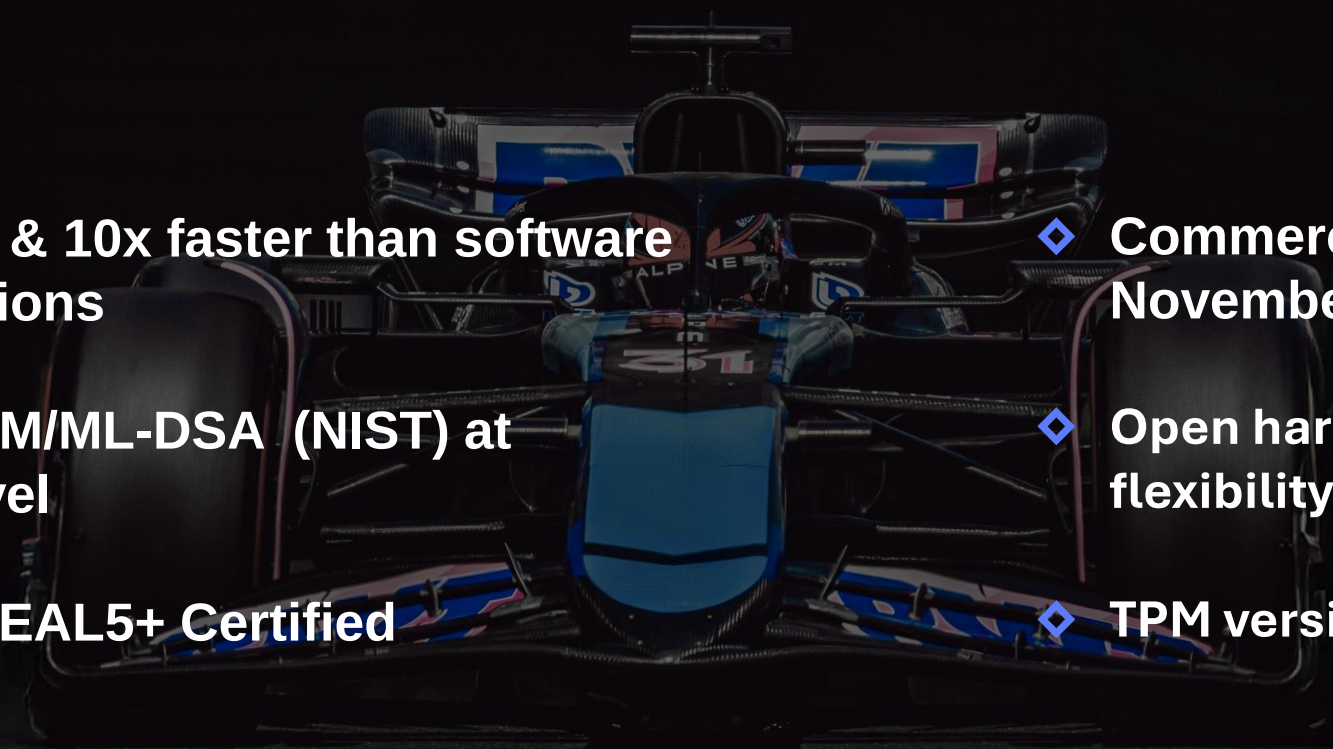


AI Meets Quantum, Building Unbreakable Post Quantum Security

By Carlos Moreira, SEALSQ CEO

Unveiling the Quantum Shield “QS7001”

- 
- ◆ More secure & 10x faster than software implementations
 - ◆ Runs ML-KEM/ML-DSA (NIST) at hardware level
 - ◆ RISC V - CC EAL5+ Certified
 - ◆ Commercial Launch November 20th 2025
 - ◆ Open hardware platform for flexibility
 - ◆ TPM version planned H1 2026

Welcomed by the industry



“Q-Day” is getting closer

- ◆ Reports of increasing Q-bit counts, error rate improvements
- ◆ Scaling of quantum hardware, investment, global R&D
- ◆ “Q-Day” (break classical public-key crypto) still challenging, though not far off for well-resourced actors

Global Regulation is catching up

EU roadmap: Member States start PQC transitions by end 2026; critical infrastructure by 2030

CNSA 2.0 in USA mandates PQC for NSS

Executive Order 14144 + amendments: timeline for product categories, PQC support

NIST PQC standards = FIPS 203, 204, 205 (Kyber / Dilithium / SPHINCS+)

Challenges

- ◆ Implementation & security: side-channels, tamper, firmware bugs
- ◆ Performance & power constraints, especially in constrained devices
- ◆ Interoperability across global regulations / standards / spectrum of devices
- ◆ Supply chain security, hardware provenance
- ◆ Getting visibility into “harvest now, decrypt later” risk in current data flows

