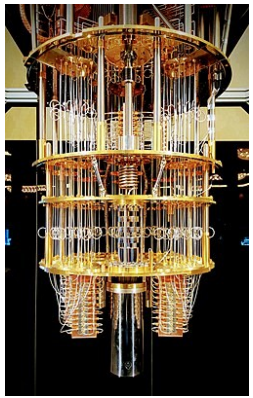
Bundesministerium
des Innern

EU-Roadmap für die Umstellung auf Post-Quanten-Kryptografie

Omnisecure, 19. Januar 2026

Dr. Heike Hagemeier, BMI, Referat CI 2

Bedrohung für Kryptografie durch Quantencomputer



Kryptografisch relevante
Quantencomputer

Aktuell genutzte
Public-Key-Kryptografie wird gebrochen

Gesammelte Daten
sind nun lesbar

Herausforderungen:

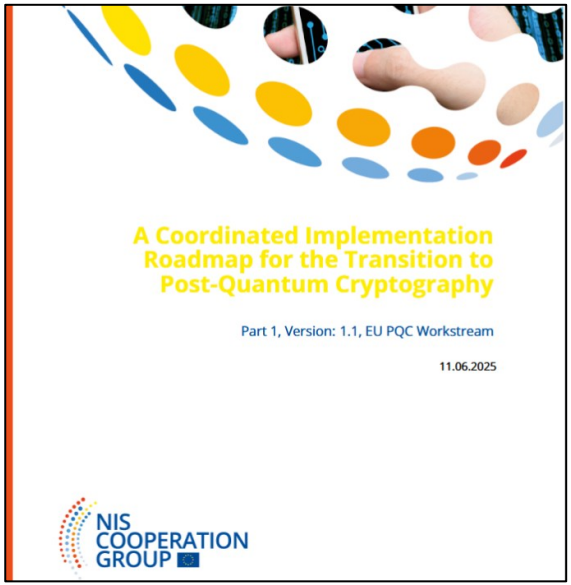
→ nicht quantensicher geschützte Daten können gesammelt und später entschlüsselt werden

→ Umstellung auf quantensichere Kryptografie benötigt viel Zeit

DE, EU: Empfehlungen, Roadmap

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

- Hauptsächliche Zielgruppe: EU Mitgliedstaaten
- Empfehlungen aber auch für Organisationen anwendbar
- Vorschlag für einen umfassenden Ansatz für die Mitgliedstaaten, um die Umstellung zu starten.
- Empfehlungen sind aufgeteilt in “First Steps”, die für den Beginn der Umstellung kurzfristig durchgeführt werden sollten, und im Anschluss durchzuführende “Next Steps”.
- Enthält einen groben Zeitplan für die Umstellung



Empfehlungen aus der Roadmap

Erste Schritte	Nächste Schritte
• Krypto-Inventarisierung • Risikoanalyse • Stakeholder identifizieren und einbinden • Awareness- Programm • Nationale Zeitpläne und Umsetzungsplan • ….	• Kryptoagilität und quantensichere Update-Mechanismen • Ressourcen für die Umstellung einplanen • Anpassung der Zertifizierungsverfahren • Regulierung anpassen • …

