Migration roadmaps and PQC standards
A European perspective

Tanja Lange

Eindhoven University of Technology, the Netherlands
and
Academia Sinica, Taiwan

15 July 2026
AsiaPQC

Who am I?

- Professor in Eindhoven (NL), Department Math & CS.
- Trained mathematician & cryptographer (also minor in physics).
- Co-organizer PQCrypto 2006: International Workshop on Post-Quantum Cryptography (held at KU Leuven, Belgium, part of EU project ECRYPT). Now chair of PQCrypto Steering Committee.

- Coordinated PQCRYPTO EU project (2015 – 2018) ;
- Coordinating PQCSA EU coordinated support action.
- Expert for NEN (NL standardization body), co-editor in ISO SC27/JTC1 WG2, expert for ISO TC68/SC2 WG11 and CCSDS.
- Submitter of Classic McEliece, NTRU Prime, and SPHINCS+ to NISTPQC.
- Co-authored two ENISA studies on PQC 2021 and 2022.
- Many reports on ePrint and project pages.

Store now, decrypt later

Urgency of moving to post-quantum cryptography

White House briefing urges move to PQC.
Deadline: 2035.

2024 EU PQC transition roadmap (link)

COMMISSION RECOMMENDATION

of 11.4.2024

on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography

(5) Member States should consider migrating their current digital infrastructures and services for public administrations and other critical infrastructures to Post-Quantum Cryptography as soon as possible, inducing a fundamental shift in cryptographic algorithms, protocols and systems. As highlighted in the Commission's recent White Paper "How to master Europe's digital infrastructure needs", this requires a coordinated effort involving government agencies, standardization bodies, industry stakeholders, researchers and cybersecurity professionals.

(9) Member States and the Union should continue to cooperate actively with their international strategic partners in the development of international standards in Post-Quantum Cryptography with a view to ensuring interoperability of communications going forward.

27 Nov 2024: Joint statement by 17 EU countries (link)

Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography

To this end, a Work Stream on PQC, co-chaired by France, Germany and the Netherlands, has been created as part of the NIS Cooperation Group following a recommendation [9] of the European Commission. **We encourage active engagement from all EU member states in this work stream** throughout the process of preparing a roadmap for the transition to Post-Quantum Cryptography to ensure the quantum resilience of the European Union's digital infrastructures.

[..]

27 Nov 2024: Joint statement by 17 EU countries (link)

Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography

To this end, a Work Stream on PQC, co-chaired by France, Germany and the Netherlands, has been created as part of the NIS Cooperation Group following a recommendation [9] of the European Commission. **We encourage active engagement from all EU member states in this work stream** throughout the process of preparing a roadmap for the transition to Post-Quantum Cryptography to ensure the quantum resilience of the European Union's digital infrastructures.

[..]

we recommend that these should be protected against 'store now, decrypt later' attacks as soon as possible, latest by the end of 2030. Moreover, we also recommend to develop detailed transition plans for public-key infrastructure systems in the same timeframe.

Australian Government

Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre

Information Security Manual

Last updated: December 2024

Guidelines for Cryptography

Disallows pre-quantum by 2030

23 Jun 2025. 1st NIS2 PQC work stream roadmap (link)

A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography

The EU Member States, supported by the Commission, issued a roadmap and timeline to start using a more complex form of cybersecurity, the so-called post-quantum cryptography (PQC).

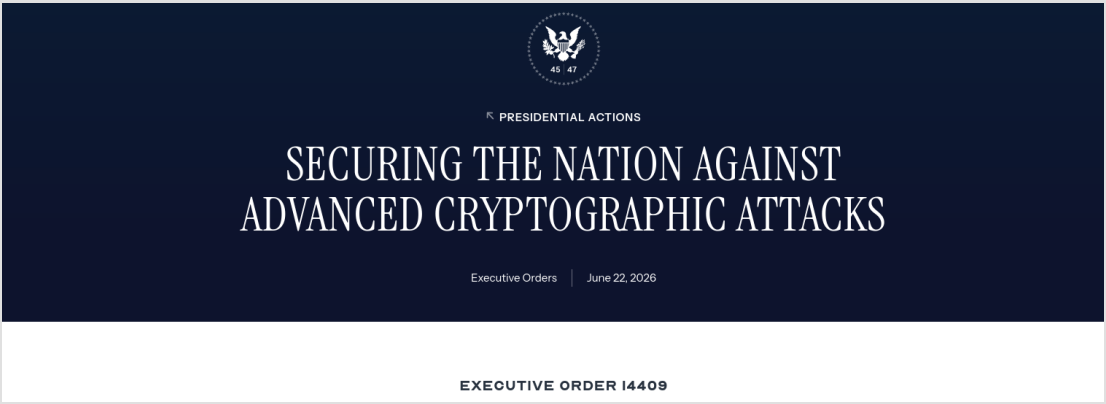
Quantum computing has been identified as a threat to many cryptographic algorithms used to protect the confidentiality and authenticity of data. This threat can be countered by a timely, comprehensive and coordinated transition to Post-Quantum Cryptography (PCQ).

