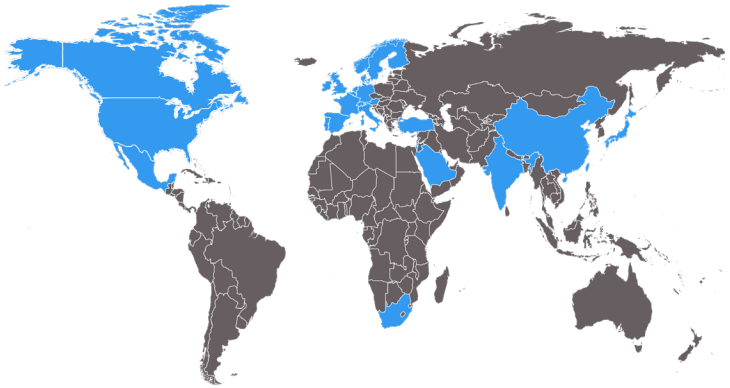
Corporate Overview

SEAL SQ
semiconductors + quantum

Johann Coudreuse

10/10/2024

History



- Spun-off from ATMEL 25 Years ago with Engineering Teams, Smart Card and Security products IPs
- Since then developing and selling secure hardware, firmware and trust services for a wide variety of customers across multiple industries and countries (Over 100 patents listed).
- Today a subsidiary of the WiseKey Group (WKEY) and a public listed **company** at the NASDAQ stock exchange (LAES).
- Presence in more than 30 countries

Value Proposition

Only player on the security market offering a truly integrated vertical suite of Microcontrollers and Trust Services to secure any kind of connected devices and systems.

- Full Range of FIPS & Common Criteria Certified Secure Microcontrollers
- Cutting edge certified chips running Post-Quantum algorithms and a Post Quantum RoT.
- A managed PKI-aaS platform combined with trusted hardware Provisioning Services
- European independent Root-of-Trust (RoT) featuring a MATTER, GSMA and WISUN accredited RoT

SEAL SQ
semiconductors + quantum

Just focus on your application, we take care of Security !

Use Cases

Smart Home

Secure Elements pre-provisioned with Matter Device Attestation Certificates: Faster compliance, easier scale-up, and highest security for lower costs

D-Link / Hager

Smart Grid

Full Root to Chip security solution FIPS 140-3 certified for leading smart meter manufacturers

Landis+Gyr

EV Charging

Managed PKI solution & ready-to-use FIPS certified secure elements for Charging Stations and Vehicles

VESTEL

Military & Government

Specific integrated solutions for secure communications and vehicles: P25 radios, Secure UAVs

Parrot

IP Protection

Personalized secure elements embedded in electronic boards to protect design Intellectual Property and avoid grey market and counterfeting.

cisco

Anti-Counterfeiting

Secure elements & PKI to prevent use of counterfeit parts, accessories or consumables

KÄRCHER

Healthcare

Solutions to protect patient data confidentiality, track and trace bio-sensitive materials, and avoid counterfeit medical devices or products

Medtronic

Secure Access:

Open hardware platform to run sensitive applications that control access to data (Crypto Wallets, Secure USB storage) or facilities (Smart cards, SIP designs)

LEGIC

SEAL SQ
semiconductors + quantum

Our Technology

SEALSQ Certificate Authority

20 years Issuing Digital Identities
Served over 3,000 corporate or gov. clients
Ubiquitous trust in browsers & operating systems

Versatile PKI as-a-Service &
SSL Certificate Platforms
Easy to Deploy & Scalable

Experienced

Accredited

Flexible

Compliant with major standards & Alliances

Certification Authorities WebTrust

Wi SUN Alliance

matter

GSMA

SEAL SQ
semiconductors + quantum

SEALSQ PKI Services for IoT

Managed PKI and Certificate lifecycle management

Hardware Root of Trust

- ✓ OISTE CA - Publicly trusted CA Recognized by Browsers (Webtrust)
- ✓ Matter PAA for customer DAC
- ✓ Private CA(s) for Corporate Root of Trust

INeS PKI-aaS

- ✓ Managed PKI platform for IoT
- ✓ Node Certificates (X509)
- ✓ Full Lifecycle management SaaS portal
- ✓ API with AWS and Azure

