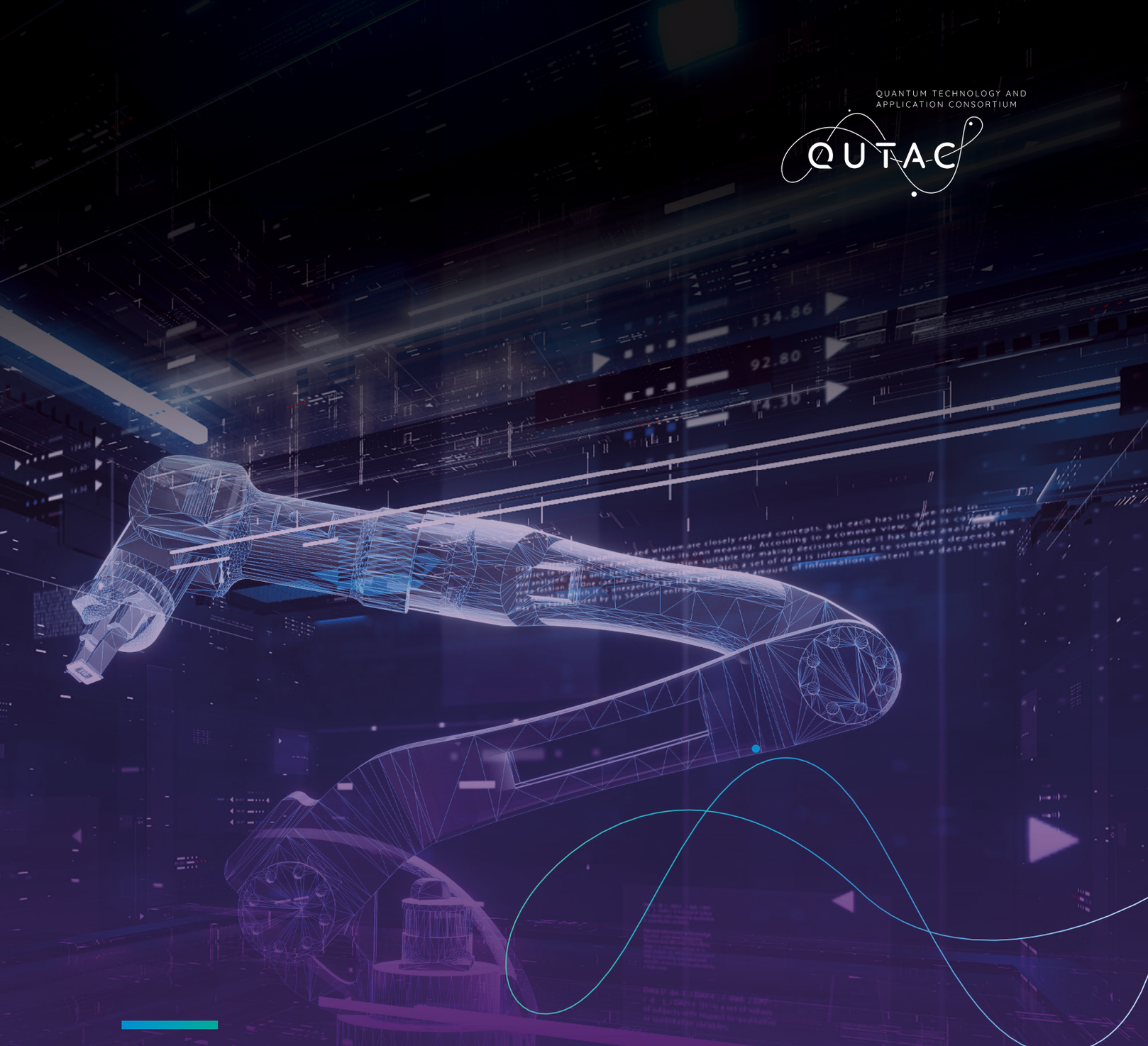
QUANTUM TECHNOLOGY AND APPLICATION CONSORTIUM

QUTAC



Einführung der Post-Quanten-Kryptografie (PQC) in industrielle Systeme

Ein Praxisleitfaden für Führungskräfte und IT-Entscheider

Oktober 2026

AUTOREN:

Harald Vogt[*1] (corresponding), Markus Ruppert[*2], Marvin Erdmann[*3], Sven Haueisen[*4], Wojciech Pawlak[*5], Sven Breitung[6]

[*]Quantum Technology & Application Consortium (QUTAC), [1]TRUMPF, [2]Lufthansa Industry Solutions, [3]BMW Group, [4]Volkswagen Group, [5]Deutsche Telekom, [6]VDMA

MIT BEITRÄGEN VON:

Christian Cohrs, Fabrizio Desantis, Florian Dommert, Christian Garske, Marc Geitz, Raoul Guiazon, Detlef Houdeau, Martin Hütter, Andreas Kind, Andre Luckow, Silke Müller, Sofia Todesca

Oktober 2026
www.qutac.de

Inhaltsverzeichnis

1. Zusammenfassung 4

2. Einleitung 4

3. Zentrale Anwendungsfälle 5

4. Bedrohungen und Risiken 6

   4.1 Kompromittierung von Schlüsseln 6

   4.2 Harvest Now, Decrypt Later 8

   4.3 Langlebige Systeme 8

   4.4 Fälschung von Signaturen 9

   4.5 Regulatorischer Druck 10

5. Das Krypto-Inventar: Voraussetzung für die PQC-Migration 11

   5.1 Die Kryptografie-Stückliste 11

   5.2 Sicherheitskritische Assets 11

   5.3 Die Pflege des Krypto-Inventars 12

6. Empfohlenes Vorgehen zur Einführung 13

   6.1 PQC-Einführung 13

   6.2 Schritt 1 — Governance und strategische Verantwortung etablieren 13

   6.3 Schritt 2 — Ein Krypto-Inventar aufbauen und pflegen 14

   6.4 Schritt 3 — Kryptoagilität als Konstruktionsprinzip verankern 14

   6.5 Schritt 4 — PQC und hybride Kryptografie pragmatisch einführen 15

   6.6 Schritt 5 — Kontinuierliche Verbesserung 15

7. Fazit 16

Quellen 17

1. Zusammenfassung

Quantencomputing ist eine vielversprechende Technologie, von der in Zukunft viele Bereiche profitieren können – Vorteile werden unter anderem in komplexen Simulationen, in der Optimierung und in der künstlichen Intelligenz erwartet. Zugleich stellen Quantencomputer eine ernsthafte Bedrohung für etablierte kryptografische Verfahren dar, die die Grundlage für sichere Kommunikation und Datenverarbeitung bilden. Als Antwort darauf wurden alternative Algorithmen entwickelt und standardisiert, die quantensichere Verschlüsselung und Authentifizierung ermöglichen, und es wurde bereits damit begonnen, diese Algorithmen in Werkzeuge wie Webbrowser zu integrieren. Da leistungsfähige Quantencomputer schnell näher rücken, sind öffentliche und private Organisationen aufgefordert, zu handeln und eine Migration der eigenen Systeme zur Post-Quanten-Kryptografie einzuleiten. Für den Maschinen- und Anlagenbau ergeben sich besondere Herausforderungen durch lange Produktlebenszyklen, weltweit verteilte installierte Basen, industrielle Kommunikationssysteme, eingeschränkte Testmöglichkeiten sowie die Abhängigkeit von komplexen Lieferketten.

Dieses Papier beschreibt die notwendigen Schritte, um eine Organisation auf die Zukunft vorzubereiten, in der klassische Kryptografie angreifbar wird. Da kryptografische Verfahren tief in viele Software- und IT-Systeme eingebettet sind, ist es komplex und zeitaufwendig, die heutigen Verfahren nicht nur zu ersetzen, sondern auch die Interoperabilität zwischen Neu- und Altsystemen sicherzustellen und sich auf kommende Änderungen der kryptografischen Mechanismen vorzubereiten. Langfristiges Ziel ist nicht allein die Einführung heutiger PQC-Verfahren, sondern die Fähigkeit, kryptografische Verfahren künftig flexibel und wirtschaftlich austauschen zu können (Kryptoagilität). Ein Vorhaben von solcher Komplexität benötigt eine gründliche Planung und ein straffes Migrationsmanagement, um erfolgreich zu sein.