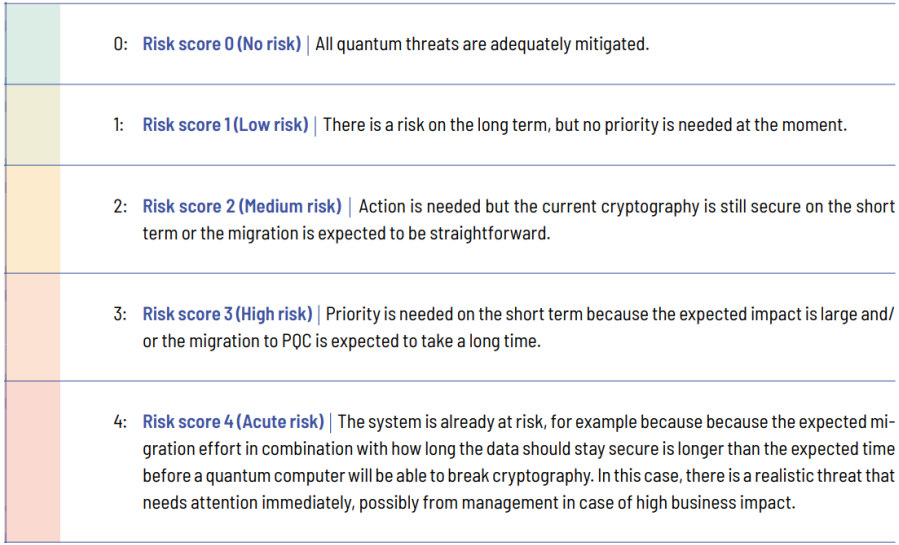
Zeitpläne für die Umstellung

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.

Einschätzung des Quantenrisikos

- Basiert auf dem Bewertungssystem des „PQC Migration Handbook“ von NL.
- 3 Faktoren sind zu berücksichtigen:
  - Angreifbarkeit der eingesetzten kryptografischen Verfahren,
  - Erwartete Auswirkung bei Bruch der Verfahren,
  - Benötigte Zeit für die Umstellung auf quantensichere Lösungen.
- Aus den Punkten für die einzelnen Faktoren wir die Risikoklasse errechnet.



0: **Risk score 0 (No risk)** | All quantum threats are adequately mitigated.

1: **Risk score 1 (Low risk)** | There is a risk on the long term, but no priority is needed at the moment.

2: **Risk score 2 (Medium risk)** | Action is needed but the current cryptography is still secure on the short term or the migration is expected to be straightforward.

3: **Risk score 3 (High risk)** | Priority is needed on the short term because the expected impact is large and/or the migration to PQC is expected to take a long time.

4: **Risk score 4 (Acute risk)** | The system is already at risk, for example because because the expected migration effort in combination with how long the data should stay secure is longer than the expected time before a quantum computer will be able to break cryptography. In this case, there is a realistic threat that needs attention immediately, possibly from management in case of high business impact.

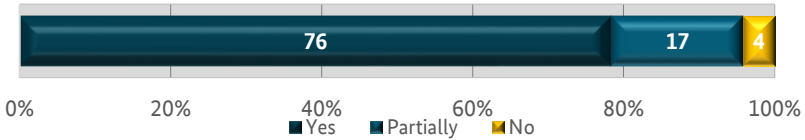
Quantum risk score following [17]	Quantum Risk Level in this document
1	low
2	medium
3 – 4	high

Umfrage zur Roadmap

Überblick für die Rückmeldungen

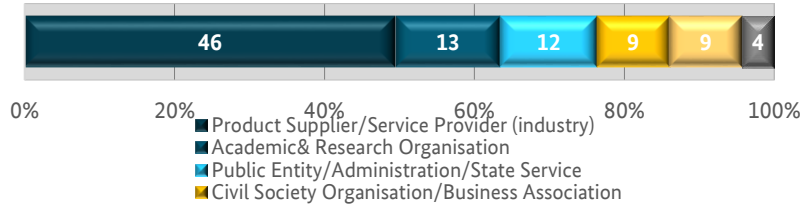
Review des Dokumentes

- 93 Rückmeldungen; 96% haben Roadmap ; 17 davon teilweise.