AdobeStock © ipopba

Timeline for the transition to PQC

1. By **31.12.2026**:
   - At least the *First Steps* have been implemented by all Member States.
   - Initial national PQC transition roadmaps have been established by all Member States.
   - PQC transition planning and pilots for high- and medium-risk use cases have been initiated.
2. By **31.12.2030**:
   - The *Next Steps* have been implemented by all Member States.
   - The PQC transition for high-risk use cases has been completed.
   - PQC transition planning and pilots for medium-risk use cases have been completed.
   - Quantum-safe software and firmware upgrades are enabled by default.
3. By **31.12.2035**:
   - The PQC transition for medium-risk use cases has been completed.
   - The PQC transition for low-risk use cases has been completed as much as feasible.

22 Jun 2026 US White House executive order (link)



Sec. 4. Accelerating the PQC Transition. (a) Within 30 days of the date of this order, each agency head shall identify its PQC migration lead and provide the name and contact details of the PQC migration lead to the Director of OMB and the National Cyber Director.

(b) Within 90 days of the date of this order, the Director of OMB shall, in consultation with the Secretary of Homeland Security through the Director of CISA and the National Cyber Director, and consistent with 6 U.S.C. 1526(c), issue guidance requiring each agency to:

(i)
Sy

(ii)
De

(iii
December 31, 2031; and

(ii) transition all HVAs and high impact systems to use PQC for key establishment by December 31, 2030;

(iii) transition all HVAs and high impact systems to use PQC for digital signatures by December 31, 2031; and

(iv) develop and submit to the Director of OMB and the National Cyber Director a plan to accomplish this directive.

(c) Within 180 days of the date of this order, the Secretary of Commerce, through the Director of NIST, shall initiate a pilot project for PQC migration on an appropriate subset of information systems owned or operated by NIST, to be completed no later than December 31, 2027.

Sec 6 – non-FIPS == lack of encryption?!

(c) Within 180 days of the date of this order, the Federal Acquisition Regulatory Council (FAR Council), in consultation with the Secretary of Homeland Security through the Director of CISA and the Director of NIST, shall publish a proposed rule amending the Federal Acquisition Regulation (FAR) to require covered contractors to comply by December 31, 2030, with NIST's FIPS, including all applicable FIPS incorporating PQC compliant algorithms.

(d) Within 270 days of the date of this order, the FAR Council, in consultation with the Secretary of Homeland Security through the Director of CISA and the Director of NIST, shall publish a proposed rule amending the FAR requirements and contract clauses for contractor vulnerability disclosure programs to ensure that covered contractors implement vulnerability disclosure policies (VDPs), consistent with NIST guidelines, and that VDPs incorporate reports of cryptographic vulnerabilities, including testing for lack of encryption and the use of non-FIPS approved algorithms.

Standardization of PQC

- Stateful hash-based signatures:
  RFC 8391 XMSS and RFC 8554 LMS in CFRG, NIST SP 800-208 (also XMSS and LMS), ISO SC27 JTC1 WG2 14888-4.
- FIPS standards for
  - FIPS 203 ML-KEM (Kyber), based on lattices
  - FIPS 204 ML-DSA (Dilithium), based on lattices
  - FIPS 205 SLH-DSA (SPHINCS+), based on hash functions
- Falcon and HQC selected by NIST, more signatures in on ramp.
- For IETF and IRTF see previous talk.
- ISO 18033-2 Asymmetric ciphers, Amendment 2 published 5 June 2026. Covers Classic McEliece, FrodoKEM, and Kyber/ML-KEM.
- ISO 29192-4 Lightweight cryptography Amendment 2 in DAmd stage. Will cover NTRU.
- ISO 14888-6 Stateless hash-based mechanisms (in CD stage).
- ISO 14888-5 Lattice-based mechanisms (upcoming).

