© 2024 Kigen

Seamless out of the box connectivity

Silicon Vendor partnerships

Incorporate Kigen's lean, certified (e)SIM OS deep inside chipsets

Module Manufacturers partnerships

Enable late-stage personalisation for their cellular network of choice for either initial provisioning or operational purposes

MNO partnerships

Enable access to a worldwide network of coverage for IoT Service Providers to leverage the best quality, most cost-effective connectivity for IoT devices to interact with the cloud securely

Connectivity Management Platform operators

Guarantee access to a wide range of local MNO subscriptions by interconnecting demand and supply through our Kigen RSP solutions

© 2024 Kigen

Kigen: Driving (integrated) eSIM to be the cornerstone of IoT

Kaleido Intelligence

High Flyer: eSIM Subscription Management

Counterpoint

Global eSIM enablement leader

INTEGRATED eUICC

Solutions for the semiconductor and device ecosystems.

OEM FOCUSED

In-factory connectivity enablement.

eSIM SOLUTIONS

In-Field Connectivity Management.

IoT SAFE

Securing Data and Transactions with Zero Touch Provisioning.

© 2024 Kigen

eSIM standards evolution

M2M RSP	CONSUMER eSIM	eSIM FOR IoT	SIM PROVISIONING
• SGP.01/02 family • Bootstrap connectivity • Supports devices with no User Interface • Strong bind between eSIM and RSP system (SM-SR) leading to complicated integration between SR and DP elements	• SGP.21/22 family • Alternative connectivity possible (and most common) for provisioning • User Intent (via LPA User Interface) needed • Any eSIM profile can be provisioned by any GSMA-certified SM-DP+	• **SGP.31/32 family** • Bootstrap or alternative connectivity may be used for provisioning • Supports devices with limited/no User Interface • User Intent moved to eSIM IoT Remote Manager, for fleet management use cases • Any eSIM profile can be provisioned by any GSMA-certified SM-DP+ • Requires Consumer RSP as building block to start from	• Helps a device to get connected to the network and provisioned with enterprise cloud credentials in one simple flow • **In-factory solutions for cellular profile loading** • **IoT SAFE** & Zero-Touch Provisioning
Separate from future RSPs and likely to be (gradually) sunset when IoT RSP is in the market for a few years	Stable for Consumer devices and will have bolt-ons put around it from IoT RSP.	Consumer RSP with bolt-ons for constrained devices & networks and enable User Intent shift to cloud.	#FutureofSIM

© 2024 Kigen
Kigen

IoT SAFE Applet for Secure End-to-End Communication

98% **Enterprises want end to end solutions that protect data from place of collection, to cloud**

GSMA Intelligence, Dec 2020

Secure element as a root of trust

Protecting data using the credentials inside the secure element

Inter-operable, advanced **cryptographic features** of a SIM

SIM protects IoT data **from chip to multi-cloud**

© 2024 Kigen

OPEN IoT SAFE manifesto

Simple, unified **zero-touch provisioning**

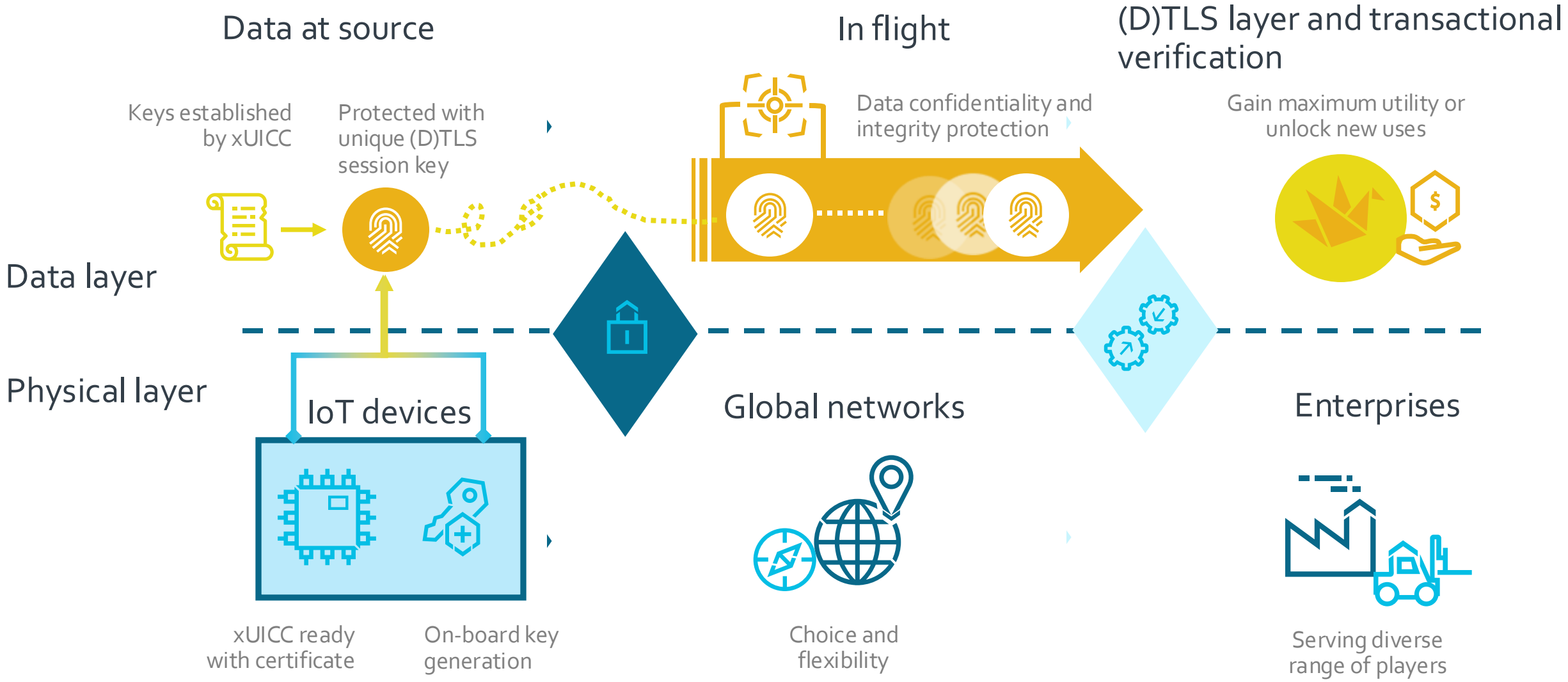
Treating enterprise security credentials with the same level of security as mobile network credentials, by **leveraging tamper-resistant hardware**

Removing barriers to access hardware-based security to better protect credentials

