Bundesministerium des Innern
Bundesamt für Sicherheit in der Informationstechnik

Nationale Umsetzung der EU-Roadmap zur Umstellung auf Post-Quanten-Kryptografie-Gemeinsame Leitlinie von BMDS, BMI und BSI

Inhaltsverzeichnis

Zusammenfassung 2
1. Einführung und Motivation 2
2. Geltungsbereich 5
3. Zeitplan 5
4. Schritte zur Umstellung auf PQC 6
4.1 Fristen verbindlich machen 6
4.2 Einrichtung von Koordinierungsgremien/verantwortlichen Stellen 6
4.3 Inventarisierung kryptografischer Verfahren und Schlüssel 7
4.4 Post-Quanten-Kryptografie als Stand der Technik 7
4.5 Abschätzung des Quantenrisikos und Verankerung im Risikomanagement 8
4.6 Umsetzung und Einbindung der Lieferkette 8
Literaturverzeichnis 10

Zusammenfassung

- Kryptografische Verfahren sind ein Grundpfeiler der Cyber- und Informationssicherheit, doch ihre Wirksamkeit wird durch die Entwicklung leistungsfähiger Quantencomputer bedroht.
- Auf EU-Ebene haben die EU-Mitgliedstaaten unterstützt durch die Europäische Kommission im Juni 2025 eine „Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography“ (im Folgenden kurz EU-Roadmap)[1] veröffentlicht.
- Die vorliegende Leitlinie enthält einen Zeitplan für die Umstellung auf Post-Quanten-Kryptografie (PQC) in Deutschland, der mit der EU-Roadmap in Einklang steht.
- Insbesondere sollten Anwendungsfälle mit hohem Risiko so bald wie möglich auf quantensichere Kryptografie umgestellt werden und die Umstellung für diese Systeme spätestens Ende 2030 abgeschlossen sein. Bis 2035 sollte die Umstellung für so viele Systeme wie möglich abgeschlossen sein.



Abbildung 1: Zeitplan für die PQC-Umstellung

1 Einführung und Motivation

Kryptografische Verfahren zum Schutz der Vertraulichkeit, der Authentizität und der Integrität von Daten sind essentiell in einer digitalen Welt. Dazu gehören beispielsweise digitale Verwaltungsdienste, das Bankensystem und Kommunikationsdienste wie Messaging-Apps. Kryptografie ist zudem von entscheidender Bedeutung, um den sicheren Betrieb von kritischen Infrastrukturen zu gewährleisten.

Wenn die derzeit eingesetzte Kryptografie gebrochen würde, wären die Folgen für unsere digitale und vernetzte Welt verheerend. Die Entwicklung von Quantencomputern stellt eine solche Bedrohung für die Kryptografie dar. Dies ist seit 1994 bekannt, als Peter Shor Quantenalgorithmen veröffentlichte, mit denen viele der verwendeten kryptografischen

[1] https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

Algorithmen gebrochen werden können. Das Fundament unserer digitalen Gesellschaft würde somit zerstört, wenn diese Algorithmen auf einem ausreichend leistungsfähigen Quantencomputer implementiert werden können und nicht rechtzeitig Gegenmaßnahmen umgesetzt würden.

Derzeit gibt es keine Belege dafür, dass Quantencomputer bereits leistungsfähig genug sind, um kryptografische Verfahren zu brechen. Um den aktuellen Entwicklungsstand und die potenzielle künftige Verfügbarkeit von Quantencomputern angemessen bewerten zu können, wurde erstmalig 2017 die Studie „Entwicklungsstand Quantencomputer“[2] im Auftrag des BSI durchgeführt und zuletzt 2025 aktualisiert. Diese aktualisierte Bewertung zeigt, dass es wahrscheinlich ist, dass ein solcher Quantencomputer in maximal 15 Jahren (d. h. bis 2040 oder früher) realisierbar sein wird. Die Grundannahmen der Quantenfehlerkorrektur wurden im Jahr 2024 vollständig verifiziert. Durch weitere Fortschritte im Bereich der Fehlerkorrektur könnte sich der Zeitraum bis zur Verfügbarkeit eines kryptografisch relevanten Quantencomputers sogar deutlich verkürzen. Eine mögliche Beschleunigung der Entwicklung hin zu einem kryptografisch relevanten Quantencomputer ändert grundsätzlich nichts an dem hier beschriebenen Vorgehen, führt jedoch dazu, dass einzelne Maßnahmen entsprechend vorgezogen werden müssten. Sollte die Entwicklung von Quantencomputern überraschende sprunghafte Fortschritte machen, müssen gegebenenfalls auch Anpassungen am Zeitplan vorgenommen werden. Auf Basis einer individuellen Risikoanalyse muss eine klare Priorisierung vorgenommen und ein Notfallplan entwickelt werden. Insbesondere sollten hierbei z.B. quantensichere Software-Update-Mechanismen, quantensichere Schlüsseleinigungsverfahren für Hochrisiko-Anwendungsfälle sowie der frühzeitige Aufbau geeigneter Public-Key-Infrastrukturen berücksichtigt werden.

