ETSI/IQC Quantum Safe Cryptography Conference 2026

Achieving operational governance of cryptographic agility in banking

Presented by: Thibaud Ecarot – Cryptography specialist

BANQUE NATIONALE

18/06/2026

Symptoms of limited cryptographic agility

The challenge is no longer only to identify cryptographic mechanisms, but to assess agility and steer cryptographic resilience.

> Cryptographic visibility is improving, but operational improvement of **cryptographic agility remains limited.**

01	**Limited change speed**	The organization cannot adapt cryptographic mechanisms fast enough when change becomes necessary.
02	**Reduced resilience**	Weak agility reduces the ability to absorb urgent cryptographic change safely.
03	**Risk response friction**	Risk signals do not easily translate into prioritized and coordinated cryptographic action.

Symptoms we observe

Decision gap

Visibility does not clearly indicate what to change, where to act first, or what impact to expect.

Fragile impact analysis

Dependencies, process roles and cascading effects remain difficult to assess.

Qualitative agility assessment

Agility cannot be measured operationally when the required information is missing, disconnected, or not contextualized.

Cryptographic Resilience difficult to steer

Without reliable assessment and bottlenecks detection, cryptographic resilience becomes hard to plan and govern.

The challenge: Cryptographic resilience depends on governed change

Root cause: cryptographic inventories start from sources, not decisions

> A structural issue is that cryptographic inventories are often source-driven, while operational governance requires question-driven models.

An inventory can improve visibility while still failing to support cryptographic change

Available inventory inputs

- Discovery tools
- CMDB
- CycloneDx CBOM
- Certificate inventories
- HSM / KMS / Code repositories

Good for visibility

Insufficient for change governance

Governance questions

Decision lens for change

- Missing process context
- Weak dependency modeling
- Unclear change impact
- Limited governance linkage

Question-driven governance

To govern cryptographic change, the model must start from decisions, not sources

Descriptive inventories lack the logic of cryptographic change

Inventories and CBOM are essential for visibility, but operational agility requires additional context to govern a transition.

> A descriptive model can tell what exists, but not reliably what will break or how the transition should be governed.

Process role	Where is this mechanism used?
Transitive dependencies	What else is indirectly affected?
Impact	What business or resilience consequence does it create?
Transition path	What should change first? And in what sequence?

Visibility is necessary, but cryptographic agility requires process-level reasoning

A process-based model to govern cryptographic agility

A **unified view** that makes usage and change options explicit.

1. Business process view

Where does cryptography support business value?

- Business functions
- Process steps
- Criticality
- Business constraints

2. Cryptographic process view

Which operations and capabilities support the process?

- Crypto capabilities
- Crypto operations
- Control points
- Policy conditions

3. Lifecycle and change view

What can change, from which state, under which constraints?

- Lifecycle states
- Allowed changes
- Pre-conditions
- Constraints

Projections that inform the model

Inventory projection

Artefacts
Implementations
Algorithms & libs
Certificates / keys
...

Architecture projection

Systems & apps
Infrastructure
Deployment context
Technical dependencies
...

Unified reasoning view

One view, multiple decisions enabled

Meaning of use
Understand why cryptography is used and where

Applicable rules
Link business, crypto, governance and policy rules

Change options
See what can change and under which conditions

Constraints conflicts
Detect incompatible rules and blocking constraints

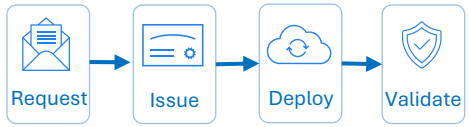
Bottlenecks
Identify what limits safe and fast change

Agility evidence
Provide objective basis to assess and track agility

Revealing the bottlenecks of cryptographic change

The process model provides transition evidence.
The agility framework reveals what slows down change.

