Transition plan to post-quantum cryptography in Estonia?

Tõnis Reimo

DISCLAIMER:

Following presentation represent my personal views and shall not considered official statement of any public institution.

EU approach …

EU coordination is crucial but MMSS lead

	United States	European Union	EU member states
Standardisation process	Since 2016 (NIST). Standardisation finished by 2024.	Ongoing: no clear results. Likely to follow NIST standards.	Participate in NIST and European standardisation efforts.
Quantum cybersecurity agenda	2022 Quantum Cybersecurity Preparedness Act. 2023 National Cybersecurity Strategy.	No	No
Roadmap to quantum-proof systems	2022 NSM-10 and M-23-03 (White House). 2022 Quantum Cybersecurity Preparedness Act.	No	Some
Support for quantum-safe technologies	National Quantum Initiative. 2023 Quantum Sandbox for Near-Term Applications.	2022 Ultra Secure Connectivity Programme. EU Quantum Flagship EuroQCI Horizon Europe.	All member states are part of the EuroQCI network. 12/27 have national quantum programmes in the form of direct strategic state-led R&D programmes, or national strategies.

… and Member States strategy

- National level quantum computing strategies should address **risks (encryption)** and **gains (quantum simulation)**.
- Comprehensive strategy should encompass a holistic and multi-tier approach to infrastructure, policy, education, and international cooperation - not just upgrading current cryptographic methods.
- **This presentation speculates about potential structure of one Member State strategy of migration to quantum proof systems.**

0. Raising Awareness and Building Support

- **Awareness**
  How get a message through to decision-makers on quantum computing-related risks and garner their support to address them?
- **Strategic Priorities**
  - **Strategy:** Develop a comprehensive approach for quantum computing risk management.
  - **Planning:** Outline detailed plans for risk mitigation.
  - **Budget:** Allocate appropriate resources for quantum security initiatives.
  - **Competencies:** Ensure the organization has the necessary skills and expertise.

1. Assessment of Vulnerabilities:

Begin by conducting a thorough assessment of existing systems to identify vulnerabilities that could be exploited by quantum computing.

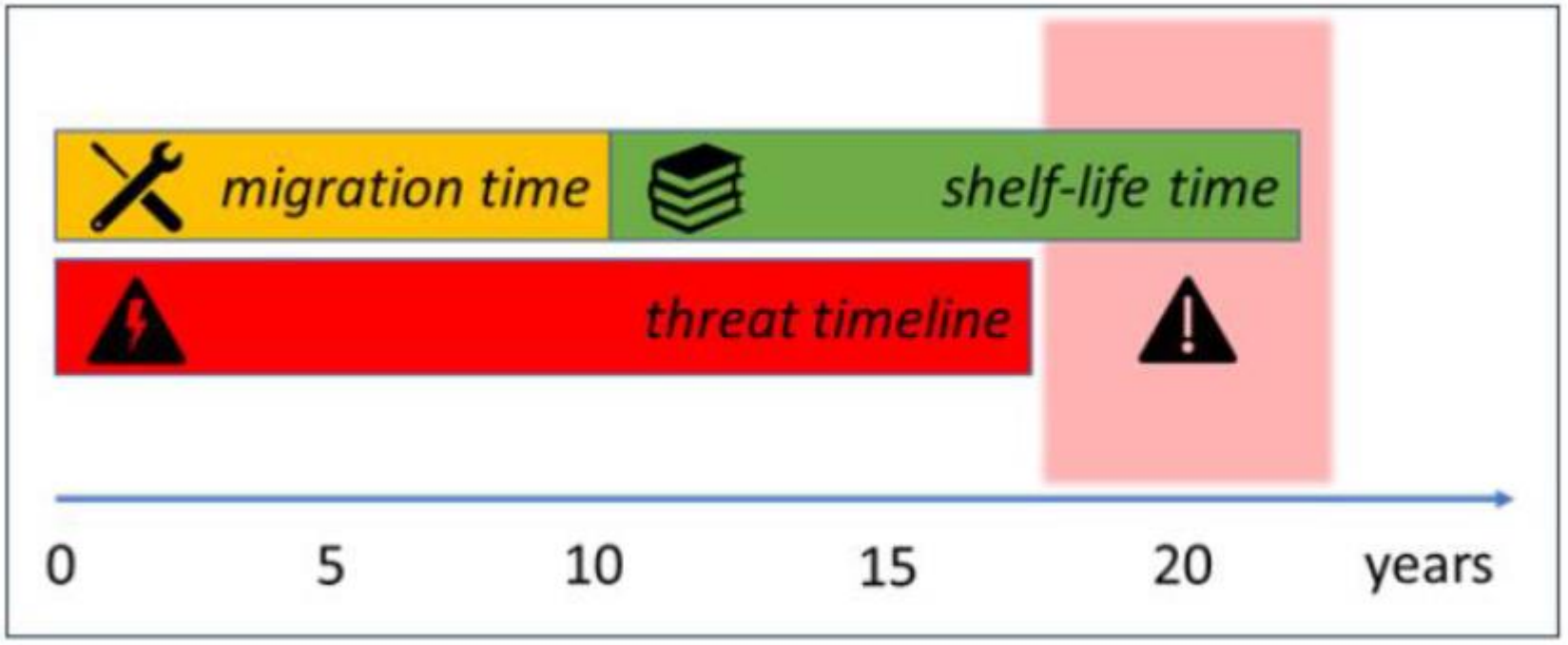
- critical infrastructure and services,
- communication networks,
- data storage facilities

