PQ-Migration – jetzt!

Dr. Inga Paul, Referat V 31 – Grundlagen kryptographischer Verfahren

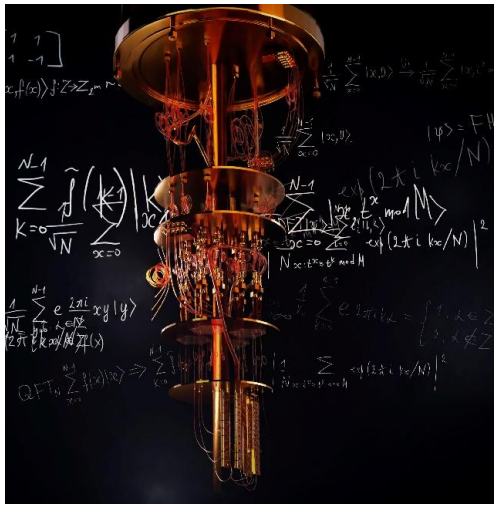
Bundesamt
für Sicherheit in der
Informationstechnik

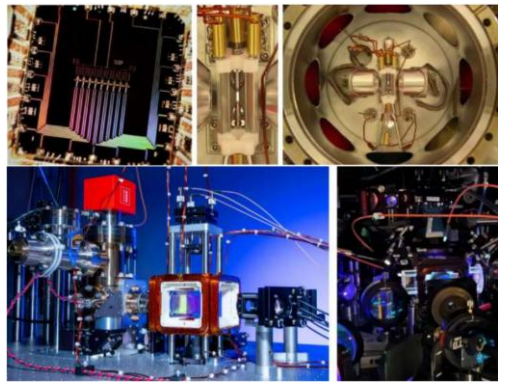
Omnisecure Berlin

20. Januar 2026

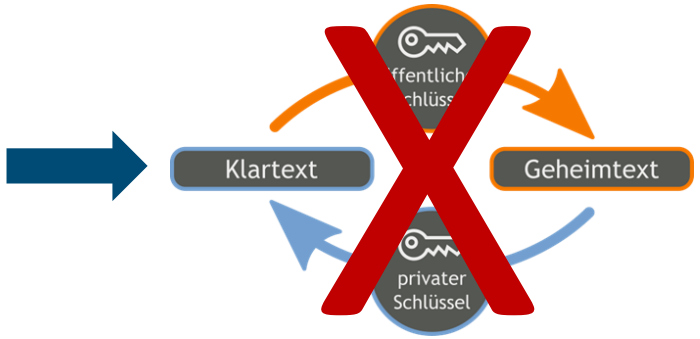
Warum beschäftigen wir uns mit quantensicherer Kryptographie?

Quantencomputer





Shors Algorithmus

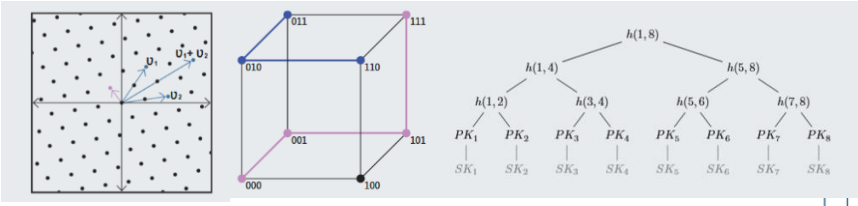


Derzeit eingesetzte Public-Key-Kryptographie

Post-Quanten-Kryptographie

HQC Classic McEliece

Mathematische Grundlagen



Gitter Codes Hashbäume

Die drei Phasen der PQ-Migration

Was muss jetzt getan werden?

Rahmenverantwortung: Steuerungsgremium aufsetzen

Inventarisierung

- Welche Verfahren verwenden Kryptografie?
- Sensibilität der Daten, Lebensdauer
- Abhängigkeiten

Priorisierung

- Abwägung: Kosten der Migration vs. Schäden bei gebrochener Sicherheitsleistung → **Risikoorientierte Priorisierung**
- Wie lange dauert die Migration?

