SEAL SQ
semiconductors + quantum

- A WISeKey company

matter

Matter – Certificates and Security Compliance

SEALSQ

- Gweltas RADENAC

  IoT Business Line Director

  - 25 May 2023

AGENDA

- Company
- Regulations
- Matter introduction

SEALSQ

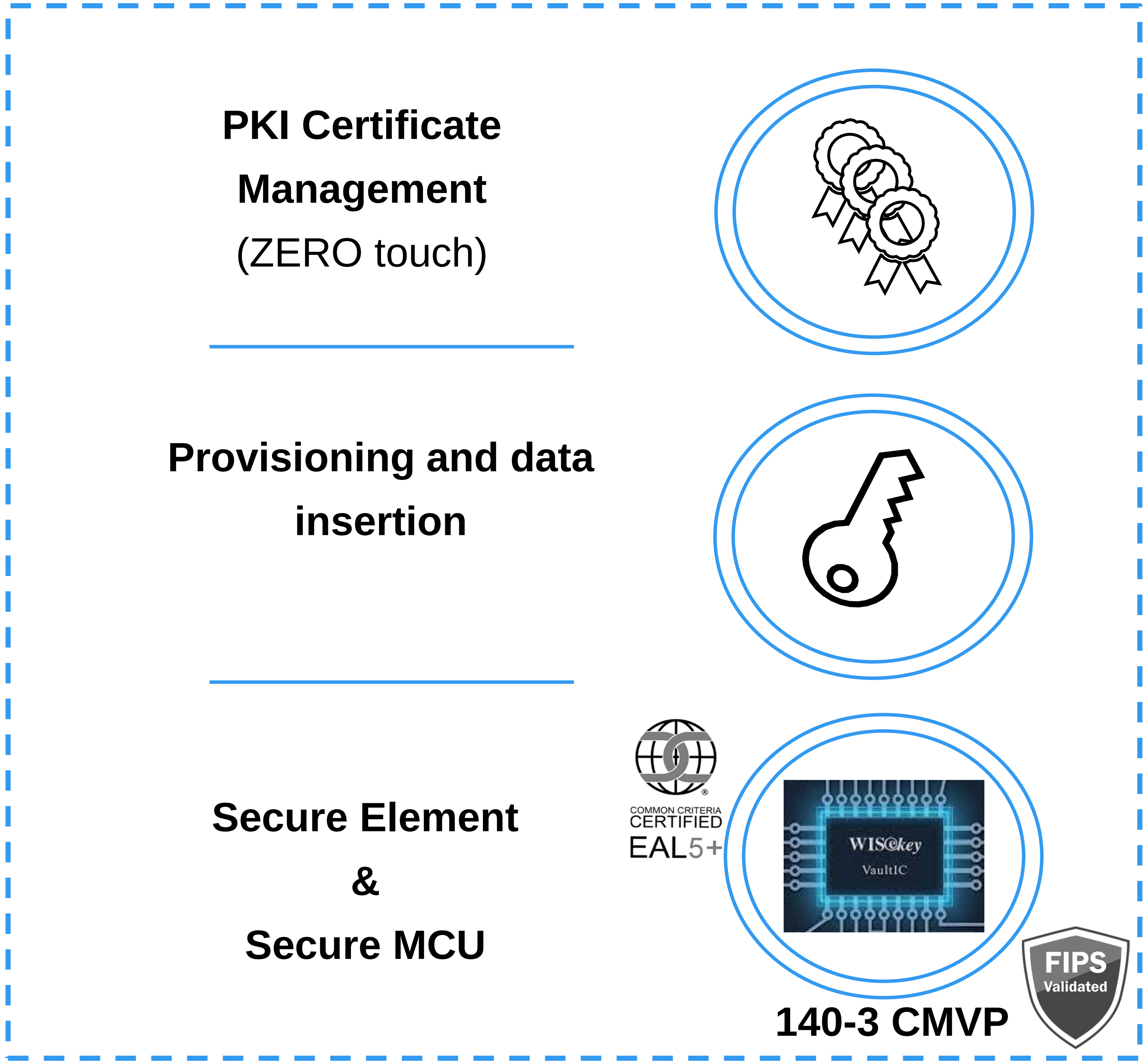
The WISeKey Group Semiconductors Subsidiary

- *Over 25 years developing highest level security solution to protect users identity, devices, data and transactions*
- *Trusted PKI CA (Public & Private) based in Europe (HQ in Switzerland)*
- *Leading hardware secure element developer and manufacturer*

25	6	WKEY	5B	1.6B
YEARS EXPERIENCE	GLOBAL OFFICES HQ IN GENEVA, SWITZERLAND	NASDAQ :LAES SIX: WIHN	RoT INSTALLED	SECURE CHIPS INTO IOT SHIPPED

UNIQUE VALUE PROPOSITION FOR IoT & Embedded

- Vertical End-to-End Solution



PKI Certificate Management

(ZERO touch)

Provisioning and data insertion

Secure Element

&

Secure MCU

COMMON CRITERIA CERTIFIED EAL5+

FIPS Validated

140-3 CMVP

SEALSQ – TRUST SERVICE PROVIDER

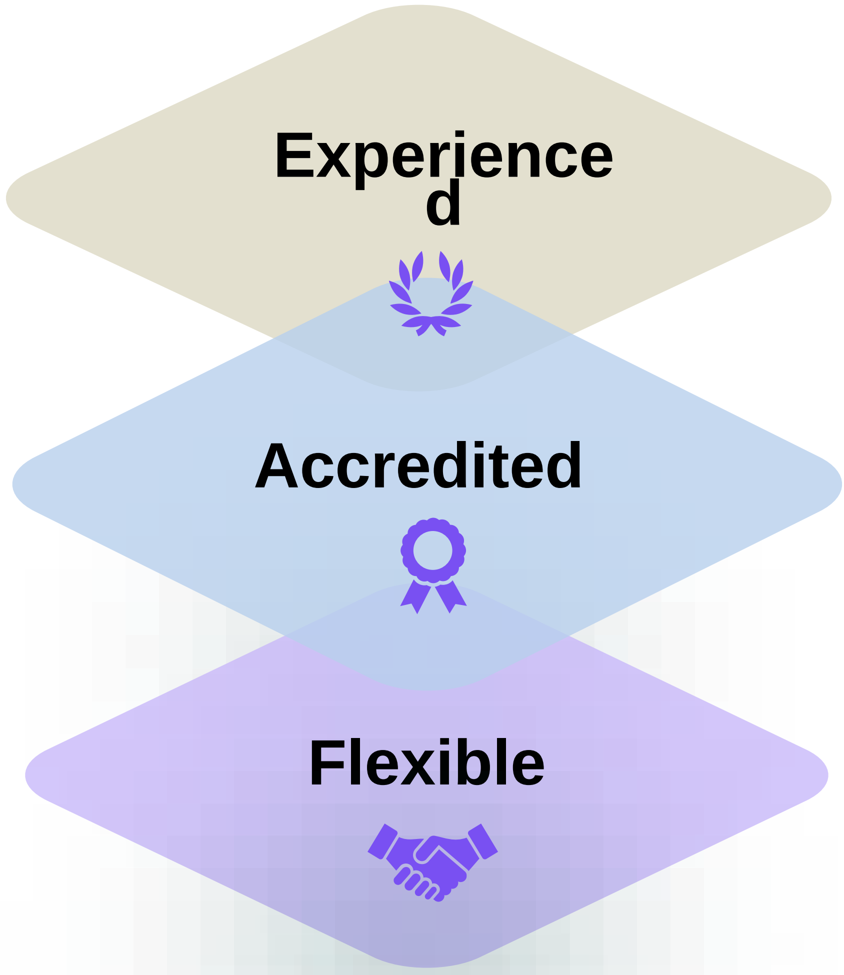
23 years in Managed PKI

Served over 3,000 clients

Trusted by all browsers & OS

Versatile SaaS mode CMS platform

High service level



Experienced

Accredited

Flexible

Universally Recognized

Swiss Based Root of Trust

Registered Firm • ISO 27001 • www.qmsi.eu

QMS

SWISS QUALIFIED CERTIFICATION SERVICE PROVIDER

Certification Authorities

WebTrust

Ernst & Young

PKI SERVICES

Root of Trust

✓OISTE CA - Publicly trusted CA Recognized by Browsers, Smart Phones, etc.
✓Private CA(s) Corporate root of trust

WISeID

✓Digital Identity Platform (B2B & B2C)
✓Personal certificate management
✓Cloud document signature services
✓MFA & API for 3rd Party integration

INeS

✓Managed PKI platform for IoT
✓Node Certificates (X509, MATTER)
✓Lifecycle management
✓API with AWS and Azure