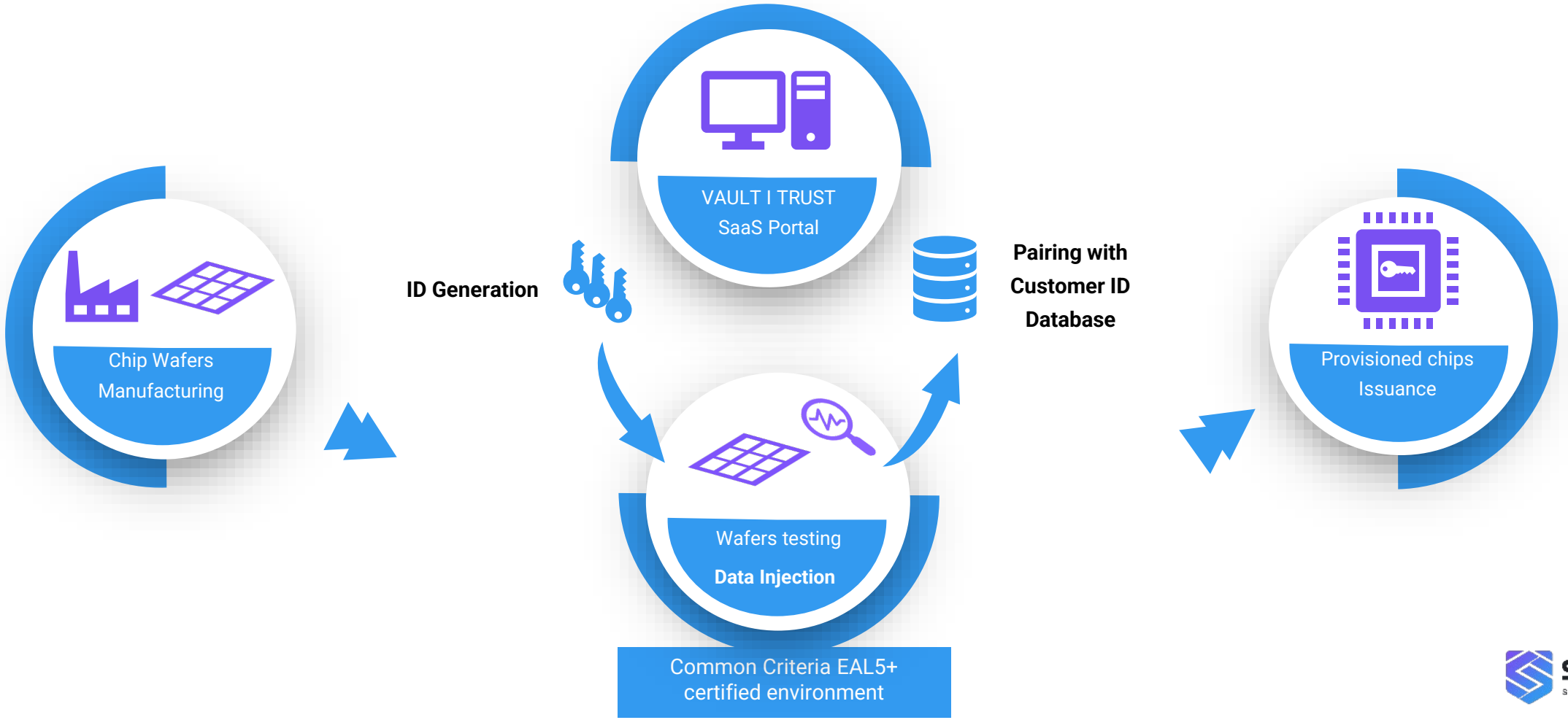
Key Applications

- ✓ Smart Home Matter compliant Ecosystems
- ✓ Smart City/Smart Grid (incl. WISUN Ecosystems)
- ✓ Any IoT Installed base/deployed device identity management

SEAL SQ
semiconductors + quantum

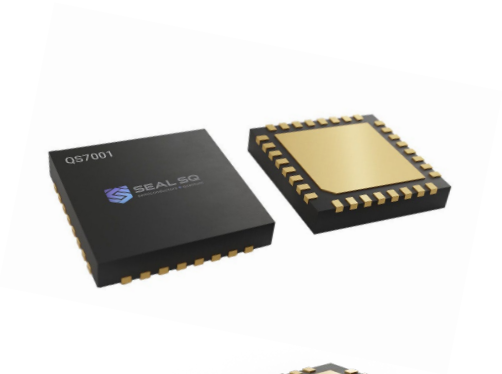
SEALSQ Semiconductor Personalization Services