2. Einleitung

Die Entwicklung des Quantencomputings erfolgt in großen Schritten. Sobald die Technologie ausgereift ist, wird sie weit verbreitete klassische kryptografische Algorithmen wie RSA und Elliptische-Kurven-Kryptografie (ECC) brechen können. Weltweit gehen Regulierungsbehörden davon aus, dass diese Algorithmen bis 2030 unsicher werden.[1]

Glücklicherweise stehen quantensichere (oder Post-Quanten-)Algorithmen (PQC) bereits zur Verfügung. International haben Standardisierungsgremien Algorithmen vorgelegt, die klassische Verfahren ersetzen können und die Sicherheit auch dann gewährleisten, wenn hinreichend leistungsfähige Quantencomputer verfügbar sind.

Dafür ist es jedoch notwendig, heute IT-Systeme zur Nutzung dieser Verfahren zu ertüchtigen, wobei besonders solche Anwendungen im Fokus stehen sollten, bei denen die Risiken durch eine Kompromittierung der Sicherheit besonders hoch sind. Dabei ist Eile geboten. Die Europäische Union empfiehlt, Anwendungen mit hohem Risiko bis 2030 zu migrieren und die komplette Migration bis 2035 abzuschließen. Das deutsche BSI aktualisiert seine Migrationsempfehlung fortlaufend und empfiehlt die alleinige Nutzung klassischer Kryptografie für alle Anwendungsfälle nur bis zum Ende des Jahres 2031.[2]

Der Markt stellt sich bereits auf diese Entwicklung ein. Große Unternehmen, die selbst an der Entwicklung von Quantencomputern beteiligt sind, verfolgen Strategien, um sich in den nächsten Jahren von klassischer Kryptografie zu lösen. Google zum Beispiel hat den eigenen Zeitplan für die PQC-Migration auf 2029 vorgezogen[3]. Viele große Softwareanbieter integrieren derzeit PQC-Funktionen in ihre Produktportfolios, etwa SAP, IBM oder Salesforce.

Die Mitglieder von QUTAC haben sich verpflichtet, die industrielle Anwendung von Quantencomputing zu fördern. QUTAC sieht es jedoch auch in seiner Verantwortung, auf die Risiken dieser neuen Technologie hinzuweisen und möchte dazu beitragen, Organisationen auf dieses neue Umfeld vorzubereiten.

Da die meisten Organisationen auf die Vertraulichkeit und Integrität elektronischer Daten angewiesen sind, müssen sie den angemessenen Schutz dieser Informationswerte gewährleisten. Quantencomputer bedrohen zentrale kryptografische Primitive, die die Grundlage für Authentifizierung, digitale Signaturen und sichere Kommunikation sind; deshalb muss eine Strategie festgelegt werden, um Systeme mit kryptografischen Mechanismen zu aktualisieren und sensible Daten unter einen neuen Schutzschirm zu bringen. Der Übergang zu PQC ist dabei nicht nur eine technische Herausforderung, sondern auch ein strategisches Gebot, um Vertrauen, operative Resilienz und Compliance zu erhalten.

Kryptografische Risikomatrix: Verwundbarkeit klassischer Verfahren und Quantenabwehr

Derzeit beruhen 90-95 % aller Sicherheitsmechanismen auf RSA und ECC. Mit dem Shor-Algorithmus können Quantencomputer diese Grundlagen vollständig brechen – ein sofortiger Umstieg auf gitter- und hashbasierte Mathematik ist zwingend erforderlich.

	Mathematische Grundlage	Risiko heute	Risiko am Q-Day	Erforderliche Maßnahme
Klassisch asymmetrisch (RSA-2048 / ECC P-256)	Faktorisierung / diskreter Logarithmus	Mittel	**Kritisch** (vollständige Kompromittierung)	Migrieren
Klassisch symmetrisch (AES-128)	Unstrukturierte Suche	Gering	**Hoch** (Grover-Algorithmus halbiert die Sicherheit)	Schlüssellänge verdoppeln auf AES-256
Post-Quanten (ML-KEM / ML-DSA)	Gitterbasiert (Learning With Errors)	Gering	**Gering** (quantenresistent)	Sofortige hybride Integration

Abbildung 1 *Quantencomputing erfordert eine Anpassung Ihrer kryptografischen Verfahren. Klassische asymmetrische Algorithmen müssen ersetzt werden; symmetrische Algorithmen lassen sich so verstärken, dass sie Quantenangriffen standhalten.*

Die Migration zu einer quantenresilienten Aufstellung ist ein komplexes Vorhaben, das nahezu jedes System betrifft, das sensible Informationen verarbeitet. Für Organisationen mit heterogenen, kapitalintensiven Umgebungen aus Informationstechnik (IT) und Betriebstechnik (OT) kann die vollständige Migration aller betroffenen Systeme mehrere Jahre dauern sowie hohen Aufwand und erhebliche Investitionen erfordern.

In diesem Dokument zeigen wir, wie eine solche Strategie umgesetzt werden kann. Naturgemäß müssen wir dabei verallgemeinern. Für jede einzelne Organisation sind die beschriebenen Schritte an die jeweiligen Anforderungen anzupassen. Unser Ziel ist es, Entscheidern, IT-Verantwortlichen und Sicherheitsverantwortlichen praxisnahe Orientierung zu geben, damit sie sich auf PQC vorbereiten und eine strukturierte Migration durchführen können.

3. Zentrale Anwendungsfälle

Eine wesentliche Grundlage für die meisten Formen des sicheren Informationsaustauschs ist die sogenannte Public-Key-Kryptografie. Dabei kommt eine Kombination aus einem privaten (geheimen) und einem öffentlichen Schlüssel zum Einsatz, um sowohl die Vertraulichkeit als auch die Echtheit von Informationen sicherzustellen. Diese Verfahren werden aus Effizienzgründen meist mit symmetrischen Verschlüsselungsverfahren kombiniert.

Die Public-Key-Kryptografie ist das Verfahren, das durch das Aufkommen des Quantencomputers am stärksten bedroht ist. Wir müssen deshalb alle Anwendungsfälle betrachten, die darauf beruhen. Wir nennen einige Beispiele, die Ihnen helfen sollen, die wichtigsten Anwendungsfälle in Ihrer Organisation zu erkennen.

Nahezu alle Organisationen betreiben eine verteilte Kommunikationsinfrastruktur: Tochtergesellschaften verbinden sich mit der Zentrale, Außendienstmitarbeiter greifen online auf Unternehmensressourcen zu, Dokumente werden mit externen Partnern ausgetauscht, Daten werden auf externen Speichern verwaltet. E-Mail oder Instant Messaging werden genutzt, um interne Themen zu besprechen oder sensible Informationen auszutauschen. Die Sicherheit dieser Kommunikationsformen beruht auf virtuellen privaten Netzen (VPN), verschlüsseltem Webverkehr (HTTPS), Ver-

schlüsselung von Nachrichten und ähnlichen Mechanismen, die durch asymmetrische Kryptografie ermöglicht werden.

Die Vertraulichkeit von Daten, die in dieser Form verarbeitet werden, gerät mit der Verfügbarkeit von Quantencomputern unter Druck. Auch wenn heute laufender Datenverkehr nicht sofort entschlüsselt werden kann, kann dieser aufgezeichnet und später entschlüsselt werden – dies ist der Harvest-now-decrypt-later-Angriff, der weiter unten beschrieben wird.

Ähnlich verhält es sich mit vertraulichen Dokumenten, die häufig verschlüsselt und durch einen privaten Schlüssel geschützt sind: Sie wären für jeden mit Zugang zu einem Quantencomputer offen lesbar. Geheime Informationen, die nur in bestimmten Kontexten und nur bestimmten Nutzern zugänglich sein sollen, wären allgemein verfügbar. Ein praktisches Beispiel sind Dokumente auf Backup-Medien: Dort können sie zwar verschlüsselt sein – künftig wären sie aber für Unbefugte zugänglich. Es muss davon ausgegangen werden, dass alle Kommunikationsdaten mit langfristigem Schutzbedarf künftig gefährdet sein können.

Nicht nur die Vertraulichkeit der Kommunikation ist durch Quantencomputer gefährdet, sondern auch die Echtheit von Dokumenten, die aufgrund ihrer Bedeutung digital signiert wurden – etwa Geschäftsverträge, Protokolle und andere rechtlich relevante Dokumente. Signaturen lassen sich künftig leicht fälschen. Der öffentliche Schlüssel reicht aus, um daraus den privaten Schlüssel zu rekonstruieren. Daher kann ein Angreifer Signaturen erzeugen, die scheinbar vom Besitzer des Schlüssels stammen. Faktisch werden viele digitale Signaturen, die nicht durch ein quantensicheres Verfahren bestätigt werden, wertlos. Auch deshalb sollten frühzeitig geeignete Gegenmaßnahmen ergriffen werden.