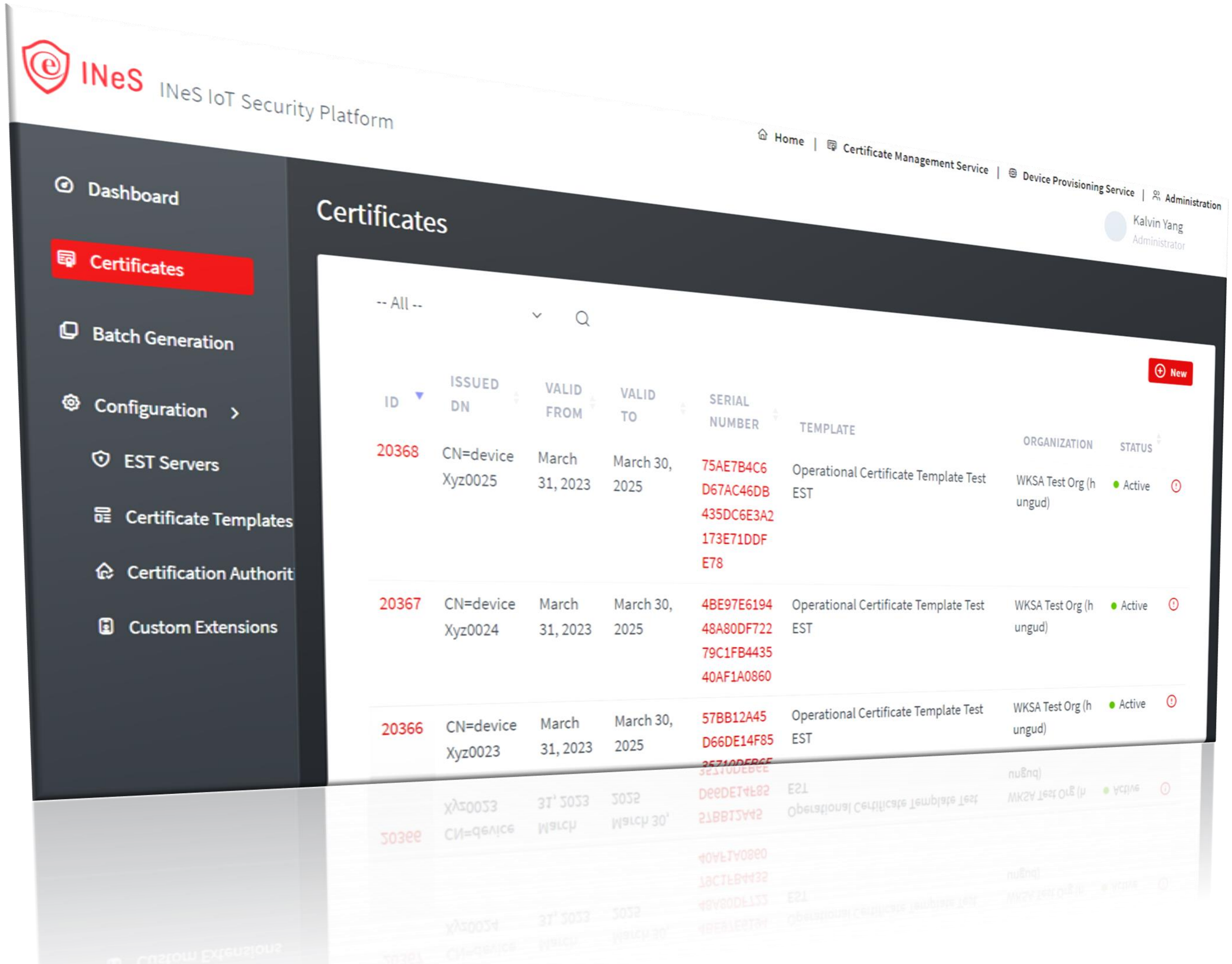
CertifyID TLS Manager

✓Managed PKI for TLS certificates
✓Full compatibility with the browsers
✓SSL management & automation

KEY APPLICATIONS

1. **IoT:** Installed base/deployed device identity management
2. **Enterprise/IT**: User access rights management (enterprise)
3. **Applications:** Certificate server in SaaS (applications)
4. **Internet:** Publishing certificate revocation (CRL and OCSP)

INeS CERTIFICATE MANAGEMENT SYSTEM (CMS)



Certificates

ID	ISSUED DN	VALID FROM	VALID TO	SERIAL NUMBER	TEMPLATE	ORGANIZATION	STATUS
20368	CN=device Xyz0025	March 31, 2023	March 30, 2025	75AE7B4C6 D67AC46DB 435DC6E3A2 173E71DDF E78	Operational Certificate Template Test EST	WKSA Test Org (h ungud)	Active
20367	CN=device Xyz0024	March 31, 2023	March 30, 2025	4BE97E6194 48A80DF722 79C1FB4435 40AF1A0860	Operational Certificate Template Test EST	WKSA Test Org (h ungud)	Active
20366	CN=device Xyz0023	March 31, 2023	March 30, 2025	57BB12A45 D66DE14F85	Operational Certificate Template Test EST	WKSA Test Org (h ungud)	Active

Certificate Management:

- Certificate Templates
- Certificate creation: standalone and batch
- Certificate management

Device Management:

- Device types
- Device creation: standalone and batch
- Inventory management

Configuration Management:

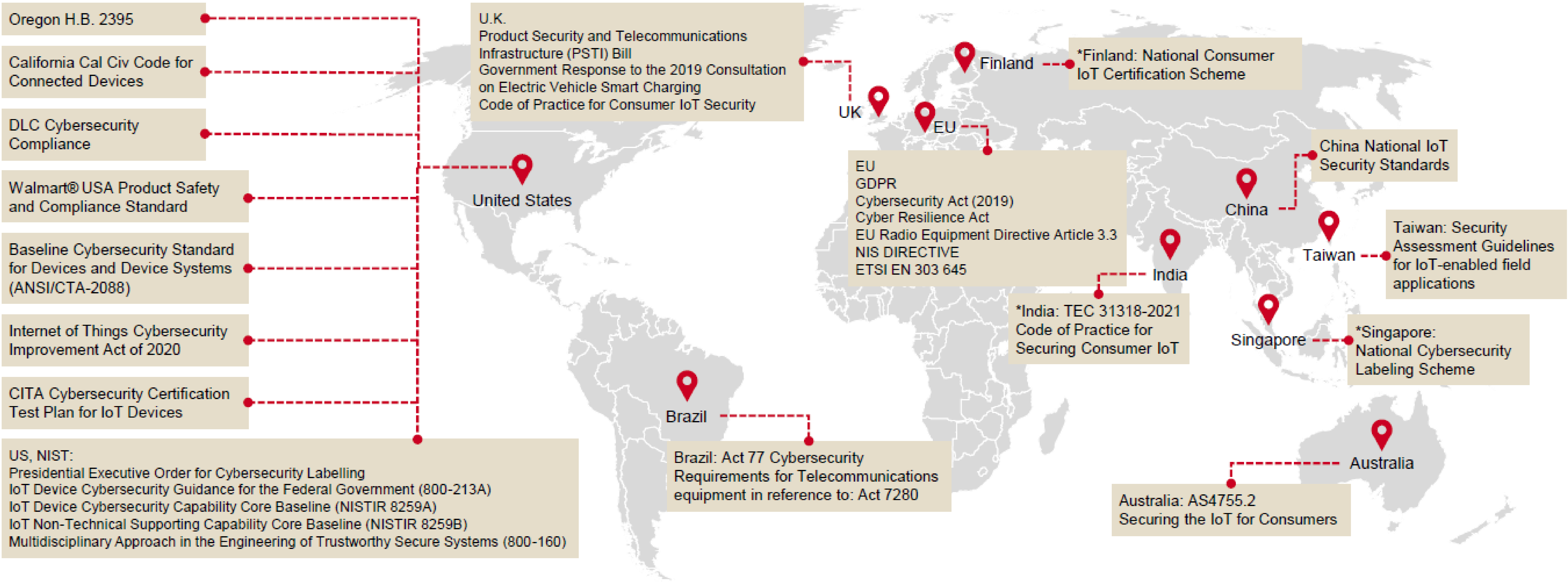
- User management
- Organization management
- CA management
- Audit log management

Public Cloud Integration:

- AWS IoT Core JITP
- Azure DPS/ IoT hub
- RESTful & EST APIs support

REGULATIONS in CYBER

Regulations, guidelines & compliance



Oregon H.B. 2395

California Cal Civ Code for Connected Devices

DLC Cybersecurity Compliance

Walmart® USA Product Safety and Compliance Standard

Baseline Cybersecurity Standard for Devices and Device Systems (ANSI/CTA-2088)

Internet of Things Cybersecurity Improvement Act of 2020

CITA Cybersecurity Certification Test Plan for IoT Devices

US, NIST:
Presidential Executive Order for Cybersecurity Labelling
IoT Device Cybersecurity Guidance for the Federal Government (800-213A)
IoT Device Cybersecurity Capability Core Baseline (NISTIR 8259A)
IoT Non-Technical Supporting Capability Core Baseline (NISTIR 8259B)
Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems (800-160)

U.K.
Product Security and Telecommunications Infrastructure (PSTI) Bill
Government Response to the 2019 Consultation on Electric Vehicle Smart Charging
Code of Practice for Consumer IoT Security

EU
GDPR
Cybersecurity Act (2019)
Cyber Resilience Act
EU Radio Equipment Directive Article 3.3
NIS DIRECTIVE
ETSI EN 303 645

*Finland: National Consumer IoT Certification Scheme

China National IoT Security Standards

Taiwan: Security Assessment Guidelines for IoT-enabled field applications

*India: TEC 31318-2021 Code of Practice for Securing Consumer IoT

*Singapore: National Cybersecurity Labeling Scheme

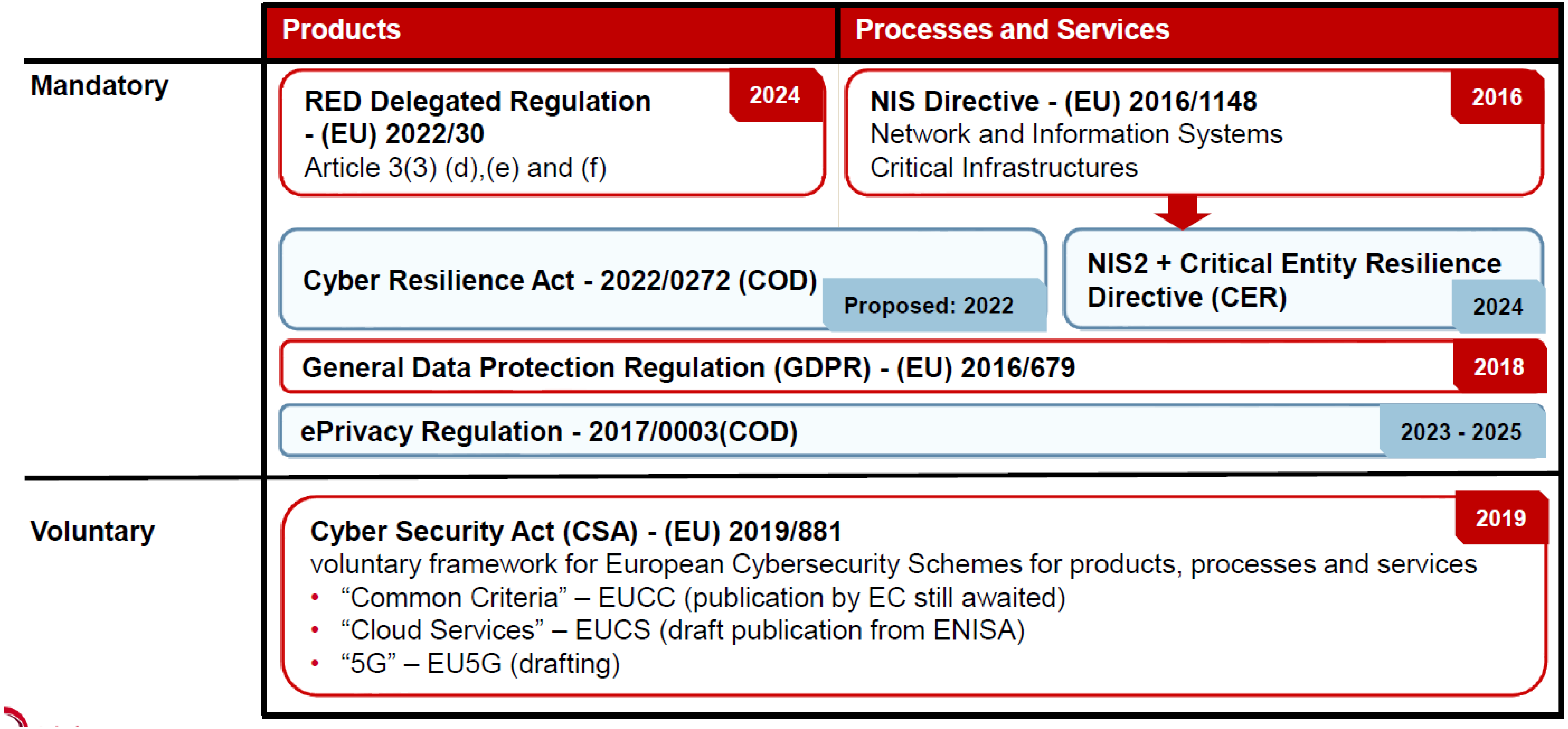
Brazil: Act 77 Cybersecurity Requirements for Telecommunications equipment in reference to: Act 7280