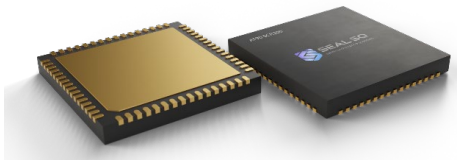
A unique SaaS Platform to inject identities into secure Hardware under a certified environment



SEAL SQ
semiconductors + quantum

SEALSQ Semiconductor & Embedded Software





APPLICATIONS

Post Quantum Chips

CCEAL 5+ RISC V Quantum Resistant Hardware platform with an **optional TPM Stack firmware**

- Secure Storage
- Access Control
- Custom Application
- Trusted Platform Modules

MS600X FAMILY

CC EAL 5+ Certified Secure Controller family delivered with SDK for OS development

- Secure Storage
- Access Control
- Custom Application

VaultIC FAMILY

CC EAL4+ & FIPS 140-3 Certified Secure Controller family with Embedded Firmware designed for IoT strong authentication & secure com' channel

- IoT Security
- Device to Device Auth.
- Device to Cloud Auth.

SCR FAMILY

Full range of chips to build Smartcard readers

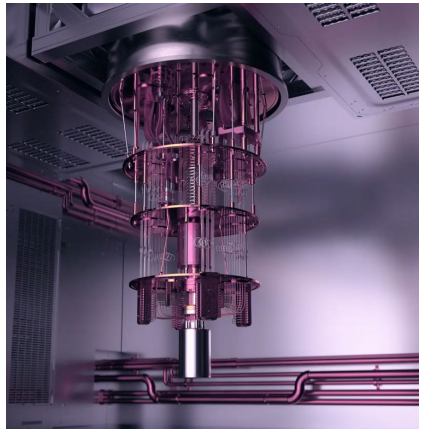
- POS terminals
- Portable readers
- NFC enabled devices

SEAL SQ
semiconductors + quantum

Strategic Roadmap

Post Quantum Chips

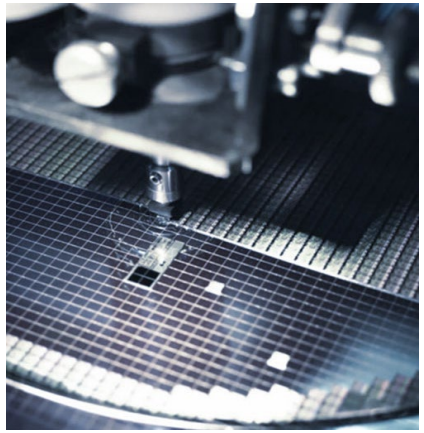
- QS7001 Platform samples availability in 2025
- QVault TPM availability in 2025
- Open to post quantum ASICs development



Post Quantum Root-of-Trust & PKI Available in November 24

Semiconductor Design & Personalization Center Project in Spain

- 60M€ project, Co-funded by Spanish Government
- Design activity to start in Q1 2025

