MINDSHARE26

CYBERSECURITY LEADERSHIP FORUM

The Eviden path to PQC

Implementing Quantum-Safe Cryptography across highly certified products

Pierre Brun-Murol, Eviden

11.06.2026 | WISSENSCHAFTSPARK | GELSENKIRCHEN

EVIDEN

MINDSHARE26

CYBERSECURITY LEADERSHIP FORUM

AGENDA

1. **Eviden status on PQC**
2. Focus n°1: Hardware Security Module
3. Focus n°2: PKI
4. Conclusion

Eviden active involvement around PQC

From agencies to markets' education

Working groups

Pole Excellence Cyber PQC WG
Alliance Confiance Numerique Crypto TF
ClubPSCo PQC WG
Campus Cyber PQC WG
PKI Consortium PQC WG
Charter of Trust PQC WG
ECSO Research and Innovation and Trusted Supply
Nexo PQC WG

Keynotes, panels

Events (ICT Spring, CoT Week, RiskIntel Media, Risk Summit, Quantum Tech Days, CyberSec Europe, ECSO days, EU PQC Conference, Q-Day Summit)

Customers' **evangelization** (Banking, Govt, Industrials…) and through orgs (AFNIC, Clusif, Numeum…)

R&D Collaborative Projects

KRITIS3M German funded project
POSEIDON Horizon Europe 2024 project
Astrolab French funded project
Update of Open Source libraries (contribution for example to SoftHSM to add ML-DSA)

Partner ecosystem

QuRISK ADVISORY
digitalberry
ISARA Crypto-Agile, Quantum-safe Security Solutions
IDQ an IonQ company
EVIDEN
CryptoNext security
PQSHIELD
SANDBOXAQ

Employee Expertise

7 Cryptographic Doctors

David Pointcheval

Recipient of the Lazare Carnot Prize from the French Academy of Sciences, is a world-renowned expert in cryptography and data security, further distinguished by the CNRS Silver Medal, the RSA Award for Excellence in Mathematics, and his 2024 IACR Fellow title