Using open systems, based upon standards and <u>without</u> complex integration

© 2024 Kigen

Kigen OPEN IoT SAFE

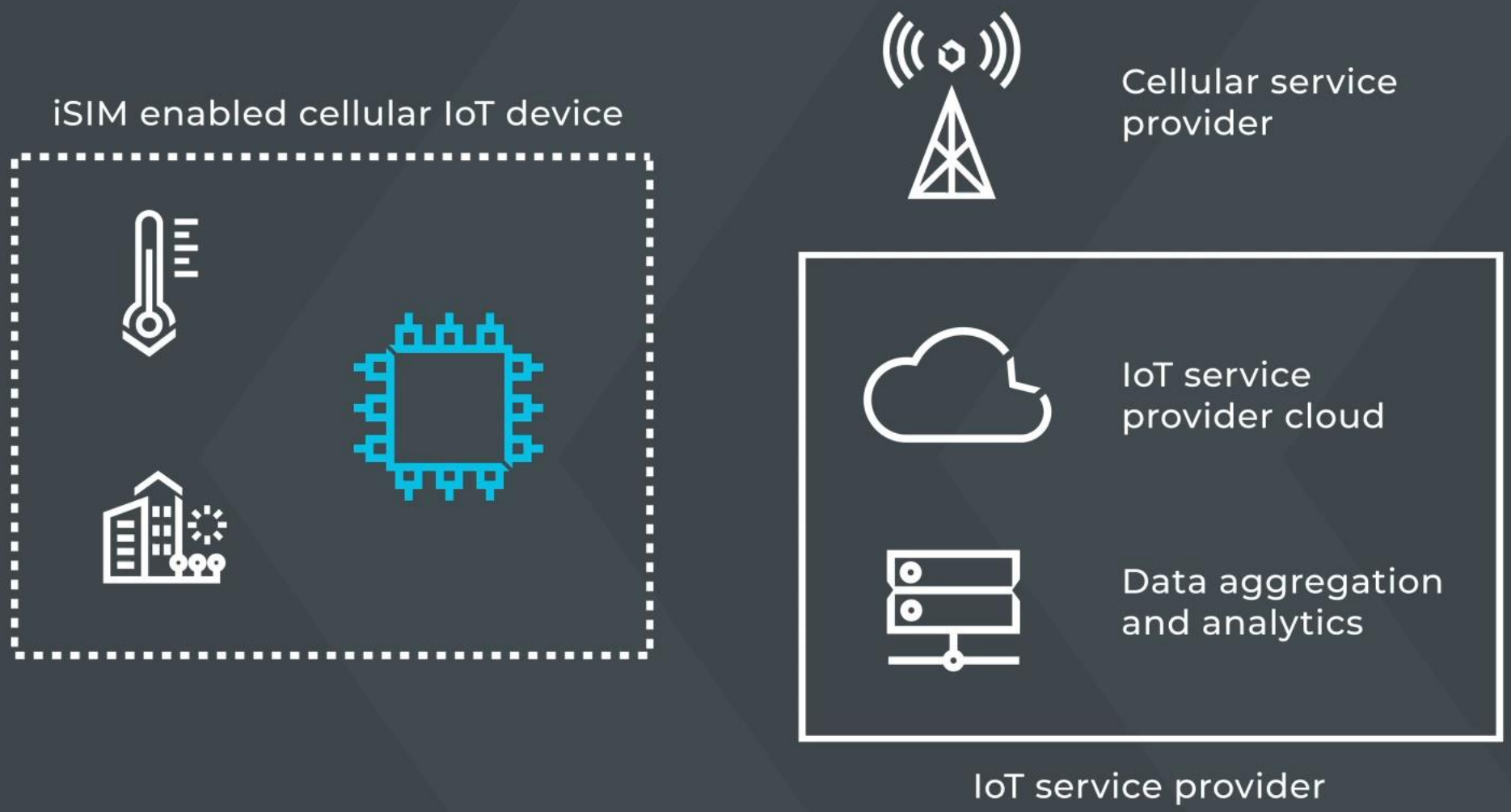


© 2024 Kigen

Kigen

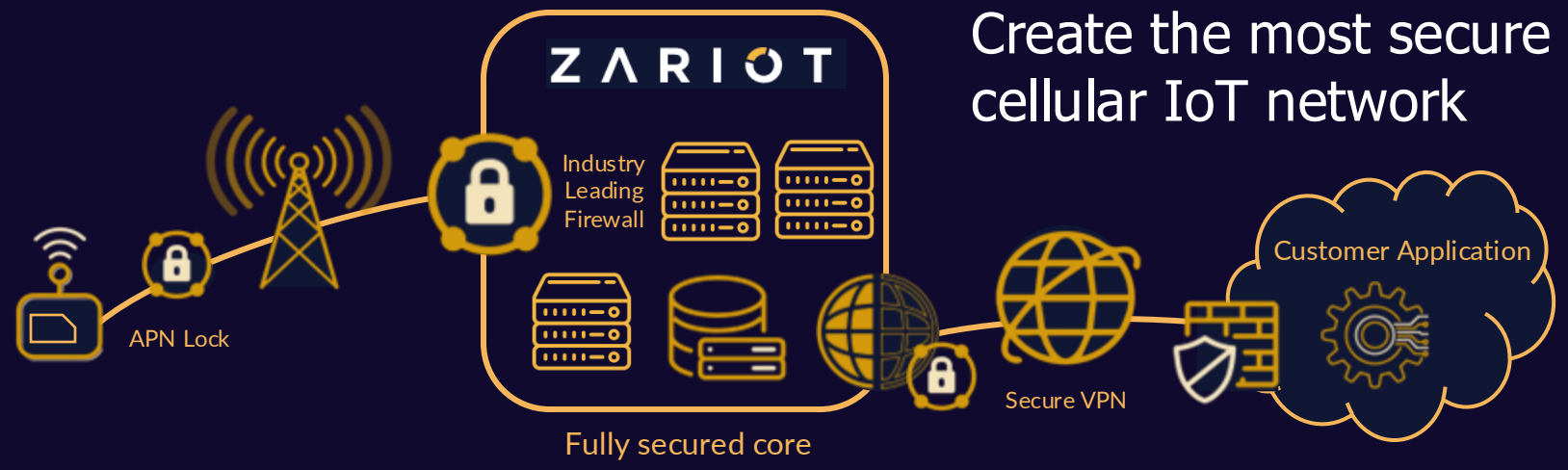
IoT SAFE

GSMA



IoT SAFE secured cellular IoT device & ecosystem

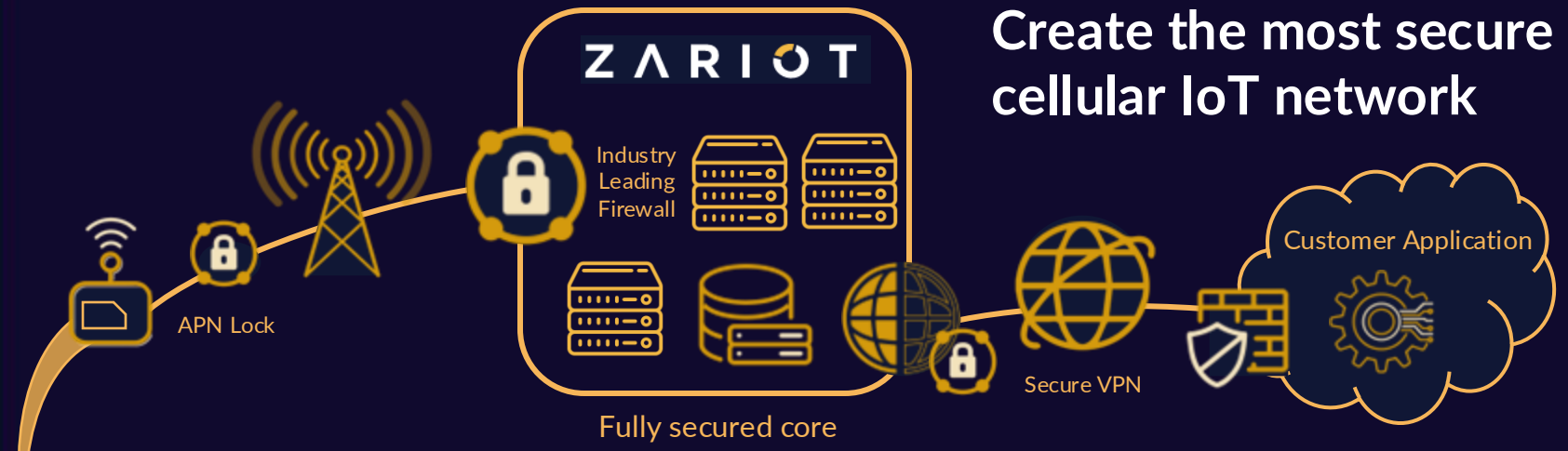
ZARIOT – IoT Connectivity Provider



Create the most secure cellular IoT network

Award Winning Network Security

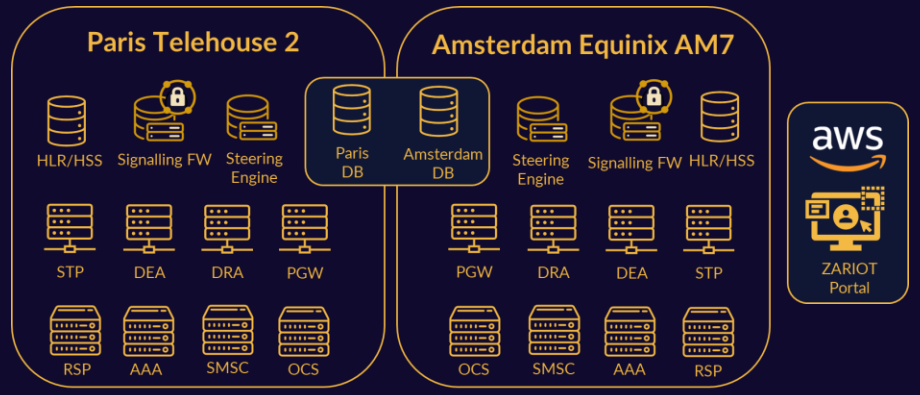
ZARIOT – IoT Connectivity Provider



Create the most secure cellular IoT network

Award Winning Network Security

- Features
- Applets



ZARIOT

Use our unique engineering skillsets to provide real-world tangible benefits for our customers

Connectivity Key in Driving Cohesive IoT Solutions

Device, Network & Application together form your IoT's DNA.

Device

Huge flexibility of design & implementation

Network

