ETSI/IQC Quantum Safe Cryptography Conference 2026

FUTUREPROOFING DATA SECURITY WITH QUANTUM-RESISTANT ALGORITHMS

PRESENTED BY:

CRYPTOMATHiC

18/06/2026

THE POST-QUANTUM REALITY

PQC READINESS

Quantum computing breaks the public-key cryptography we rely on today. **The migration to quantum-resistant algorithms has to begin now** - and standards bodies worldwide are already converging on a core set.

NIST · United States
Federal Standard

ML-KEM · ML-DSA · SLH-DSA
FN-DSA (tba)

CNSA 2.0 · NSA
The strict mandate

ML-KEM-1024 · ML-DSA-87 · AES-256
SHA-384/512 · XMSS & LMS

BSI · Germany
Recommendation

Hybrid first
FrodoKEM · Classic McEliece

ANSSI · France
Recommendation

Hybrid schemes as the
primary solution

NCSC · United Kingdom
Recommendation

NIST-aligned PQC
migration guidance

ISO · International
Standard (tba)

Classic McEliece
under standardisation

THE MIGRATION AVALANCHE

PQC READINESS

PQC migration is complex because organizations have to manage **standards, mandates, and deployment choices** all at the same time.

Conflicting standards

- NIST / CNSA 2.0 treat hybrid encryption as temporary.
- EU bodies (BSI / ANSSI) make hybrid schemes the primary solution.

Algorithm uncertainty

- RSA worked for 40 years
- Lattice structures are unproven and can change in the future

Operational Complexity

- PQC algorithms are not a drop in replacement
- PQC features use-case bound algorithms:
  - ML-DSA / SLH-DSA / XMSS for signing
  - ML-KEM for encapsulation

CRYPTOGRAPHIC AGILITY IS THE ONLY OPTION

EVALUATING MIGRATION STRATEGIES

Embedded Cryptography

Applications own both the keys and the logic.

- ✓ Maximum performance
- ✓ Lowest entry cost
- ✗ No central CBOM
- ✗ Massive implementation cost
- ✗ Continuous maintenance

Centralized KMS

Keys are centrally managed and distributed

- ✓ Solves the central-asset problem
- ✗ Still needs continuous maintenance
- ✗ Huge implementation effort & risk

Crypto-as-a-service

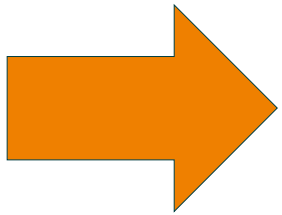
Applications consume cryptographic API. Cryptography platform owns both keys and logic.

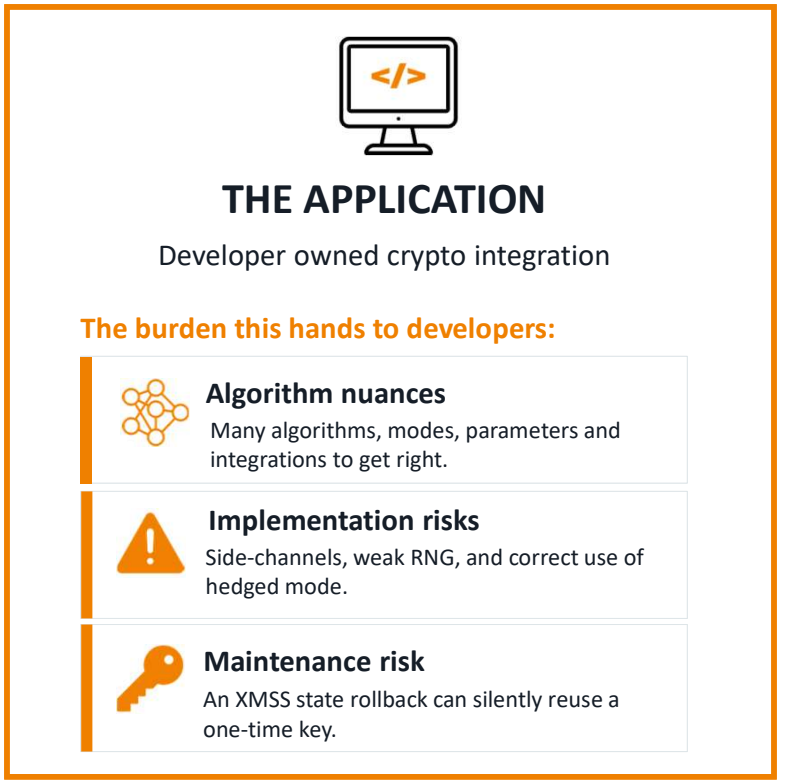
- ✓ Decouples crypto from applications
- ✓ Centralized policy management
- ✓ Swap algorithms without touching apps