Australia: AS4755.2 Securing the IoT for Consumers

Priority market standards:
U.S.: NIST/Global Acceptance: EN 303 645/ EU: RED Article 3.3/ Brazil ANATEL/UK: Code of Practice for Consumer IoT Security/ Global: PSA IoT Security Framework and Certification

UL Lab source 2022

EU regulatory landscape on cybersecurity



Products | **Processes and Services**

Mandatory

RED Delegated Regulation - (EU) 2022/30 2024
Article 3(3) (d),(e) and (f)

NIS Directive - (EU) 2016/1148 2016
Network and Information Systems
Critical Infrastructures

Cyber Resilience Act - 2022/0272 (COD) Proposed: 2022

NIS2 + Critical Entity Resilience Directive (CER) 2024

General Data Protection Regulation (GDPR) - (EU) 2016/679 2018

ePrivacy Regulation - 2017/0003(COD) 2023 - 2025

Voluntary

Cyber Security Act (CSA) - (EU) 2019/881 2019
voluntary framework for European Cybersecurity Schemes for products, processes and services

- “Common Criteria” – EUCC (publication by EC still awaited)
- “Cloud Services” – EUCS (draft publication from ENISA)
- “5G” – EU5G (drafting)

UL Lab source 2022

CYBER RESILIENCE ACT

In scope

It will apply to all **products with digital elements** whose intended, and reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network.

Not in scope

- Regulation (EU) 2017/745 [medical devices]
- Regulation (EU) 2017/746 [in vitro diagnostic medical devices]
- Regulation 2018/1139 [high uniform level of civil aviation safety]
- Regulation (EU) 2019/2144 applies [on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles]

a) Rules for the placing on the market of **products with digital elements** to ensure their cybersecurity

b) Essential requirements for the design, development and production of products with digital elements, and obligations for economic operators in relation to these products

c) Essential requirements for the **vulnerability handling processes** put in place by manufacturers to ensure the cybersecurity of products with digital elements during the whole life cycle, and obligations for economic operators in relation to these processes. **Manufacturers will also have to report actively exploited vulnerabilities and incidents**

d) Rules on market surveillance and enforcement

UL Lab source 2022

HOW CRA WORKS ?

- La conformité est documentée et “démontrée” par un examen de conformité qui se fait:

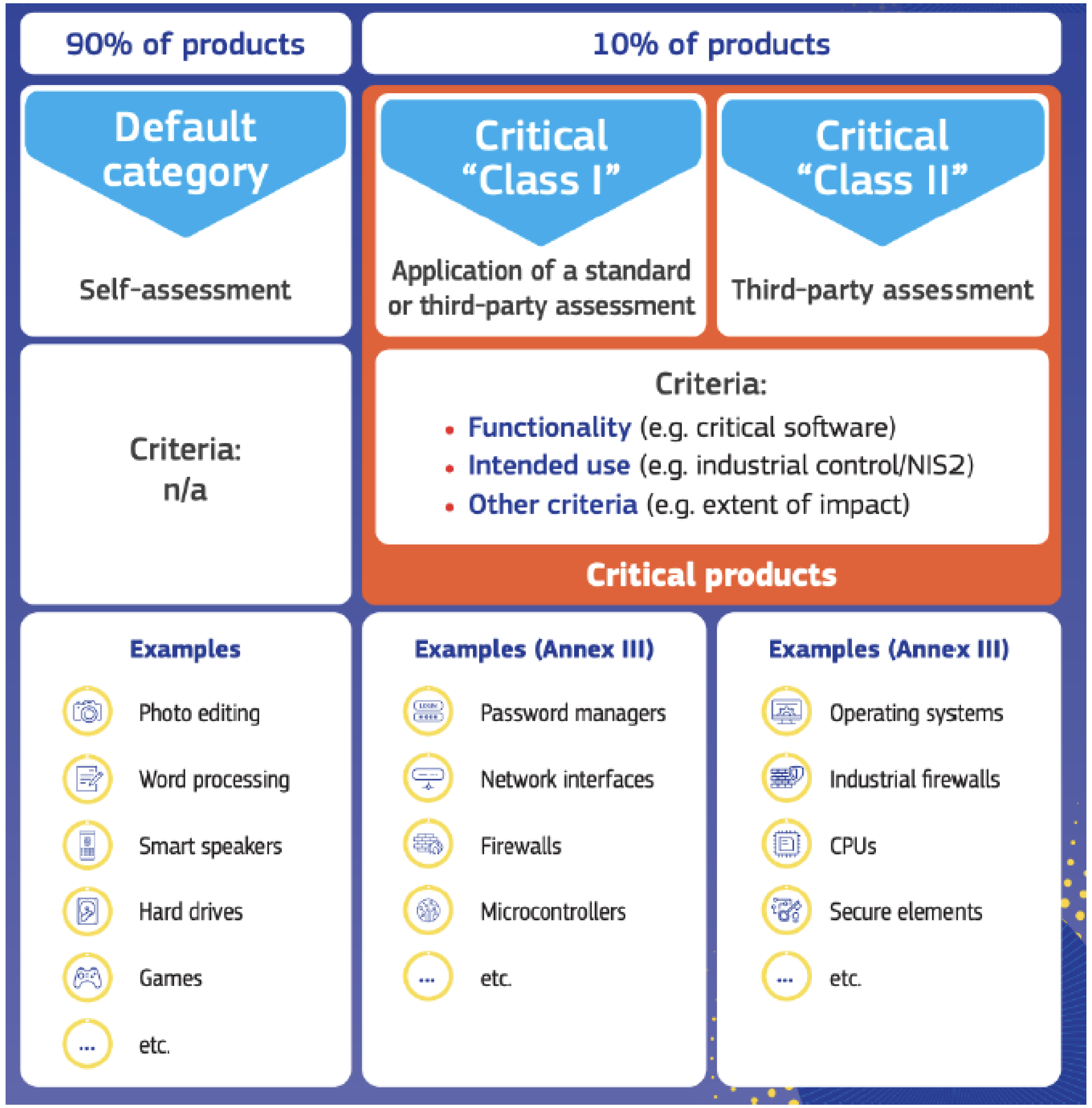
  - Soit par le contrôle interne du fabricant

  - Soit par une déclaration “sous sa seule responsabilité” que le fabricant a validée

  - Soit par un organe de contrôle européen
- Comme désormais de nombreuses réglementations

  - Obligations by design

  - Transposition obligatoire dans les contrats fournisseurs
- Importance des normes techniques : CRA n’impose aucune norme
- Sanctions : 15M$ / 2.5% du CA mondial



90% of products	10% of products	
Default category Self-assessment	Critical “Class I” Application of a standard or third-party assessment	Critical “Class II” Third-party assessment
Criteria: n/a	Criteria: • Functionality (e.g. critical software) • Intended use (e.g. industrial control/NIS2) • Other criteria (e.g. extent of impact) Critical products	
Examples Photo editing Word processing Smart speakers Hard drives Games etc.	Examples (Annex III) Password managers Network interfaces Firewalls Microcontrollers etc.	Examples (Annex III) Operating systems Industrial firewalls CPUs Secure elements etc.

MATTER

Emerging IoT Adoption of Certificate-Based Authentication

- **Matter** is actively using X509 certificates
- Zigbee Smart Energy requires certificates
- **Wi-SUN** requires certificates
- **Bluetooth Mesh** v1.1 supports certificates
- ioXt is defining security certificates
- **OPC** requires X509 certificates
- **BAC net** (Modbus) for Smart Building requires certificates

CSA (Connectivity Standards Alliance)

Now 584 Members!

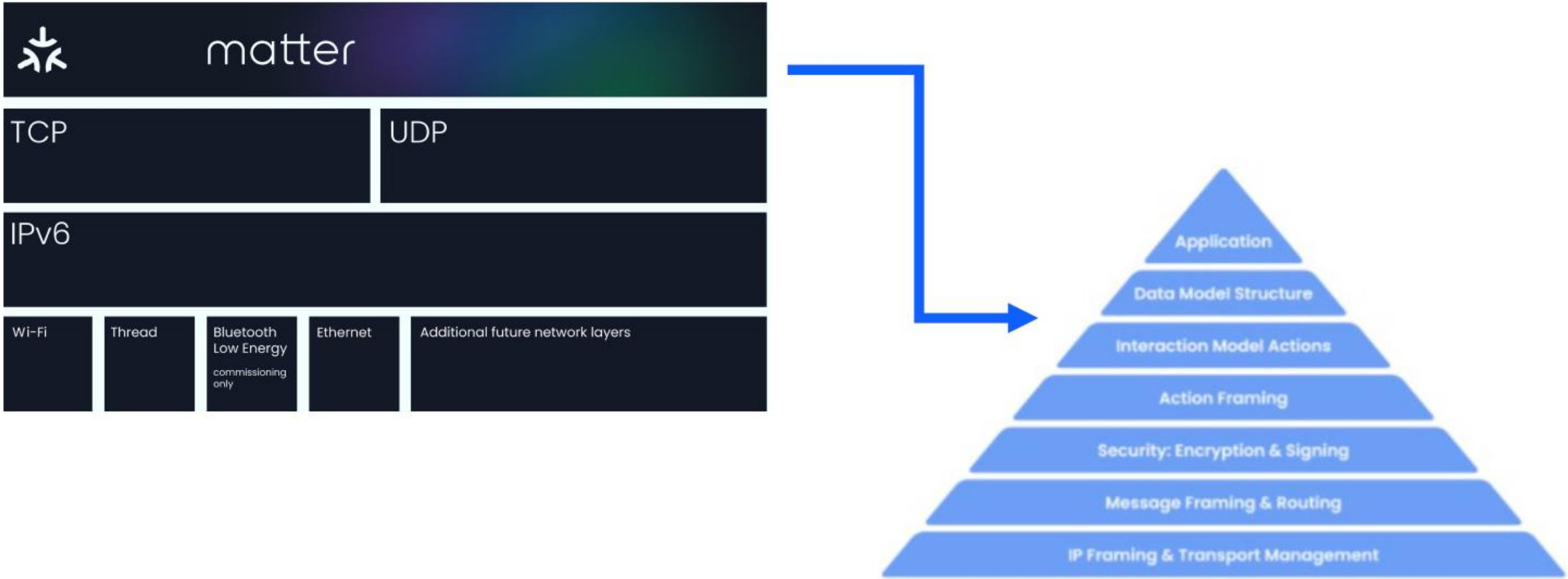
with over **6100** individuals participating in **45** countries