Neben Dokumenten sind auch Geräte betroffen, die im öffentlichen Raum betrieben werden, etwa Verkaufsautomaten, Tankstellen, Verkehrsinfrastruktur oder Überwachungstechnik. Die Aktualisierung solcher Produkte ist kein Unterfangen der IT-Abteilung allein, sondern hängt von der Leistungsfähigkeit der gesamten Lieferkette ab: von Geräteherstellern, Backend-Infrastruktur, Chipherstellern und Softwareanbietern.

Sowohl Daten, die aus solchen Geräten stammen, als auch Daten, die in sie eingespielt werden, müssen geschützt sein. Software-Updates, Konfigurationseinstellungen, die Durchführung von Bezahltransaktionen, Funktionserweiterungen (z. B. softwaredefinierte Funktionen in Fahrzeugen) oder die Aktualisierungen von KI-Modellen können alle entscheidend sein für die korrekte Funktion dieser Geräte. Jede Verletzung der Integrität solcher Daten kann schädliche, sogar tödliche Folgen haben, insbesondere wenn kritische Infrastruktur betroffen ist, etwa die Wasserversorgung oder Stromnetze.

Da persönliche Identifizierung und Authentifizierung zunehmend digital erfolgen, werden auch personalisierte Dienste angreifbar. Physische Objekte wie Reisepässe, Personalausweise, Türschlüssel und ähnliche Objekte für Hochsicherheitsanwendungen nutzen Public-Key-Kryptografie, um Vervielfältigung oder Fälschung zu verhindern. Für den Wechsel auf eine PQC-Infrastruktur müssen diese Objekte ersetzt werden. Wegen ihrer großen Zahl und der begrenzten Kapazitäten in Produktion und Vertrieb kann der Austausch im Feld jedoch sehr viel Zeit beanspruchen.

Ein weiterer Bereich, in dem Quantencomputer zu Umbrüchen führen werden, ist die Welt der Blockchains. Sie werden für die Verifikation von Lieferketten, für das Management von Produktidentitäten und für digitale Währungen eingesetzt. Da globale Finanzinstitute diese nutzen, kann die Entwertung ihrer kryptografischen Grundlage zu erheblichen finanziellen Verlusten und zum Verlust von Informationsintegrität führen.

Diese Beispiele zeigen, dass viele Organisationen anfällig für quantencomputerbasierte Angriffe auf die Vertraulichkeit und Integrität ihrer Informationswerte sind. Ein breiter und wirtschaftlicher Zugang zu Quantencomputern wird vielleicht erst in Zukunft Realität. Diese Zukunft ist jedoch nicht so fern, wie es scheinen mag – und der Übergang zu einer vollständig PQC-fähigen Infrastruktur und der angemessene Schutz aller Informationswerte ist sehr aufwendig und erfordert sorgfältige Planung und Verbindlichkeit.

4. Bedrohungen und Risiken

4.1 Kompromittierung von Schlüsseln

Die Grundlage der meisten Mechanismen zum Schutz von Informationen vor unbefugtem Zugriff oder Manipulation ist die Kombination aus privaten und öffentlichen Schlüsseln. Zu einem öffentlichen Schlüssel gehört genau ein privater Schlüssel und umgekehrt. Der private Schlüssel wird geheim gehalten, der öffentliche Schlüssel darf frei verteilt werden. Dies wird als „asymmetrische Kryptografie" bezeichnet, da sich die Funktionen beider Schlüssel

unterscheiden. Für solche Schlüsselpaare gibt es zwei wesentliche Anwendungsfälle:

- Die Erzeugung einer Signatur für Daten, die jeder mit dem öffentlichen Schlüssel prüfen kann.
- Die Verschlüsselung von Daten, die geheim bleiben müssen und die nur der Inhaber des privaten Schlüssels lesen kann.

Üblicherweise funktioniert ein kryptografischer Mechanismus zum Schutz der Vertraulichkeit von Daten (oder Dokumenten) wie folgt. Da es sehr ineffizient ist, ein vollständiges Dokument direkt mit dem öffentlichen Schlüssel zu verschlüsseln, wird zuerst ein „symmetrischer" Schlüssel erzeugt. Die Verschlüsselung mit einem symmetrischen Schlüssel ist sehr schnell und effizient. Nur der symmetrische Schlüssel wird mit dem öffentlichen Schlüssel verschlüsselt. Der Inhaber des privaten Schlüssels kann nun zuerst den symmetrischen Schlüssel entschlüsseln und dann damit das vollständige Dokument. Da niemand sonst den symmetrischen Schlüssel entschlüsseln kann, bleibt das Dokument geheim.

Ein Quantencomputer verändert die Ausgangslage. Mit dem „Shor-Algorithmus" lässt sich die Geheimhaltung des Dokuments brechen. Da der Angreifer Zugang zum öffentlichen Schlüssel hat – wovon wir ausgehen können, weil dies leicht zu bewerkstelligen ist –, erlaubt dieser Algorithmus die Rekonstruktion des zugehörigen privaten Schlüssels. Mit herkömmlichen Rechnern ist dies in begrenzter Zeit nicht durchführbar. Hinreichend ausgestattete Quantencomputer schaffen es jedoch mit relativ geringem Aufwand.

Mit dem gewonnenen privaten Schlüssel kann der Angreifer nun den symmetrischen Schlüssel entschlüsseln, mit dem das Dokument geschützt wurde, und das verschlüsselte Dokument in ein lesbares Format überführen.

Das Fälschen einer Signatur funktioniert ähnlich, ist aber noch einfacher. Verfügt der Angreifer über den öffentlichen Schlüssel und einen Quantencomputer, kann er den zugehörigen privaten Schlüssel rekonstruieren. Damit kann er Signaturen für beliebige Dokumente erzeugen. Für den Prüfer eines signierten Dokuments wird es unmöglich, ein Original von einer Fälschung zu unterscheiden.

Damit ist die technische Bedrohung beschrieben, die die Sicherheit der meisten heute mit herkömmlicher Kryptografie geschützten Informationen gefährdet. Wer es jedoch versäumt, Systeme so zu aktualisieren, dass sie dieser Bedrohung standhalten, geht zusätzlich regulatorische und möglicherweise rechtliche Risiken ein.

Hintergrund

Seit die Idee des Quantencomputings Anfang der 1970er-Jahre aufkam, hat die Forschung Wege gefunden, das Potenzial von Quantencomputern zu nutzen. Es wurden Algorithmen entworfen, die klassische Verfahren theoretisch übertreffen – darunter auch solche, die eine erhebliche Bedrohung für die klassische Kryptografie darstellen.

Shors Algorithmus, 1994 entdeckt, ermöglicht es Quantencomputern, große Ganzzahlen zu faktorisieren und diskrete Logarithmen exponentiell schneller zu berechnen als klassische Algorithmen. Das bedroht RSA, DH und ECC, die auf der Schwierigkeit dieser Probleme beruhen. RSA-2048 zum Beispiel, dessen klassische Faktorisierung heute Millionen von Jahren erfordert, ließe sich in Tagen oder sogar Stunden brechen[4]. Shors Algorithmus nutzt die Quanten-Fourier-Transformation und die Periodensuche, um die Faktorisierung auf ein Problem zurückzuführen, das ein Quantengerät lösen kann. Damit bricht er die mathematischen Grundlagen der klassischen asymmetrischen Kryptografie.