Klaus Schmeh

The world's most widely published cryptology author

Eviden cryptographic products

Most highly EU certified products

kms

covercrypt

ETSI TS 104 015

Client Side Encryption
Access policies & attributes

CC EAL4+ ANSSI QS ANSSI DR

Cosmian KMS & libraries

Trustway Proteccio HSM

Trustway IP Protect VPN

IDnomic ID PKI

Cryptovision GreenShield

Cryptovision secure elements

EVIDEN

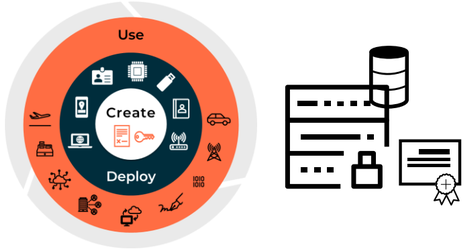
HR & **XR** versions

CryptoNext security

CC EAL4+ eIDAS NATO RESTRICTED

ANSSI QR SOG-IS EU RESTRICTED

CC EAL4+



BSI VS-NfD approved NATO OTAN

Smartcard OS

PQC Learning Machine

CC EAL4+ SOG-IS eIDAS

LEGEND

PQC ready

EVIDEN

Eviden cryptographic products

Most highly EU certified products

kms

covercrypt

Client Side Encryption
Access policies & attributes

ETSI TS 104 015

CC EAL4+ ANSSI QS ANSSI DR

Cosmian KMS & libraries

Trustway Proteccio HSM

Trustway Crypt2pay HSM

FIPS VALIDATED 140-2

PCI Security Standards Council

Trustway IP Protect VPN

IDnomic ID PKI

EVIDEN

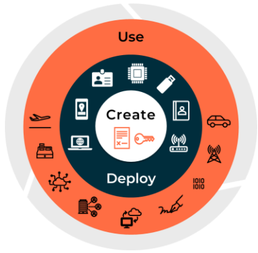
HR & **XR** versions

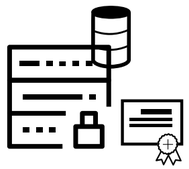
CryptoNext security

CC EAL4+ eIDAS NATO RESTRICTED

ANSSI QR SOG-IS EU RESTRICTED

CC EAL4+





Cryptovision GreenShield

Cryptovision secure elements

BSI VS-NfD approved

NATO OTAN

Smartcard OS

CardOS Atos

IDnomic SIGN

Eviden IAM suite

short security shelf life

microSD

PQC Learning Machine

eID javacard

CC EAL4+ SOG-IS eIDAS

LEGEND

PQC ready

In Roadmap

EVIDEN

Concrete end-to-end PQC use cases

Allowing already end-to-end customer tests

LEGEND

Roadmap: Ext DONE WIP

Key management and third-party integration

Cloud infrastructure encryption

Application encryption

Database encryption

Key Management System

Usage

Key Generation

Crypto HW

Digital identity production

Deployment

Usage

Production of PQC certificates

Integration of PQC credentials

Strong Authentication

Digital Signature

File/Mail Encryption

PQC implementation challenges

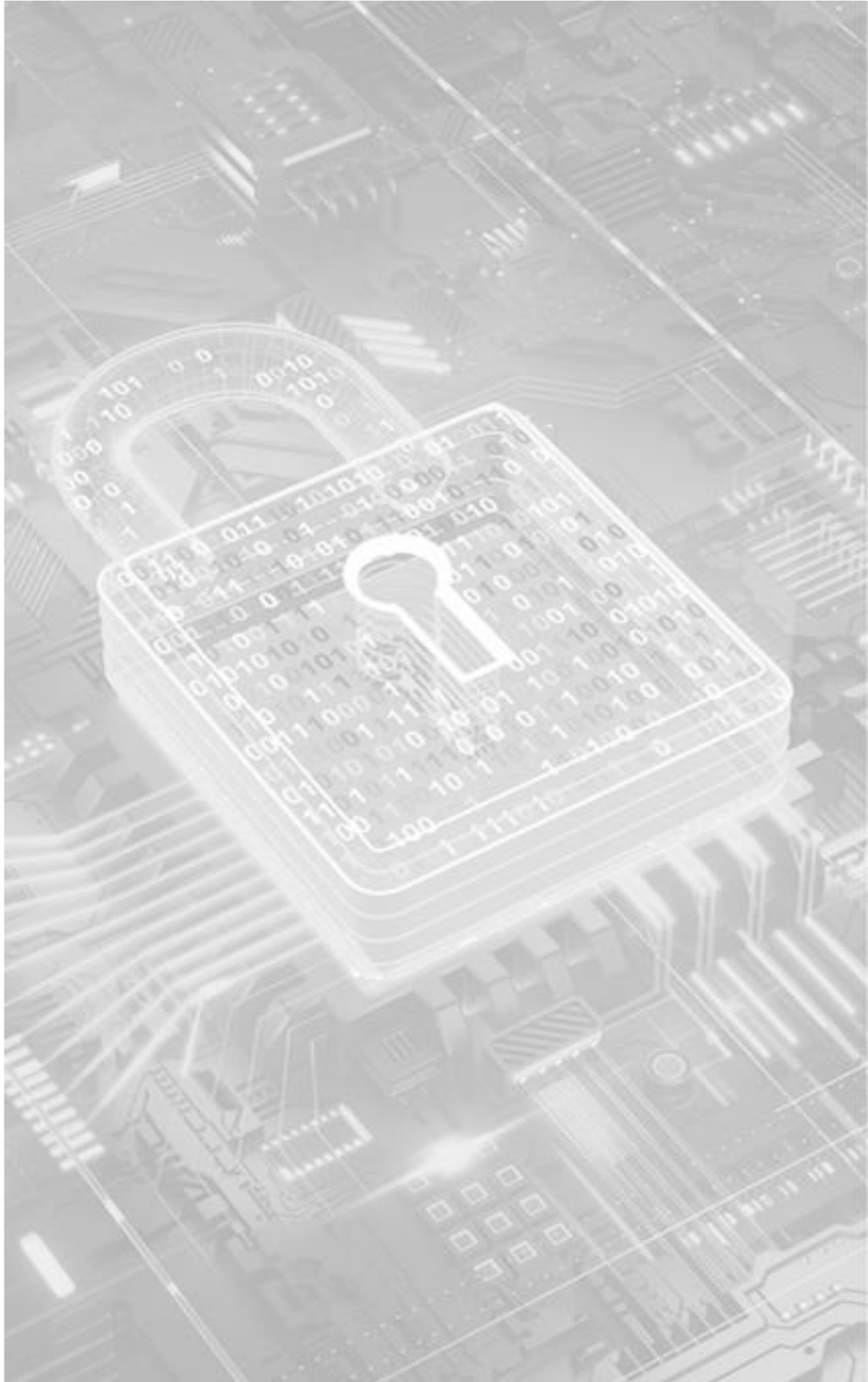
From technical constraints to standardization uncertainty

Technical integration into products

- Post-quantum algorithms: larger key and signature sizes
- Need more computing power and storage
- Performance and latency of new cryptographic schemes
- Interoperability and compatibility with existing systems

Tracking PQC standards & normalization

- Standards are continuously evolving
- A multi-level migration strategy
- Too few industrial initiatives



EVIDEN

AGENDA

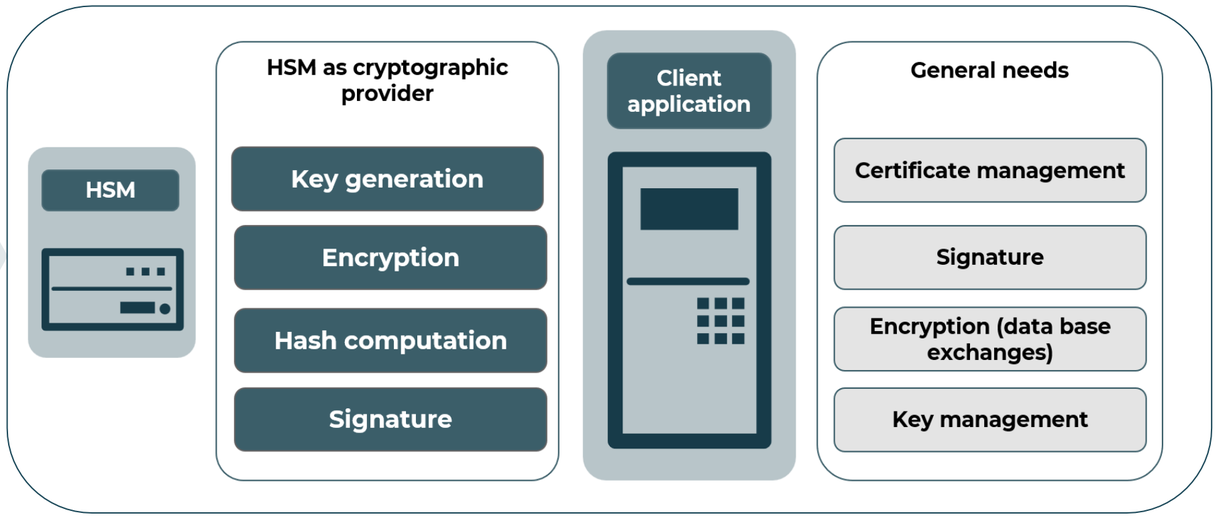
1. Eviden status on PQC
2. **Focus n°1: Hardware Security Module**
3. Focus n°2: PKI
4. Conclusion

