Cryptographic Infrastructure for the Post-Quantum Transition

Hassan Kholil
nShield HSM Product Manager
Entrust





What is Crypto-Agility?

Crypto-agility is the ability to safely change cryptography across applications and infrastructure without disrupting security or operations.

ENTRUST

Crypto-Agility Is an International Priority

"The transition to post-quantum cryptography does not end with the selection and standardisation of post-quantum algorithms. Integration with existing systems and protocols is also required."

ENISA | European Union Agency for Cybersecurity

Post-Quantum Cryptography: Integration Study

Crypto products should be designed so that they can be adapted as flexibly as possible through cryptographic agility.

BSI | German Federal Office for Information Security

Quantum Technologies and Quantum-Safe Cryptography

"Cryptographic (crypto) agility refers to the capabilities needed to replace and adapt cryptographic algorithms in protocols, applications, software, hardware, firmware, and infrastructures while preserving security and ongoing operations."

NIST | Considerations for Achieving Crypto Agility

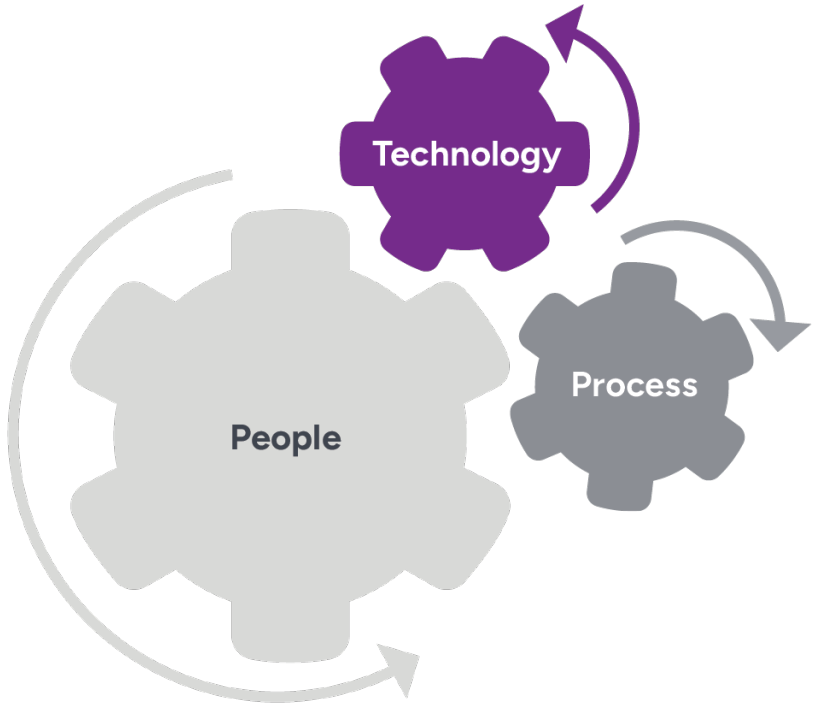
CSWP 39upd1, updated June 2026

From principle to implementation



Crypto-agility in Organisations

Crypto-agility is an organisation-wide capability, not a feature belonging to one product or team.



People	Accountability, skills and collaboration
Process	Governance, policy, risk and change management
Technology	Visibility, control, automation and adaptable infrastructure

How does crypto-agility support a real post-quantum transition?

ENTRUST

PQC has entered the implementation phase

Standardised mechanisms now have to work within real infrastructure and operating processes.

Standards

ML-KEM, ML-DSA and SLH-DSA

Concrete mechanisms for planning

Software ecosystem

Libraries such as OpenSSL make standardised mechanisms accessible.

Example: OpenSSL 3.5

Operational challenge

Applications, protocols, certificates, protected key stores and operating processes must absorb the change.

Algorithm availability moves the discussion from selection to implementation.

ENTRUST

PQ migration is not one project

Cryptographic functions create different assets, dependencies and migration priorities.