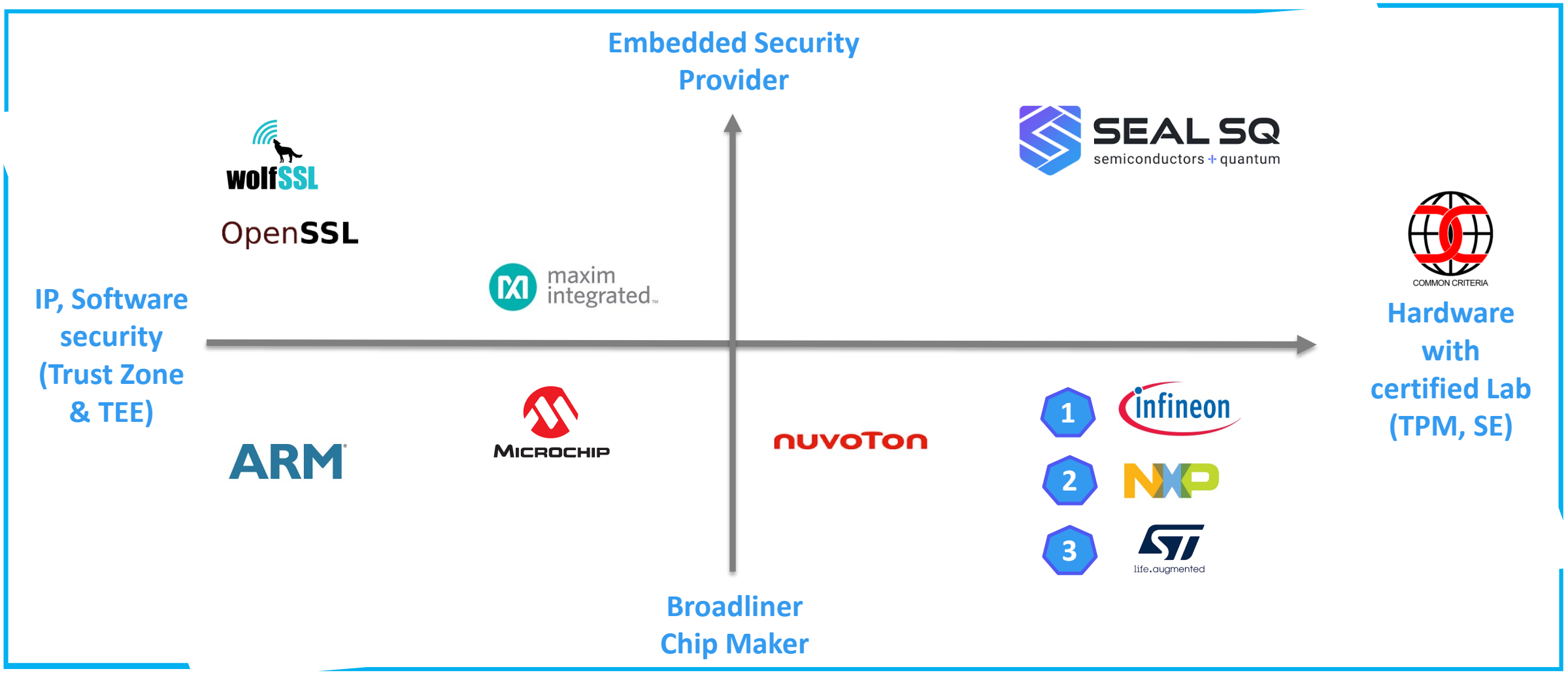


SEAL SQ
semiconductors + quantum

Competitive differentiation

Competition Mapping on Embedded Security

(Software & Hardware)