Parallel zur Entwicklung von Quantencomputern wird seit über zwei Jahrzehnten an kryptografischen Verfahren geforscht, die als resistent gegenüber Angriffen durch Quantencomputer gelten und auf derzeit verwendeten Systemen und handelsüblicher Hardware (keine Quantencomputer) eingesetzt werden können. Die ersten Verfahren der sogenannten Post-Quanten-Kryptografie wurden nach einem mehrjährigen Standardisierungsprozess durch das US-amerikanische National Institute of Standards and Technology (NIST) im Jahr 2024 standardisiert und sind nun einsatzbereit.

Die Umstellung auf Post-Quanten-Kryptografie wird jedoch erhebliche Zeit und Ressourcen erfordern. Nach den Erfahrungen früherer kryptografischer Umstellungen zu urteilen, könnte dieser Prozess einige Jahre in Anspruch nehmen. Daher ist eine gut vorbereitete und systematische Umstellung auf PQC notwendig. Behörden und Organisationen in Deutschland müssen jetzt handeln, um diese Umstellung rechtzeitig abzuschließen.

Im Einklang mit anderen internationalen Organisationen, z.B. der NATO, läuft die Umstellung auf quantensichere Kryptografie im Geheimschutzbereich bereits seit vielen Jahren.[3] Durch die Verfügbarkeit von Standards und die zunehmende Produktverfügbarkeit kann die dringend notwendige flächendeckende Umstellung nun geplant und durchgeführt werden. Bereits 2023 wurde die „Erstellung einer Strategie der Bundesregierung zur Migration zu Post-Quanten-

[2] https://www.bsi.bund.de/qcstudie

[3] „Im Hochsicherheitsbereich agiert die Bundesregierung unter der Arbeitshypothese, dass zu Beginn der 2030er Jahre kryptografisch relevante Quantencomputer zur Verfügung stehen [siehe auch die Bundestagsdrucksache 19/25208, Bundestagsdrucksache. 19/27310 sowie Bundestagsdrucksache 19/26340], und hat den Wandel zur Post-Quanten-Kryptografie eingeleitet.“ [Bundestagsdrucksache 20/14986]

Kryptografie“ im „Handlungskonzept Quantentechnologie“ als Ziel für 2026 verankert. Auch die im Sommer 2025 vorgestellte Hightech Agenda für Deutschland betrachtet neben den Chancen durch Quantencomputer auch das Risiko für „klassische kryptografische Verfahren und damit unsere gesamte Informationsinfrastruktur“.

Die folgenden zwei Szenarien machen eine Umstellung auf PQC besonders dringlich:

- Das Szenario „Store now, decrypt later“, bei dem Angreifer verschlüsselte Daten speichern, um diese zu entschlüsseln, sobald ein kryptografisch relevanter Quantencomputer verfügbar ist. Dies ist eine realistische Bedrohung, wenn die Vertraulichkeit von Daten über einen langen Zeitraum geschützt werden muss (z. B. Verschlusssachen, sensible personenbezogene Daten, Geschäftsgeheimnisse).
- Lange Umstellungszeiten, die bei komplexen Systemen oder Geräten mit langer Lebensdauer auftreten. Selbst wenn ein System nicht vom „Store now, decrypt later“-Szenario betroffen ist, besteht die Gefahr, dass der Übergang auf PQC nicht rechtzeitig abgeschlossen wird. Dies könnte die Vertraulichkeit und Authentizität aller mit diesem System verarbeiteten Daten beeinträchtigen.