Grover-Algorithmus reduziert die Brute-Force-Schlüsselsuche ungefähr auf die Quadratwurzel des klassischen Aufwands. Das führt oft zur Einschätzung, dass dadurch die effektive Schlüssellänge halbiert wird und es geboten sein kann, die verwendete Schlüssellänge zu verdoppeln. [5] Diese Einschätzung beruht auf einer theoretischen Anzahl von Abfragen und nicht auf einer realistischen Kostenschätzung. In der Praxis würden die erforderlichen AES-Berechnungen weitgehend sequenziell auf einem fehlertoleranten Quantencomputer ablaufen und einen erheblichen Schaltungs- sowie Fehlerkorrektur-Overhead mit sich bringen. Aktuelle Ressourcenschätzungen kommen daher zu dem Schluss, dass der praktische Einfluss von Grover auf AES mit bestehenden Techniken und plausibler naher Zukunftshardware stark begrenzt ist. Dementsprechend geht das NIST davon aus, dass AES-128 auf „die kommenden Jahrzehnte" gesehen sicher bleiben wird.[6]

Grovers Algorithmus bietet eine quadratische Beschleunigung für unstrukturierte Suchprobleme. Das betrifft symmetrische Kryptografie und Hashfunktionen, deren Sicherheitsniveau dadurch effektiv halbiert wird. So sinkt die Sicherheit eines symmetrischen 128-Bit-Schlüssels gegenüber einem Angreifer mit Grovers Algorithmus auf etwa 64 Bit. Als Gegenmaßnahme

wird empfohlen, die Schlüssellängen zu verdoppeln (z. B. AES-256), um das Sicherheitsniveau zu erhalten.

Post-Quanten-Kryptografie (PQC) besteht aus kryptografischen Algorithmen, die Angriffen mit Quantencomputern widerstehen. Zu den wichtigsten Familien von PQC-Algorithmen gehören:

- **Codebasierte Kryptografie:** Beruht auf fehlerkorrigierenden Codes, etwa dem McEliece-Kryptosystem, und nutzt die Schwierigkeit, zufällige lineare Codes zu dekodieren. Diese Verfahren bieten hohe Sicherheit, haben aber oft große Schlüssel.
- **Gitterbasierte Kryptografie:** Baut auf schwierigen Gitterproblemen wie Learning With Errors (LWE) und Ring-LWE auf. Gitterbasierte Verfahren (z. B. CRYSTALS-Kyber für Verschlüsselung, CRYSTALS-Dilithium für Signaturen) sind effizient und skalierbar, haben moderate Schlüsselgrößen und sind NIST-Standards.
- **Hashbasierte Kryptografie:** Vor allem für digitale Signaturen; sie nutzt die Einwegeigenschaften von Hashfunktionen. Verfahren wie XMSS und SPHINCS+ bieten hohe Sicherheit, erhöhen aber den Speicherbedarf und sind teilweise in der Anzahl der Signaturen pro Schlüssel begrenzt.

Weitere Ansätze sind multivariate Polynomkryptografie und Isogenie-Kryptografie auf supersingulären elliptischen Kurven; diese sind jedoch weniger ausgereift.

4.2 Harvest Now, Decrypt Later

Wie beschrieben, wird es möglich sein, herkömmliche Verschlüsselung mit Quantencomputern zu brechen. Auch wenn solche Rechner heute nicht verfügbar sind, können Angreifer verschlüsselte Kommunikation oder gespeicherte Daten schon jetzt sammeln und sie entschlüsseln, sobald hinreichend leistungsfähige Quantencomputer verfügbar sind. Sensible Informationen lassen sich so rückwirkend offenlegen.

Diese Bedrohung ist besonders kritisch für Daten, die heute oder in der Vergangenheit mit herkömmlichen Mitteln geschützt wurden, aber wegen regulatorischer Vorgaben oder ihres Geschäftswerts über lange Zeiträume vertraulich bleiben müssen.

Betroffen sind alle Informationen mit langfristigen Vertraulichkeitsanforderungen, darunter:

- Kunden- und personenbezogene Daten (einschließlich medizinischer Unterlagen)
- Geistiges Eigentum
- Konstruktions- und Produktdaten
- Vertrags- und Finanzdokumente
- Behördliche Kommunikation
- Forschungsdaten

Als Gegenmaßnahme sind alle Dokumente zu ermitteln, die langfristigen Schutz benötigen, und in Systeme zu überführen, in denen sie mit quantensicheren Verfahren verschlüsselt werden.

4.3 Langlebige Systeme

Viele Organisationen, etwa in der Automobil- oder Telekommunikationsbranche, betreiben OT-, IoT- und eingebettete Systeme mit Betriebslebensdauern von 10 Jahren und mehr. Solche Systeme werden noch im Einsatz sein, wenn Quantencomputer die heutigen klassischen kryptografischen Sicherheitsmechanismen brechen können. Sie lassen sich oft nicht einfach aktualisieren oder ersetzen. Das erhöht die Dringlichkeit, PQC-fähige kryptografische Mechanismen früh im Lebenszyklus umzusetzen. Vernetzte Geräte sind für Funktionen wie Fernzugriff, Software-Updates und Telemetrie auf sichere kryptografische Protokolle angewiesen. Diese Systeme quantenresilient zu machen, ist entscheidend für Sicherheit, Datenschutz und Geschäftskontinuität. Bei langlebigen Industrieanlagen ist frühzeitig zu bewerten, ob quantensichere Verfahren durch Software-Updates eingeführt werden können oder Hardwareanpassungen erforderlich werden.

Besondere Herausforderungen im Maschinen- und Anlagenbau

Der Maschinen- und Anlagenbau steht bei der Einführung von Post-Quanten-Kryptografie vor besonderen Herausforderungen. Im Vergleich zu klassischen IT-Systemen weisen Maschinen, Produktionsanlagen und industrielle Automatisierungslösungen deutlich längere Lebenszyklen auf und werden häufig über Jahrzehnte betrieben. Entscheidungen, die heute bei Entwicklung, Beschaffung und Auslegung von Produkten getroffen werden, können daher weit über den Zeitpunkt hinaus wirken, zu dem leistungsfähige Quantencomputer verfügbar werden.

Viele Maschinen und Anlagen verbleiben 10 bis 30 Jahre oder länger im Einsatz. Während dieser Zeit müssen sie sicher betrieben, gewartet, aktualisiert und teilweise an neue Anforderungen angepasst werden. Ein

vollständiger Austausch ist häufig wirtschaftlich nicht vertretbar. Stattdessen werden Modernisierungen und Retrofits durchgeführt. Deshalb müssen Hersteller bereits heute prüfen, ob ihre Produkte künftig auf neue kryptografische Verfahren umgestellt werden können.

Hinzu kommt, dass moderne Maschinen zunehmend vernetzt sind. Fernwartung, Condition Monitoring, digitale Serviceangebote, Software-Updates, Cloud-Anbindungen und digitale Zwillinge sind heute wesentliche Bestandteile vieler Geschäftsmodelle. Die dafür eingesetzten Authentifizierungs-, Verschlüsselungs- und Signaturverfahren beruhen in vielen Fällen auf Kryptografie, die langfristig durch Quantencomputer gefährdet werden könnte.

Eine weitere Besonderheit ist die enge Verzahnung von Informationstechnik (IT), Betriebstechnik (OT) und eingebetteten Systemen. Während Server und Arbeitsplatzrechner vergleichsweise regelmäßig aktualisiert werden können, gelten für industrielle Steuerungen, Feldgeräte und eingebettete Komponenten häufig hohe Anforderungen an Verfügbarkeit, Sicherheit und Langzeitunterstützung. Kryptografische Umstellungen müssen deshalb sorgfältig geplant und mit Herstellern, Integratoren und Betreibern abgestimmt werden.

Auch die globale installierte Basis stellt eine Herausforderung dar. Maschinen werden oft über viele Jahre in unterschiedlichen Ländern betrieben. Sicherheitsupdates, Zertifikatsaustausch oder Softwaremigrationen müssen deshalb weltweit umgesetzt werden können. Die technische Möglichkeit zur Aktualisierung kryptografischer Funktionen wird damit zu einem wichtigen Kriterium für die Zukunftsfähigkeit von Produkten.

Für den Maschinen- und Anlagenbau bedeutet die Einführung von PQC daher mehr als die Anpassung der Unternehmens-IT. Sie betrifft gleichermaßen Produkte, Serviceprozesse, Lieferketten und den gesamten Lebenszyklus von Maschinen und Anlagen. Frühzeitige Planung, Kryptoagilität sowie eine enge Zusammenarbeit mit Lieferanten und Kunden sind entscheidende Voraussetzungen, um langfristige Sicherheit und Investitionsschutz zu gewährleisten.

4.4 Fälschung von Signaturen

Wie oben beschrieben, lässt sich mit einem Quantencomputer der geheime Schlüssel zu einem öffentlichen Schlüssel eines klassischen Signaturverfahrens konstruieren. Damit kann ein Angreifer Signaturen erzeugen, die legitim aussehen. Der Prüfer hat keine Möglichkeit, eine echte, legitime Signatur von einer gefälschten zu unterscheiden. Unter dieser Bedingung kann Dokumenten und Datenobjekten, die mit klassischen Signaturverfahren signiert wurden, nicht mehr vertraut werden, sobald Quantencomputer verfügbar sind.