141 New Members in 2022

ABB
ACCEL LAB
adb
AIDOT
altice labs
ANCHOR by Panasonic
AMINA CHARGING
apynov
ARC
ARLEC
AT&T
BREL HOME
BURG WÄCHTER
COMMAX
Dusun
DISIGN Incorporated
DUCTECH
ECOFLOW
ECOVACS
ELEGRP
EUREVIA
FEIT Electric
Ford
Freedompro
Focus
GOLDTek
heatmiser
HEAVN
helbling
Hitachi Solutions
HKT
HOOBS
HT
Hidintech
ITIUS
KLiTE
KEYFACTOR
KOHLER
konnected
lierda
NELDTV
Nodle
NOKIA
NOVUS
novuslabs.com
OpenValley
PHATEN
QUECTEL
Rang Dong
RATOC
RAZER
SECU YOU
SENSIRION
sense
SinuxSoft
SRTC
StreamUnlimited
BOIT
SwitchBot
THIRDREALITY
tietoevry
TRUSTAsia
Wirepas
wiDom
WISeKey
woven planet
Y
YUKAI ENGINEERING
ZEMISMART
zomai
1HOME

MATTER Protocol

What is MATTER ?



matter

TCP

UDP

IPv6

Wi-Fi

Thread

Bluetooth Low Energy
commissioning only

Ethernet

Additional future network layers

Application

Data Model Structure

Interaction Model Actions

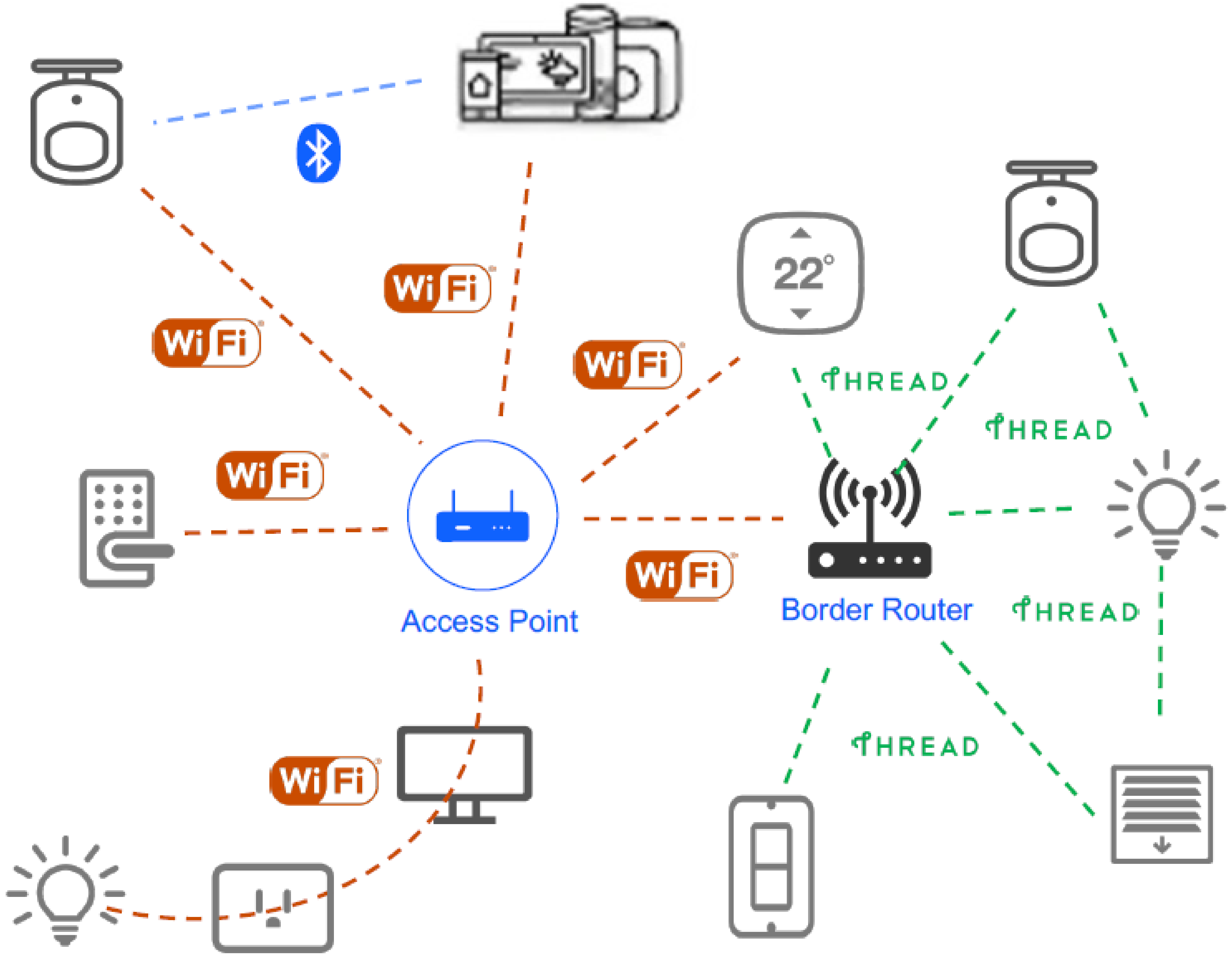
Action Framing

Security: Encryption & Signing

Message Framing & Routing

IP Framing & Transport Management

MATTER network



- Focus on Ethernet / WiFi / Thread
- BLE is used as the commissioning channel
- Thread devices connect to other IP networks through border routers
- Bridges can link to other protocols like Zigbee and Z-Wave

MATTER structure

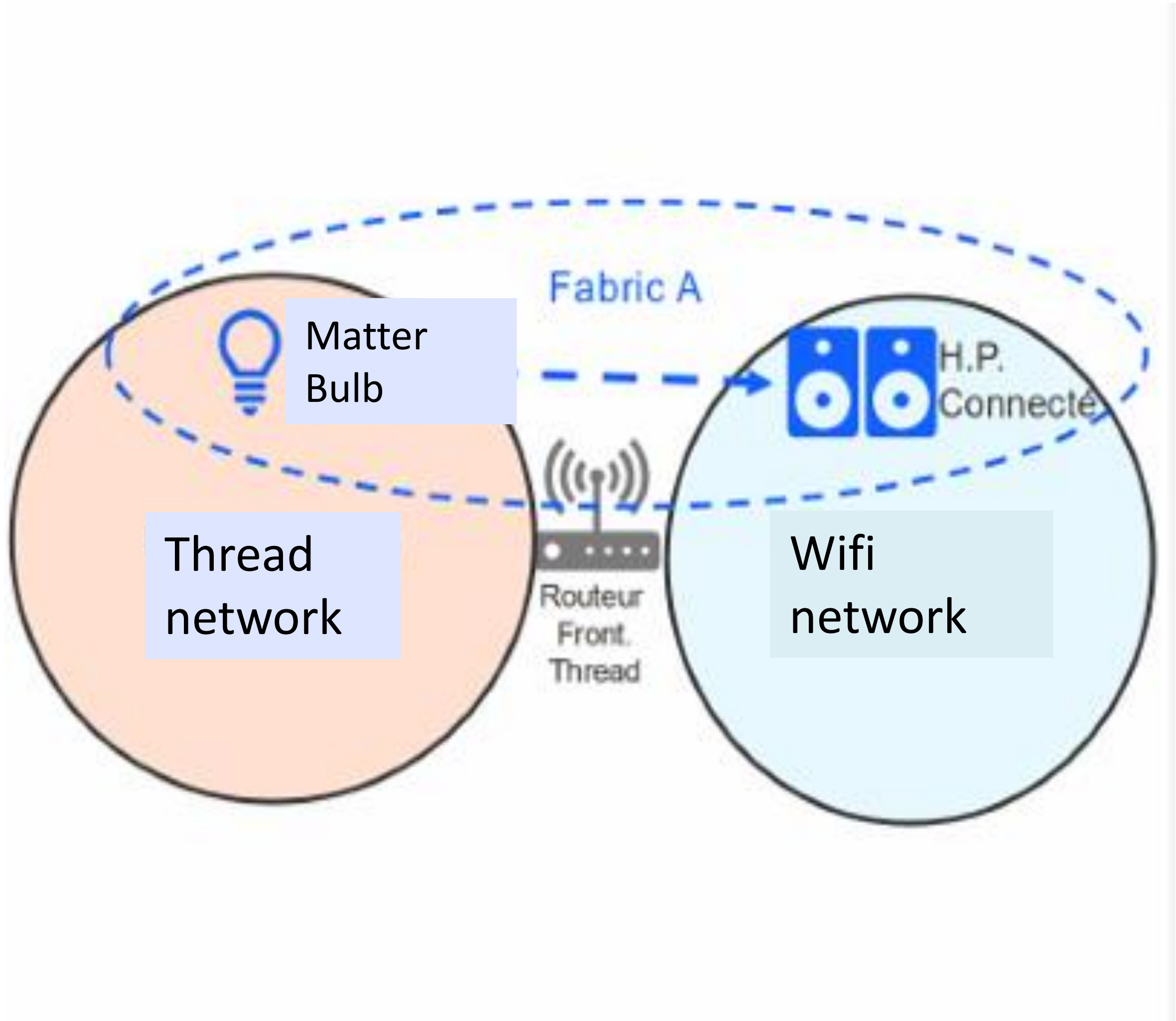
Node: An addressable entity which supports the Matter protocol stack and (once Commissioned) has its own Operational Node ID and Node Operational Credentials (NOC). A device may host multiple Nodes.

