Lessons Learned from Constructing Estonia's PQC Migration Roadmap

Jelizaveta Vakarjuk

What This Talk Covers

- Not a roadmap walkthrough – it's the construction story
- Practical constraints, difficulties, and blind spots that shaped the design
- Two sides:
  - struggles with PQ migration at large scale
  - challenges in writing the roadmap itself
- What we'd tell ourselves if we would need to do it again



Our approach

LITERATURE

Identified gaps in existing roadmaps



REPEATING INFO

Many repeating and generic information

GENERIC STEPS

Not going into details about actual execution

Our approach

LITERATURE

Identified gaps in existing roadmaps



REPEATING INFO

Many repeating and generic information

GENERIC STEPS

Not going into details about actual execution

OUR GOAL

We can do better… Or can we actually?

Public sector organisations

TOTAL

≈ 2200 organisations

LONG LIVED COMPONENTS

NO SYSTEM DOCUMENTATION

LEGACY COMPONENTS

OUTSOURCED COMPONENTS

MODERN SERVICES

EMBEDDED DEVICES

The main lesson

01
PQC migration is not only a cryptographic challenge

02
PQC migration is an organisational and governance challenge

03
Unrealistic to provide detailed, system-specific instructions to every organisation

Unawareness

PROBLEM

“Maybe ECDSA is still secure?” and “PQC standards are not ready yet”

- Many organisations simply don’t know that PQC migration applies to them
- Incomplete visibility into organisation own cryptographic assets
- Cryptography awareness levels vary wildly across sectors

Unwillingness

PROBLEM

"I will just use AI to figure everything out"

- Security awareness mostly emerges after an incident
- How do you secure funds to protect against a potential future threat?
- No quantum computer has broken RSA yet, urgency is hard to communicate
- Competing priorities: operational cost, compliance, business as usual

Vendors Will Handle It

PROBLEM

"It will eventually be handled automatically by vendors, we will be fine"

- Cryptography is too embedded into different layers of systems for full automation
- Even with vendor patches someone must validate, configure, test updated systems
- Every system owner must take some action during PQC migration

Crypto Management is Complex

PROBLEM

“I don’t know how to perform cryptographic inventory”

- Compiling a cryptographic inventory is hard task
- Sometimes, organisations even do not know where to start and what to do
- Protecting code from outside experts doesn’t help

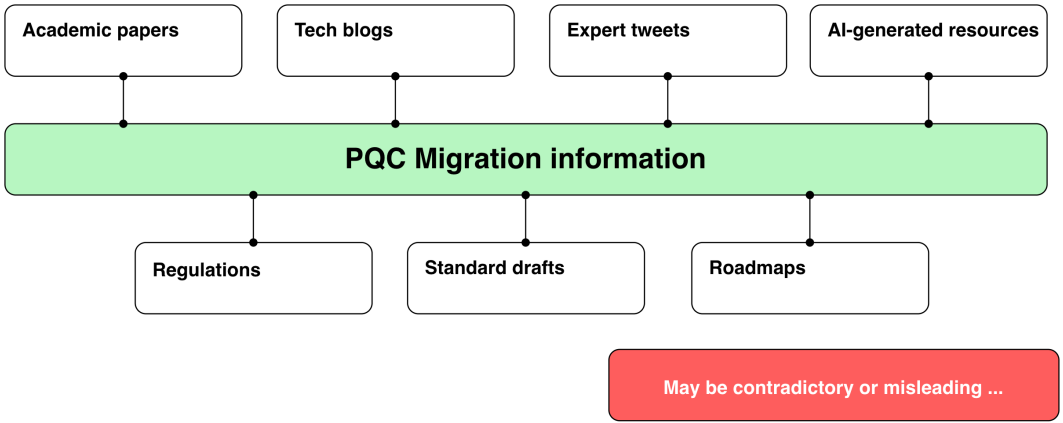
Crypto Management is Complex

PROBLEM

"I don't know how to perform cryptographic inventory"

- Compiling a cryptographic inventory is hard task
- Sometimes, organisations even do not know where to start and what to do
- Protecting code from outside experts doesn't help
- Crypto implementation and engineering is not a common knowledge
- **Yet:** PQC migration means every IT admin/developer must suddenly understand cryptography
- Even a hired expert can't migrate all foreign systems alone

A lot of information ...



... that can be contradictory

"Hybrid modes are super great for backward interoperability"

- yet another PQC migration blog post

... are they really?

"X introduces experimental support for PQC ML-DSA sign and verify functionality. This allows customers to protect data from harvest now decrypt later attacks "

- tech company blog post

... does it?

"Ed25519 curve is designed to be resistant to various types of attacks, including side-channel attacks. Additionally, it is based on 128-bit encryption, which is considered to be strong enough to protect against attacks from modern computational power and potential quantum threats"

- tech company blog post

... hm?

Writing roadmap may be discouraging

PROBLEM

It's impossible to write a roadmap that fits all

- Every organisation's PQC migration experience will be different
- Writing a national roadmap means trying to be simultaneously:
  - Specific enough to be actionable and useful
  - Generic enough to be applicable to all organisations

Shifting Timelines

PROBLEM

Quantum computing research does not stop

- Weeks after roadmap publication: Google and Cloudflare moved deadlines to 2029
- Urgency of migration keeps shifting with new developments
- How to plan a timeline for migration when the clock itself is moving?

IDEALLY

The roadmap must be a living document that can be updated

Keeping It Concise

PROBLEM

No one reads 200+ pages unless truly and fully committed

- Intro and background information about PQC migration takes space, but still should be included as awareness is limited
- Core roadmap should stay simple and navigable
- Detail, examples, checklists can go to appendices
- More visuals - pictures, tables, graphs help

Clearly define roles

- Who is responsible for **coordination** of PQC migration effort?
- Who is responsible for **supervising** the process?
- Who is responsible for making sure nation-scale systems get migrated?

Roadmap is not enough

PROBLEM

The roadmap is just recommendation – no one feels need to follow recommendation

- There should be enforceable document that makes organisation to take actions
- Roadmap itself was focused on the public sector, but private sector should also perform their migration steps

Our approach

RISK ANALYSIS

Identified risks of late migration and risks related to the migration itself



CATEGORISATION

Proposed a way to divide organisations into priority categories

STEPS

Proposed different steps for different priority categories

Our approach

RISK ANALYSIS

Identified risks of late migration and risks related to the migration itself



CATEGORISATION

Proposed a way to divide organisations into priority categories

STEPS

Proposed different steps for different priority categories

RESULTS

We did not get rid of generic and repeating information

Thank you!

- Questions?

cybernetica
Cybernetica
cybernetica_ee
Cybernetica