Das Bewusstsein für die Notwendigkeit einer Umstellung auf PQC hat in den letzten Jahren deutlich zugenommen, nicht zuletzt durch Initiativen wie die Bundesquantenallianz, in der sich Bundesbehörden und bundeseigene Unternehmen austauschen.

Das BSI weist seit Langem auf die Bedrohung der Cyber- und Informationssicherheit durch Quantencomputer hin und hat frühzeitig Handlungsleitfäden[4] sowie Studien zu quantensicherer Kryptografie veröffentlicht. In den zentralen kryptografischen Empfehlungen des BSI[5] sind bereits seit 2020 konkrete Empfehlungen zu PQC-Verfahren enthalten. Ferner wirkt das BSI aktiv in Standardisierungsgremien, z.B. ISO und IETF, mit. Damit gestaltet das BSI bereits jetzt aktiv den Übergang zu PQC im Rahmen seiner Zuständigkeit.

Über koordinierende Gremien wie den IT-Planungsrat müssen die Vorgaben und Lösungen auch Länder- und Kommunalverwaltungen erreichen, für die BSI-Vorgaben oft nur empfehlenden Charakter haben.

Außerhalb regulierter Bereiche zeichnet sich ein durchmischtes Bild mit großem Handlungsbedarf ab: Während Cybersicherheit zunehmend als Wettbewerbsvorteil erkannt wird, muss gleichzeitig noch die Erkenntnis reifen, dass unabhängig von der Bedrohung durch Quantencomputer der Einsatz veralteter oder verwundbarer Kryptografie als fahrlässig bewertet werden kann und damit ein hohes Risiko für Unternehmen darstellt. Eine Marktumfrage[6] des BSI aus dem Jahr 2023 kommt zu dem Ergebnis, dass fast 90 % der Teilnehmenden schätzen, den Gefährdungen der Kryptografie durch Quantencomputer nicht rechtzeitig begegnen zu können.

[4] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Kryptografie-quantensicher-gestalten.html

[5] https://www.bsi.bund.de/TR-02102

[6] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Marktumfrage_Kryptografie_Quantencomputing.html

2 Geltungsbereich

Das vorliegende Dokument ist eine Leitlinie für die nationale Umsetzung der EU-Roadmap „A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography“ des NIS-Workstreams zu PQC. Gerichtet an Bundes-, Landes- und Kommunalverwaltungen, Organisationen und Unternehmen, insbesondere Betreiber kritischer Infrastrukturen, werden strukturierte Empfehlungen für die Umstellung auf quantensichere Kryptografie ausgesprochen, um einen synchronisierten Übergang in Deutschland zu gewährleisten.

Die empfohlenen Zeitschienen der EU-Roadmap werden übernommen.

3 Zeitplan

Der EU-Roadmap folgend, wird für Deutschland ein risikobasierter Ansatz für die Einführung von quantensicherer Kryptografie empfohlen. Anwendungsfälle werden in die Risikokategorien „hoch“, „mittel“ und „niedrig“ eingestuft und die Umstellung dem Risiko gemäß priorisiert, s. Abschnitt 4.5. Anwendungsfälle mit hohem Risiko sollten bis Ende 2030 quantensicher sein. Analog sollte dies für Anwendungsfälle mit mittlerem Risiko bis Ende 2035 umgesetzt sein.

Bei den meisten Anwendungen sollte die Einhaltung des empfohlenen Zeitplans einen angemessenen Schutz vor der Quantenbedrohung bieten und gleichzeitig einen chaotischen Übergang vermeiden, der zu neuen Schwachstellen durch unzureichend getestete Lösungen führen könnte. Können die empfohlenen Fristen jedoch nicht eingehalten werden, muss das individuelle Risiko bewertet werden.