Quick reminder: Hardware Security Module

The cryptographic root of trust

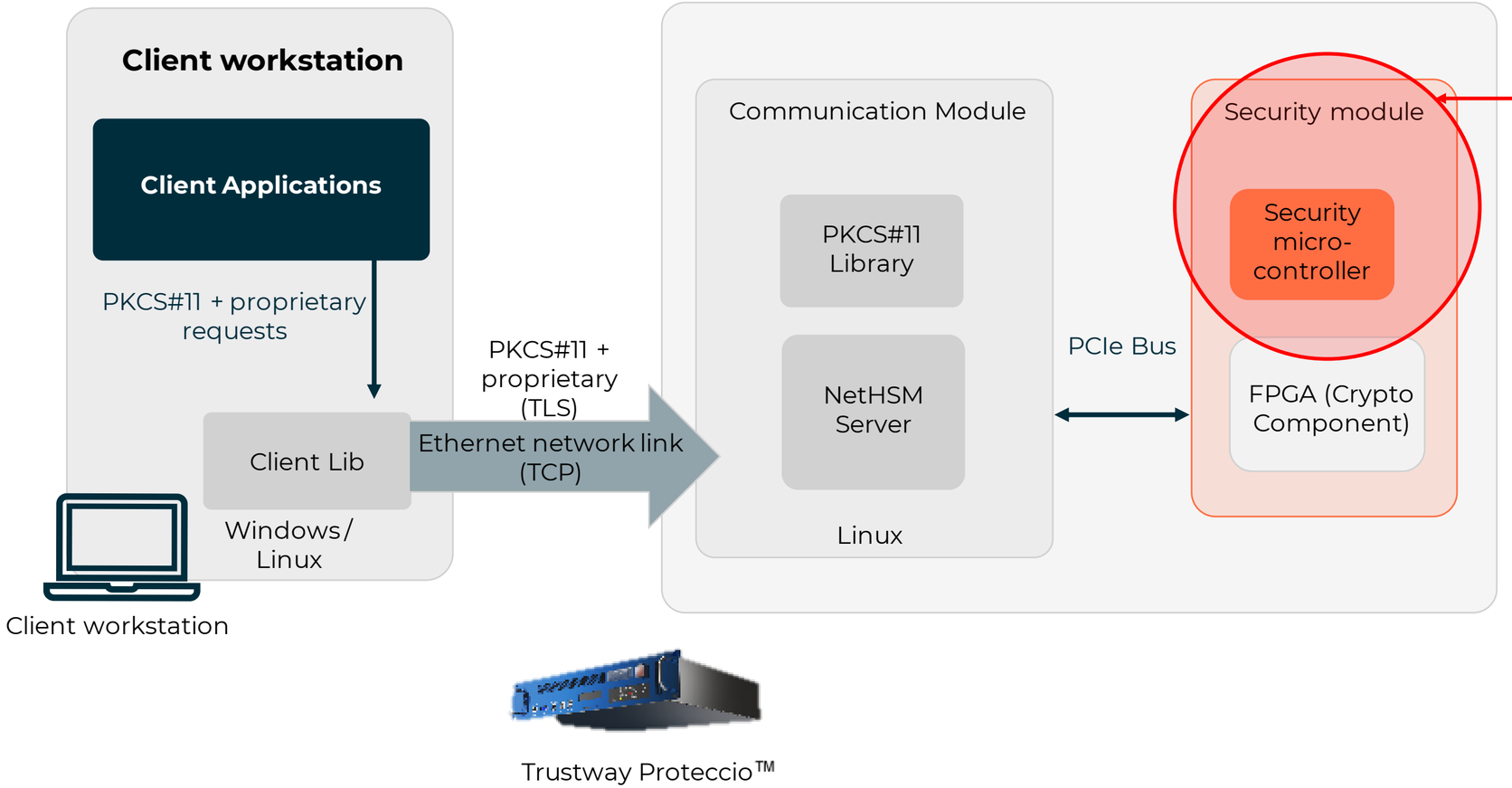
Role and features of an HSM :

- Cryptographic key storage and protection
- Acceleration of cryptographic operations
- Standards Compliance(CC EAL4+, QR, DR, FIPS 140-2/3, eIDAS, PCI)