Opaque element with formulated, constricted functionality & lack of flexibility.

Application

Huge flexibility of design & implementation

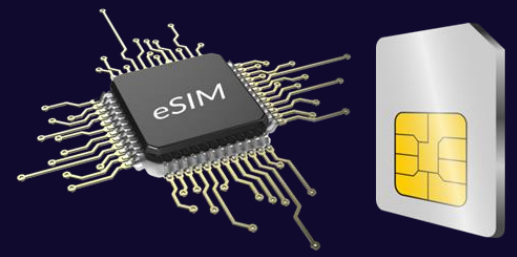
- *By opening the potential of the Network to make available new, or existing unutilized features makes cohesive, secure by design IoT solutions possible.*
- *The Network's position is unique, as it directly touches both ends, by opening its flexibility it can aid end-to-end integration.*

Access to Innovate

ZARIOT benefits from a unique set of circumstances. Our partnership with Kigen & in-house SIM expertise allows us to deploy ZARIOT & partner features directly on the non-volatile area of the SIM.

While our sister company owning and developing the Signalling Firewall give us a Swiss Army knife in our core.

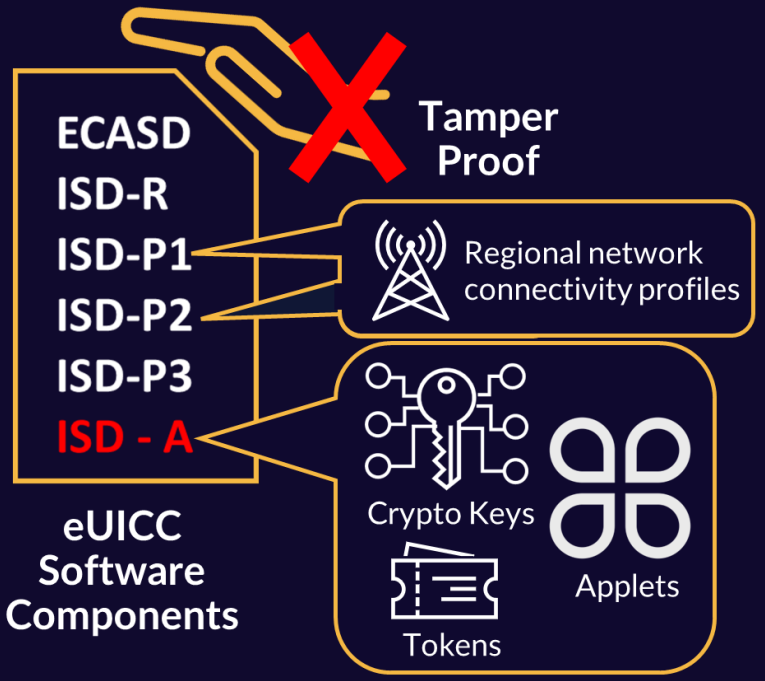
All supported by a home-grown portal, opens cellular connectivity like never before.

