CRYPTO4A

Free to Leave: Why Cryptographic Mobility Matters in the Quantum Era

October 14th, 2026

Prague

Entrust – nShield5

CRYPTO4A

Thales – LunaHSM (K7)

CRYPTO4A

Utimaco – u.Trust Anchor CSe

CRYPTO4A

Crypto4A – QASM/QxHSM

CRYPTO4A

The Foundational Era of Digital Trust. (Netscape circa 1995)

CRYPTO4A

Characteristics of the 90s

- Cryptography “politics” or “Crypto-Rigidity”
  - 40 bits for export (no stronger)
  - No cryptographic changes allowed in products
- PKI were still pretty small/simple systems
  - Verisgn and Entrust both adopted FIPS 140 Level 3 H/W HSM to store the Root Private Keys
  - PKCS#11 became the de facto API (worked on Linux, Microsoft, Unix, AIX, Mac and others)
- Designed before the advent of AES… (in other words DES & 3-DES)

LunaCA3™
CERTIFICATION
AUTHORITY
TOKEN
INSERT THIS SIDE UP
Chrysalis-ITS

LUNAPED
Awaiting command..
POWER
KEY IN
1 2 3 YES
4 5 6 NO
7 8 9 CLR
0 ENT
Chrysalis-ITS

CRYPTO4A

For the Quantum Era

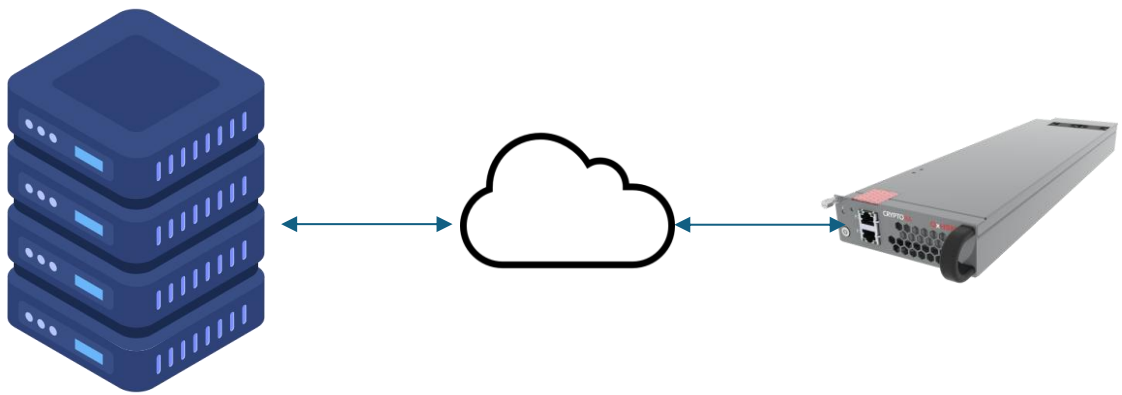
- Cloud native tools everywhere
- Highly scalable systems
- Critical dependencies on cryptographic processes
- Importance of “System design resilience”
  - Crypto-Agility is fundamental here
  - So is the need for cryptographic mobility