HSM PQC migration with hardware implementation

Main challenges

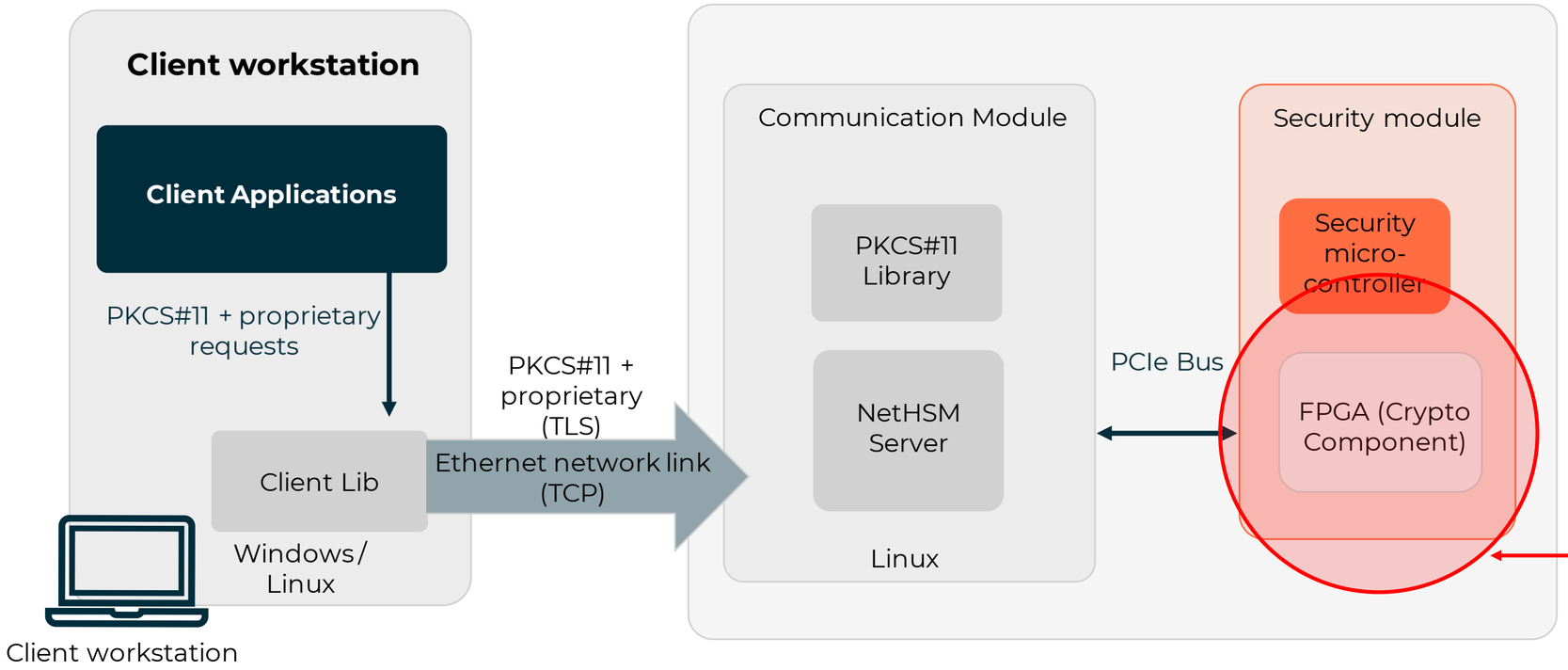


Main challenge on security microcontroller:

- Certification and/or existence of such component
- then **performance** !