1.2. Risk based prioritization

- The Quantum threat to cryptography can impact Santander in different areas and applications. Actions will span a multiyear timeframe (10-15 years) and need to be prioritized.
- Risk-based priotization will ensure that most relevant use cases will be addressed earlier.
- The following table shows how the risk analysis can be executed. The table features minimum feature relevance as 1 and maximum as 5. The risk is evaluated as a multiplication of the value of all features.

Dimension	Use Case	Time validity	External availability	Sensibility	Risk
Confidentiality	Public websites encryption with TLS	1	5	5	25
	Internal access to servers using SSH	2	1	3	6
	Teleworking using VPNs	3	3	5	45
	Site to site VPNs using IPSEC	5	3	5	75
	Encryption of data at rest on premises (disks, backups...).	5	2	3	30
	Encryption of data at rest in the cloud	5	3	5	75
Authentication	Public digital certificates	2	5	5	50
	Internal digital certificates	2	1	4	8
Legal History	Digital signatures in contracts	5	4	5	100

1.3. More considerations about time.



https://globalriskinstitute.org/publications/quantum-threat-timeline-report-2020/

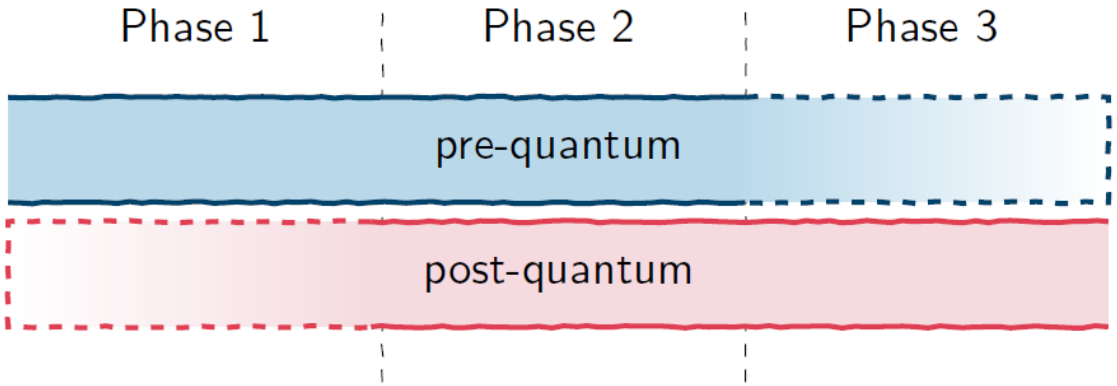
2. Adoption of Quantum-Resistant Cryptography:

- Aiming **interoperability and based on international standards.**
  - NIST (National Institute of Standards and Technology) standards of quantum-resistant algorithms.
  - SOG-IS ACM will be part of EU CSA Schemes.
- Implementation requires much more though…

3. Infrastructure Upgrade:

Upgrade existing hardware and software infrastructure to support the implementation and operation of quantum-resistant algorithms. This may involve significant investment in new technology and the retrofitting of existing systems.

- quantum key exchange – skepticism in other member-states
- **standardization, interoperability and support from software libraries.**
- multi-tier process, requires crypto agility and hybrid use of existing and postquantum protocols



4. Policy and Legislation:

Develop and implement policies and legislation that mandate the use of quantum-resistant technologies in critical sectors. This should include standards for quantum-proofing new technologies before they are deployed.

- **EU level regulations will catch up … eventually**
- Changes in standards will become mandatory in conformity assessments.
- Non-PQC solutions may not get certified.

Eventually doing nothing will not be sustainable strategy.