Protecting confidentiality

ML-KEM

Key establishment

TLS and protocol migration

Information lifetime and harvest-now-decrypt-later risk

Protecting authenticity

ML-DSA and SLH-DSA

Digital signatures

Certificates, code signing and firmware

Signing and verification ecosystems

Protecting the trust infrastructure

Key generation and authorisation

Hardware security boundaries

Audit, rotation, backup and recovery

Different cryptographic functions create different migration dependencies, owners and timelines.

ENTRUST

PQ readiness spans people, process and technology

The transition needs an accountable programme as well as working cryptography.

People

Accountable transition leadership

Application, infrastructure and security teams

Training and technical ownership

Process

Inventory and prioritisation

Policy and approved migration patterns

Testing, change management and audit

Technology

Adaptable applications and interfaces

Cryptographic asset visibility

Protected keys and scalable infrastructure

ENTRUST

Crypto-agility needs both control and execution

Management and technical layers connect organisational decisions with cryptographic operations.

Management and control

Inventory and ownership

Policy and approved algorithms

Risk, compliance and migration status

Audit and reporting

Policy flows down

Evidence and status flow up

Technical execution

Applications and cryptographic libraries

PKI, KMS and HSM services

Keys, certificates and secrets

Integration and automation

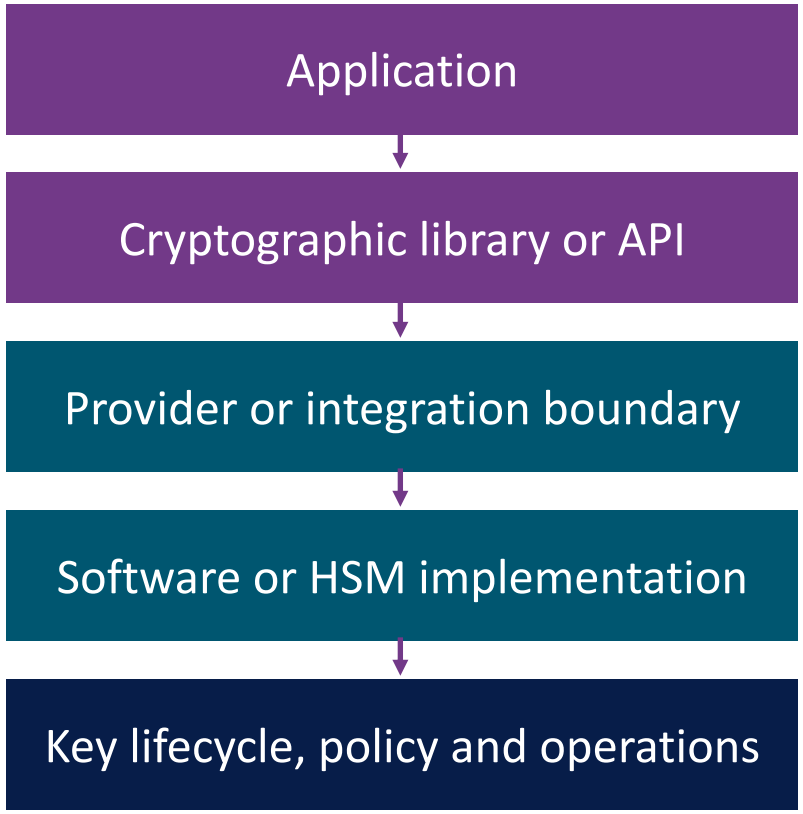
ENTRUST

From readiness to infrastructure

How applications, interfaces, protected keys and operating processes connect



Migration flows through the entire stack



Business function and embedded assumptions

OpenSSL is one practical example

Implementation and protected-key access

Execution environment and security boundary

Generation, authorisation, backup, rotation, audit and destruction

HSMs provide a protected boundary for critical keys and operations.

A change in algorithm can affect every layer, but the need to protect and govern private keys remains.

ENTRUST

What meaningful PQ support must include

Support must describe the complete deployment and key lifecycle.