Umsetzung/ Planung

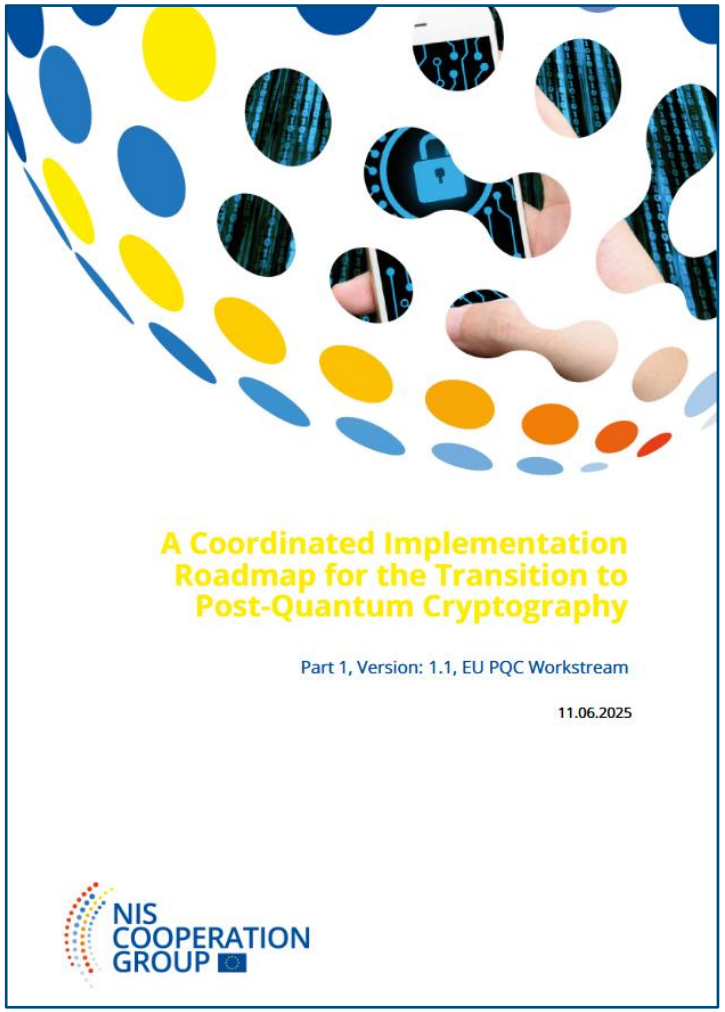
- Programmsteuerung aufsetzen
- **Verantwortlichkeit festlegen**, Kosten einkalkulieren
- Nötige ad-hoc-Maßnahmen sofort umsetzen

Rücksprache mit Dienstleistern, Softwarelieferanten, bei Einkauf auf **Kryptoagilität** achten etc.

(Internationale) Absprache mit Partnern

Zeitplan für PQ-Migration in der EU

Die EU-Roadmap



Inventarisierung, Priorisierung, Umsetzungsplanung

Pilotprojekte starten

Nationale Roadmap erstellen

2026

2030

Hochrisiko-Anwendungsfälle sind migriert

Soft- und Firmwareupdates quantensicher

2035

Anwendungsfälle mittleren Risikos sind migriert

Zeitpläne für PQ-Migration im BSI

Bild: © AdobeStock/Azazul

Nationale Zeitpläne

Gemeinsames Ziel: Hochsensitive Daten sind bis 2030 quantensicher geschützt

Leitlinie für die nationale Umsetzung der EU-Roadmap

Technische Richtlinie TR-02102

Zeitplan für die Migration von VS-IT (VS-NfD)