DISTRIBUTING KEYS ≠ DISTRIBUTING EXPERTISE

THE KEY DELIVERY TRAP

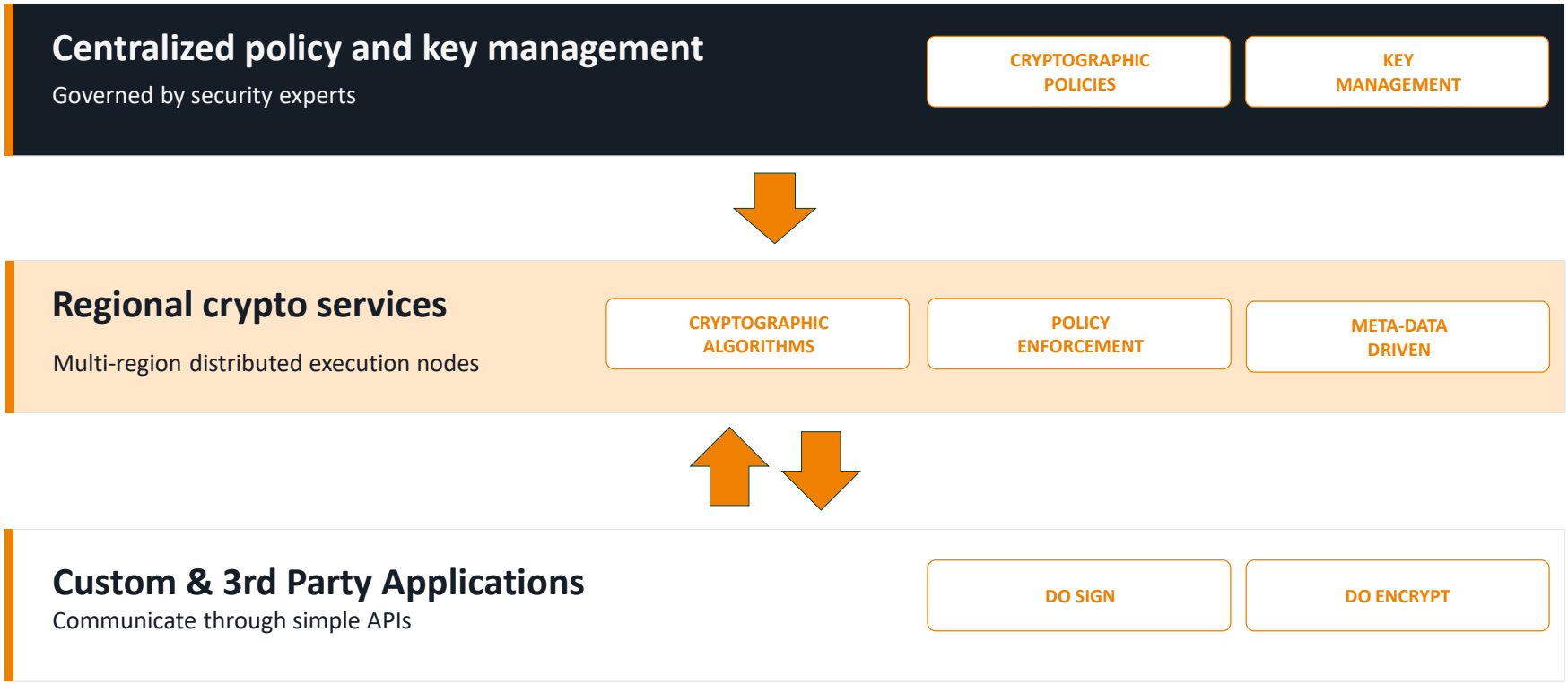
A central KMS can ship keys to every application. It cannot ship the cryptographic expertise that using them safely demands.