X **Ranking in Market Share**

SEAL SQ semiconductors + quantum

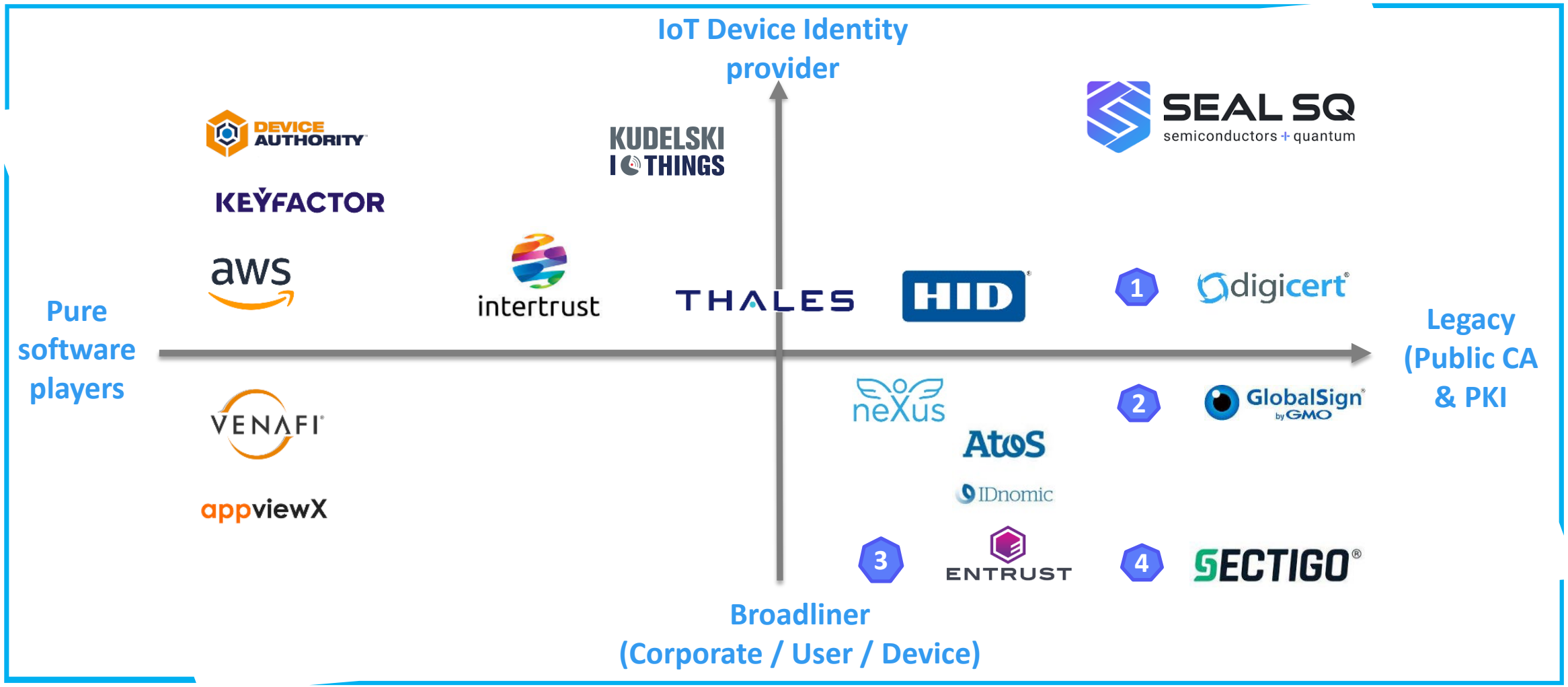
Main advantages vs Competition

On Security IC

Competitors	Type of Solution	SEALSQ competitive advantages
STMicro **Infineon** **NXP** **Microchip**	**AUTHENTICATION IC** **TPM**	«Pure» general purpose semiconductors players (design and manufacture chips). SEALSQ differentiates with: 1. Security IC specifically designed & “tuned” for the IoT and the anti-counterfeiting market 2. Larger set of crypto APIs, which can be customized on demand 3. Set of SaaS services for the provisioning and the life cycle management of the digital Identities which shall be injected into the Security IC, meaning better commercial terms with a real Secure End 2 End service
ARM	**Security Enclave** **Trust Zone Software**	Microprocessor core provider, ARM offers secure enclave/crypto cells IPs. Microcontrollers makers can now integrate security functions at SoC level, as an alternative to the Secure Element standalone chip. This solution has 3 drawbacks: 1. SEALSQ chips are offering a much higher security resistance 2. SEALSQ chips are much easier to integrate, and we are acting as a “one stop shop” 3. SEALSQ chips are resolving OEM’s brand protection/anticounterfeiting problem vis a vis their contract manufacturers, ARM is not.

13

Competition Mapping on Trust Services



X *Ranking in Market Share*

14

Main Advantages vs Competition

On Trust Services / IoT Identity & PKI

In IoT space, competitors are mainly Keyfactor Inc, Digicert, Device Authority, Kudelski IoT or home-made solutions

Criteria	SEALSQ Solutions	SEALSQ competitive advantages
Innovation	**INeS Zero Touch Provisioning**	• INeS Zero Touch Provisioning solves not only the Secure Identity Generation challenge but also brings easy to implement embedded software SDK to streamline customer development and Time-To-Market • INeS Trust Services platform is designed around micro-services architecture to envision new features promoted by Standards, Industry bodies and specific customer needs.
Flexibility for IoT Ecosystem	**Managed PKI – as – a - Service**	• INeS managed PKI service helps organizations to provision their devices to meet security requirements more securely, and at lower cost, than in house. • INeS managed PKI enables SEALSQ to deliver across the globe, digital identities without overhead.
Certification & Governance	**Public & Private CA**	• Based on WebTrust certification, Trust Services can be delivered according to strict CP compliance.

15

Barriers to Entry & Alliances: SEALSQ is ahead of the game

- **Standards / Consortiums:**

  GSMA selects only 2 Root CA / PKI, WISeKey accredited to start business in 2024. More on MATTER (https://csa-iot.org/certification/paa/)

- **Certifications mandated by cybersecurity regulation bodies**

  For SECURITY IC market, SEALSQ products have passed certifications like FIPS 140-3 or Common Criteria
  For PKI and Certificates, certification is WEBTRUST

Thank You

More about SEALSQ solutions on https://www.sealsq.com