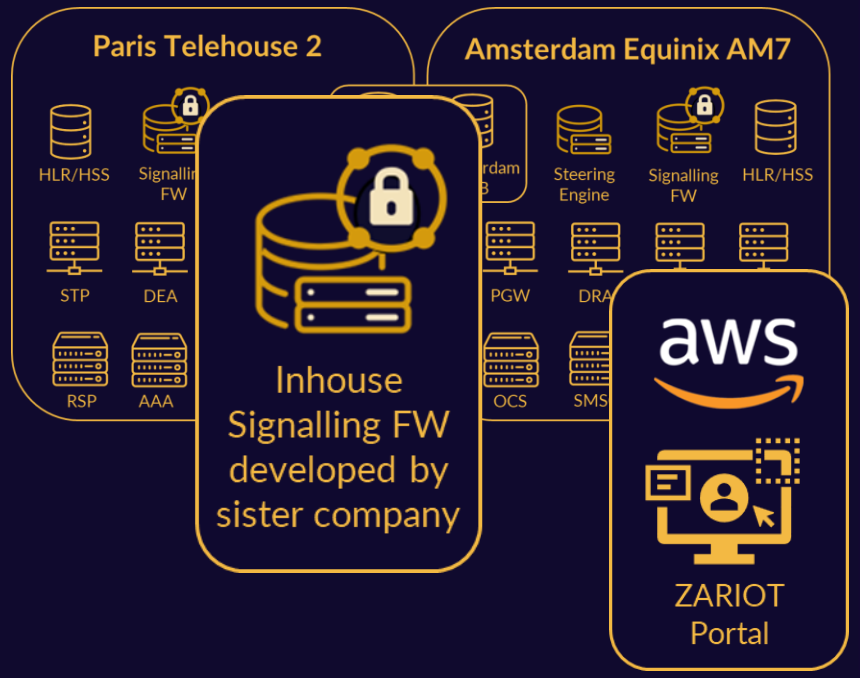


Kigen

GSMA TCA TRUSTED CONNECTIVITY ALLIANCE Enabling trust in a connected future

IoT SAFE
IoT SIM Applet For Secure End-2-End Communication





Connectivity Ecosystem Driving Unified, Feature Rich IoT Solutions

ZARIOT continues to build & expand a transparent ecosystem of partnerships to drive IoT success.

Atsign's opensource software provides E2E encryption and simple device management. The solution has 32 patents

Able Device

provide multiple device solutions, from remote admin and troubleshooting to QoS & Security, & more

SevenShift

deliver IoT device security testing via the Bunkai platform. Speeding protection & certification.

teragence NETWORK INSIGHT

maps out coverage & mobile signal strength in any location across Europe and North America.

wadaro new wave data and insights

offer QoS metrics from the device giving virtual boots on the ground visibility & avoiding site visits.

SMARTAXIOM

deliver a full blockchain platform specifically designed & built to fully support IoT solutions.

binaré

Binare offer binary code inspection securing your device & creating an SBoM. Then monitoring & informing of new threats

CRYPTO QUANTIQUE

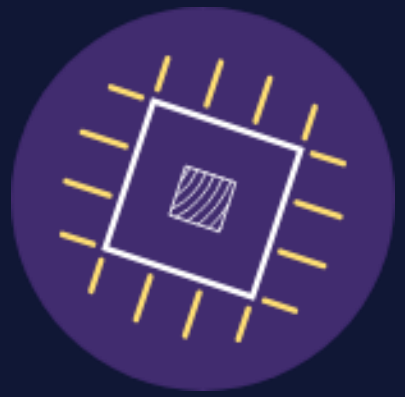
provides E2E encryption, zero-trust secure provisioning, onboarding, & device life-cycle management.

CRYPTO QUANTIQUE

ZARIOT

QuarkLink™

IoT security platform that uses advanced cryptography techniques to securely connect IoT devices.



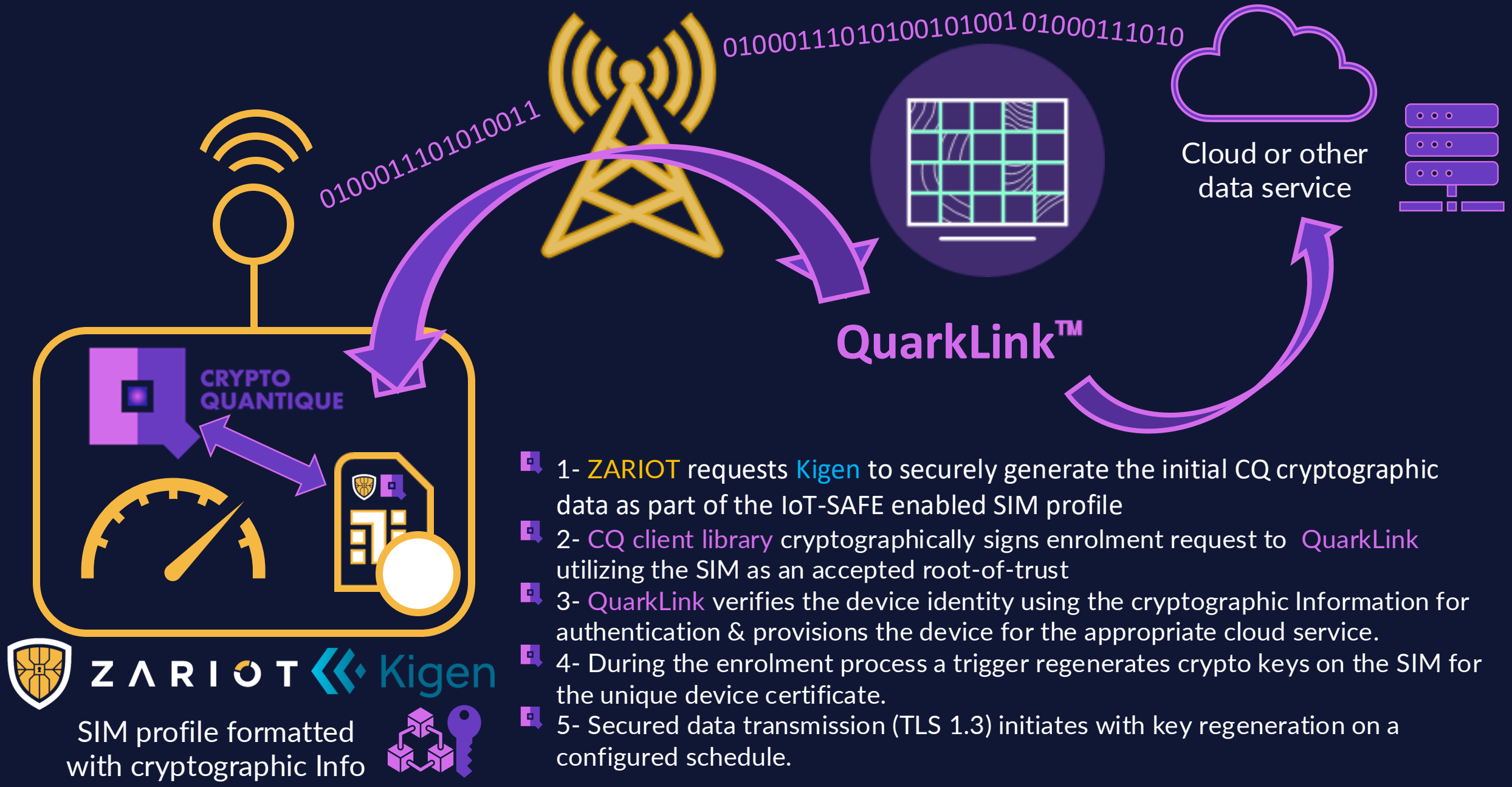
QDID™

Quantum-**D**riven **ID**entity, is a physical unclonable function (PUF). It provides a unique device identity and cryptographic keys that cannot be counterfeited, hacked or breached.

SIM Based

ZARIOT utilize the crypto properties derived from GSMA's IoT-SAFE in a novel way to produce non-volatile root of trust environment, that can create & securely store the CQ certificates.

Each can work independently to secure IoT systems but combined offer the highest standard of security available.