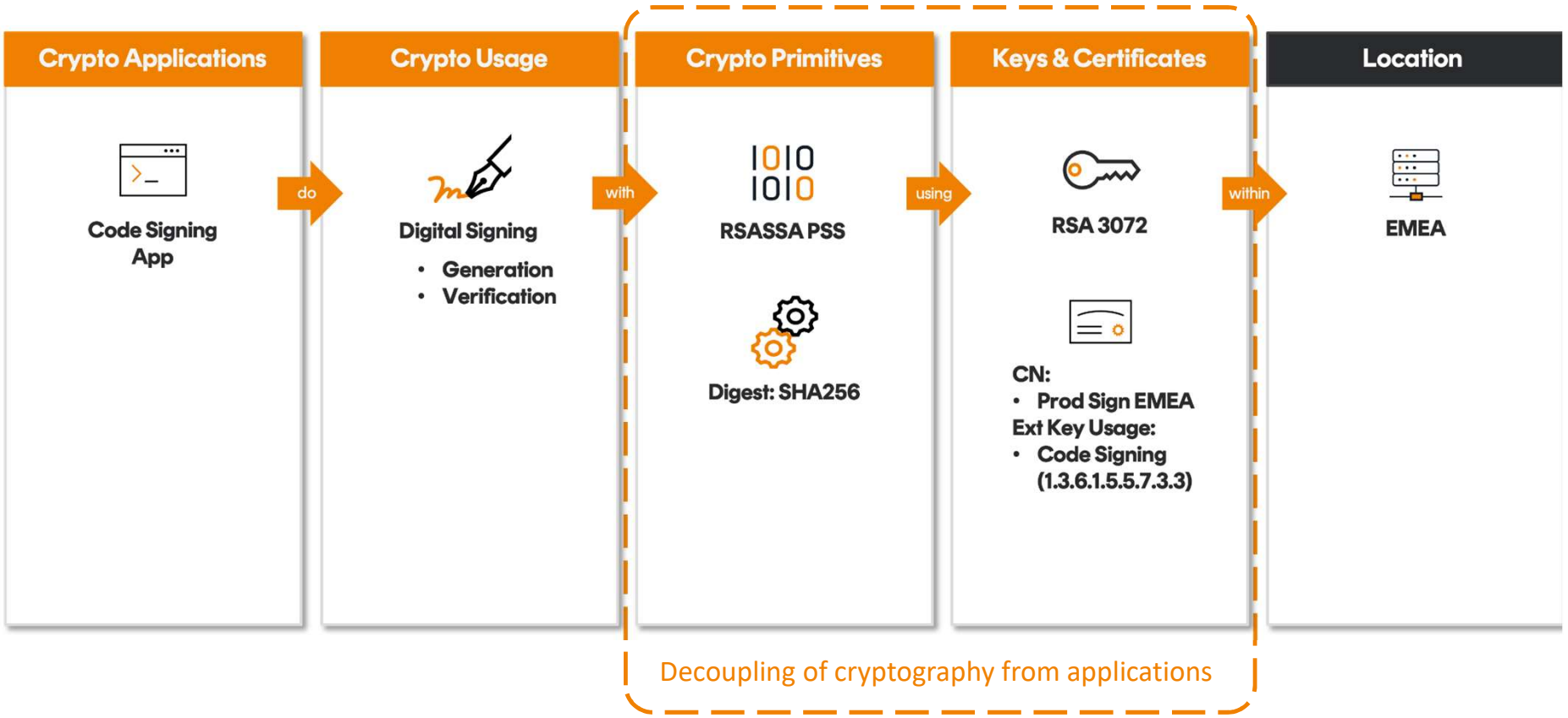
CRYPTOGRAPHY-AS-A-SERVICE (CAAS)