Meilensteine für die Umstellung auf PQC

1. Zum **31.12.2026**:
   - Vorbereitungsphase: Verantwortlichkeiten und verbindliche Umsetzungspläne (inkl. Fristen) werden festgelegt, siehe Abschnitte 4.1 und 4.2.
2. Zum **31.12.2030**:
   - Anwendungsfälle mit hohem Risiko sind quantensicher.
   - Bei Neubeschaffungen werden nach Möglichkeit nur quantensichere Produkte berücksichtigt. Dies umfasst mindestens quantensichere Updatemöglichkeiten.
3. Zum **31.12.2035**:
   - Die Umstellung auf PQC ist für Anwendungsfälle mit mittlerem Risiko abgeschlossen.
   - Die Umstellung auf PQC wurde für Anwendungsfälle mit geringem Risiko so weit wie möglich abgeschlossen.

Abbildung 2: Meilensteine für die Umstellung auf PQC

4 Schritte zur Umstellung auf PQC

In diesem Abschnitt werden Maßnahmen definiert, um die Meilensteine aus Abschnitt 3 zu erreichen. Bis Ende 2026 sollte die initiale Vorbereitungs- und Planungsphase zur Umstellung auf Post-Quanten-Kryptografie abgeschlossen sein (PQC-Readiness) sowie erste Schritte der Umstellung begonnen werden, bis 2030 sämtliche Hochrisiko-Anwendungen auf quantensichere Verfahren umgestellt sein und bis 2035 sollte die vollständige Umstellung für nahezu alle Systeme abgeschlossen sein.
Das BSI stellt Hinweise und Anleitungen zur Vorbereitung der Umstellung auf PQC bereit, die sich an Behörden, kritische Infrastrukturen und Unternehmen richten, siehe insbesondere den Leitfaden *Kryptografie quantensicher gestalten*[7]. Kern dieser Empfehlungen ist der Dreiklang aus Inventarisierung, Priorisierung und Umsetzung. Die Bundesverwaltung wird bereits für die initialen Schritte der Inventarisierung und Priorisierung vom BSI unterstützt.

4.1 Fristen verbindlich machen

Die in dieser Roadmap enthaltenen Fristen sind dringende Empfehlungen aufgrund des akuten Handlungsdrucks. Es bedarf aber darüber hinaus einer verbindlichen Festlegung dieser Fristen für verschiedene Bereiche, z.B. Bundesverwaltung, Länder und Kommunen, KRITIS. Die verantwortlichen Gremien sollten bis Ende 2026 die genannten Fristen möglichst verbindlich verabschieden. Hierzu zählen:

- IT-Planungsrat
- UP KRITIS

Für zugelassene VS-IT-Sicherheitsprodukte hat das BSI verbindliche Fristen festgelegt, um die Umstellung im Verschlusssachen-Bereich bis 2030 umzusetzen. Hinweise zu mit dieser Roadmap kompatiblen Fristen für nicht-zuzulassende Produkte finden sich in der Technischen Richtlinie TR-02102 des BSI.

4.2 Einrichtung von Koordinierungsgremien/verantwortlichen Stellen

In einigen Bereichen oder auch in großen Organisationen kann es sinnvoll sein, ein Gremium einzurichten, das die Umstellung auf Post-Quanten-Kryptografie koordiniert. Mindestens sollte eine verantwortliche Stelle benannt werden.

Diese Koordinierungsgremien bzw. verantwortlichen Stellen sollten folgende Aufgaben wahrnehmen:

- Umsetzungsplan und Prioritätensetzung,
- Monitoring über die Fortschritte der Umsetzung,
- Beobachten der weiteren Entwicklung; Austausch mit anderen Stakeholdern aus Industrie, Forschung und Behördenlandschaft,
- Ggf. Abstimmung mit relevanten Gremien,
- Ggf. interne Informations- und Sensibilisierungsmaßnahmen

[7] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Kryptografie-quantensicher-gestalten.html

Zur Erledigung dieser Aufgaben müssen ausreichende personelle und finanzielle Ressourcen eingeplant werden.