How we can help: Four Pillars of Action



**Securing Devices at the
Edge with quantum
resistant chips**



**Root-of-Trust & PQ Root
Certificate Infrastructure
(PKI)**



**Secure communications
(IoT, satellites, etc.),
personalization & supply
chain integrity**



**Trusted identities &
secure transactions for AI
/ agents**

SEALSQ Post-Quantum Stack of Trust Services

Root of Trust

PKI

Device Provisioning

Field Deployment



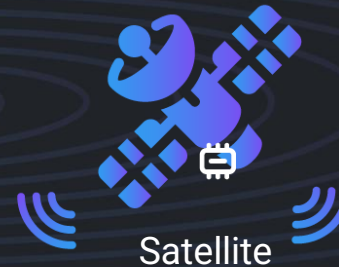
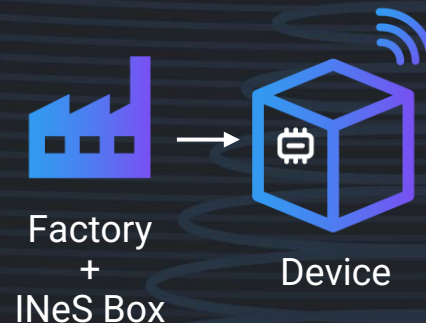
◆ WISeKey Quantum RoT

◆ INeS PKI

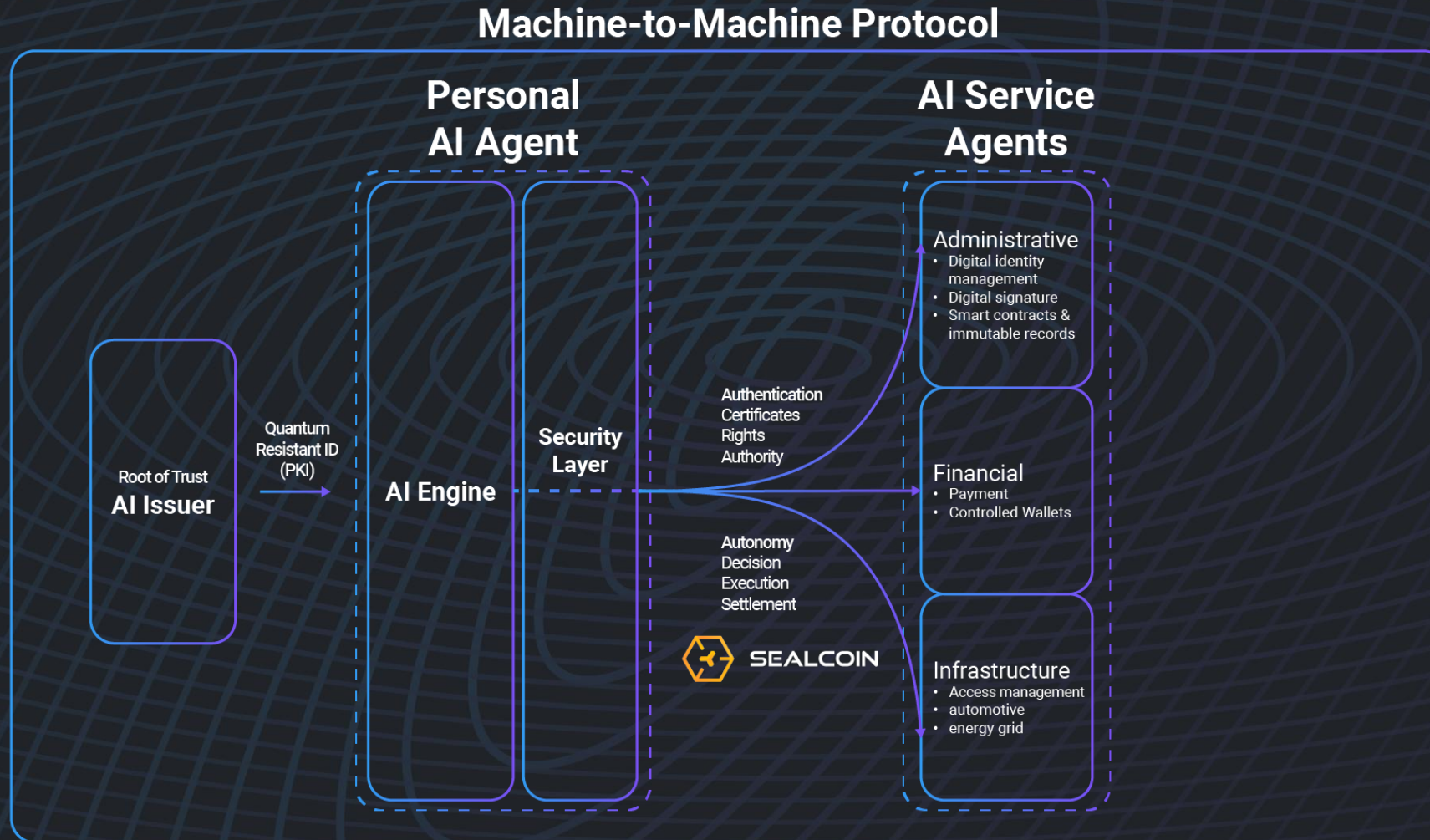
◆ OSPT Centers

Secure Communications & Infrastructure

- ◆ Encrypted data using PQC algorithms
- ◆ Secure edge devices & gateways:
Devices, Routers, Satellite connectivity
- ◆ •Secure supply chains (Over the Air or Secure Factory provisioning) to prevent backdoors / hardware tampering