- 1- ZARIOT requests Kigen to securely generate the initial CQ cryptographic data as part of the IoT-SAFE enabled SIM profile
- 2- CQ client library cryptographically signs enrolment request to QuarkLink utilizing the SIM as an accepted root-of-trust
- 3- QuarkLink verifies the device identity using the cryptographic Information for authentication & provisions the device for the appropriate cloud service.
- 4- During the enrolment process a trigger regenerates crypto keys on the SIM for the unique device certificate.
- 5- Secured data transmission (TLS 1.3) initiates with key regeneration on a configured schedule.

We are a software and IP company exponentially transforming IoT cybersecurity

Well established with an exceptional, substantial engineering team

- 30 engineers – full-time employees, of which 5 PhDs
- Unique combined expertise in cryptography, hardware, embedded and cloud software, and quantum physics
- 6 Hardware IC Designers — 11 Embedded and cloud software engineers

Thorough understanding of silicon and embedded software

- Crypto Quantique has developed its own quantum driven Root-of-Trust in silicon
- We integrate 3rd party devices into our cloud platform in a matter of days with our embedded expertise

Certification readiness

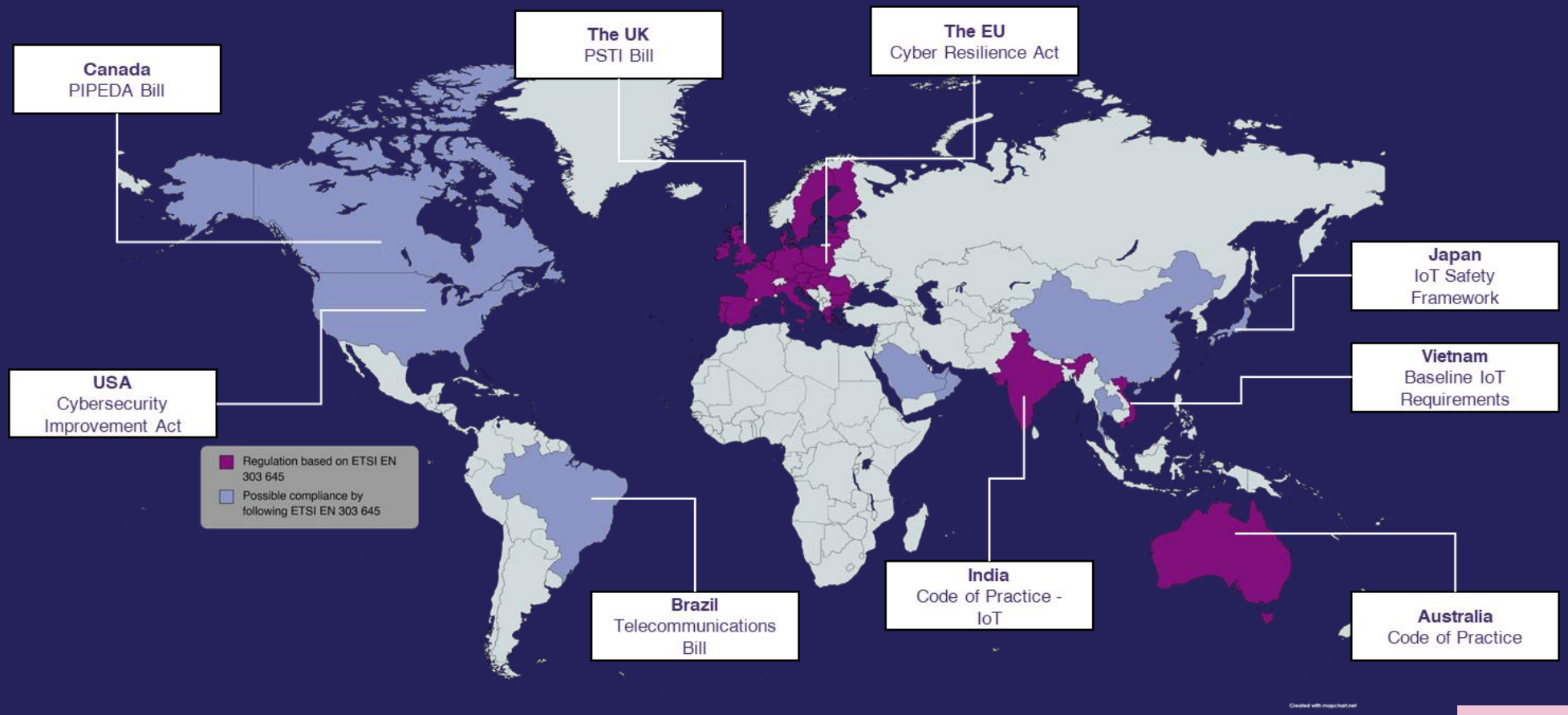
- PSA Level 2 Ready Certified for QDID (quantum driven PUF)
- EAL 4+ (quantum driven PUF)
- 3rd party pen testing and cyber essentials for the cloud platform

Highly flexible architecture

- Built with fast integrations and customizations in mind
- New deployments in a matter of minutes, compatible with any infrastructure

One of many

Regulation and legislation is rolling out worldwide



Source - CETOME

CRYPTO QUANTIQUE

Why you need cybersecurity!

CE Mark

- EU Cyber Resilience Act (CRA) is asking for Hardware and Software security
- Securely store unique secrets onto each device
- Trust the software devices is running
- Patch vulnerability and bugs remotely for five years or during the device lifecycle