Daraus ergeben sich fünf Konsequenzen:

- Wertvolle, legitime Dokumente wie digital signierte Geschäftsverträge werden angefochten. Geschäftspartner haben keinen Anreiz mehr, ihre vertraglichen Pflichten einzuhalten.
- Es werden unrechtmäßige Dokumente und Datenobjekte erzeugt und in verarbeitende Systeme eingebracht. Die Signaturprüfung dieser Systeme verläuft erfolgreich, und die Informationen werden entsprechend verarbeitet. Betrügerische Geschäftsvorgänge werden ausgeführt und kompromittierte Software-Updates werden eingespielt.
- PKI-Zertifikate werden unglaubwürdig, da Angreifer eigene Zertifikate erstellen oder bestehende nachahmen können. Der Infrastruktur kann daher grundsätzlich nicht mehr vertraut werden, selbst wenn kompromittierte Zertifikate widerrufen werden.
- Signierte Software für Produkte mit und ohne Kundenkontakt ist mehrfach betroffen: Die Nachweisbarkeit (Nichtabstreitbarkeit) geht verloren, da digitale Signaturen nicht mehr als Beweis dienen können. Das führt auch zum Verlust der rechtlichen und regulatorischen Konformität. Hinzu kommen Lieferkettenangriffe durch manipulierte oder schädliche Firmware bzw. Software.
- KI-Modelle und ihr Lebenszyklus sind nicht mehr vertrauenswürdig, da es trotz gültiger Signatur vergiftete Modelle geben wird. Zudem lassen sich bestehende Modelle durch eingeschleuste Gewichte oder Hintertüren manipulieren. Signierte Trainingsdaten, Labels oder Artefakte sind kompromittiert.

Mit klassischen Algorithmen erzeugte Signaturen werden praktisch wertlos. Alle Systeme, die auf die Prüfung solcher Signaturen angewiesen sind, unterliegen einem hohen Manipulationsrisiko.

Nicht nur Dokumente sind von gefälschten Signaturen betroffen. Da sichere Kommunikationskanäle in der Regel auf Zertifikaten beruhen, die auf mehreren Ebenen durch Signaturen beglaubigt sind und so eine Vertrauenskette bilden, sind die meisten davon nicht mehr vertrauens-

würdig, sobald Signaturen gefälscht werden können. Die Identität von Kommunikationspartnern lässt sich dann nicht mehr zuverlässig bestimmen.

4.5 Regulatorischer Druck

Standardisierung und Regulierung sind entscheidend für Interoperabilität, Sicherheitsnachweise und die breite Einführung von Post-Quanten-Kryptografie in allen Branchen. Ohne klare Standards und regulatorische Vorgaben riskieren Organisationen uneinheitliche Umsetzungen, Sicherheitslücken und Compliance-Probleme. Das kann die Widerstandsfähigkeit digitaler Infrastruktur gegen quantenbasierte Angriffe untergraben.

Das US-amerikanische National Institute of Standards and Technology (NIST) hat die weltweiten Bemühungen zur Standardisierung von PQC-Algorithmen in einem strengen, mehrjährigen Auswahlverfahren angeführt. Bisher sind drei Algorithmen als offizielle Federal Information Processing Standards (FIPS) veröffentlicht: CRYSTALS-Kyber für Public-Key-Verschlüsselung und Schlüsselaustausch sowie CRYSTALS-Dilithium und SPHINCS+ für digitale Signaturen. Diese Standards decken die wesentlichen kryptografischen Aufgaben ab und bieten quantenresistente Alternativen zu RSA und ECC.[7] Weitere Algorithmen sind in der Warteschlange.

NIST empfiehlt Organisationen nachdrücklich, zügig mit der Migration auf diese neuen Algorithmen zu beginnen. Zivile Bundesbehörden sind nach dem Quantum Computing Cybersecurity Preparedness Act von 2022 gesetzlich verpflichtet, verwundbare kryptografische Systeme zu inventarisieren und Migrationspläne zu erstellen. Das National Security Memorandum 10 (NSM-10) des Weißen Hauses gibt zudem das Ziel vor, dass alle IT-Systeme des Bundes bis 2035 quantensichere Kryptografie einsetzen. Mit der IR 8547 setzt NIST das Ende des Einsatzes von RSA und ECC für digitale Signaturen generell auf 2035.

Auf europäischer Ebene hat die Europäische Kommission die unverbindliche Empfehlung (EU) 2024/1101 veröffentlicht. Sie fordert die Mitgliedstaaten auf, koordinierte nationale Strategien mit klaren Zielen und Zeitplänen für die Einführung von PQC zu entwickeln, insbesondere in kritischen Sektoren. Die Empfehlung hebt hybride kryptografische Verfahren während des Übergangs hervor, um durchgehende Sicherheit zu gewährleisten. Mitte 2025 hat die NIS-Kooperationsgruppe daraus eine Roadmap für den PQC-Übergang entwickelt, mit dem 31.12.2030 als letzter Frist für die Migration von Anwendungsfällen mit hohem Risiko.[8]

Cybersicherheitsbehörden aus 18 europäischen Ländern haben die Industrie und öffentliche Verwaltung gemeinsam aufgefordert, den Übergang zu PQC unverzüglich einzuleiten. Sie empfehlen „No-Regret"-Maßnahmen wie Asset-Inventare, risikoorientierte Roadmaps und frühe hybride Einführungen. Damit lässt sich die Cybersicherheit insgesamt verbessern und zugleich die Vorbereitung auf Quantenbedrohungen vorantreiben.[9]

Während die EU Empfehlungen für den Übergang ausgesprochen hat, haben nationale Regierungen eigene Empfehlungen und Vorgaben erlassen.

Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) hat ausführliche Leitlinien veröffentlicht, die PQC in seine kryptografischen Empfehlungen aufnehmen. Die Technische Richtlinie TR-02102-1 von 2026 empfiehlt, PQC-Algorithmen während der Migrationsphase im Hybridmodus zusammen mit klassischer Verschlüsselung einzusetzen. So bleibt die Sicherheit auch dann erhalten, wenn ein Verfahren kompromittiert wird.[10]

In Frankreich ist quantenresistente Verschlüsselung für die Beschaffung in Behörden bereits ab 2027 vorgeschrieben. Anders als bei NIST sind hybride Verfahren erforderlich, damit Systeme zertifiziert werden können.[11]

Die Niederlande verfolgen einen ähnlichen Ansatz. Kritische Infrastruktur muss spätestens 2030 umgestellt sein. Auch dort sind hybride Verfahren vorgeschrieben. Niederländische Institutionen waren die treibenden Kräfte hinter dem PQC Migration Handbook.

Weitere Länder, darunter das Vereinigte Königreich, China, Südkorea und Kanada, haben eigene PQC-Strategien und Roadmaps entwickelt, die sich grob am Zeitraum 2030–2035 für die Migration orientieren. Internationale Normungsgremien wie ISO/IEC und die IETF arbeiten aktiv daran, PQC-Spezifikationen zu formalisieren und quantensichere Algorithmen in Kommunikationsprotokolle wie TLS zu integrieren.

5. Das Krypto-Inventar: Voraussetzung für die PQC-Migration

Der Übergang zur Post-Quanten-Kryptografie beginnt damit, zu verstehen, wo in der Organisation Kryptografie eingesetzt wird und welche Informationswerte davon abhängen. Der Begriff „Krypto-Inventar" bezeichnet häufig nur kryptografische Assets wie eingesetzte Verfahren, Zertifikate und Schlüssel. Wir verwenden ihn hier jedoch für beides: für die kryptografischen Assets (dokumentiert als Cryptography Bill of Materials) und für die Menge der schützenswerten Assets.

Kryptografische Funktionen sind über eine Vielzahl von Anwendungen, Infrastruktur, Cloud-Dienste, Betriebstechnik, vernetzte Geräte und Produkte Dritter verteilt – oft ohne explizites Wissen über Abhängigkeiten, Interoperabilität und Risiken. In vielen Organisationen fehlt die Transparenz über diese Zusammenhänge.