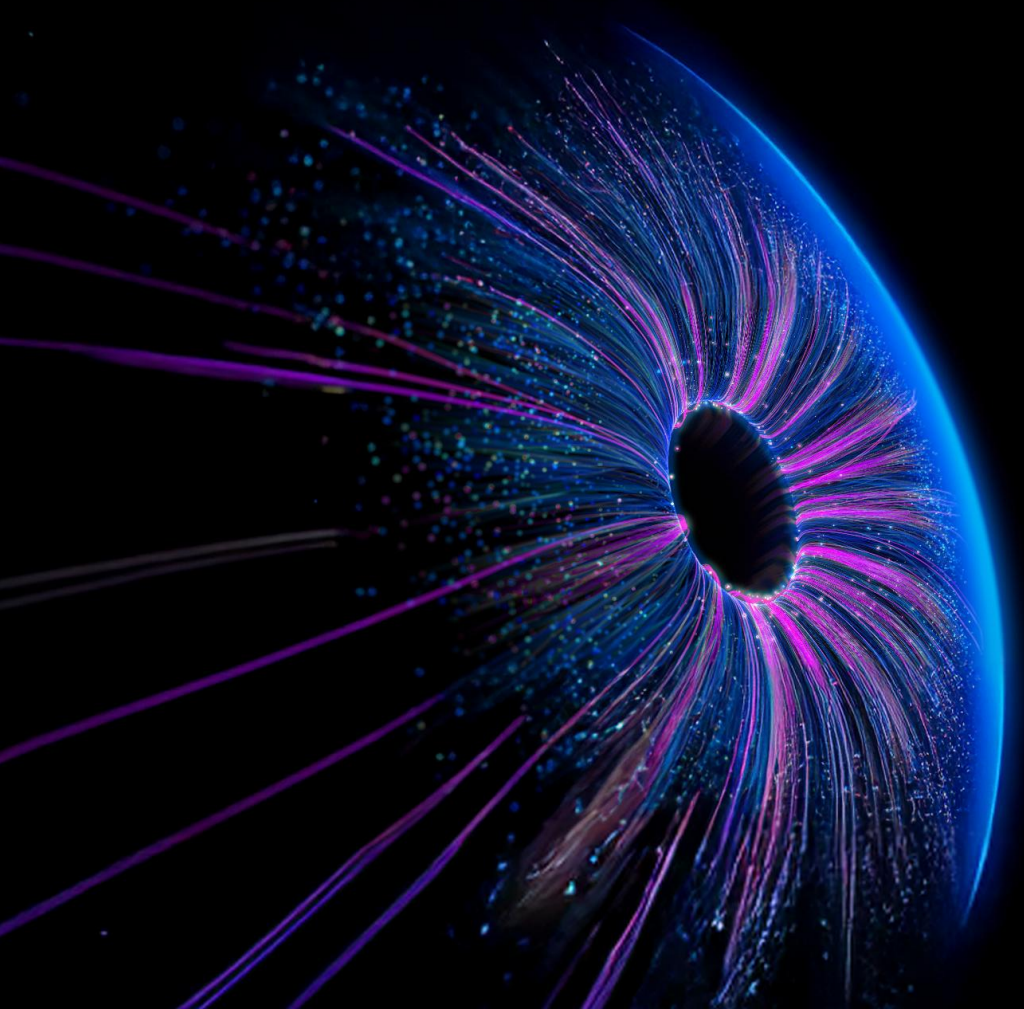
Autonomous & Accountable AI Agents



We Make it all real, and we make it now!

- ◆ Quantum Shield QS7001 dev. kits available November 2025
- ◆ Very large US semiconductor / electronics companies in discussions to achieve future compliance using PQC chips & trust services
- ◆ First Personalization center started in Spain
- ◆ SEALCOIN PoCs & Satellite Launches integrating PQC chips for secure space communications

And we will continue in 2026

- 
- ◆ QVault TPM version (Gateways, PC, Mobile, Tablets, IoT)
 - ◆ Quantum Resistant custom chips (ASICs): Automotive, Healthcare, Industry 4.0
 - ◆ Quantum Resistant Hardware design IPs: Semiconductor industry
 - ◆ Further Satellite Launches
 - ◆ Starting activity at OSPT centers

Our Vision: A Quantum+AI Future in 2030

- ◆ Infrastructure where all critical communications & identities are quantum-resistant
- ◆ AI agents, devices, satellites interacting over PQC-backed trust frameworks
- ◆ Cryptographic agility embedded in every layer so we can upgrade again if required
- ◆ Norms of transparency, secure supply chain, and regulatory compliance globalized



Let's build it together

- ◆ Semiconductors: FPGAs, Chiplet and Design partnerships
- ◆ Pilot programs, compliance roadmap partnerships welcome
- ◆ Research, academia, regulatory bodies, industry: we need all voices



SEAL SQ
semiconductors + quantum