IoV
ISO 21434

AMI
IEC 62056/62351

EVSE
OCPP/ISO15118

IACS
IEC62443

SEMI
E187

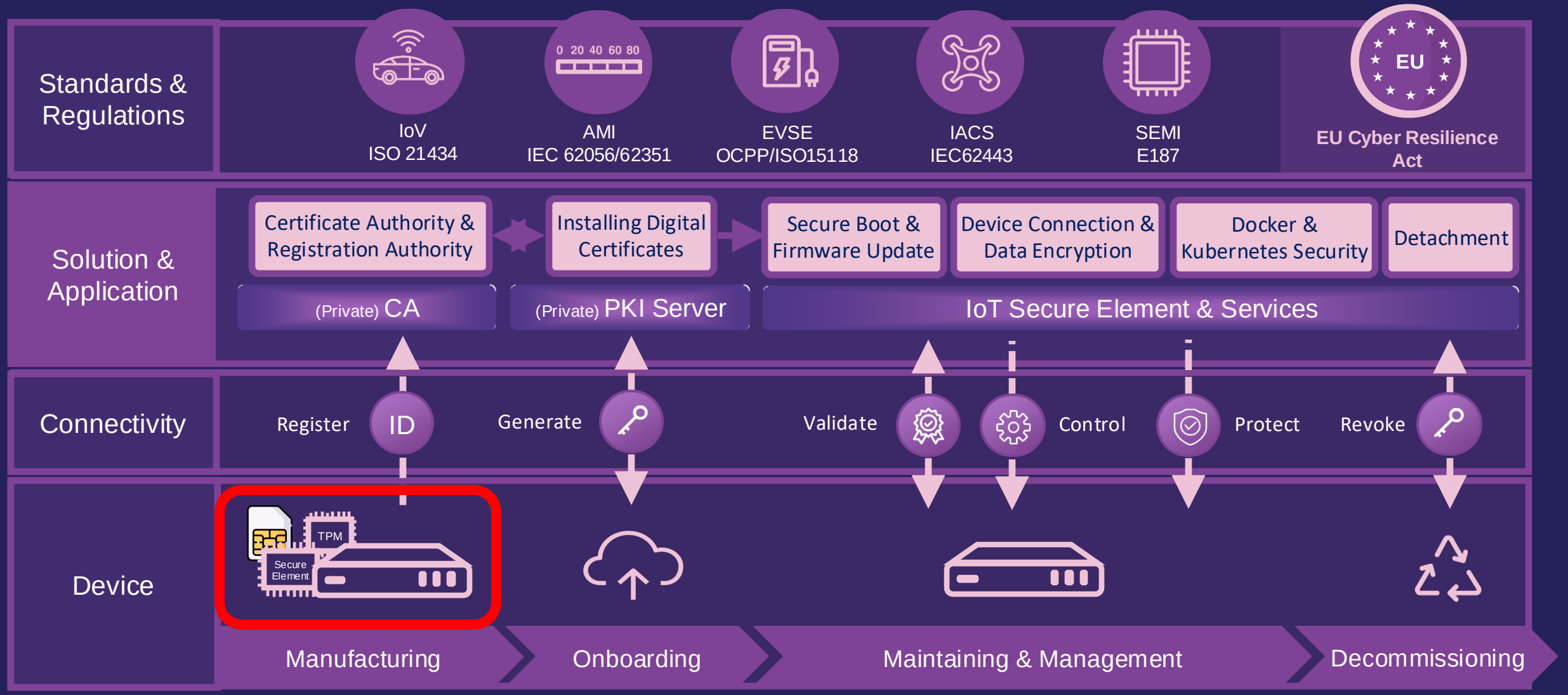
Global regulation

- 20+ countries including the US and the UK regulators are enforcing IoT security
- Secure boot, Data integrity, Firmware security and OTA update

CRYPTO QUANTIQUE

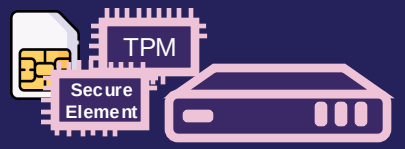
Secure Connected Devices Life-Cycle

Security is a chain, only as secure as the weakest link



Provable identity

Provable identity requires a device (microcontroller, microprocessor, ASIC or SoC) to include a <u>root of trust</u>



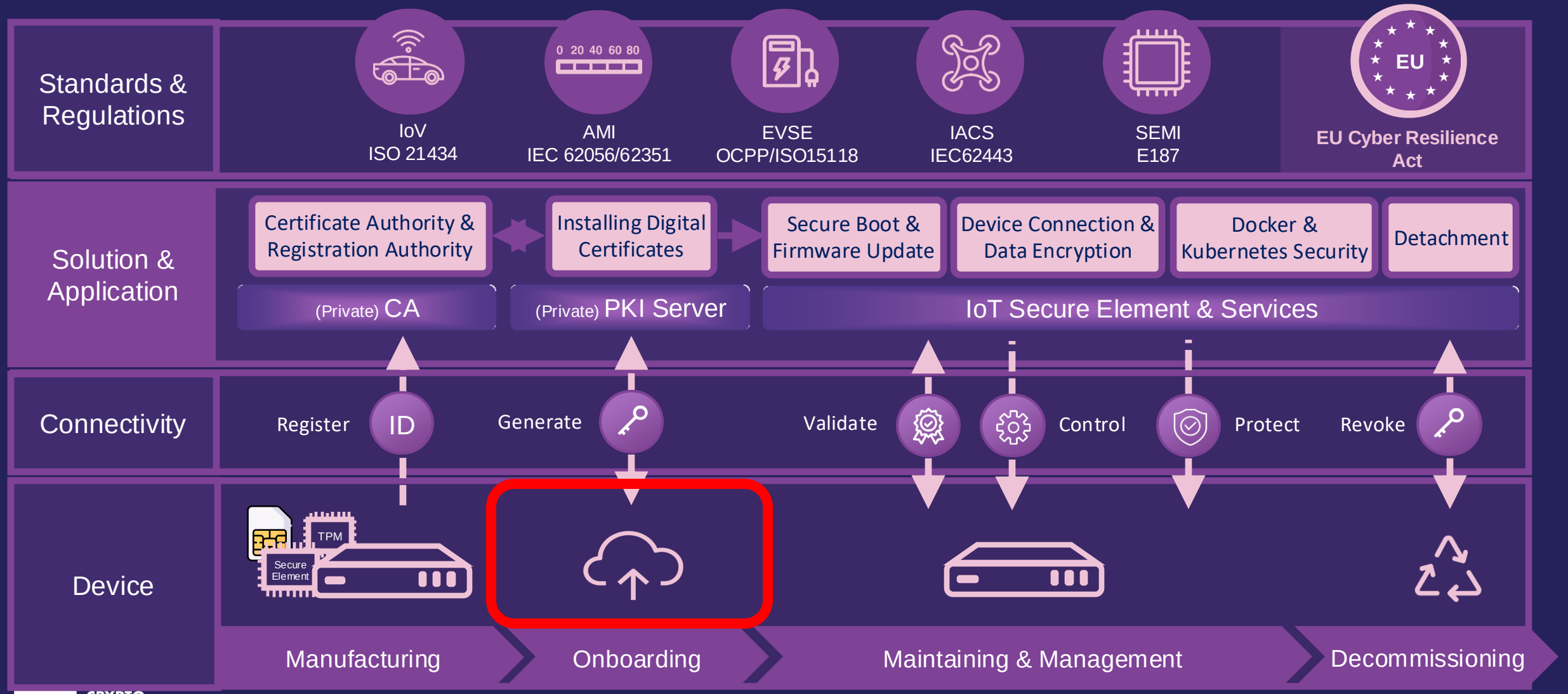
Root of Trust requirements :

- An **immutable boot path** that cannot be interrupted by the debug/JTAG interface
- The ability to ensure a **secure boot process** that authenticates the software image before it is executed
- The ability to program and lock a section of boot flash memory (~64KB) so that it is immutable (i.e. MCU boot manager cannot be erased/reprogrammed).
- In addition, the MCU can increase security by supporting a **secure key storage facility** that prevents the access to the keys from unauthorized users (i.e. The security data storage cannot be accessed by the main application).