Nationale Zeitpläne

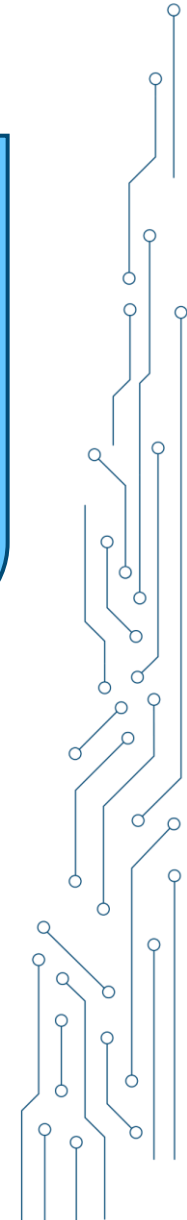
Gemeinsames Ziel: Hochsensitive Daten sind bis 2030 quantensicher geschützt

Leitlinie für die nationale Umsetzung der EU-Roadmap

- In Erstellung durch BMI und BSI
- Bestätigt die Fristen aus der EU-Roadmap

Zeitplan für die Migration von VS-IT (VS-NfD)

Technische Richtlinie TR-02102



Nationale Zeitpläne

Gemeinsames Ziel: Hochsensitive Daten sind bis 2030 quantensicher geschützt

Leitlinie für die nationale Umsetzung der EU-Roadmap

- In Erstellung durch BMI und BSI
- Bestätigt die Fristen aus der EU-Roadmap

Zeitplan für die Migration von VS-IT (VS-NfD)

- 2030: Schlüsselaustausch und Updatesignaturen quantensicher
- 2031: Signaturen quantensicher
- 2031: Rollout quantensicherer PKI-Zertifikate

Technische Richtlinie TR-02102

Nationale Zeitpläne

Gemeinsames Ziel: Hochsensitive Daten sind bis 2030 quantensicher geschützt

Leitlinie für die nationale Umsetzung der EU-Roadmap

- In Erstellung durch BMI und BSI
- Bestätigt die Fristen aus der EU-Roadmap

Zeitplan für die Migration von VS-IT (VS-NfD)

- 2030: Schlüsselaustausch und Updatesignaturen quantensicher
- 2031: Signaturen quantensicher
- 2031: Rollout quantensicherer PKI-Zertifikate

Technische Richtlinie TR-02102

- Klassischer Schlüsselaustausch (RSA, ECDH) nur noch bis 2031 empfohlen
- Ausnahme: Einsatz in hybriden Verfahren

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Vielen Dank für Ihre Aufmerksamkeit!

Dr. Inga Paul
inga.paul@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 87
53175 Bonn
www.bsi.bund.de

Follow us:

Bild: © AdobeStock/ The Little Hut

Zeitplan für VS-NfD

Ziel: Umstellung bis 2030

- Zugelassene Produkte müssen ab dem 1.1.2030 quantensichere Verfahren zum Schlüsselaustausch und zur asymmetrischen Verschlüsselung verwenden.
- Zugelassene Produkte müssen ab 1.1.2030 über quantensichere Signaturen für Soft- und Firmwareupdates verfügen.
- Eine PKI muss bis 31.12.2030 quantensichere Zertifikate auf allen Ebenen (Root, Sub-CA, Endnutzer) anbieten.
- Für Authentisierung, die keine PKI benötigt, wird eine Umstellung auf quantensichere Verfahren bis Ende 2030 gefordert.

Position Paper (2024)

- Initiiert von Deutschland (BSI), Frankreich (ANSSI) und den Niederlanden (Innenministerium)
- Unterschrieben von 21 europäischen Mitgliedsstaaten

„To ensure an acceptable level of readiness,
we recommend that [the most sensitive use cases] 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.”

Steuerungsgruppe Quantensichere Kryptographie

Inventarisierung, Priorisierung und Maßnahmenplanung für PQ-Migration im Gestaltungsbereich des BSI

- **Technische Richtlinien, Schutzprofile, Anforderungskataloge, …**
- **Gremienarbeit, Zertifizierung und Zulassung**