5. Education and Training, R&D, PR:

- Invest in research and development to have a practical understand of potential future threats posed by quantum computing.
  - defensive measures against quantum attacks
  - the exploration of quantum computing for national interests.
- Update educational and professional programs: Educate and train the specialists in quantum information science and quantum-resistant technologies.
- Targeted awareness campaigns about the importance of quantum-proofing national infrastructures.

6. International Cooperation:

- International cooperation: standardization, competence sharing to gain better insight about development of the PQC field.
- Internet, ICT products and systems are global, international collaboration will be critical for effective defense against quantum threats.

7. Public-Private Partnerships:

Private sector must be involved to leverage the strengths and resources in developing and implementing quantum-proof technologies.

- Training of private sector to be able provide needed competencies and technical solutions
- **Training and education of software integrators and administrators will become crucial at implementing quantum proof solutions.**
- Market research to have a comprehensive overview about qualified quantum proof solutions and products

8. Continuous Monitoring and Adaptation:

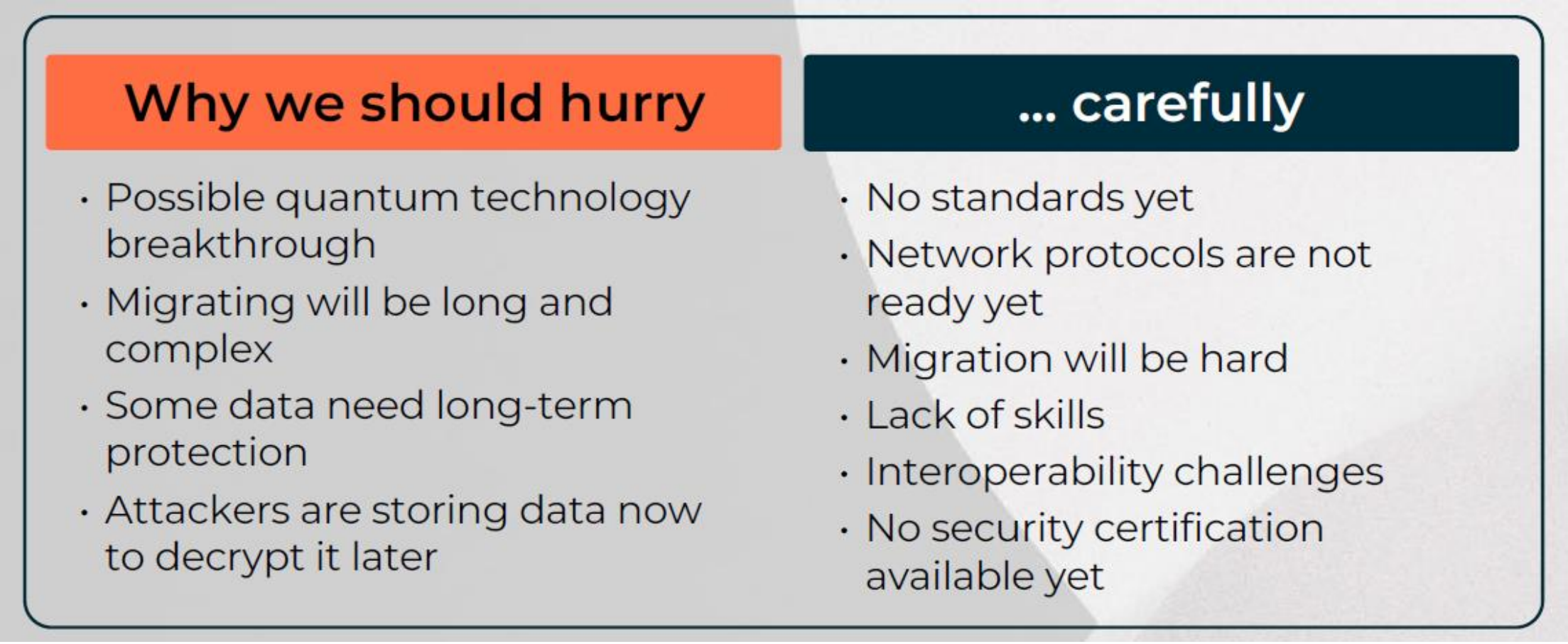
Define roles and establish a system for continuous monitoring of quantum computing developments and threats.

- The strategy should be adaptable to incorporate new technologies and countermeasures as quantum computing evolves.

9. Incident Response Planning:

Develop quantum-specific incident response plans to quickly and effectively respond incidents that may occur during or after the transition.

Festina Lente - Hurry slowly?




Thank You
Tänan