Algorithm

Which algorithm, parameter set and operation?

Integration

Which API, library, protocol and application architecture?

Security boundary

Where is the key generated, stored and used?

Operations

How is the key authorised, backed up, replicated, rotated, audited and destroyed?

Assurance

Which validation or certification applies to the exact deployment configuration?

ENTRUST

Why HSMs matter in a post-quantum world

Post-quantum algorithms change the mathematics.

Organisations still need to protect and govern private keys.

Hardware-backed root of trust

PROTECT	CONTROL	PROVE	ADAPT
Protect private keys	**Control critical operations**	**Demonstrate accountability**	**Maintain trust through change**
Generate, store and use sensitive keys within a dedicated security boundary.	Enforce policy, authorisation, separation of duties and multi-person control.	Audit critical operations and support secure recovery and lifecycle management.	Allow algorithms and integrations to evolve without abandoning the protected operating model.

PQC readiness means protecting and governing the full key estate through transition

ENTRUST

The operational value of crypto-agility

Guardrails, visibility and repeatable processes enable change without losing control.

MOVE FASTER

Apply trusted guardrails

Approved policies and interfaces let teams adopt change without redesigning security.

REDUCE RISK

Control the transition

Visibility and ownership reduce unmanaged change and operational disruption.

DEMONSTRATE READINESS

Provide evidence

Inventory, audit and reporting show risks, priorities and migration progress.

PREPARE FOR CHANGE

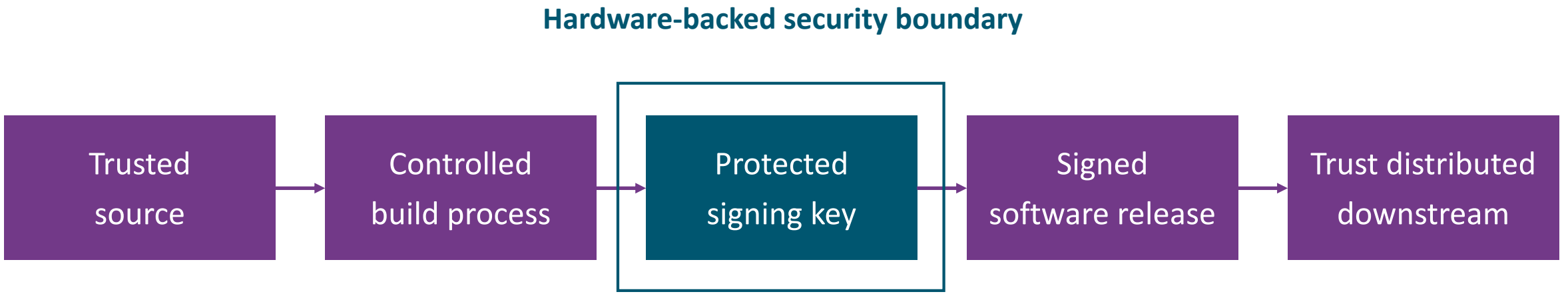
Build repeatability

Reusable processes make PQC and future transitions easier to manage.

ENTRUST

From algorithm support to a trusted signing service

Trust in a software release depends on the complete signing service, not only the signature algorithm.