4.3 Inventarisierung kryptografischer Verfahren und Schlüssel

Jede Organisation sollte eine Übersicht über ihre kryptografischen Komponenten erstellen – analog zum Krypto-Kataster im BSI IT-Grundschutz (Baustein CON.1 Kryptokonzept, Anforderung CON.1.A19 Erstellung eines Krypto-Katasters). Diese Maßnahme ist unabhängig von der Umstellung auf PQC ein Beitrag zur Steigerung der Cyber- und Informationssicherheit. Cryptographic inventory tools, repository scans und CBOMs (Cryptographic Bill of Materials, z.B. basierend auf dem CycloneDX-Standard) können die Erstellung des kryptografischen Inventars unterstützen. Das kryptografische Inventar sollte regelmäßig auf Aktualität geprüft werden; die initiale Erstellung sollte bis Ende 2026 abgeschlossen sein. Sollte kein Kryptokataster in ausreichender Qualität vorhanden sein, bietet es sich an auf Basis einer priorisierten Betrachtung der Geschäftsprozesse (Fachaufgaben im Behördenkontext) die darin eingesetzten IT-Komponenten und deren Kryptomodule einschließlich des potenziellen Schadensausmaßes bei Entschlüsselung zu erheben.

Ferner sollte eine Übersicht über die internen und externen Abhängigkeiten der kryptografischen Komponenten erstellt werden. Beispielsweise müssen sowohl Kartenlesegerät als auch die zugehörigen Karten quantensichere Verfahren implementiert haben, damit die Kommunikation zwischen den beiden Instanzen quantensicher erfolgen kann.

4.4 Post-Quanten-Kryptografie als Stand der Technik

Kryptografische Anwendungen müssen dem Stand der Technik genügen, z.B. durch Einhaltung der Empfehlungen aus der Technischen Richtlinie BSI-TR-02102. Dort ist nachvollziehbar, welche Verfahren als quantensicher gelten und wie sie eingesetzt werden sollten. Das BSI empfiehlt die Verwendung hybrider Verfahren, also eine Kombination von klassischen Verfahren mit Post-Quanten-Verfahren, die die Sicherheitsleistung beider Einzelverfahren kombiniert. Wichtige und besonders wichtige Einrichtungen sind nach dem „Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen“ (BSI-Gesetz, BSIG), § 30 dazu verpflichtet, den Stand der Technik für Kryptografie gemäß ihrem Risikomanagement einzuhalten.

Das kryptografische Inventar aus Abschnitt 4.3 sollte entsprechend dem Stand der Technik genügen, insbesondere ist eine Abschätzung des Quantenrisikos gemäß Abschnitt 4.5 zu berücksichtigen.

4.5 Abschätzung des Quantenrisikos und Verankerung im Risikomanagement

Die Abschätzung des Quantenrisikos sollte in das reguläre Risikomanagement integriert werden. Insbesondere sollten Fristen zur Mitigation im Risikomanagement verankert werden. Die Abschätzung des Quantenrisikos wird zur Priorisierung der Anwendungsfälle aus dem kryptografischen Inventar benötigt.

Die Quantenrisikoanalyse kann beispielsweise wie in der EU-Roadmap beschrieben auf der Systematik aus Abschnitt 2.4 des „PQC Migration Handbooks“[8] (PQC-Migrationshandbuch), die

[8] https://www.tno.nl/en/newsroom/2024/12/renewed-handbook-quantum-safe-crypto/

mit der allgemeinen IT-Risikomanagementmethodik gemäß ISO-Norm 27005 „Informationssicherheit, Cybersicherheit und Datenschutz - Leitfaden zur Handhabung von Informationssicherheitsrisiken“ und nationalen Normen wie dem BSI-Standard 200-3 „Risikoanalyse auf der Grundlage von IT-Grundschutz“[9] kompatibel ist, basieren.

Im empfohlenen Zeitplan wird zwischen den drei grundlegenden Quantenrisikostufen „hoch“, „mittel“ und „niedrig“ unterschieden. Nach diesem Ansatz, basierend auf dem PQC-Migrationshandbuch, wird das Quantenrisikoniveau eines Anwendungsfalles (eine Anwendung oder ein System) von drei Faktoren beeinflusst:

- der Angreifbarkeit der verwendeten kryptografischen Verfahren;
- dem zu erwartenden Schadensausmaß (z.B. durch Verlust von Vertraulichkeit);
- dem geschätzten Zeit- und Arbeitsaufwand für die Umstellung auf PQC.

Für weitere Details wird auf die EU-Roadmap und das PQC-Migrationshandbuch verwiesen[10].