HSM PQC migration with hardware implementation

Main challenges



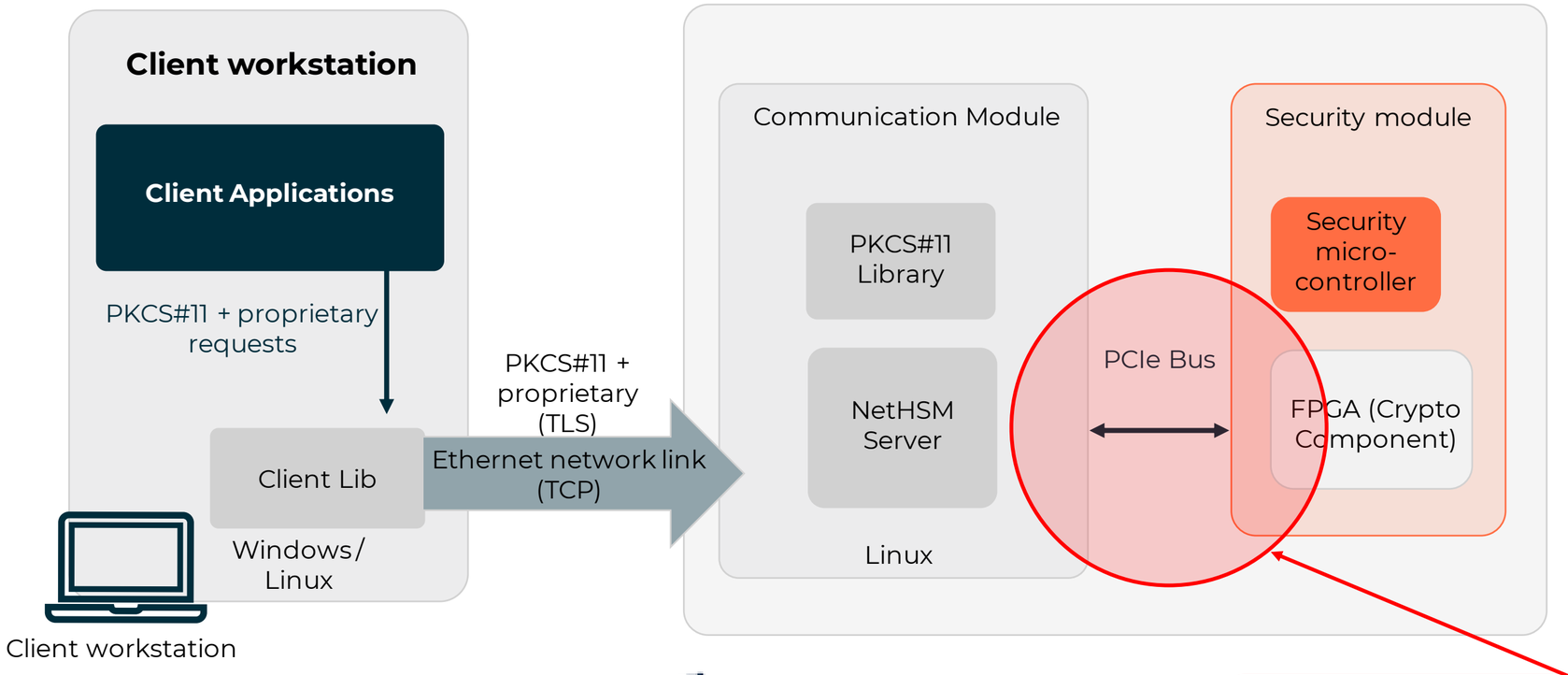
Trustway Proteccio™

Main challenges on FPGA :

- Algorithms standardization VS FPGA implementation time and ease of change
- No certification target yet

HSM PQC migration with hardware implementation

Main challenges

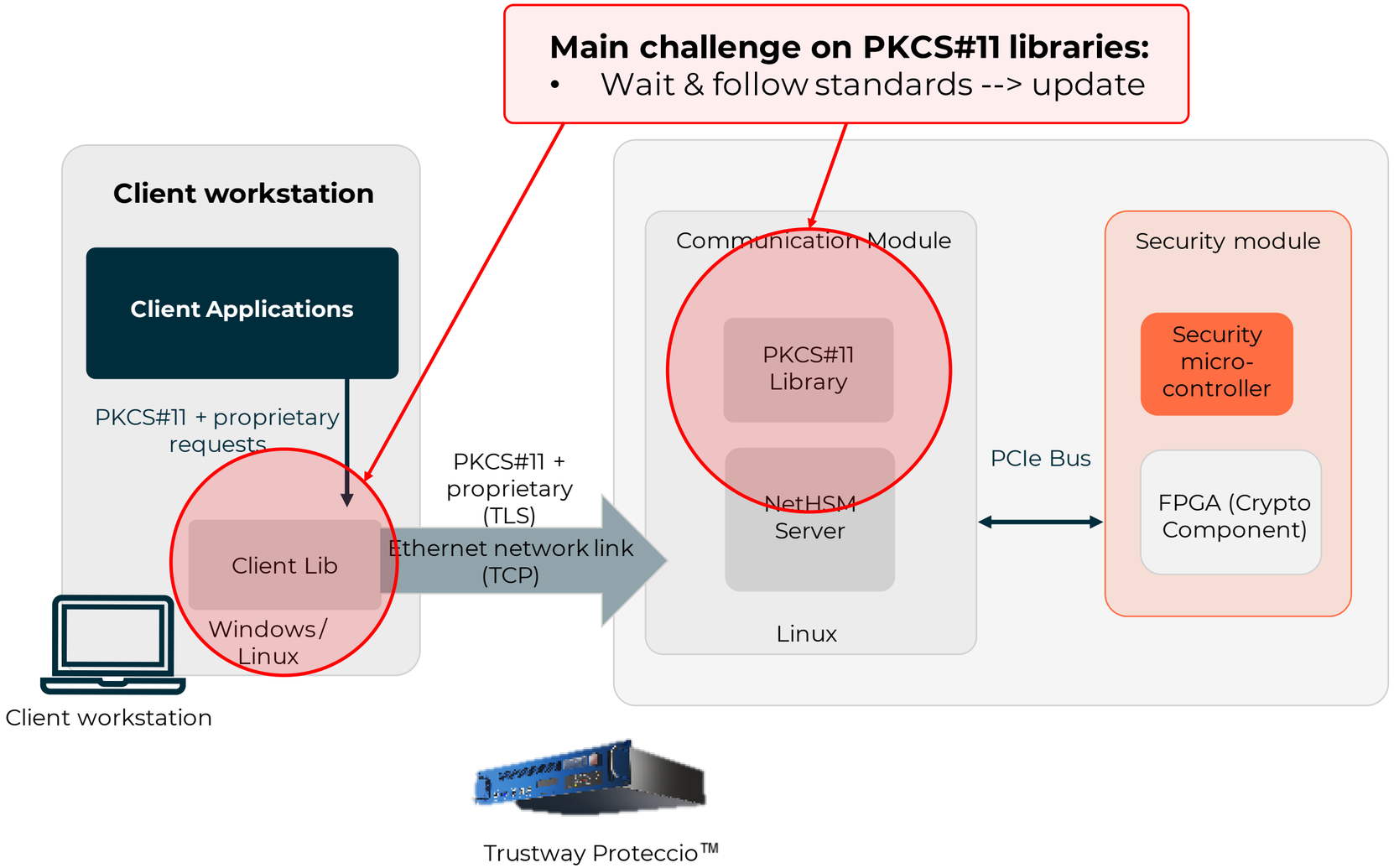


Main challenge on PCIe Bus:

- PQC communication implementation on both sides

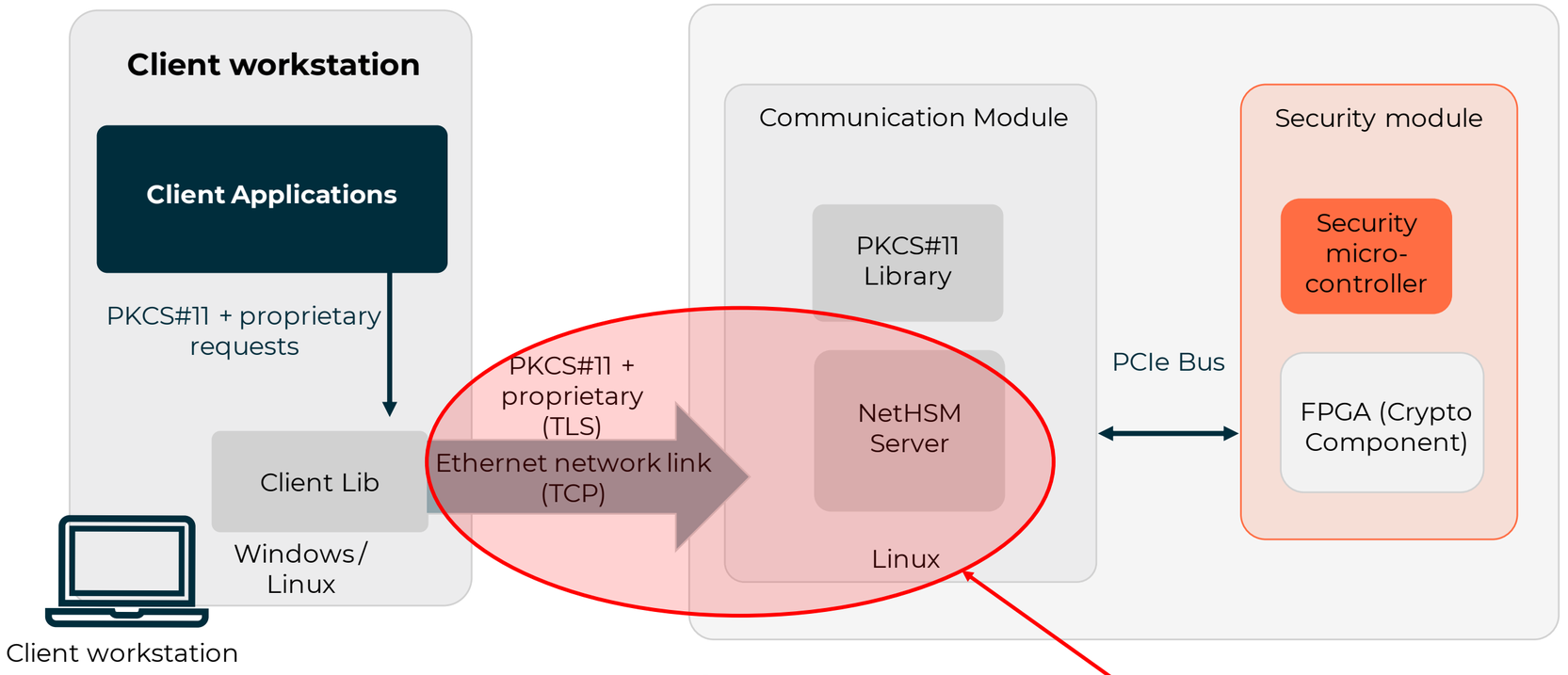
HSM PQC migration with hardware implementation

Main challenges



HSM PQC migration with hardware implementation

Main challenges



Main challenge on network link :