Multi-person authorisation

Audit and operational governance

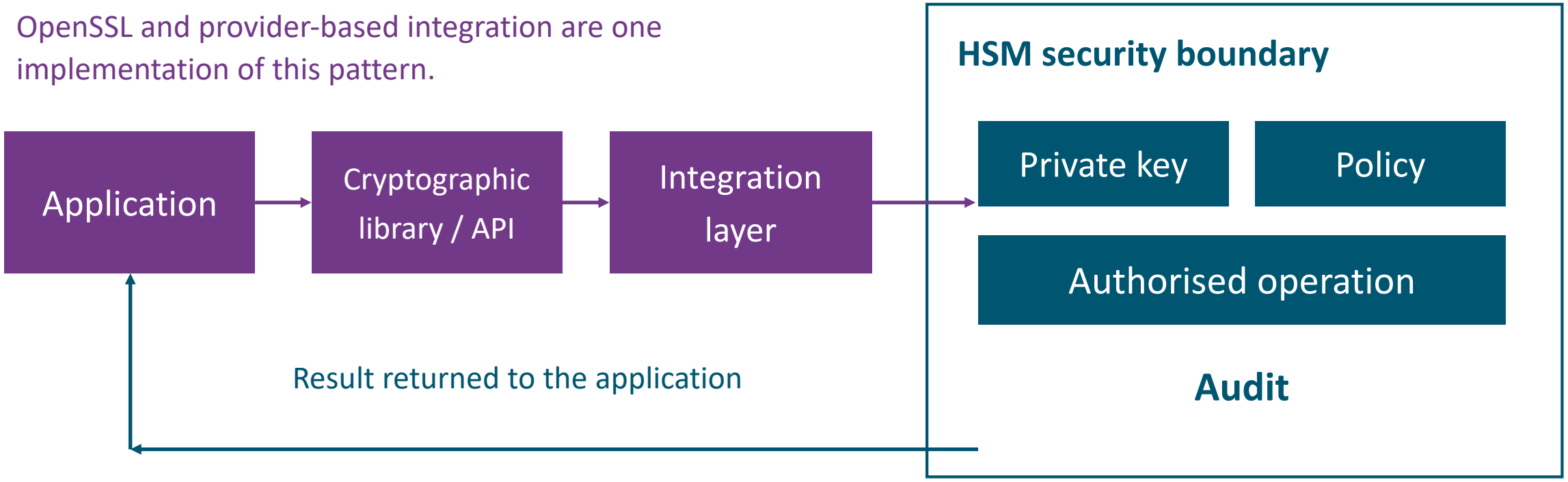
Protected root of trust for the signing service

ENTRUST

The security boundary still matters

The precise boundary input depends on the algorithm and integration model.

OpenSSL and provider-based integration are one implementation of this pattern.



ENTRUST

From implementation to transition

Managing coexistence, migration debt and organisation-wide change



We will operate in a mixed world



Technology

Algorithms, systems and protocols move at different speeds.

Process

Testing, rollback and exception handling are required.

Governance

Policy determines when classical, hybrid or PQ-only approaches are permitted.

The security property of a hybrid construction depends on its definition and implementation.

ENTRUST

PQC reveals architectural and operational debt

PQC migration exposes embedded technical assumptions and gaps in ownership, inventory and operating processes.