DECOUPLING OUTCOMES FROM APPLICATIONS



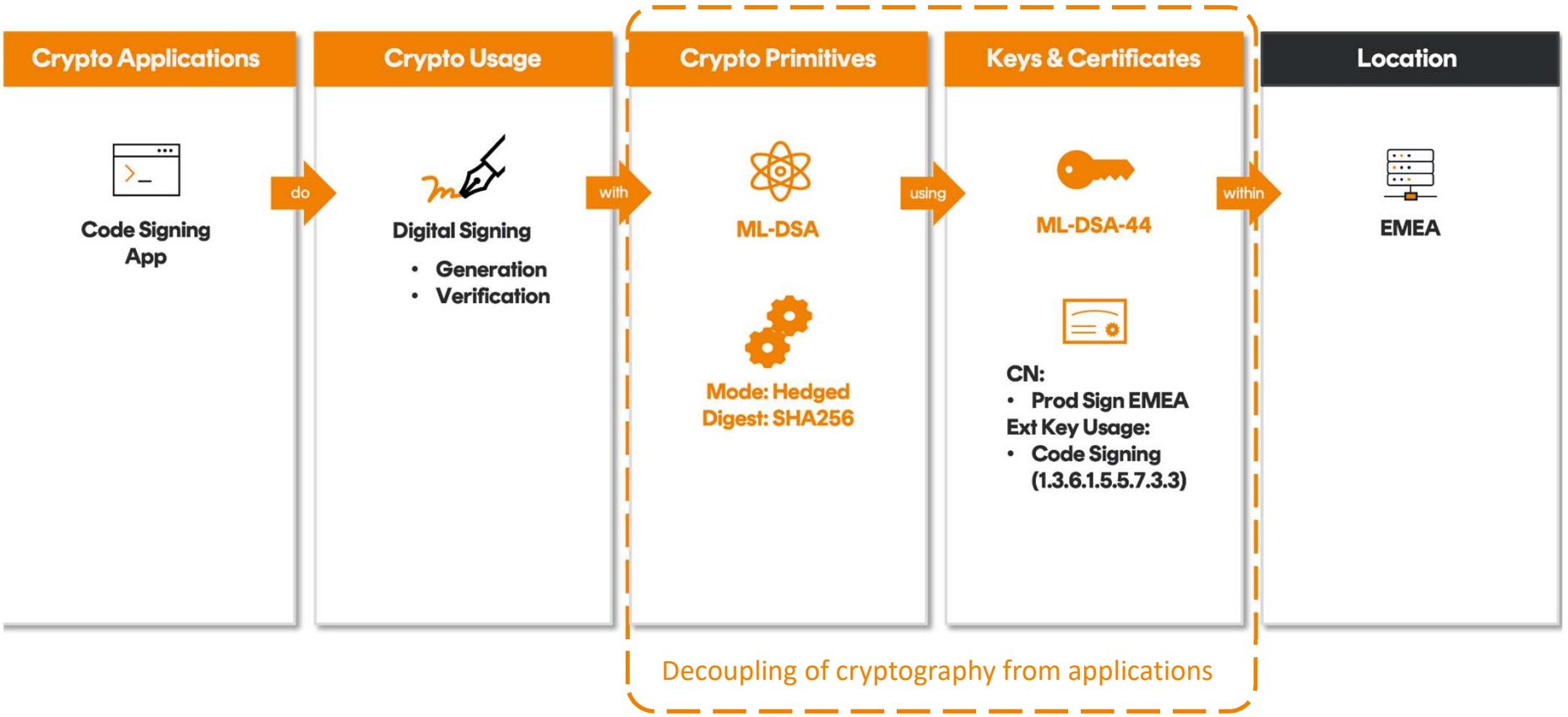
EXAMPLE | TRANSPARENT MIGRATION

TRANSITION TO PQC RESISTANT ALGORITHMS



EXAMPLE | TRANSPARENT MIGRATION

TRANSITION TO PQC RESISTANT ALGORITHMS



PROACTIVE STEPS FOR ACHIEVING CRYPTO AGILITY

ARCHITECTURE FOR PQC REALITY

1

Discovery & CBOM

You can't migrate what you can't see.

- Build a centralised Cryptographic Bill of Materials
- Audit hard-coded math libraries
- Identify hidden key locations

2

Intent-based APIs

Stop letting developers request specific algorithms

- Refactor architecture boundaries to focus on outcomes, not implementations
- Express business intent: DO ENCRYPT, not encrypt(RSA-OAEP)
- Enables agility and safer evolution

3

Schema readiness

Prepare databases for the physical reality of PQC assets

- Treat signatures as larger, opaque blobs
- Capture crypto-operation context
- Size schemas, indexes & storage for bigger assets

Cryptographic Agility Is Built TODAY

See everything
Know your cryptography end to end

Think in intent
Request outcomes not algorithms

Prepare your data
Make room for tomorrow's cryptographic reality

THREE THINGS TO ACT ON NOW

THE TAKEAWAY

01

STOP DISTRIBUTING EXPERTISE.

Start distributing cryptographic services. CaaS is the most sustainable path forward.

02

CENTRALIZE CRYPTOGRAPHY LOGICALLY.

PQC algorithms and modes are too complex for app-level implementation.

03

PLAN FOR THE FUTURE.

Prepare the application layer now: gather metadata and size for the physical reality of PQC assets.