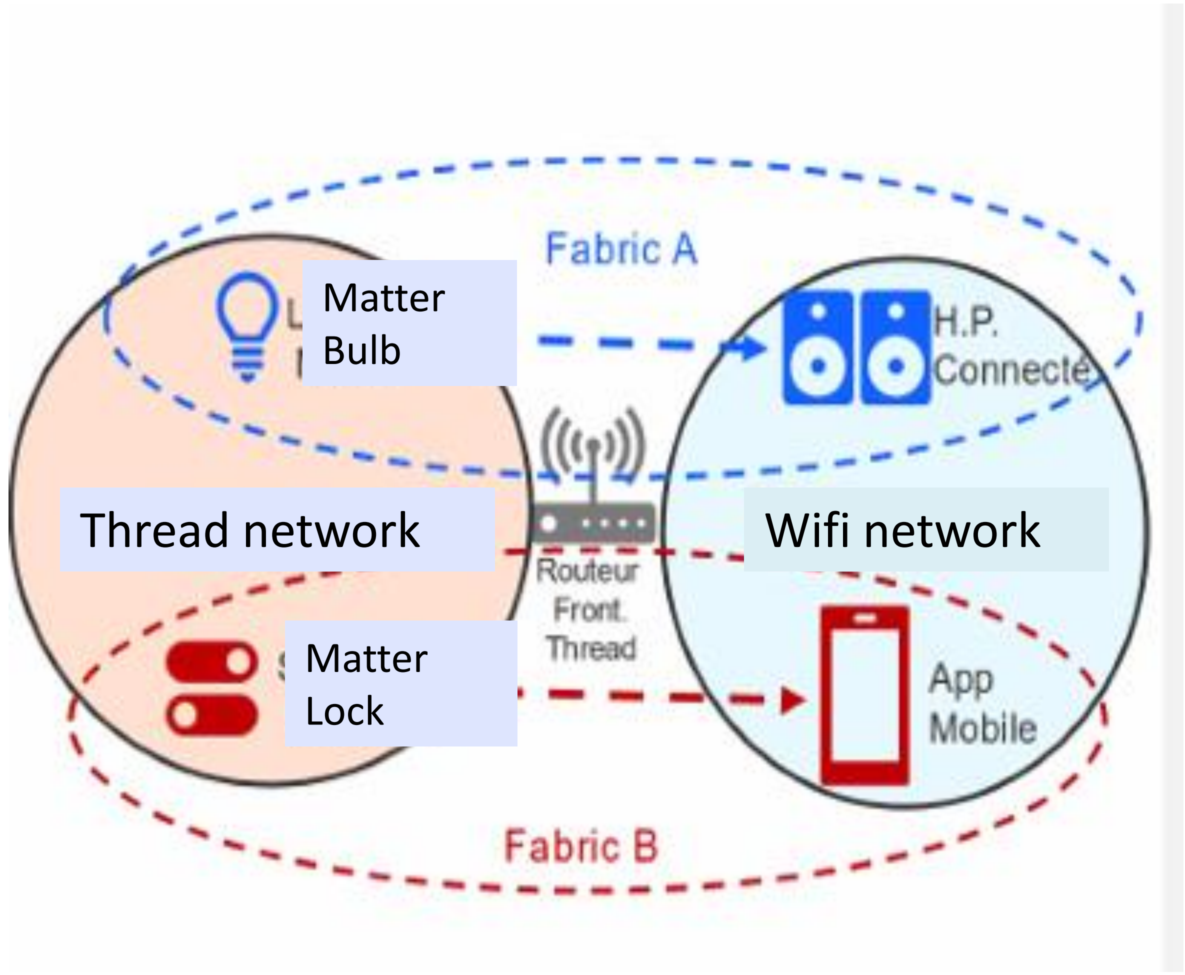
Fabric: A logical collection of communicating Nodes, sharing a common root of trust, and a common distributed configuration state.

Commissionee: A new device that will be added/comissioned to a Fabric, to become a Node.

Commissioner: The role that adds new devices to the Fabric. The commissioning will be done by a Smartphone or a Smart Speaker, which are in themselves Nodes of the Fabric.

Administrator: A Node having Administer privilege over another Node.





MATTER definitions

Vendor Identifier (VID) (OEM/Device maker) is a 16-bit number that uniquely identifies a particular product manufacturer or a vendor. It is allocated by the Connectivity Standards Alliance (CSA).

Product Identifier (PID) is a 16-bit number that uniquely identifies a product of a vendor. It is assigned by the vendor

VID-PID combination uniquely identifies a Matter product.

Device Attestation Certificate (DAC) is a X509 digital Certificate proves the authenticity of the device manufacturer. Every Matter device must have a DAC and corresponding private key, unique to it.

The device should also have a Product Attestation Intermediate (**PAI**) certificate that was used to sign and attest the DAC. The PAI certificate in turn is signed and attested by **Product Attestation Authority (PAA).**

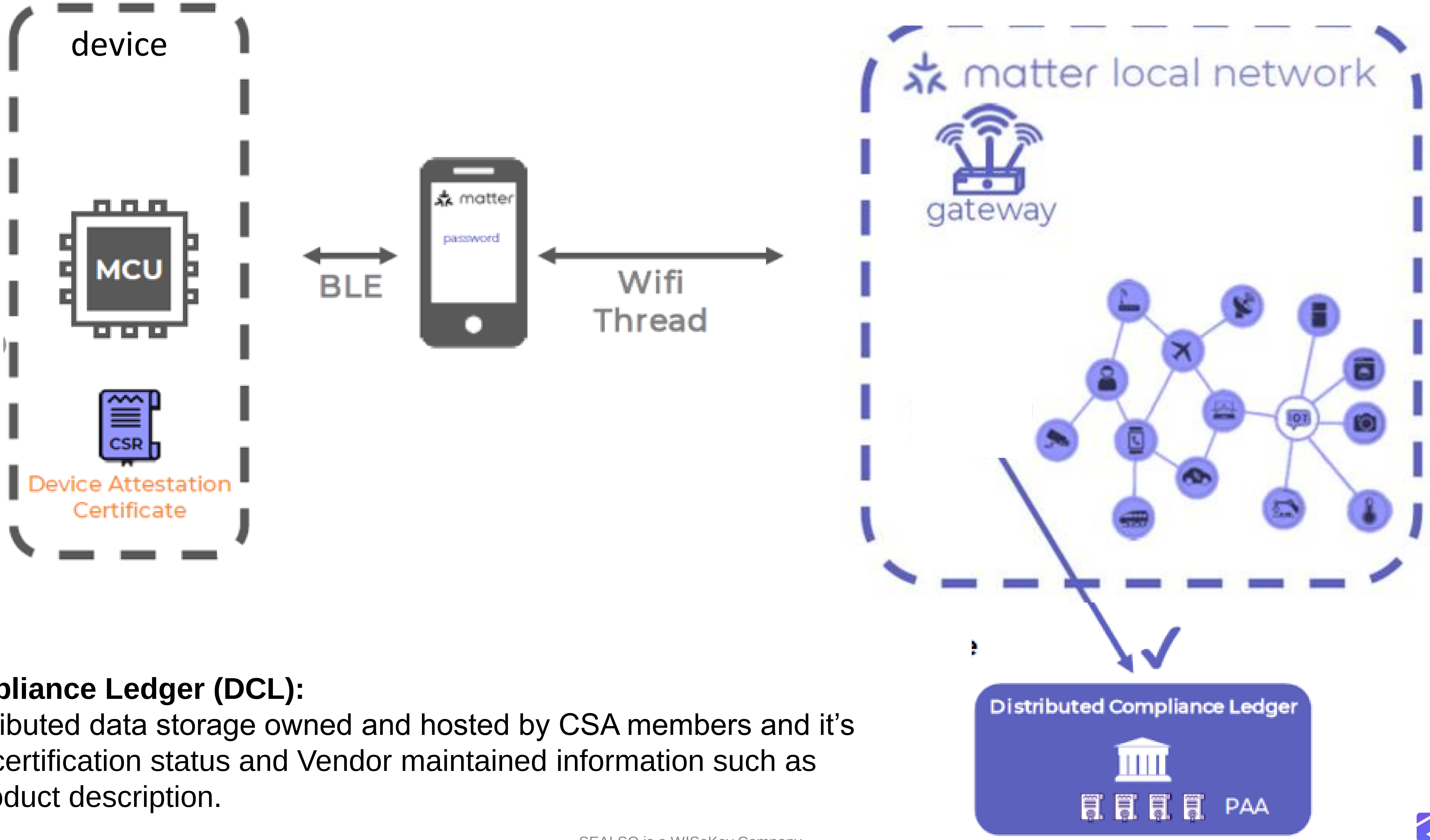
The PAA certificate is an implicitly trusted **self-signed root certificate**.

WISEKEY is one of few PAA (Root CA for Matter)

Matter’s Security Principles

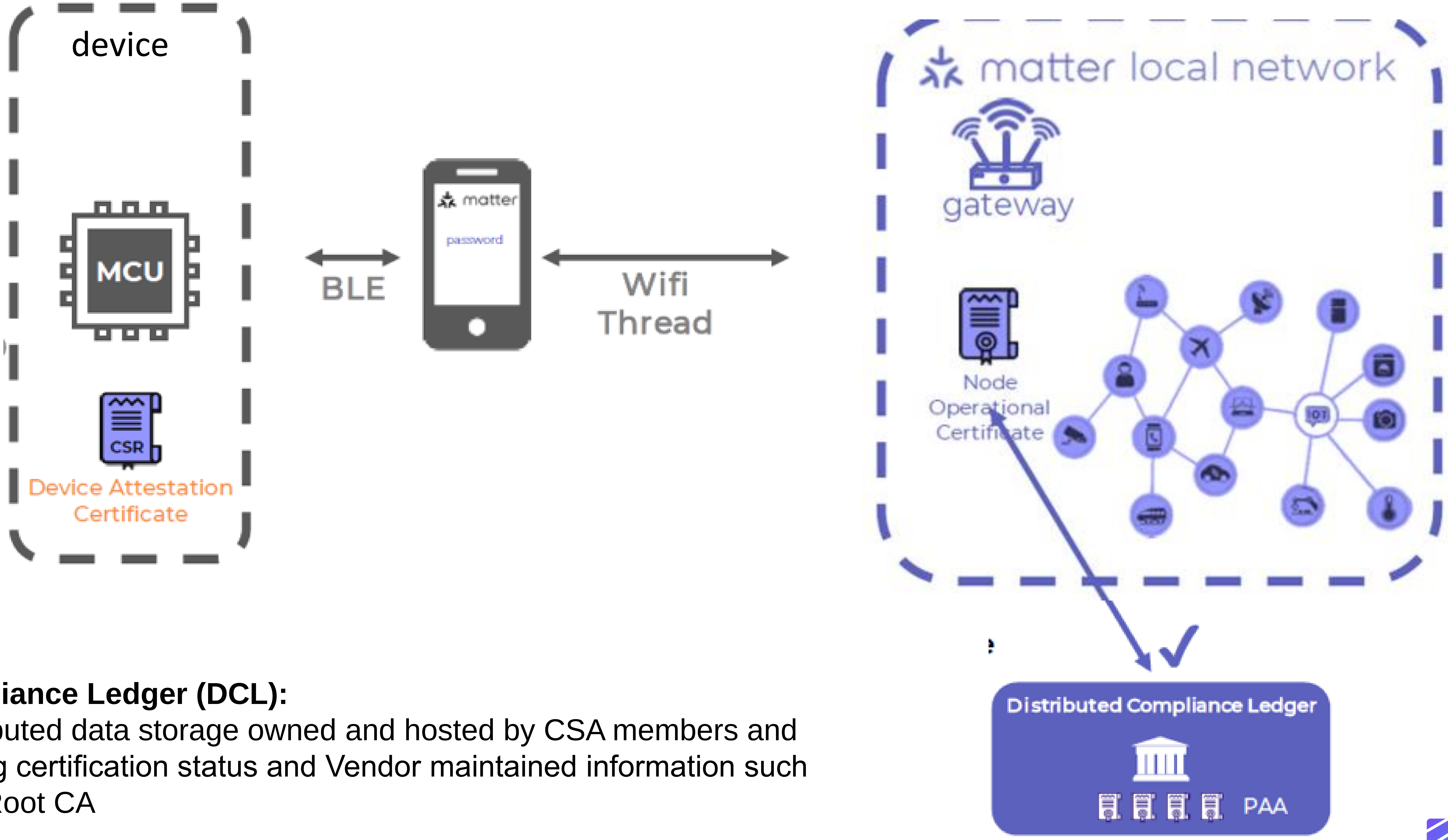
- No anonymous joining
- Device identity and authentication is verified though Device Attestation (DAC)
- Unique operational credentials are generated for each Matter device on each Fabric
- Network credentials are given only *after* device authentication