Cryptographic-Mobility

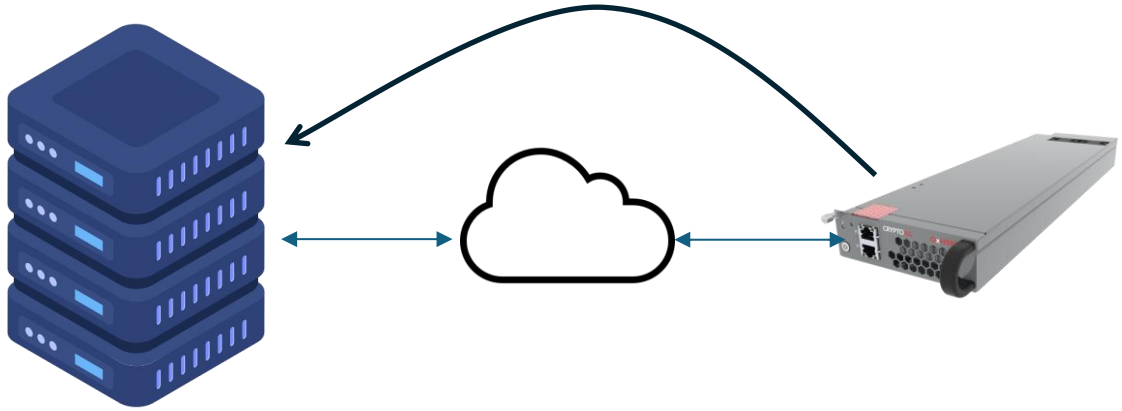
- Ability to securely transfer YOUR cryptographic keys from one vendor’s HSM to another.
  - Without extra costs
  - Without needing the vendor’s permission
  - From the moment you purchase a product
  - On your own schedule
  - Under your control

Nomenclature

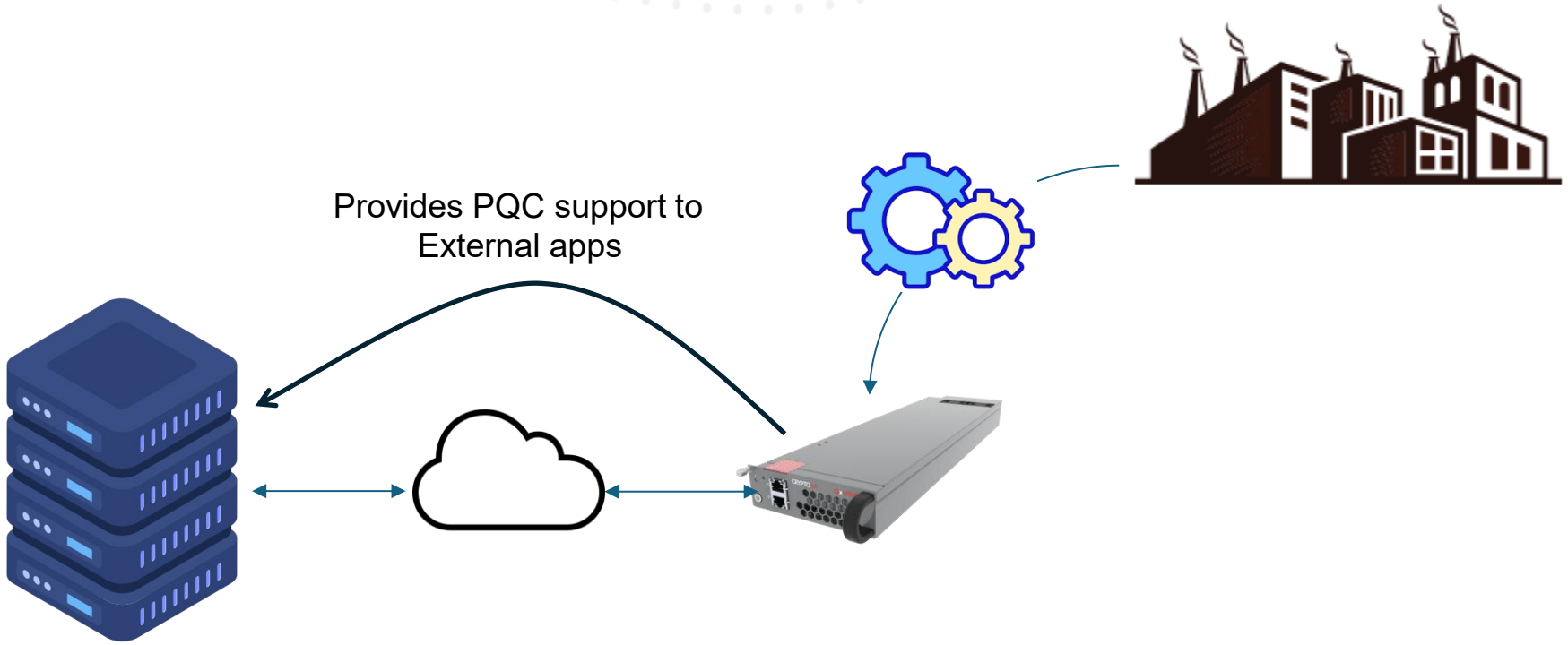
- Quantum-Safe
- Quantum-Ready
- Quantum-Resilient
- PQC-Safe
- PQC-Ready
- PQC-Supporting
- …