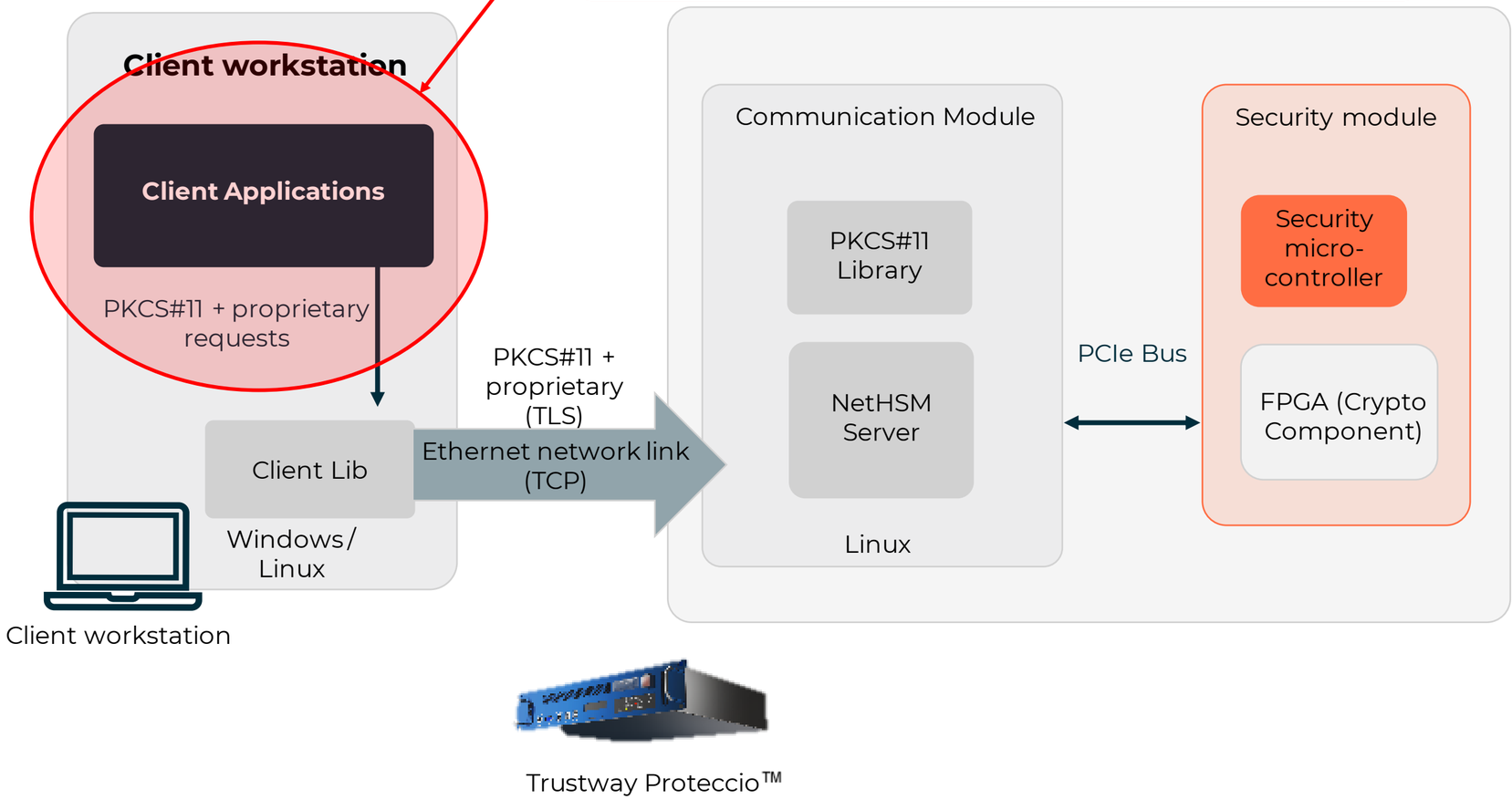
- Industry standard situation for TLS-PQC

HSM PQC migration with hardware implementation

Main challenges

Main challenges on client applications :

- POC
- Inventory
- Impact analysis



Trustway Proteccio™

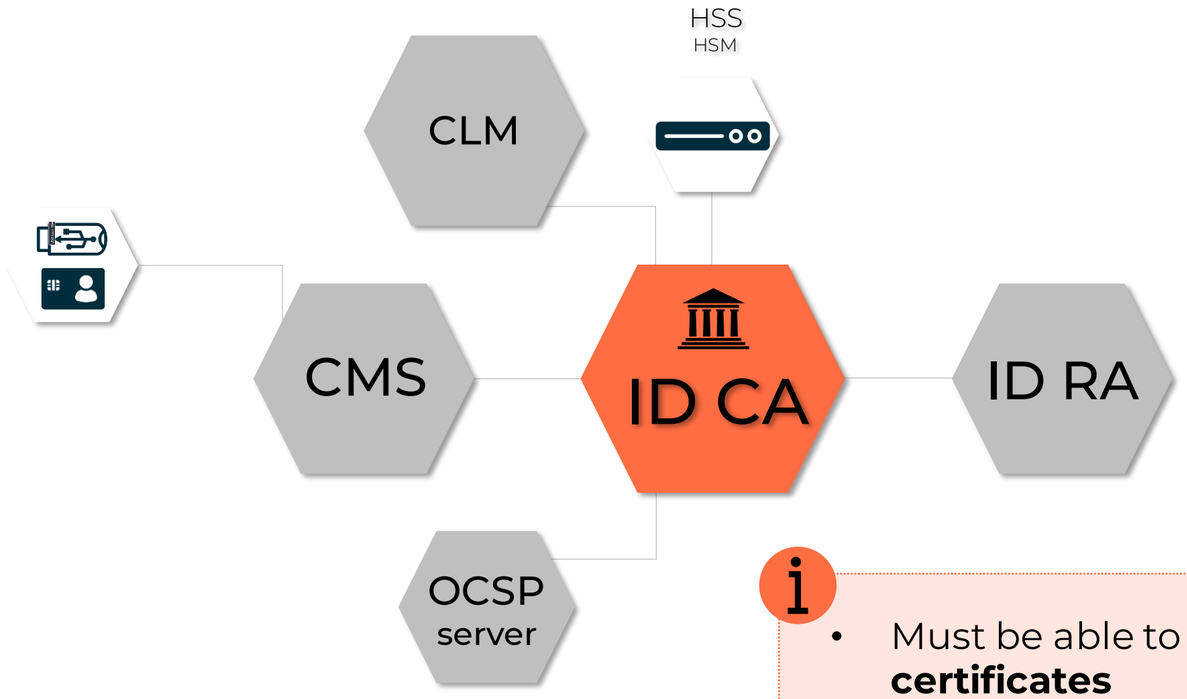
We are all in this together, hence the need to act now