Device Commissioning in summary



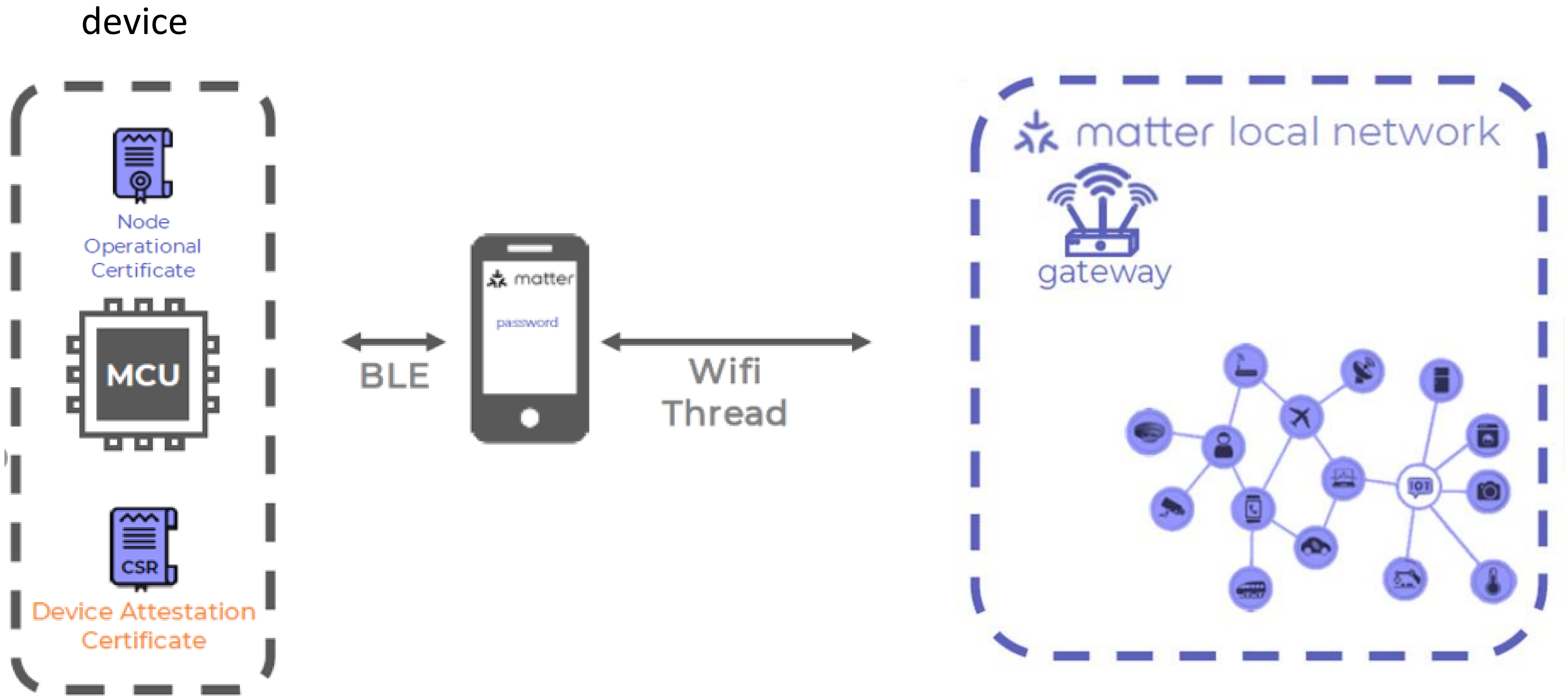
Distributed Compliance Ledger (DCL):
The DCL is a distributed data storage owned and hosted by CSA members and it’s used for tracking certification status and Vendor maintained information such as product name, product description.

Device Commissioning in summary


device
MCU
CSR
Device Attestation Certificate
BLE
matter
password
Wifi
Thread
matter local network
gateway
Node Operational Certificate
Distributed Compliance Ledger
PAA

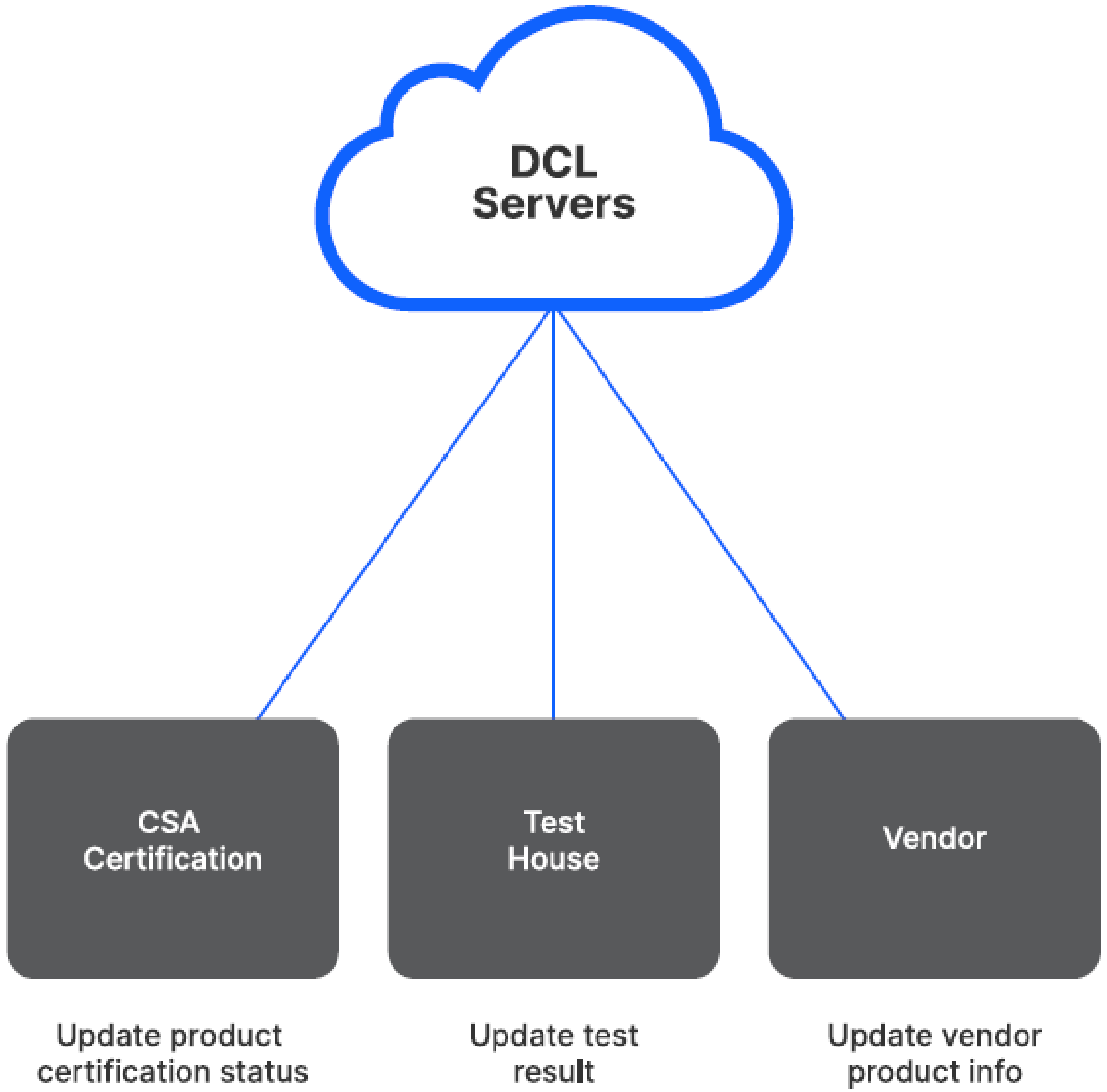
Distributed Compliance Ledger (DCL):
The DCL is a distributed data storage owned and hosted by CSA members and it’s used for tracking certification status and Vendor maintained information such as product name, Root CA

Device Commissioning in summary



What is DCL (Distributed Compliance Ledger)

- **What is it?**
  - Distributed database of all certified products
    - Certification status
    - Product name / description
    - Firmware Upgrade URI
- **What is the benefit?**
  - Commissioners can restrict access to only certified devices
  - Users can verify that a device is authentic
- **How is it managed?**
  - All Matter certified products are publicly available
    - https://webui.dcl.csa-iot.org
  - Write to the DCL is restricted to the following roles
    - CSA Certification role
    - Test House role
    - Vendor role
  - A certified product record is entered by the CSA Certification



