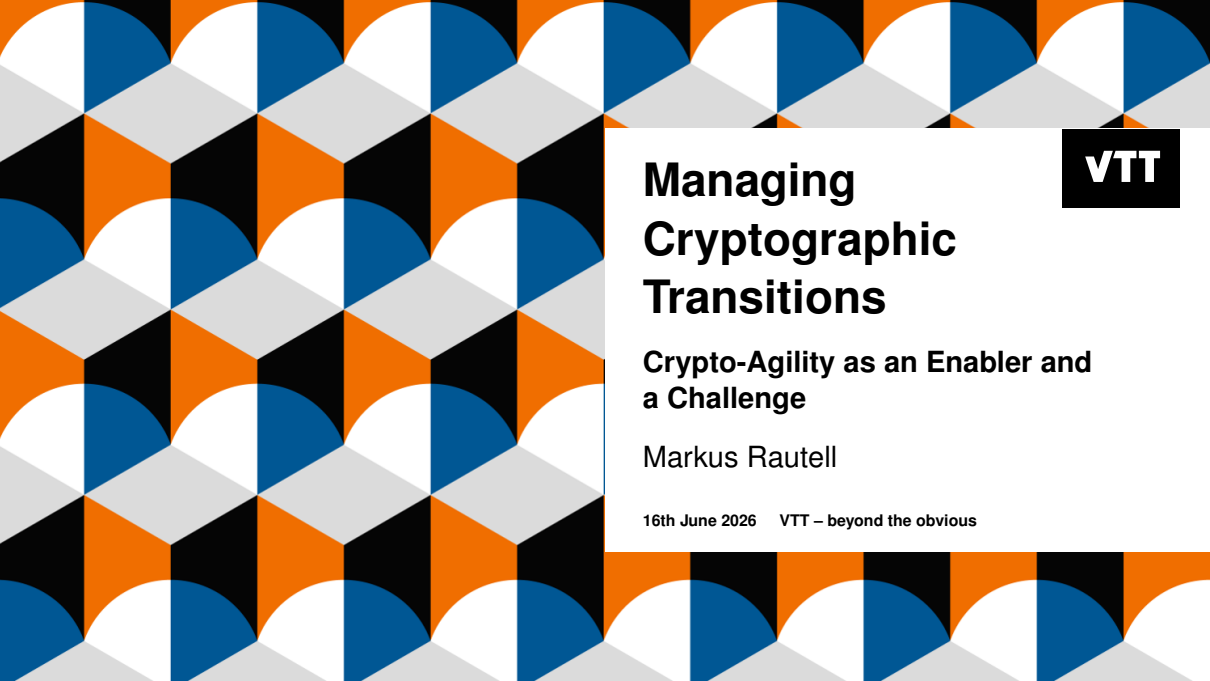


Managing Cryptographic Transitions

Crypto-Agility as an Enabler and a Challenge

Markus Rautell

16th June 2026 VTT – beyond the obvious

Presentation Structure

- Motivation
  - PQC Transition Landscape
  - Limitations of Current Practices
  - Transition Barriers
- Cryptographic Agility
  - Concept
  - Key Benefits
- Open Challenges
- Summary

BUSINESS FINLAND

Beyond the Limits of PQC

Motivation

Why the PQC Transition Matters

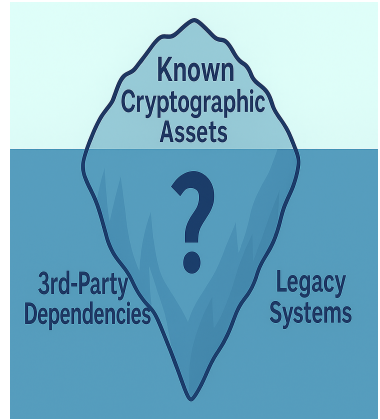
- Public-key cryptography
  - **Confidentiality**: Secure channel via key exchange
  - **Authenticity**: Verify identity and integrity
- Emerging quantum threat
  - Harvest Now, Decrypt Later $\rightarrow$ immediate impact
  - Trust Now, Forge Later $\rightarrow$ impact after Q-Day
  - Uncertain timing of Q-Day
  - Exposes the fragility of cryptographic longevity
- Lessons from the past transitions
  - Slow, complex, and operationally problematic