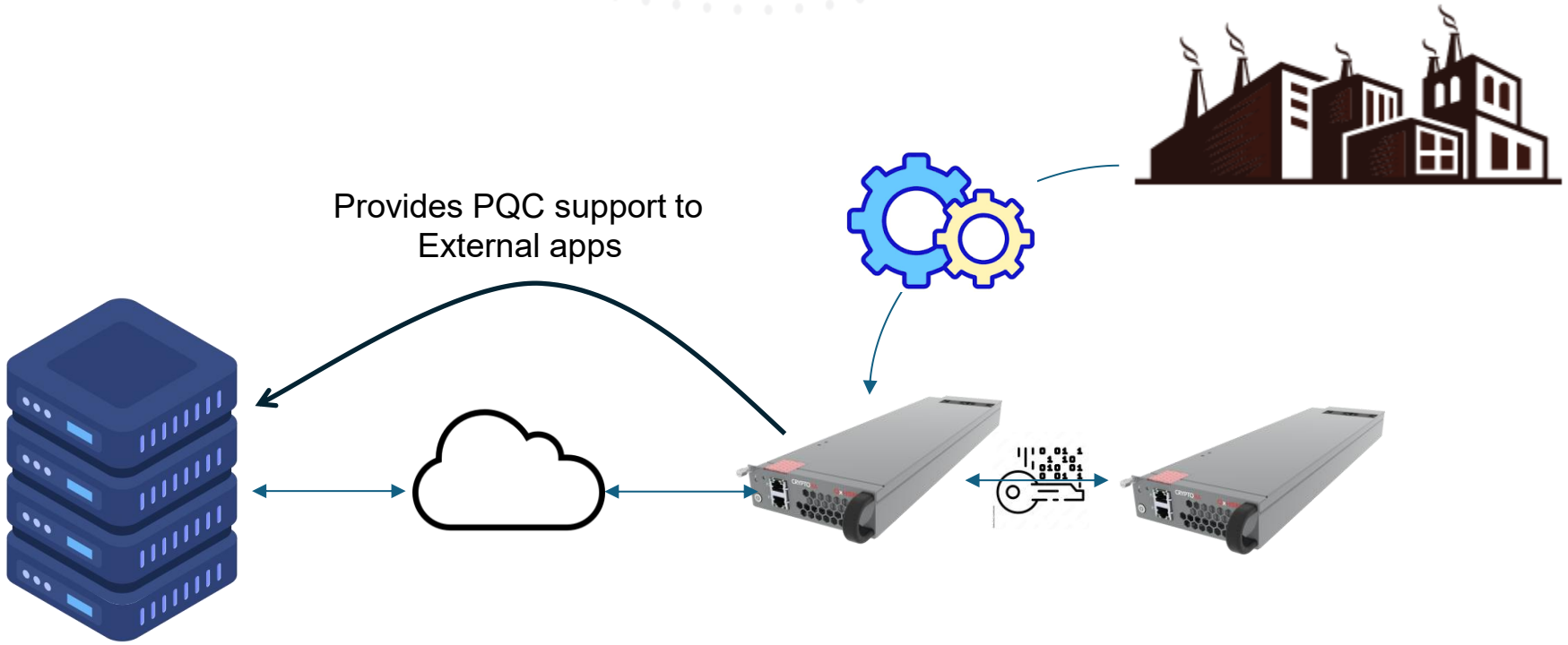


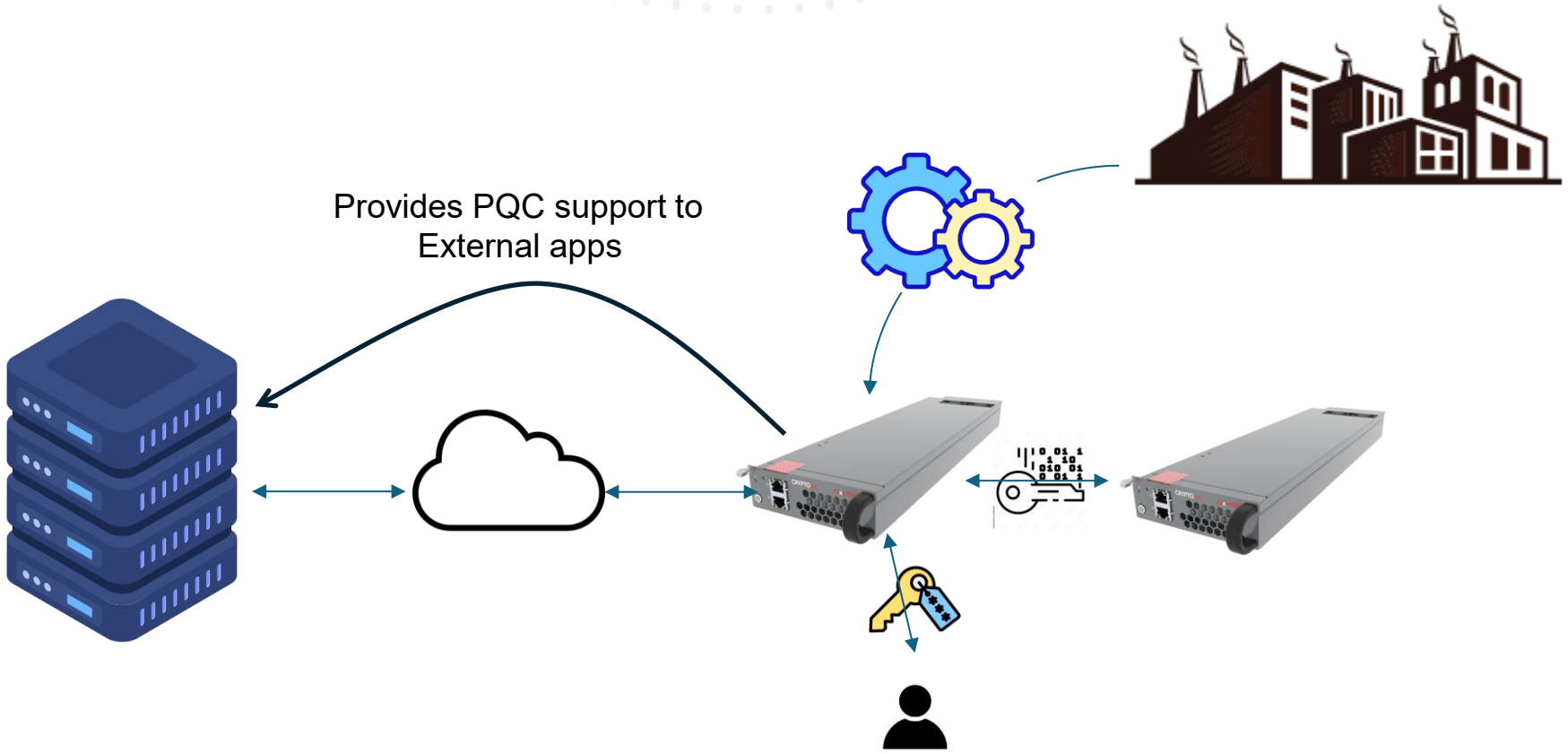
Provides PQC support to
External apps



CRYPTO4A

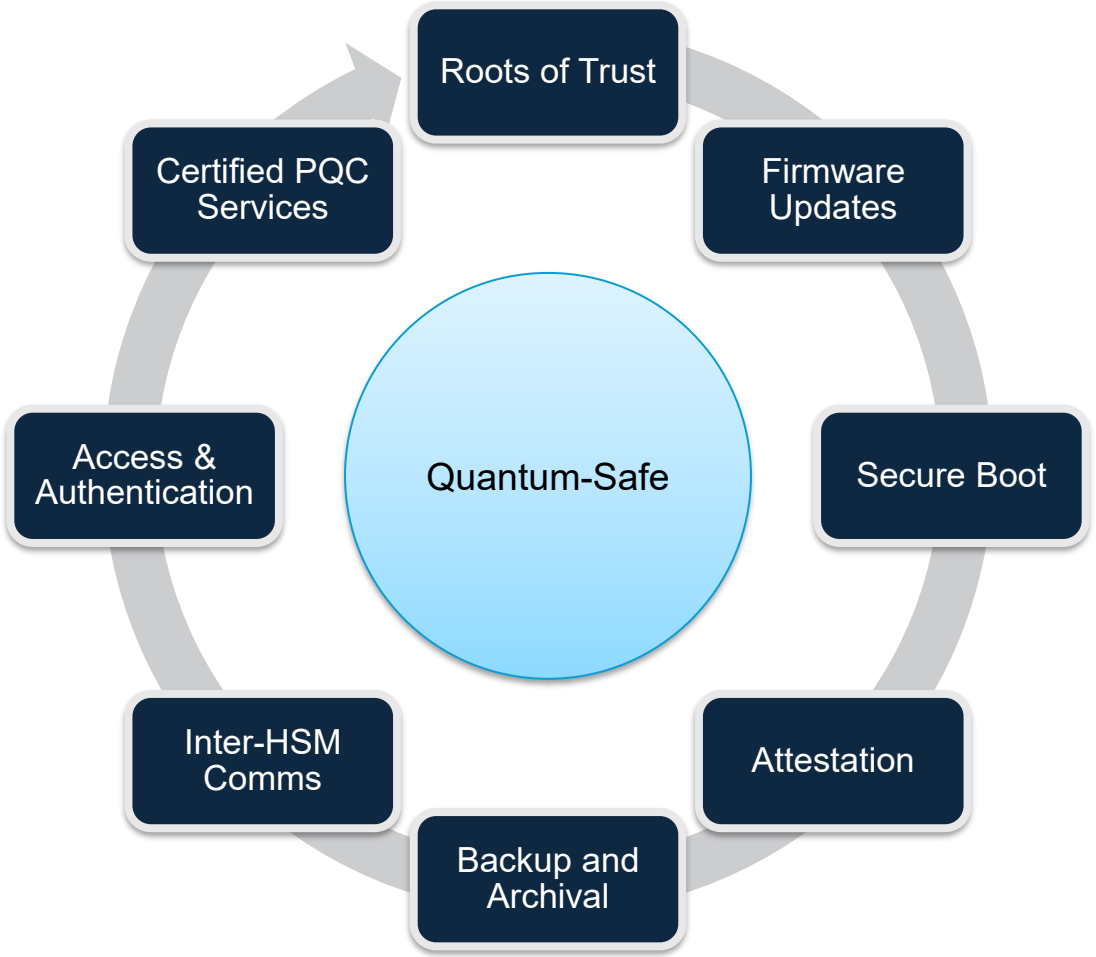

Provides PQC support to
External apps


Provides PQC support to
External apps



CRYPTO4A

What Makes an HSM Quantum Safe by Design?



https://crypto4a.com/resources/docs/2026-01-08-what-makes-an-hsm-quantum-safe-by-design

Call to action

- Check how “quantum-ready” your HSMs really are?
  - Is it only supporting PQC or is it both supporting and using PQC?

- Demand support for “Cryptographic Portability”
  - DES/3-DES have long been replaced, more than time for portability

CRYPTO4A

Thank you

For more information please contact:

Bruno Couillard
CEO & Co-founder

bruno@crypto4A.com
www.crypto4A.com