CRYPTO QUANTIQUE

Secure Connected Devices Life-Cycle

Security is a chain, only as secure as the weakest link



CRYPTO QUANTIQUE

Connecting to the cloud

Device “onboarding” or “deployment” involves several steps, including setting up the cloud infrastructure, configuring the microcontroller, and ensuring secure communication between the device and the cloud

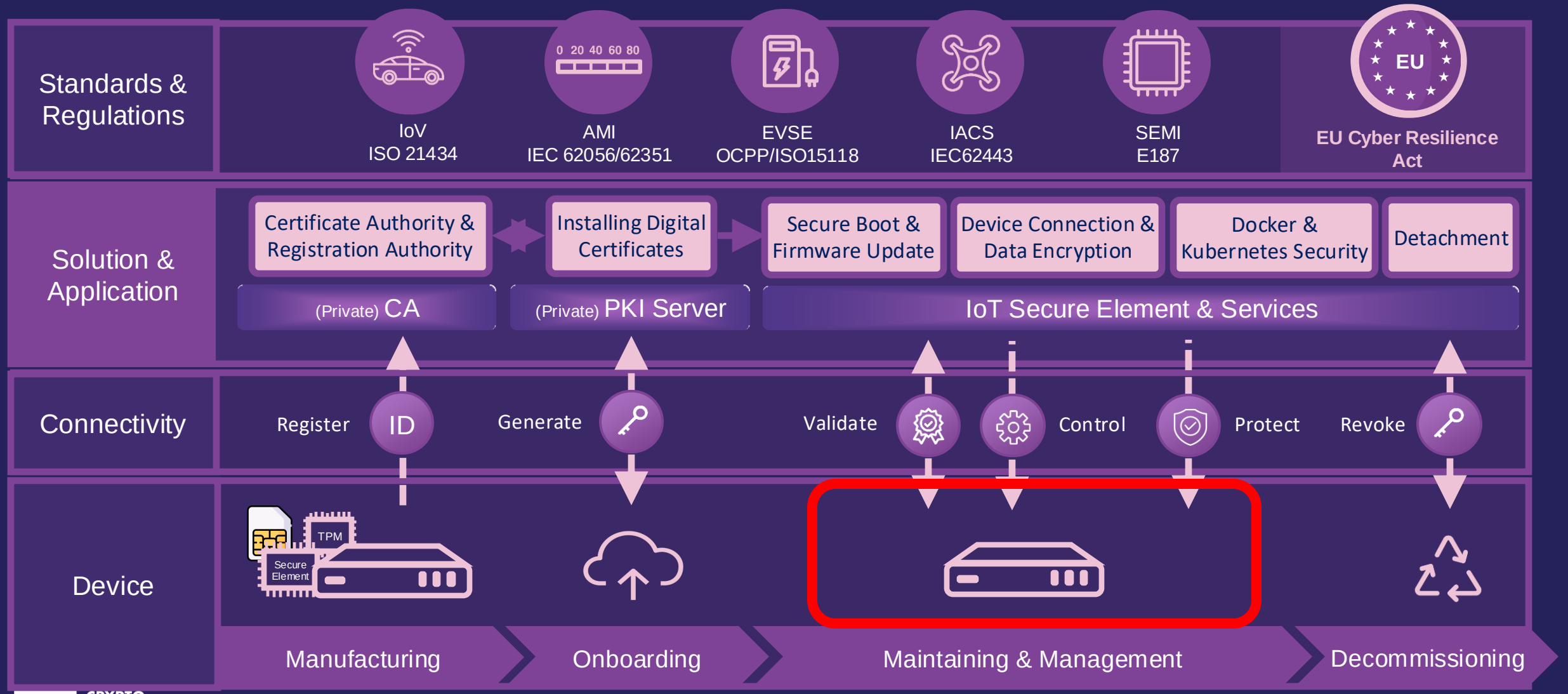
Deployment requirements:

- A compatible MCU/MPU/SoC – supports necessary protocols and libraries for secure communication.
- Establishment of a Public Key Infrastructure and a Certificate Authority
- Generation of unique device certificates and cryptographic keys
- Create security policies for the connected devices
- Securely provision the device with the security credentials (certificates, keys, policies etc)

CRYPTO QUANTIQUE

Secure Connected Devices Life-Cycle

Security is a chain, only as secure as the weakest link



CRYPTO QUANTIQUE

Life-cycle management

Refers to the comprehensive process of overseeing and maintaining the device from its initial deployment through to its eventual decommissioning.

Life-cycle management requirements:

- Secure hardware provisioning
- Health monitoring
- Firmware and software updates
- Ensuring data integrity and secure transmission
- Ensuring the device complies with relevant regulatory standards and certifications
- Certificate management (renewal, revocation etc)

CRYPTO QUANTIQUE

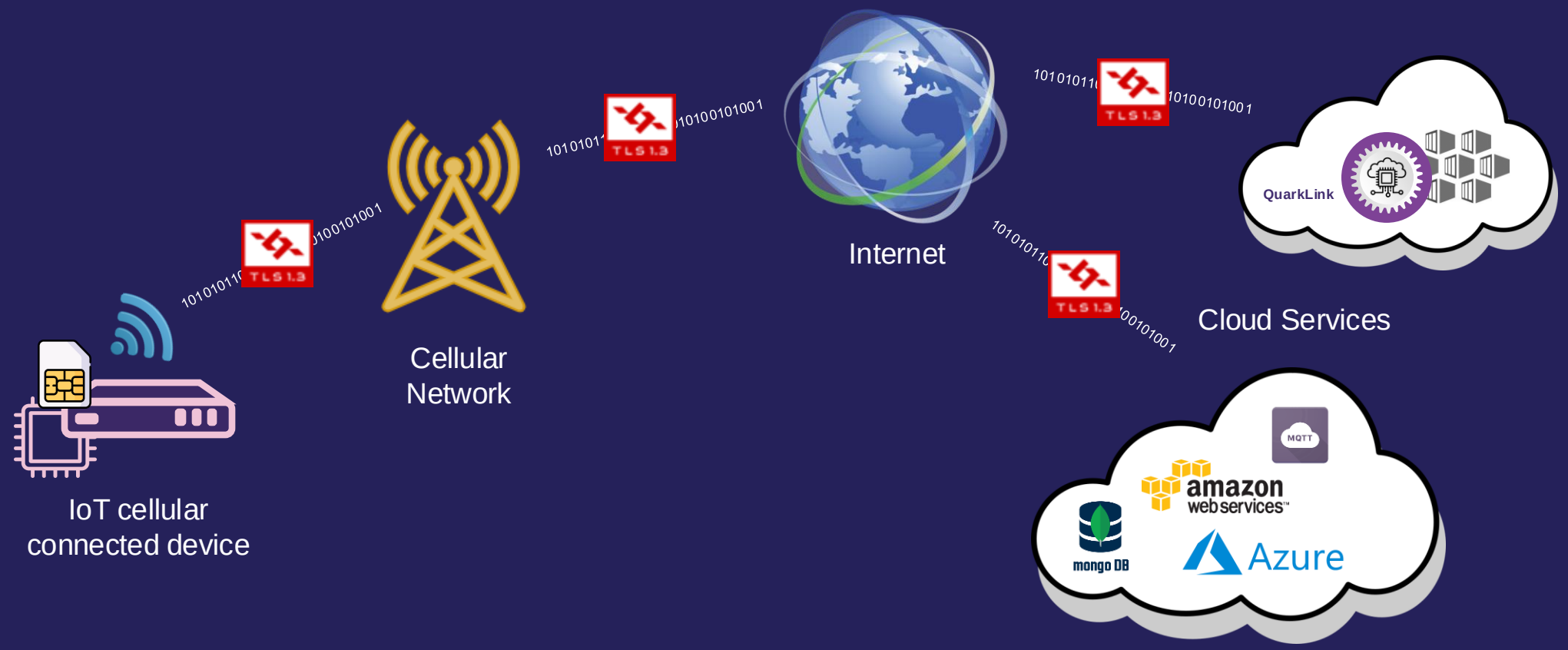
QuarkLink addresses the security needs for edge devices at the embedded, OS and the cloud