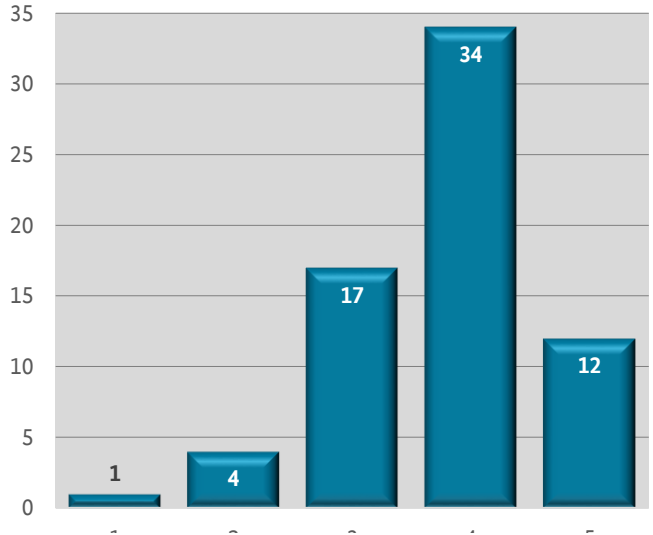
Organisationen

- Fast die Hälfte der Rückmeldungen kam von Produkt-herstellern or Service Providern aus der Industrie.



- **Skala 0 bis 5, wobei:**

gar nicht klar
sehr klar und umsetzbar



Feedback aus der Umfrage

Welche Teile der Roadmap benötigen Verbesserungen/Klarstellungen?

Analyse der Rückmeldungen

- 63 Rückmeldungen gaben Feedback zu möglichen Verbesserung/Klarstellungsbedarf → FAQ wird erstellt
- Folgende Themen:

  - ✓ Quantum Risk Estimation, Milestones, Prioritization,
  - ✓ Hybrid
  - ✓ Milestones, First steps, Next steps
  - ✓ National Roadmaps
  - ✓ EU
  - ✓ Other

Auswahl von Fragen aus FAQ

Q. How does the EU Roadmap on PQC relate to EU legislation such as NIS 2, CRA, GDPR, CSA, DORA?

Q. What resources are available from EU institutions to support the implementation of PQC solutions?

Q. Is symmetric cryptography impacted by CRQCs? And if so, does that change prioritisation?

Q. Which aspects of the EU Roadmap should be included in a national roadmap?

Q. What does “mature cryptographic asset management mean”?

Q. Is the use of hybrid cryptographic schemes combining several public-key cryptographic schemes seen as a long-term or a short-term strategy?

Q. Will or can the workstream publish additional sector specific guidance?

Q. How is the threat posed by “harvest now, decrypt later” attacks covered by the risk model presented in Section 5 “Estimating the quantum risk?”

Q. Do the “First Steps” need to be completed before moving on to the “Next Steps”?

Proposal for Contribution

- 46 Rückmeldungen haben einen Vorschlag für einen Beitrag eingereicht, 37 davon mit Abstract.
- Vorgeschlagene Themen u.a. hybride Lösungen, Standards, sektorspezifische Roadmaps, Lightweight PQC, konkrete Maßnahmen, Anwendungsfälle, ...
- Geplantes weiteres Vorgehen:
  - Meeting mit Autoren der vielversprechendsten Einreichungen
  - Bildung von Arbeitsgruppen zu 2-3 ausgewählten Themen
  - Ziel: gemeinsame Publikation (in 2026)
- Vorbild: NIST NCCoE Publikation SP 1800 38 “Migration to Post-Quantum Cryptography”

Maßnahmen zur Umstellung auf Post-Quanten-Kryptografie

Inventarisierung

- Betroffene Verfahren ermitteln
- Sensibilität bewerten
- Abhängigkeiten klären

Priorisierung

- Aufwand und Schadenspotential abwägen
- Dauer der Migration berücksichtigen

Umsetzung/Planung

- Verantwortlichkeiten festlegen
- Ressourcen bereitstellen
- Ad-hoc-Maßnahmen sofort umsetzen

BSI und CI erarbeiten (in Abstimmung mit BMDS)
eine nationale Roadmap zur Umstellung auf quantensichere Kryptografie

Vielen Dank für die Aufmerksamkeit!

Kontakt

Bundesministerium des Innern
Referat CI 2 – Internationale Cybersicherheit und Cybersicherheitsforschung
Alt-Moabit 140
10557 Berlin

Ansprechpartnerin
Dr. Heike Hagemeier
heike.hagemeier@bmi.bund.de
www.bmi.bund.de
Tel. +49 30 18681 13318

Bundesministerium des Innern und für Heimat