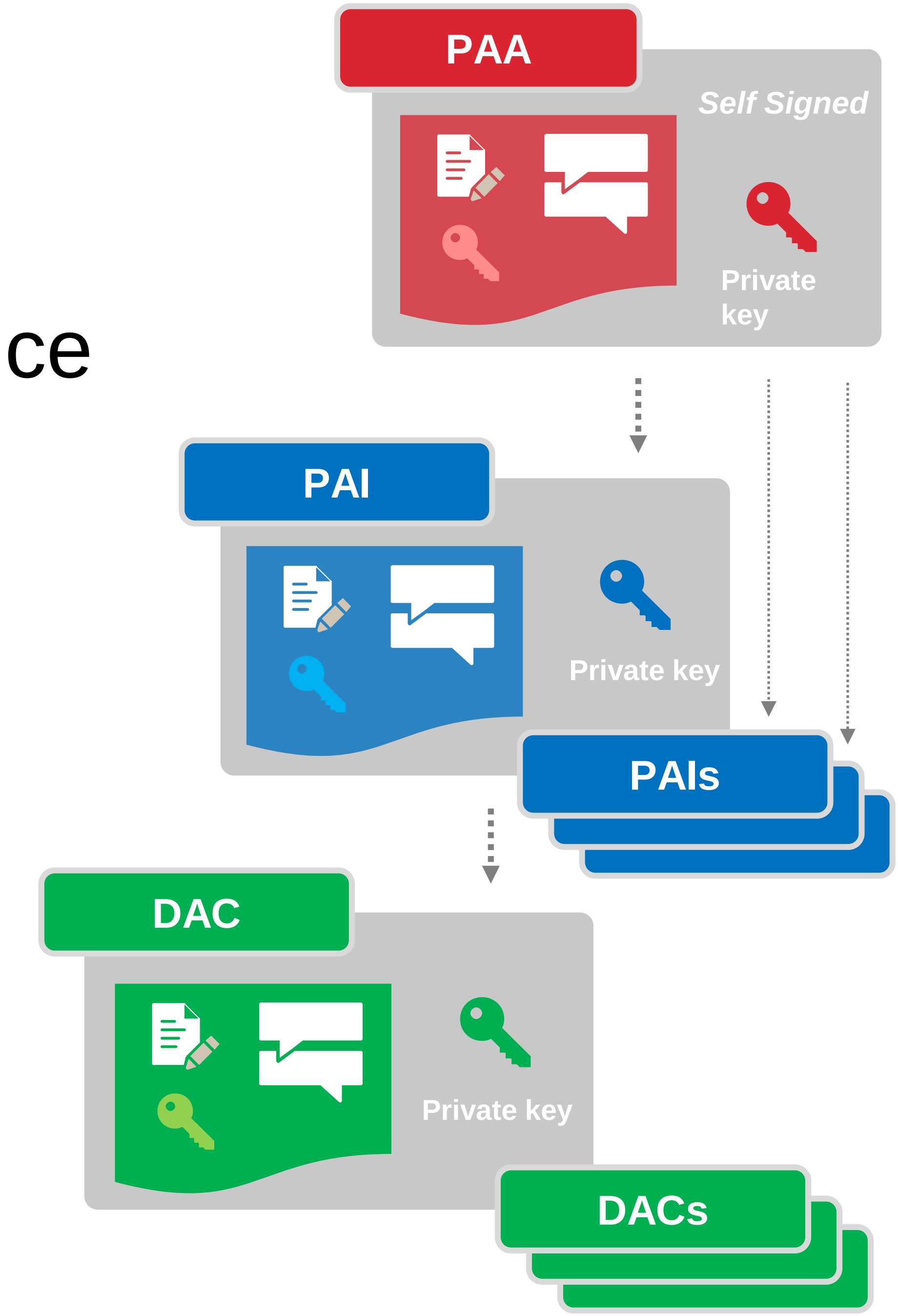
MATTER DEVICE CERTIFICATE SPECIFICATIONS

◇ New spec v1.0 released in September 2022; v1.1 in May 2023

◇ Matter assumes that each certified Device includes the following values:

- Device Attestation Certificate (DAC)
- Private key that matches the DAC
- Product Attestation Intermediate (PAI) certificate
- Verifier
- Certification Declaration (CD)

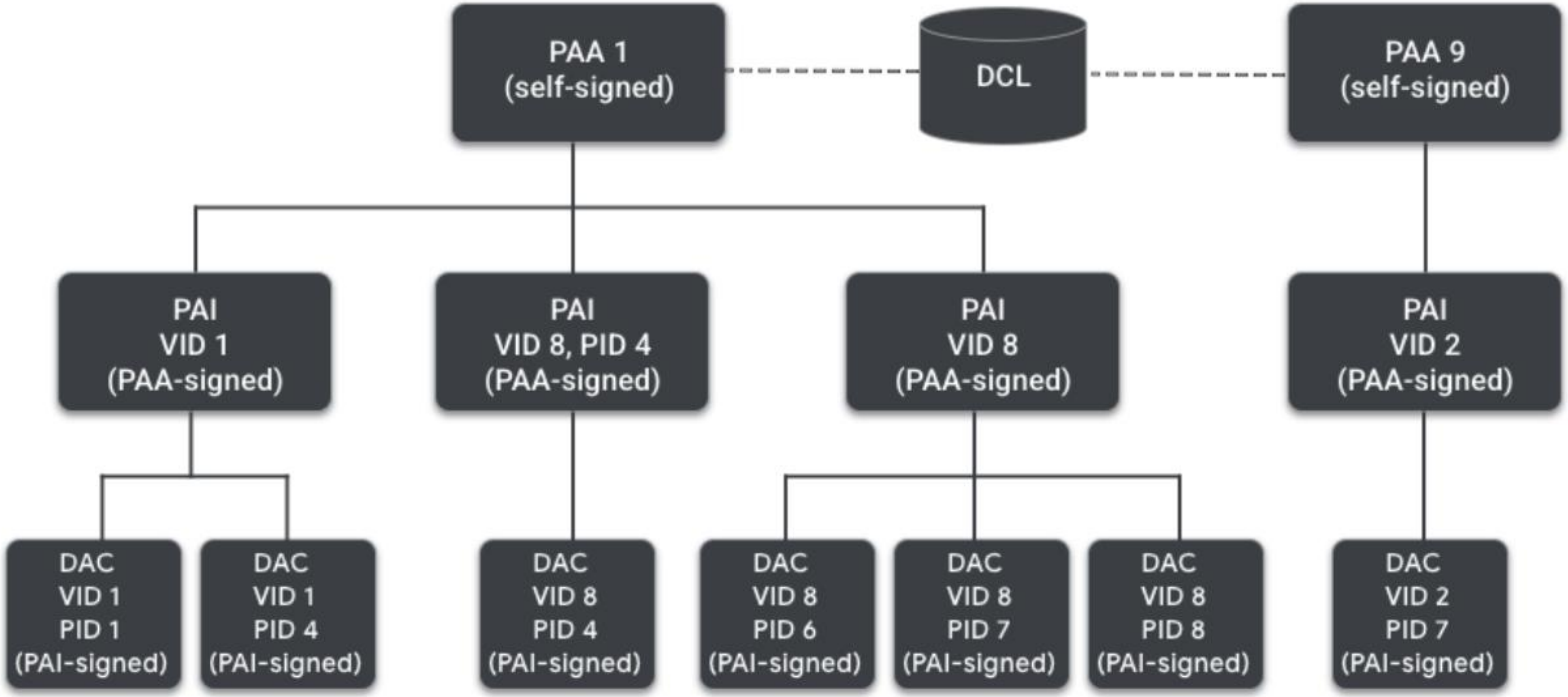
All of these files are used during commissioning.