Example: internal TLS certificate migration



Current	Target
Leaf cert: RSA-2048	Leaf cert: ML-DSA-65
CA hash: SHA-256	CA hash: SHA3-256
Deployment: Manual	Deployment: Automated

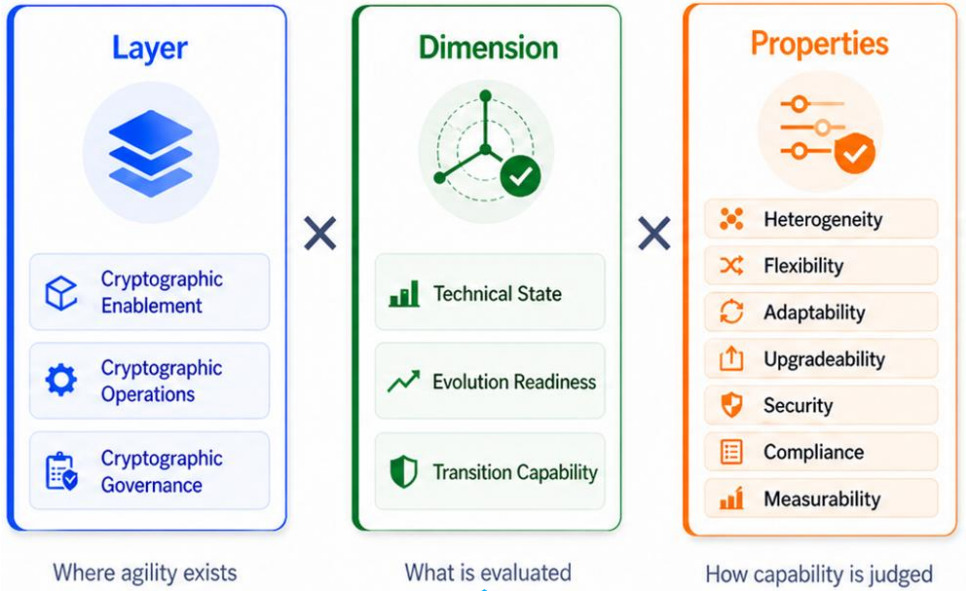
Parameter changes

- Signature algorithm
- CA hash
- Certificate profile

Dependencies & constraints

- CA policy
- Legacy client
- Change window
- Rollback readiness

Cryptographic agility assessment lens



What the model reveals

Cryptographic agility profile

- Transition capability limited
- Upgradeability constrained
- Operational friction visible
- Measurability incomplete

Bottlenecks revealed

- Manual validation gate
- CA policy / parameter mismatch
- Missing process documentation
- Untested certificate rollover

Targeted improvement plan

- Document end-to-end process
- Automate validation and issuance checks
- Prepare rollback and fallback patterns

Conclusion

Process-based reasoning for governed cryptographic change

Key takeaway

- Process modeling makes cryptographic change analyzable.
- Agility assessment reveals bottlenecks, not just score
- Improvement actions target change velocity and resilience

Thank you

Questions and discussion

Acknowledgements
Thanks to colleagues across organizations, and to the discussions within the CFDIR Quantum Readiness Working Group, especially John Buselli, for helping raise the ambition for actionable cryptographic agility.

Open Cryptographic Process Standard (OCPS) example

```
ubuntu@ocps: ~/projects

$ ocps compile ./diploma-sign-usecase
OCPS Compiler 0.1.0

Scanning directory: ./diploma-sign-usecase
Discovered 9 OCPS files

Loaded models:
  [business]    diploma_issuance_business_process
  [crypto]      diploma_signature_process
  [blueprint]   signing_key_lifecycle_blueprint
  [blueprint]   digital_signature_architecture_blueprint
  [blueprint]   crypto_inventory_evidence_blueprint

Loaded projections:
  business_to_crypto
  crypto_to_lifecycle
  crypto_to_architecture
  crypto_to_inventory

Compiled artifact: diploma_issuance.bundle.ocps
Compilation report: diploma_issuance.compile-report.txt
Result: success
```

All models and projections are aggregated into one compiled bundle

Multiple process and projection views can be compiled into one reasoning model.