CRYPTO QUANTIQUE

Securing the connected world with zero trust

The Zariot/Kigen/Crypto Quantique Solution

End to end secure communication

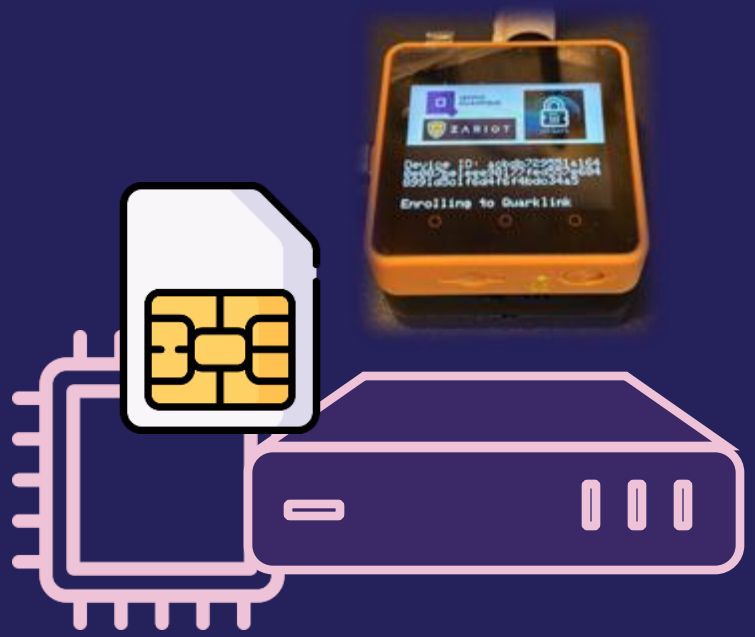


CRYPTO QUANTIQUE

Connected Device support

QuarkLink security platform provides:

- Software (QuarkLink client library)
  - FreeRTOS support
  - C source code
  - mbedTLS support
- Hardware
  - ESP32 Microcontroller (M5Stack)
  - SIMCOMM 7600G-H 4G LTE modem
  - Zariot IoTSafe SIM cards
- SaaS Platform
  - Custom QuarkLink instance
  - Annual license fee



CRYPTO QUANTIQUE

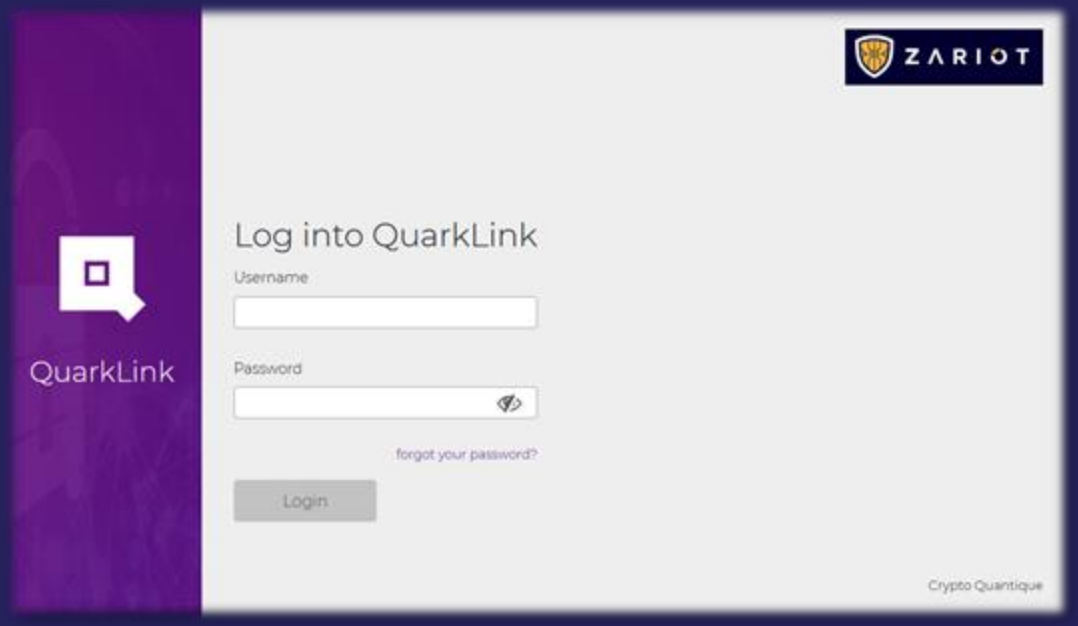
QuarkLink Value Add to customers

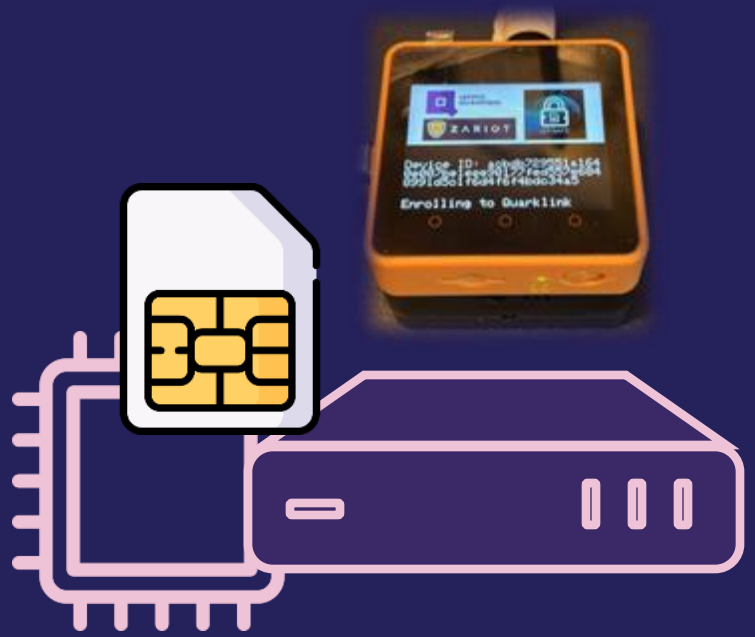
The customer owns their QuarkLink Server.

- Preventing counterfeiting
  - Is it genuine?
  - Has it been manipulated?
  - Enable secure boot
- Device CE Mark compliance
- Making it easy for the customer to be compliant for CRA or other industry regulations such as ISO62443
- Enable Plug&Play deployment
- Reduces complexity and lowers the cost

CRYPTO QUANTIQUE

Demo Time!





CRYPTO QUANTIQUE

#FutureofSIM

@Kigen

@Kigen_Ltd

Thank You
Go raibh maith agaibh
Merci
Dank u wel
谢谢
ありがとう
Diolch
Dziękuję
Tak
감사합니다
धन्यवाद
شكرًا
Paldies

© 2024 Kigen