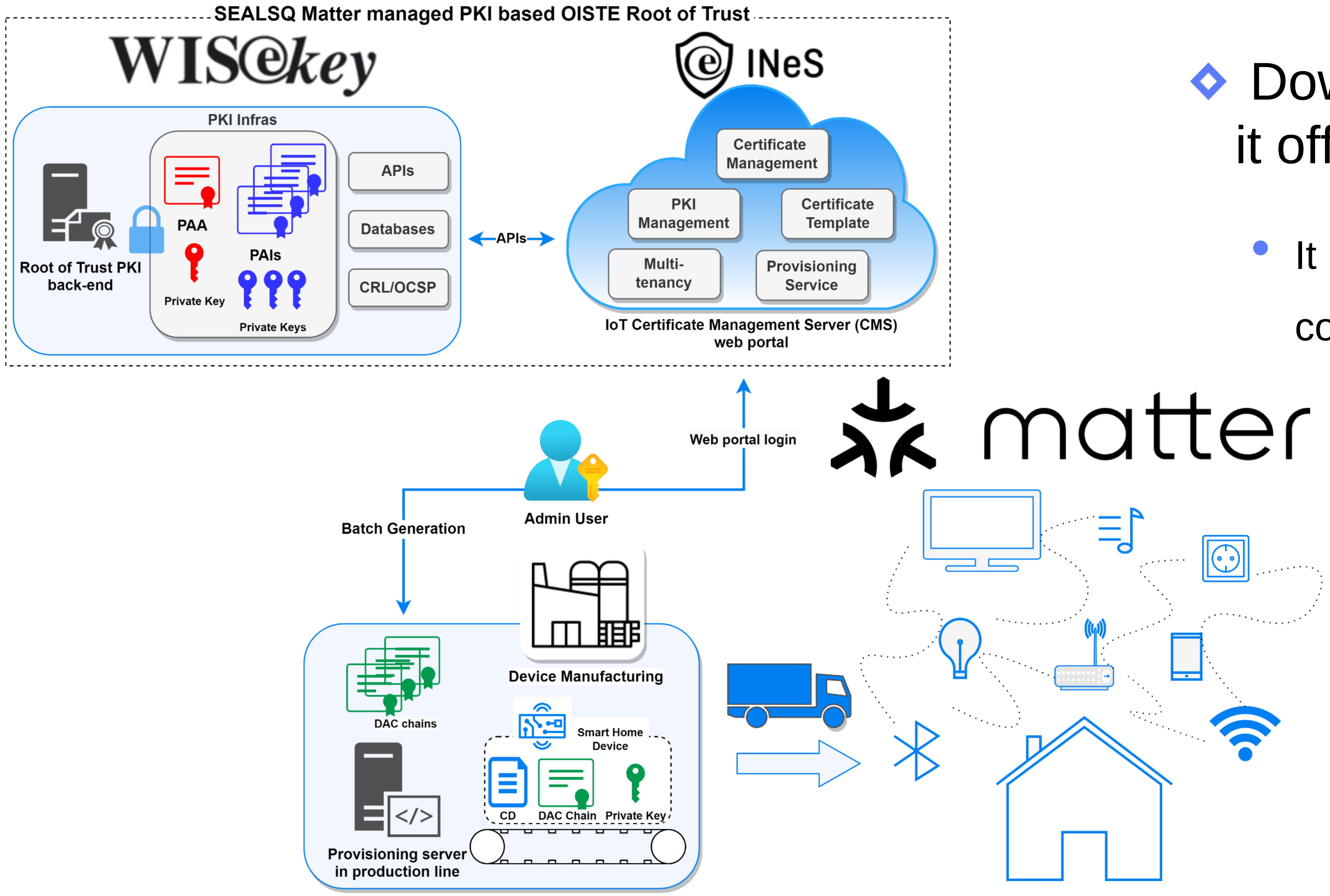
matter

SEAL SQ semiconductors + quantum

PKI HIERARCHY OPTIONS



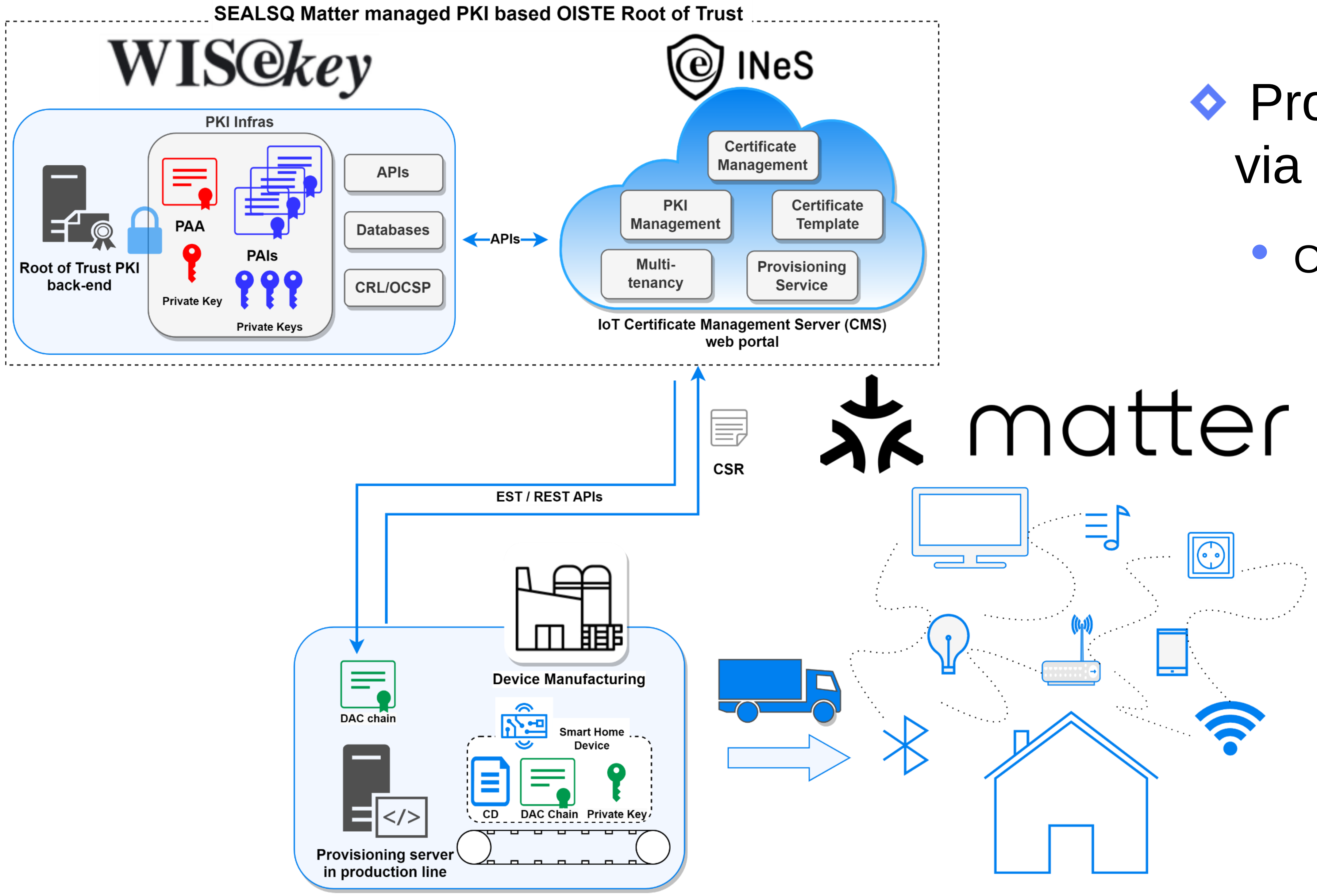
DAC provisioning – DAC generation in a batch



- Download the certificates in a batch and provision it offline in the production line
  - It can be applied to the production line where the Internet connectivity is challenging

*Device Attestation Certificate (DAC)

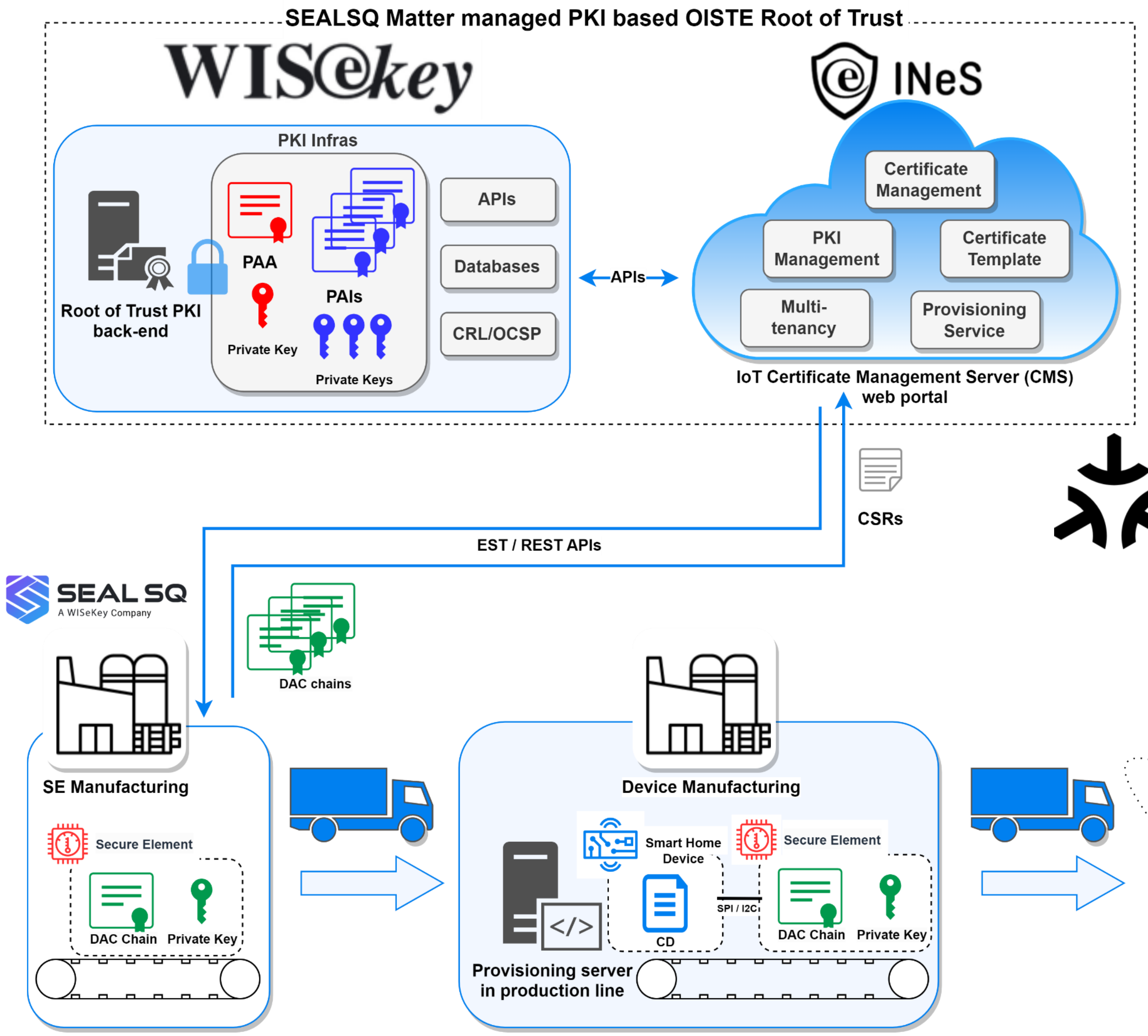
DAC provisioning – DAC generation through APIs



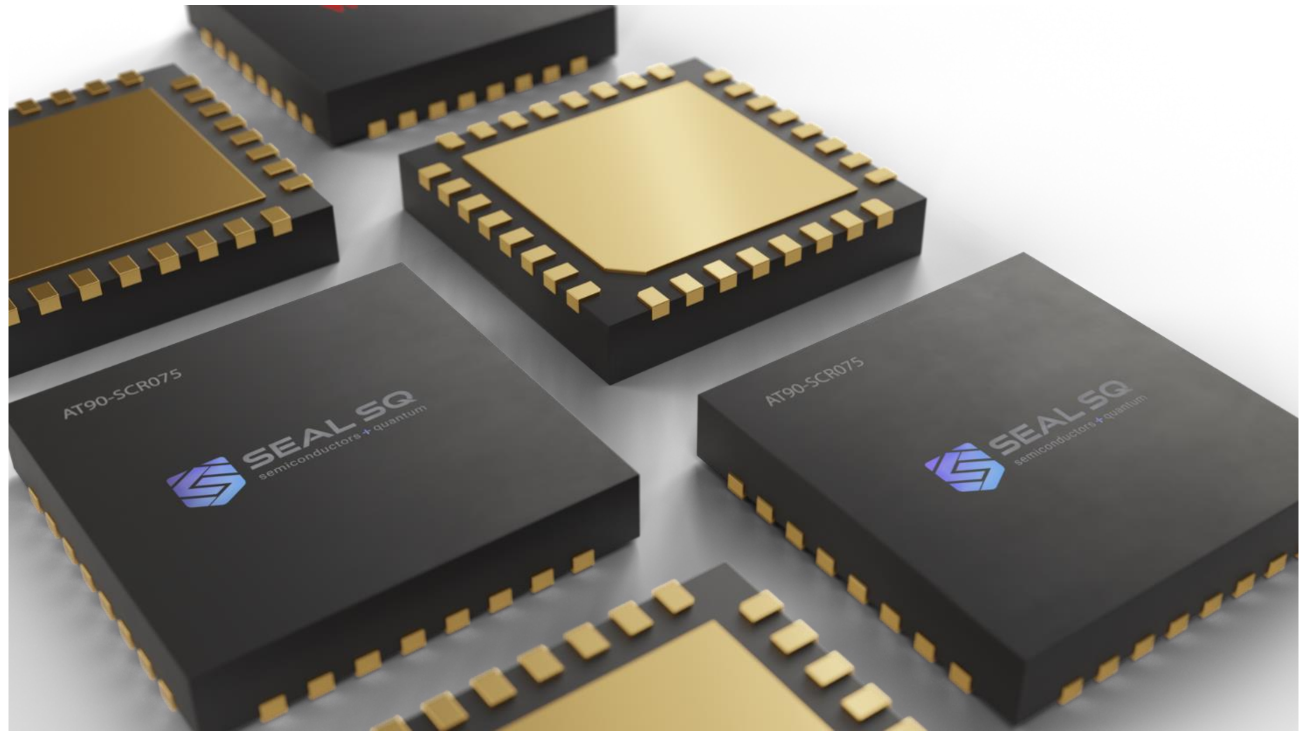
- Provisioning on-the-fly by requesting the certificate via RESTful or EST APIs
  - Open interfaces for automating the certificate enrollment process

*Device Attestation Certificate (DAC)

DAC provisioning – Pre-provisioned Secure Element



- ◇ Pre-provisioning DAC in the secure element and integrating the SE in the smart home devices
  - Securely protect the private keys
  - Less effort for provisioning DAC in the smart home device



*Device Attestation Certificate (DAC)

Q&A

SEALSQ semiconductors

www.sealsq.com