Why Current Practices Fall Short

- All major cryptographic primitives have either been weakened or replaced
  - Technological advances
  - Cryptanalytic breakthroughs
- Past transitions have taken decades
  - DES $\rightarrow$ 3DES $\rightarrow$ AES
  - SHA-1 $\rightarrow$ SHA-2
- Systems often built without considering future cryptographic updates
- PQC transition anticipated to be even more complex
  - Algorithm updates vs. PKI-wide re-engineering
- How do we avoid repeating this cycle beyond PQC transition?

Why PQC Transition is Hard in Practice

- Systemic constraints on the transition
  - Emerging standards vs. shrinking timelines
  - Limited resources and economic burden
  - Operational continuity vs. transition effort
- Organizational inertia
  - Cryptographic maintenance deprioritized
  - Limited visibility into cryptographic assets
  - Lack of structured update processes
  - Shortage of cryptographic expertise



Crypto-Agility Enabling Smoother Transitions

Concept of Crypto-Agility

- **Capability**: Ability to adapt cryptography with minimal operational disruption
- **Key enablers**
  - **Visibility**:
    Inventory of cryptographic assets
  - **Abstraction**:
    Isolation of cryptographic details from apps
    $\rightarrow$ crypto-agnostic design
  - **Governance**:
    Centralized policies and update workflows
    $\rightarrow$ controlled and repeatable changes

Figure 1: Traditional case

```
function signDocument(document):

    # 1. Generate keys
    keyPair = ML_DSA_65_GenerateKeyPair()

    # 2. Get signing key
    privateKey = keyPair.privateKey

    # 3. Sign document
    signature = ML_DSA_65_Sign(
        key = privateKey,
        message = document
    )

    return signature
```

Figure 2: Agile case

```
function signDocument(document):

    # 1. Create signing identity
    signer = CryptoProvider.createSigner()

    # 2. Sign document
    signature = signer.sign(document)

    return signature
```

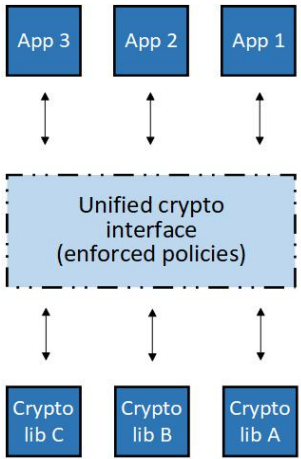
Key Benefits of Crypto-Agility

- Supports centralized management of cryptographic assets
- Flexibility enables resilience in the face of evolving threats
- Enables transition while standards are still evolving
- Policy-driven updates reduce manual effort
- Supports controlled rollback of cryptographic changes
- Crypto-agnostic design abstracts cryptographic details from developers

Open Challenges

Challenges in Achieving Crypto-Agility

- Conceptual fragmentation → no unified definition
  - Vertically across abstraction layers
  - Horizontally across stakeholders
- Lack of standardized design for abstraction layers
  → Heterogeneous implementations
  → Interoperability challenges
- Lack of methodologies for incremental adoption
- Increased architectural complexity
  → Potential expansion of the attack surface



Summary

Key Takeaways

- The PQC transition highlights fundamental challenges in current cryptographic practices
- Crypto-agility provides a structured approach to managing cryptographic change
- Flexibility in cryptographic mechanisms enables long-term resilience
- Achieving crypto-agility introduces its own set of technical and organizational challenges
- PQC transition is a multi-year enterprise-level challenge
  $\rightarrow$ Preparation should start now

Beyond the Limits of PQC

VTT

BUSINESS FINLAND

beyond the obvious

Markus Rautell
markus.rautell@vtt.fi
+358 50 531 5094

@VTTFinland

www.vtt.fi
www.pqc.fi
Playbook