Vorhandene Werkzeuge liefern oft unvollständige Informationen, und die Erhebung der benötigten Daten erfordert erhebliche Abstimmung über mehrere Teams und Technologiebereiche hinweg. Dennoch ist der Aufbau dieses Inventars eine unverzichtbare Voraussetzung für jedes erfolgreiche PQC-Programm. Das Krypto-Inventar bietet mehrere strategische Vorteile:

- Es zeigt, wo verwundbare Algorithmen eingesetzt werden.
- Es legt Abhängigkeiten offen, die gemeinsam migriert werden müssen.
- Es ermöglicht eine risikobasierte Priorisierung.
- Es liefert messbare Fortschrittsindikatoren.

Ohne ein Krypto-Inventar können Organisationen eine koordinierte Migration zu quantensicherer Kryptografie weder wirksam planen noch priorisieren oder durchführen.

5.1 Die Kryptografie-Stückliste

Um Einblick in die kryptografischen Assets der Organisation zu gewinnen, muss eine systematische Übersicht aufgebaut und gepflegt werden. Vorhandene Werkzeuge liefern oft lückenhafte oder uneinheitliche Daten, und die Informationsbeschaffung erfordert erheblichen manuellen Aufwand. Für eine systematische kryptografische Migration werden folgende Informationen benötigt:

- Algorithmen
- Schlüssel, Passwörter und Zugriffstoken
- Zertifikate (inkl. Laufzeiten)
- Protokolle
- Kryptografische Bibliotheken
- Verschlüsselungskonfigurationen
- Update-Mechanismen

Technisch lassen sich diese Informationen in einer Kryptografie-Stückliste – oder Cryptography Bill of Materials (CBOM) – erfassen, einem umfassenden Verzeichnis aller kryptografischen Assets. Für Softwaresysteme kann die Erstellung einer CBOM weitgehend automatisiert werden. In Umgebungen mit Altgeräten ist dagegen manueller Aufwand wahrscheinlich notwendig. Die CBOM dient als Grundlage, um schwache Algorithmen oder Abhängigkeiten von kryptografischen Bibliotheken zu erkennen, die während des Übergangs überwacht werden müssen. Es empfiehlt sich, für Erfassung, Dokumentation und Versionierung der CBOM ein standardisiertes Format zu verwenden, etwa „CycloneDX". Dies ist ein offener Standard zur Datenbeschreibung, der Informationen mit Bezug zur Cybersicherheit erfassen soll. Er wird von der Industrie breit unterstützt und lässt sich in den meisten Werkzeugen nutzen.

5.2 Sicherheitskritische Assets

Zu den kryptografisch geschützten Assets gehören üblicherweise:

- Konstruktions- und Entwicklungsdaten (CAD, Schaltpläne, Software-Quellcode), die einen Wettbewerbsvorteil bieten
- Anlagenkonfigurationen und Maschinenparameter
- Forschungs- und Entwicklungsdaten mit geistigem Eigentum
- Kunden- und Beschäftigtendaten, die durch die DSGVO und vergleichbare Vorschriften geschützt sind
- Finanz- und Vertragsdaten
- Betriebsdaten und Telemetrie
- Softwarecode und Software-Installationspakete

Künftig können weitere Assets hinzukommen, etwa digitale Zwillinge und Simulationsdaten.

Für jedes Asset muss festgehalten werden, in welchen Systemen es gespeichert oder verarbeitet wird. Zu diesen Systemen zählen:

- Speichersysteme wie Datenbanken für Backup, Archivierung und Datenverarbeitung, sowohl lokal als auch cloudbasiert
- Kommunikationskanäle wie VPNs und Webverkehr
- IoT-Geräte, Produktionsanlagen
- Blockchains

Da es sehr viele Assets geben kann, müssen sie nach Priorität behandelt werden. Die Priorität ergibt sich aus dem geforderten Grad an Vertraulichkeit und Integrität sowie aus dem Zeitraum, über den die Daten relevant sind. Sitzungstoken zum Beispiel sind flüchtig und nur für eine einzelne Sitzung relevant. Andere Datenbestände müssen dagegen über Jahre oder sogar unbegrenzt geschützt werden. Einige Anforderungen ergeben sich aus Vorschriften wie DSGVO, HIPAA, SOX oder PCI DSS.

5.3 Die Pflege des Krypto-Inventars

Das Krypto-Inventar muss einmal aufgebaut, danach aber fortlaufend gepflegt werden, während sich die IT-Landschaft verändert und die Post-Quanten-Migration fortschreitet.

Auf Basis der Klassifizierung kryptografischer Assets lassen sich Prioritäten setzen. Die Kriterien für die Klassifizierung können je nach Organisation unterschiedlich sein; als allgemeine Orientierung sind die folgenden Kriterien nützlich:

Die Voraussetzung: Vom Chaos zur kryptografischen Stückliste (CBOM)

Kryptografie ist tief in Systeme eingebettet und oft undokumentiert. Ein dynamisches Krypto-Inventar, standardisiert als CycloneDX-CBOM, ist die Grundlage für eine risikobasierte Migration und die Einhaltung regulatorischer Anforderungen.

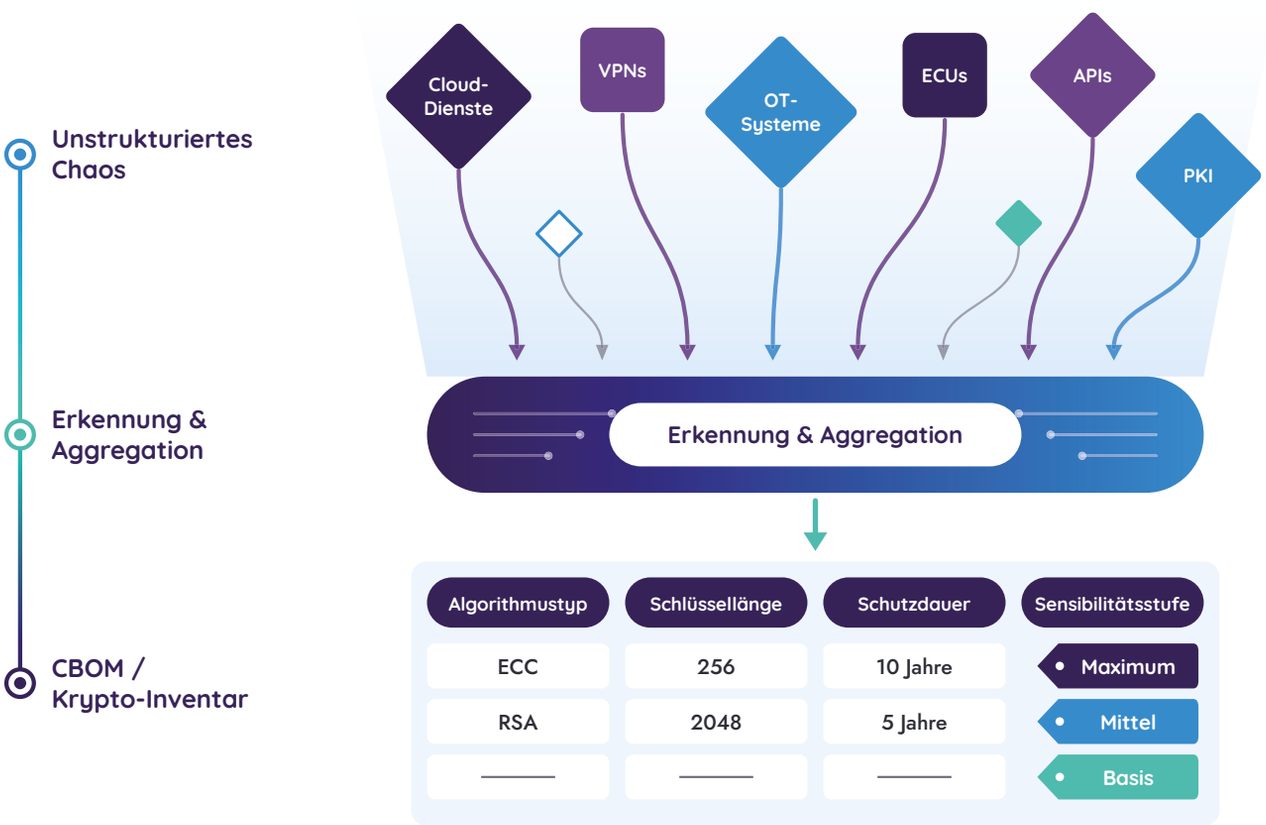


Abbildung 2 *Eine CBOM umfasst alle kryptografischen und informationsbezogenen Assets, die die Informationssicherheit Ihrer Organisation ausmachen.*

Sensitivitätsstufe

- **Höchster Schutz:** Daten mit den höchsten Anforderungen an Vertraulichkeit und Integrität, etwa kryptografische Schlüssel und geistiges Eigentum.
- **Besonderer Schutz:** Daten, die erhebliche Schutzmaßnahmen erfordern, darunter Kundeninformationen und interne Geschäftsunterlagen.
- **Basisschutz:** Daten mit geringerer Sensitivität, die dennoch angemessenen Sicherheitsmaßnahmen unterliegen.