Technical assumptions

Often embedded in applications

01 A key is always RSA

02 A signature is always this size

03 A certificate always uses this algorithm family

04 This API always represents this mechanism

Operational assumptions

Often assumed, not always verified

01 Every key has a known owner

02 Backup workflows support every key type

03 Cryptographic policy can be changed centrally

04 Dependencies and relying parties are documented

ENTRUST

A practical organisation-wide migration sequence

1 Establish accountability

Create a cross-functional owner for the transition

2 Discover

Inventory cryptographic assets, data flows and dependencies

3 Prioritise

Assess information lifetime, exposure, service importance and complexity

4 Modernise

Reduce avoidable technical and operational debt

5 Experiment

Use standardised PQ mechanisms in representative systems

6 Test and migrate

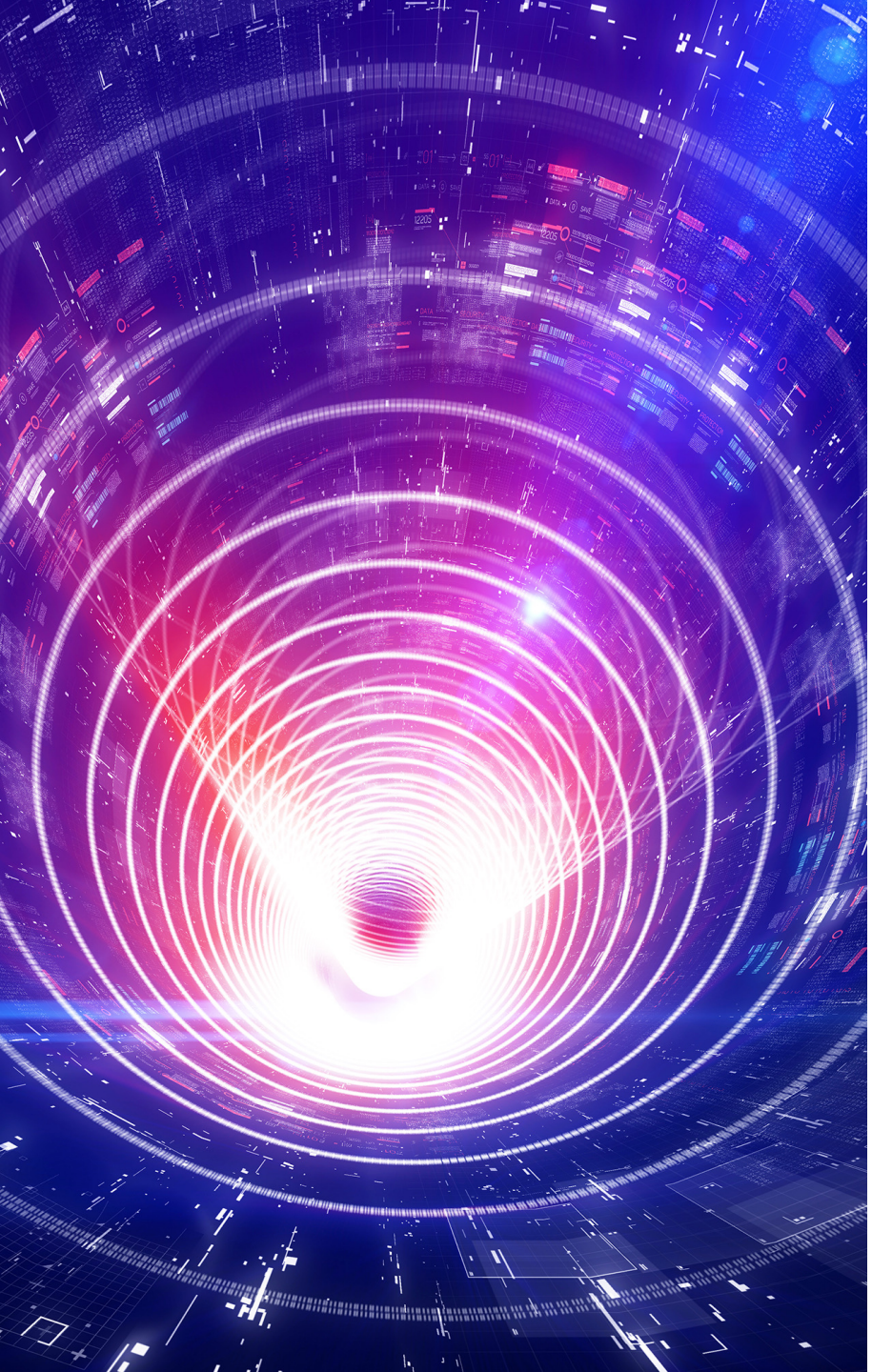
Validate applications, cryptographic libraries, interfaces, HSM integration, key lifecycle, interoperability, recovery and rollback

7 Govern and repeat

Monitor approved mechanisms, protected-key configurations and operational controls

PQ readiness is a managed programme across people, process and technology, not a single software upgrade.

ENTRUST



Summary

Post-quantum migration goes beyond algorithm transitions.

It is an infrastructure and organisational transition.

- Standardised algorithms are only the starting point.
- Applications, infrastructure and operating processes must move with them.
- Crypto-agility is what makes that transition manageable.

ENTRUST

Thank You

Hassan.Kholil@entrust.com

entrust.com

© Entrust Corporation