4.6 Umsetzung und Einbindung der Lieferkette

Die Umstellung auf PQC sollte schrittweise erfolgen und mit den kritischsten Anwendungen beginnen. Eine frühzeitige Abstimmung mit Herstellern, IT-Dienstleistern und Kommunikationspartnern ist unerlässlich, um Kompatibilität und Interoperabilität sicherzustellen. Die Bereitstellung von CBOMs verein-facht den Vergleich von kryptografischen Fähigkeiten innerhalb der Lieferkette. Eine solche Bereitstellung kann vertraglich festgehalten werden.

Ferner sollte die Umstellung auf PQC im Lifecycle Management berücksichtigt werden. Beispielsweise kann es in einigen Fällen sinnvoll sein, den Ersatz für ein bestimmtes Produkt hinauszuzögern, bis ein PQC-fähiger Ersatz verfügbar ist, während in anderen Fällen ein vorzeitiger Austausch nötig ist, um der Bedrohung durch Quantencomputer zu entgehen.

Insbesondere bei Neuentwicklungen sollte darauf geachtet werden, dass ausschließlich quantensichere kryptografische Verfahren eingesetzt werden. Bei der Beschaffung und Vergabe sollten die Anforderungen bzgl. PQC und Kryptoagilität gemäß TR-02102 standardmäßig beachtet werden.

[9] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-3-Risikomanagement/bsi-standard-200-3-risikomanagement_node.html

[10] Im PQC-Migrationshandbuch wird zwar auch der Begriff „akutes Risiko“ verwendet, für die Zwecke dieses Dokuments reichen jedoch drei Risikostufen aus.

Literaturverzeichnis

AVID, CWI und TNO. (Dezember 2024). The PQC Migration Handbook. 2nd Edition. https://publications.tno.nl/publication/34643386/fXcPVHsX/TNO-2024-pqc-en.pdf

Bundesamt für Sicherheit in der Informationstechnik. (Oktober 2017). BSI-Standard200-3. Risikoanalyse auf der Basis von IT-Grundschutz. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.pdf

Bundesamt für Sicherheit in der Informationstechnik. (Dezember 2021). Kryptografie quantensicher gestalten. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Kryptografie-quantensicher-gestalten.pdf

Bundesamt für Sicherheit in der Informationstechnik. (August 2025). Status of quantum computer development. Entwicklungsstand Quantencomputer. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/Entwicklungstand_QC_V_2_2.pdf

Bundesamt für Sicherheit in der Informationstechnik. (Dezember 2026). Kryptographische Verfahren: Empfehlungen und Schlüssellängen. BSI TR-02102-1. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf

Deutscher Bundestag. (Februar 2025). Aktueller Umsetzungsstand des Handlungskonzeptes Quantentechnologien der Bundesregierung. Drucksache 20/14986. https://dserver.bundestag.de/btd/20/149/2014986.pdf

KPMG, Bundesamt für Sicherheit in der Informationstechnik. (April 2023). Marktumfrage Kryptografie und Quantencomputing. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Marktumfrage_Kryptografie_Quantencomputing.html

NIS Cooperation Group. (Juni 2025). A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography. Part 1, Version: 1.1, EU PQC Workstream vom 11.06.2025. Roadmap_on_postquantum_cryptography_PzBJxNUYyeuEdVUacWL696DofZQ_117507.pdf

Impressum

Herausgeber
Bundesministerium des Innern, 11014 Berlin
Internet: www.bmi.bund.de

Bundesministerium für Digitales und Staatsmodernisierung, 10557 Berlin
Internet: www.bmds.bund.de

Bundesamt für Sicherheit in der Informationstechnik, 53175 Bonn
Internet: www.bsi.bund.de

Stand
August 2026

Artikelnummer
BMI26024

Weitere Publikationen der Bundesregierung zum Herunterladen und zum Bestellen finden Sie unter:
www.publikationen-bundesregierung.de

Diese Publikation wird von der Bundesregierung im Rahmen ihrer Öffentlichkeitsarbeit herausgegeben. Die Publikation wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt. Sie darf weder von Parteien noch von Wahlwerbern oder Wahlhelfern während eines Wahlkampfes zum Zwecke der Wahlwerbung verwendet werden. Dies gilt für Bundestags-, Landtags- und Kommunalwahlen sowie für Wahlen zum Europäischen Parlament.