Dauer der Vertraulichkeit

- **Kurzfristig:** Daten, die nur während der Übertragung oder für einen begrenzten Zeitraum geschützt werden müssen (z. B. Sitzungstoken).
- **Mittelfristig:** Daten, die über Monate oder wenige Jahre geschützt werden müssen (z. B. Projektdokumentation).
- **Langfristig:** Daten, die über viele Jahre oder unbegrenzt geschützt werden müssen (z. B. Patente, Finanzarchive).

Dauer der Integrität und Authentizität

- **Kurzfristig:** Integrität nur während der Übertragung oder für kurze Zeiträume erforderlich.
- **Mittelfristig:** Integrität über Monate oder Jahre erforderlich.
- **Langfristig:** Integrität über lange Zeiträume zu erhalten, möglicherweise so lange, wie die Daten existieren.

Regulatorische und Compliance-Anforderungen

- Geltende Gesetze, Normen und Vorschriften (etwa DSGVO, HIPAA, SOX, PCI DSS) beeinflussen verbindliche Schutzfristen und Sicherheitsmaßnahmen. Sie bestimmen, wie Daten zu behandeln und zu schützen sind. Medizinische Unterlagen zum Beispiel müssen nach HIPAA mindestens 6 Jahre geschützt werden.

Geschäftliche Auswirkungen

- **Operative Auswirkungen:** Folgen für Geschäftsprozesse und Geschäftskontinuität.
- **Finanzielle Auswirkungen:** Mögliche finanzielle Verluste.
- **Auswirkungen auf die Reputation:** Schaden für das Vertrauen in die Marke und für das Kundenvertrauen.
- **Rechtliche Auswirkungen:** Risiken von Bußgeldern, Klagen oder Sanktionen.

6. Empfohlenes Vorgehen zur Einführung

6.1 PQC-Einführung

Der Übergang zur Post-Quanten-Kryptografie ist keine einzelne technische Migration, sondern eine mehrjährige Umgestaltung der kryptografischen Grundlagen einer Organisation und zahlreicher externer Abhängigkeiten. Branchenübergreifende Erfahrungen zeigen: Eine erfolgreiche Einführung hängt weniger vom frühen Einsatz bestimmter Algorithmen ab als davon, zuerst Transparenz, Governance und kryptoagile Strukturen zu schaffen.[12]

Der allererste Schritt besteht darin, ein Bewusstsein für das wachsende Risiko der Offenlegung sensibler Daten zu schaffen. Zu den sensiblen Informationen können geistiges Eigentum, personenbezogene Daten und Kundendaten gehören; auch Kryptowährungen können für Ihre Organisation relevant sein. Dieses Bewusstsein zeigt sich in einer klaren Zuweisung von Verantwortlichkeiten – bis hinauf zur Geschäftsleitung.

Ein nächster Schritt ist es, die Systeme zu ermitteln, die diese Informationswerte speichern und verarbeiten. Selbst wenn die „großen" Softwarelösungen erfasst sind, sind in einem Unternehmen meist mehr IT- und Softwaresysteme im Einsatz, als die IT-Abteilung kennt. Proprietäre oder eigenentwickelte Software kann ein zusätzliches Risiko darstellen.

Sobald die Grundlage geschaffen ist, kann ein Migrationsplan erstellt werden. Die Organisation sollte den Auslösepunkt für den Beginn der Umstellung festlegen. Der Plan kann in mehreren Schritten umgesetzt werden, die anhand des jeweiligen Risikos festgelegt werden. Am Ende ist die Organisation vollständig umgestellt und setzt PQC in allen relevanten Systemen ein.

Das folgende Vorgehen zur Einführung folgt einem pragmatischen, industrieorientierten Ansatz. Es soll Organisationen ermöglichen, schrittweise voranzukommen, Risiken zu steuern und technische Maßnahmen mit geschäftlichen Prioritäten und regulatorischen Erwartungen in Einklang zu bringen.

6.2 Schritt 1 — Governance und strategische Verantwortung etablieren

Der Übergang zu PQC überschreitet klassische Organisationsgrenzen. Kryptografie liegt Authentifizierungsmechanismen, sicherer Kommunikation, Maschine-zu-Maschine-Vertrauen, Software-Updates und regulatorischer

Konformität zugrunde. Deshalb lässt sich die PQC-Migration nicht an ein einzelnes technisches Team oder allein an die Sicherheitsfunktion delegieren.

Organisationen sollten frühzeitig **klare Verantwortlichkeiten und Governance-Strukturen** für die Einführung von PQC festlegen. Dazu gehört, die Zuständigkeiten von IT-Leitung, Informationssicherheit, Unternehmensarchitektur, Systemverantwortlichen, Softwareentwicklung, Einkauf und – soweit zutreffend – OT oder Produktentwicklung aufeinander abzustimmen.

Über die Rollenverteilung hinaus verfolgt dieser Schritt einen weitergehenden strategischen Zweck: Er stellt sicher, dass Post-Quanten-Kryptografie als geschäftskritische, langfristige Initiative für Risikomanagement und Resilienz verstanden wird und nicht nur als künftige kryptografische Aktualisierung. Die Unterstützung durch die Geschäftsleitung ist unerlässlich, um Prioritäten zu setzen, Ressourcen zu sichern und Zielkonflikte zwischen Sicherheit, Leistung, Einschränkungen durch Altsysteme und Geschäftskontinuität zu lösen.

Ebenso wichtig ist die Festlegung von Entscheidungsgrundsätzen. Organisationen sollten klären, wie kryptografische Risiken bewertet werden, welche Datenkategorien und Systeme vorrangig zu schützen sind und wie regulatorische Fristen in interne Meilensteine übersetzt werden.

Zentrale Entscheidungen:

- Einen PQC-Sponsor oder eine Steuerungsfunktion auf oberster Führungsebene benennen
- Bereichsübergreifende Verantwortlichkeiten festlegen (IT, Sicherheit, Architektur, Einkauf, OT)
- Leitprinzipien vereinbaren: risikobasierte Priorisierung, Kryptoagilität als langfristiges Ziel
- Das Rahmenwerk für Informationssicherheit und die zugehörigen Richtlinien um PQC-spezifische Anforderungen ergänzen

6.3 Schritt 2 — Ein Krypto-Inventar aufbauen und pflegen

Ein Krypto-Inventar ist der zentrale Wegbereiter jeder glaubwürdigen PQC-Strategie. Organisationen können nicht schützen, was sie nicht sehen, und Kryptografie ist oft tief in Systeme, Protokolle, Geräte und Komponenten Dritter eingebettet, ohne explizit sichtbar zu sein.

Der Zweck des Krypto-Inventars ist nicht allein die Dokumentation. Es liefert vielmehr ein lebendes, strukturiertes Bild davon, wie Kryptografie in der gesamten Organisation genutzt wird, einschließlich:

- welche Algorithmen, Protokolle, Zertifikate und Schlüsselmaterialien im Einsatz sind
- wo langfristig vertrauliche Daten verarbeitet oder gespeichert werden
- wie Systeme voneinander abhängen und einander vertrauen
- welche Assets langlebig und damit künftigen Quantenbedrohungen ausgesetzt sind

In der Praxis stellen viele Organisationen fest, dass kryptografische Informationen über Werkzeuge, Teams und Lieferanten verstreut sind. In den frühen Phasen erfordert das oft erheblichen manuellen Aufwand. Das ist zu erwarten und sollte den Fortschritt nicht aufhalten. Der Wert des Inventars wächst schrittweise, je größer die Abdeckung und je besser die Datenqualität wird.

Um Nachhaltigkeit und Interoperabilität sicherzustellen, sollten kryptografische Informationen in einem strukturierten und standardisierten Format erfasst werden, etwa als Cryptography Bill of Materials (CBOM). Mit der Zeit wird das Krypto-Inventar zur Grundlage für Auswirkungsanalysen, Compliance-Berichte, Lieferantenmanagement und künftige kryptografische Umstellungen.