ECCG Agreed Cryptographic Mechanisms

- EUCC Guidelines on Cryptography has open consultation till end of July on ECCG Agreed Cryptographic Mechanisms - version 3 - draft for public review.
- Guidelines prepared by ECCG subgroup on cryptography. These are the security agencies of EU countries.
- Relevant for: Common Criteria-based Cybersecurity Certification Scheme (EUCC).

Primitive	Scheme	R/A	Notes
FF-DLOG	DH [SP800-56A, ISO11770-3]	A	60-KE-Auth, 61-DHSubgroupAttacks 62-QuantumThreat
	DLIES-KEM [ISO18033-2]	A	
EC-DLOG	EC-DH [SP800-56A, ISO11770-3]	A	60-KE-Auth, 61-DHSubgroupAttacks, 62-QuantumThreat
	ECIES-KEM [ISO18033-2]	A	
	X25519, X448 [RFC7748]	A	60-KE-Auth, 62-QuantumThreat
LWE	ML-KEM [FIPS203]	R	60-KE-Auth, 63-Hybridization, 64-ML-KEM Parameters
	FrodoKEM [FRODO-KEM]	R	60-KE-Auth, 63-Hybridization, 65-FrodoKEM Parameters

Where to go from here?

- Some deployment needs interoperability and agreements/standards.
  But much data and traffic could be protected now already.

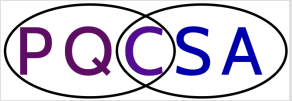
Where to go from here?

- Some deployment needs interoperability and agreements/standards.
  But much data and traffic could be protected now already.
- PQConnect `https://www.pqconnect.net/` ready-to-use software for adding extra PQC layer.
- Migration needs testing phase and safety nets.
  Dangerous to remove pre-quantum crypto now & no harm keeping.
- Several recommendations available already, to highlight two from the European Union Agency for Cybersecurity (ENISA)
  - Current state and quantum mitigation
  - Post-Quantum Cryptography – Integration study
- TNO, AIVD, CWI (all NL) The PQC Migration Handbook
- Several positive signs of awareness and progress in migration, but much more work needed.

Where to go from here?

- Some deployment needs interoperability and agreements/standards.
  But much data and traffic could be protected now already.
- PQConnect `https://www.pqconnect.net/` ready-to-use software for adding extra PQC layer.
- Migration needs testing phase and safety nets.
  Dangerous to remove pre-quantum crypto now & no harm keeping.
- Several recommendations available already, to highlight two from the European Union Agency for Cybersecurity (ENISA)
  - Current state and quantum mitigation
  - Post-Quantum Cryptography – Integration study
- TNO, AIVD, CWI (all NL) The PQC Migration Handbook
- Several positive signs of awareness and progress in migration, but much more work needed.
- New EU project PQCSA on migration and standardization (started January 2025). `https://www.pqcsa.eu/`

WP3: Migration roadmap



This work package drafts the roadmap for migration to post-quantum cryptography. The objectives of this work package are as follows:

- 3.1 Prepare the supply chain for the demand in PQC solutions.
- 3.2 Provide stakeholders with a roadmap of how to migrate to PQC.
- 3.3 Establish that the PQCSA migration to PQC roadmap is fit for purpose.
- 3.4 Demonstrate that the versatility of the PQCSA migration to PQC roadmap on at least one sector.

Links to further information

- PQCSA deliverables (so far)
  - D1.1 Survey of PQC algorithms
  - D1.3 Hot Topics and Op en Problems in Post-Quantum Cryptography
  - D2.1 Survey of PQC protocols
- NIST PQC competition.
- Quantum Threat Timeline 2019; updates from 2021, 2022, 2023, 2024, and 2025.
- Status of quantum computer development (by German BSI).
- ENISA studies: Post-quantum cryptography: Integration study, Post-quantum cryptography: current state and quantum mitigation
- YouTube channel Tanja Lange: Post-quantum cryptography.
- PQCRYPTO summer school with 21 lectures on video; slides; exercises.
- Less math, more perspective: Executive school I and Executive school II.
- pqcrypto.org overview page by D.J. Bernstein & T. Lange.
- PQCrypto 2016, 2017, 2018, 2019, 2020, 2021, 2022, 2023, 2024, 2025, 2026.
- PQCRYPTO project (ended in 2018, but still lots of useful resources).
- PQConnect ready-to-use tunnel, adding extra PQC layer.