AGENDA

1. Eviden status on PQC
2. Focus n°1: Hardware Security Module
3. **Focus n°2: PKI**
4. Conclusion

Main challenges for a Certificate Authority

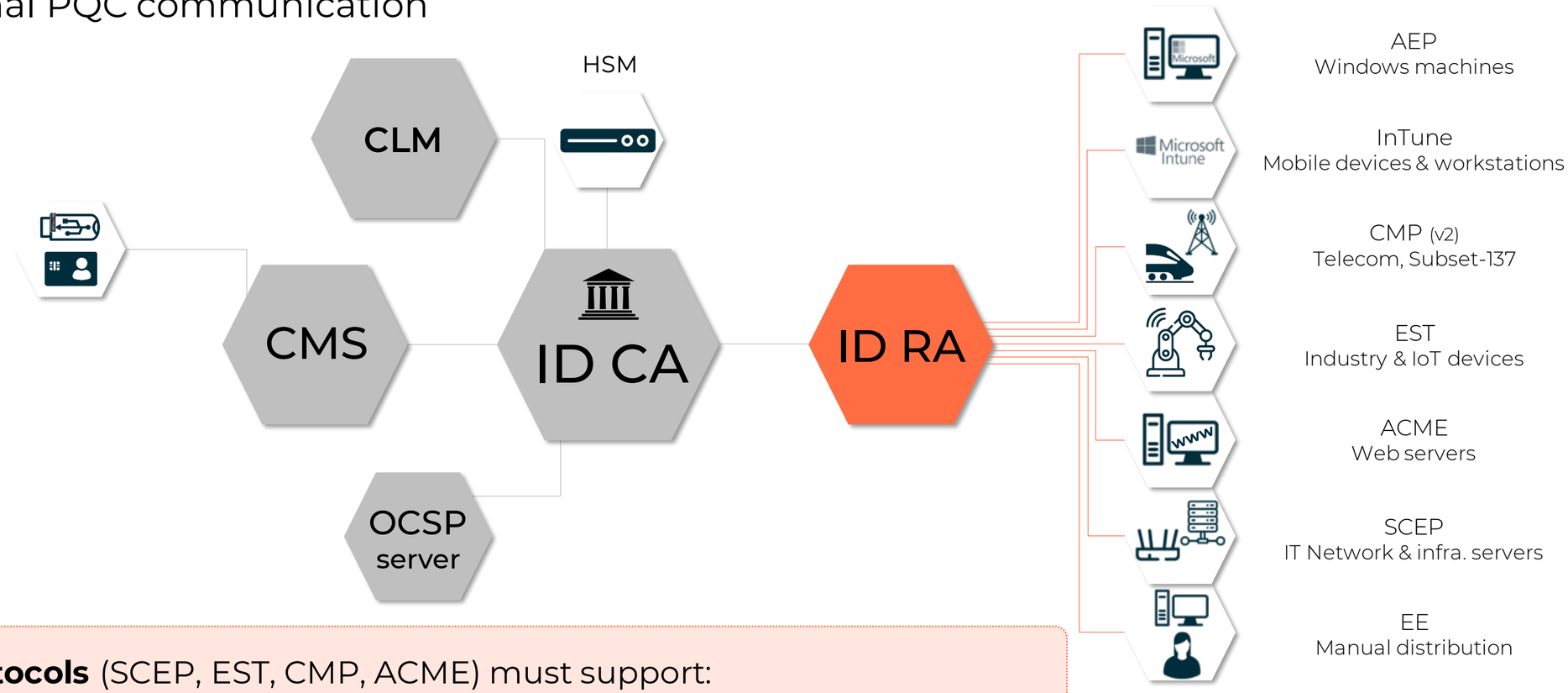
Multi-level evolution needed



- Must be able to issue **post-quantum and hybrid certificates**
- Existing **PoP** (CSR and CRMF) must support **new OIDs and extensions**
- **New PoP mechanism** are required for KEM keys (e.g., ML-KEM) and dual key usages (e.g., RSA + ML-DSA)
- Must support **PKCS#11 v3.2** to integrate post-quantum mechanisms

Main challenges for a Registration Authority

Internal and external PQC communication



- **Enrollment protocols** (SCEP, EST, CMP, ACME) must support:
  - ✓ **Hybrid** certificate profiles, and **larger** message sizes
  - ✓ **PoP** for KEM or dual key usages
  - ✓ **PQC in vulnerable building blocks**, such as JWS in ACME
  - ✓ Challenge–response authentication flows (e.g. TLS client authentication, etc.)
- Internal communication must be secured by **TLS with hybrid key exchange**

AGENDA

1. Eviden status on PQC
2. Focus n°1: Hardware Security Module
3. Focus n°2: PKI
4. **Conclusion**

EVIDEN

State of affairs

We already have results...

But still a lot of work to be done

Open-source libraries

Protocols standardization

Interoperability validation

Adoption

Certification

EVIDEN

Questions?

Pierre Brun-Murol, Eviden
pierre.brun-murol@eviden.com