Nächste Schritte:

- Mit Assets mit hohem Risiko und langer Lebensdauer beginnen, nicht mit Vollständigkeit
- Systeme ermitteln, die Daten mit langfristigen Vertraulichkeits- und Integritätsanforderungen verarbeiten
- Kryptografische Nutzung, Abhängigkeiten und Vertrauensbeziehungen erfassen
- Das Krypto-Inventar als fortlaufenden Prozess etablieren, nicht als einmaliges Projekt

6.4 Schritt 3 — Kryptoagilität als Konstruktionsprinzip verankern

Post-Quanten-Kryptografie sollte nicht als einmaliger Austausch von Algorithmen verstanden werden. Die Geschichte zeigt, dass sich kryptografische Annahmen weiterentwickeln und künftige Schwachstellen – ob quantenbezogen oder nicht – nicht auszuschließen sind. Das strategische Ziel geht deshalb über PQC hinaus und zielt auf Kryptoagilität.

Kryptoagilität bezeichnet die Fähigkeit, kryptografische Mechanismen ohne größere Architekturänderungen, Betriebsunterbrechungen oder lange Migrationszyklen zu er-

setzen oder anzupassen. Für viele Organisationen bedeutet das, bestehende Entwürfe zu überarbeiten, in denen Kryptografie fest codiert, eng gekoppelt oder implizit in Produkte und Prozesse eingebettet ist.

In dieser Phase sollten Organisationen bewerten, wo kryptografische Flexibilität bereits vorhanden ist (z. B. konfigurierbare TLS-Stacks) und wo Einschränkungen bestehen (z. B. eingebettete Systeme, ältere Appliances). Abstraktionsschichten, standardisierte Kryptobibliotheken und richtliniengesteuerte Konfigurationen verringern den künftigen Migrationsaufwand erheblich.

Kryptoagilität hat auch organisatorische Dimensionen: Beschaffungskriterien, Richtlinien für die Softwareentwicklung und Prozesse des Lebenszyklusmanagements müssen Anpassungsfähigkeit ausdrücklich unterstützen, nicht nur Konformität zum Zeitpunkt der Einführung.

Vorgehensweise:

- Systeme mit fest codierter oder nicht austauschbarer Kryptografie ermitteln
- Architekturmuster einführen, die kryptografische Komponenten kapseln
- Entwicklungs- und Beschaffungsrichtlinien so anpassen, dass sie Kryptoagilität verlangen
- Die PQC-Migration als einen Anwendungsfall einer umfassenderen kryptoagilen Strategie behandeln

6.5 Schritt 4 — PQC und hybride Kryptografie pragmatisch einführen

Sobald Transparenz und Kryptoagilität geschaffen sind, können Organisationen mit der kontrollierten Einführung von PQC-Mechanismen beginnen. Derzeit sind hybride kryptografische Verfahren – die klassische und Post-Quanten-Algorithmen kombinieren – der robusteste und am häufigsten empfohlene Übergangsansatz.

Hybride Verfahren stellen sicher, dass die Sicherheit auch dann erhalten bleibt, wenn sich eine Klasse von Algorithmen später als verwundbar erweist. Sie ermöglichen es Organisationen zudem, Betriebserfahrung mit Post-Quanten-Algorithmen zu sammeln und dabei die Interoperabilität mit bestehenden Systemen zu wahren.

Anbieter von IT-Systemen sollten frühzeitig angesprochen werden, um Informationen über ihren Stand und ihre Roadmap zur Unterstützung von PQC-Mechanismen sowie über ihren Ansatz zur Kryptoagilität zu erhalten.

Erste Einführungen sollten sich auf Anwendungsfälle konzentrieren, in denen kryptografische Änderungen betrieblich machbar sind und die Sicherheitswirkung hoch ist, zum Beispiel:

- sichere Kommunikationskanäle (TLS, VPN)
- Authentifizierung und digitale Signaturen
- interne Vertrauensbeziehungen zwischen Diensten

Leistung, Interoperabilität und Betriebsstabilität sollten genau beobachtet werden. Dabei auftretende Hindernisse dürfen jedoch nicht das gesamte Vorhaben gefährden, sondern müssen gezielt angegangen werden. Frühe, eng begrenzte Einführungen verringern die Unsicherheit erheblich und bereiten die Teams auf einen breiteren Rollout vor.

Vorgehensweise:

- „Low-Regret"-Anwendungsfälle ermitteln, die sich für hybride Einführungen eignen
- Vollständige Austauschstrategien vermeiden, solange Standards oder Ökosysteme noch in Entwicklung sind
- Die Aktivierung von PQC mit Anbietern, Cloud-Providern und Integratoren abstimmen
- Frühe PQC-Einführungen als Lernschritte behandeln, nicht als Endzustand

6.6 Schritt 5 — Kontinuierliche Verbesserung

Die Einführung von PQC ist ein langfristiger, fortlaufender Weg und kein einzelner Meilenstein. Sobald die ersten Einführungen beginnen, sollten Organisationen den Schwerpunkt auf Messung, Governance und Verfeinerung verlagern.

Kennzahlen, die aus dem Krypto-Inventar abgeleitet werden, helfen der Geschäftsleitung, Fortschritt, Restrisiko und verbleibende Abhängigkeiten zu verstehen. Diese Kennzahlen unterstützen zudem die regulatorische Berichterstattung, die Auditfähigkeit und interne Entscheidungen.

Während Standards reifen, die Unterstützung im Ökosystem zunimmt und sich regulatorische Erwartungen weiterentwickeln, sollten Organisationen ihre Roadmaps entsprechend anpassen. Das langfristige Ziel ist nicht nur, „PQC-bereit" zu sein, sondern kryptografische Resilienz als dauerhafte Fähigkeit der Organisation zu erhalten.

Wesentliche Elemente dabei sind:

- KPIs für Quantenexposition und Migrationsfortschritt definieren
- Das Krypto-Inventar regelmäßig aktualisieren und Prioritäten neu bewerten
- Die PQC-Reife von Anbietern und Lieferanten fortlaufend überprüfen
- Wo sinnvoll, von hybriden Verfahren zu vollständigen Post-Quanten-Lösungen übergehen

7. Fazit

Die PQC-Migration ist eine strategische Notwendigkeit, denn die klassische Kryptografie – die Grundlage der Informationssicherheit – wird in absehbarer Zeit gebrochen sein. Der Zeitraum **2026–2030** ist entscheidend für die Vorbereitung. Wer jetzt beginnt, sichert Resilienz, schützt langfristige Vertraulichkeit und ermöglicht die Einhaltung entstehender Vorschriften. Zudem vermeidet er höhere Kosten für eine späte Einführung unter erhöhtem Druck.

Für eine erfolgreiche Migration muss eine Organisation zwei Fragen beantworten:

- Welche Objekte müssen zuerst geschützt werden, und mit welchen Systemen wird dies erreicht?
- Künftige Änderungen werden kommen – wie erreichen wir also kryptografische Agilität?

In den vorangegangenen Kapiteln haben wir die Schritte beschrieben, mit denen Post-Quanten-Sicherheit erreicht werden kann. Als Erstes muss eine Governance-Struktur mit starker Unterstützung der Geschäftsleitung geschaffen werden. Der zweite Schritt ist der Aufbau eines Krypto-Inventars, das die folgenden Fragen beantwortet:

- In welchen Systemen liegen die kritischen Informationswerte?
- Welche kryptografischen Mittel schützen diese Werte?

Auf dieser Grundlage lässt sich eine risikobasierte Migrationsstrategie entwickeln. Systeme externer Lieferanten müssen je nach Strategie des Lieferanten aktualisiert oder ersetzt werden. Zusätzlich muss eine angemessene Unterstützung für eigenentwickelte Softwaresysteme sichergestellt werden.

Nicht nur interne Prozesse sind zu berücksichtigen, sondern auch die Produkte und Dienstleistungen der Organisation. Insbesondere langlebige Güter müssen zukunftssicher ausgelegt werden, und die besonderen Anforderungen von PQC sind zu beachten – vor allem der größere Speicherbedarf für digitale Signaturen und die benötigte Rechenleistung. Kryptoagilität, also die Fähigkeit, auch innerhalb von Produkten über den gesamten Lebenszyklus hinweg die kryptografischen Mechanismen zu aktualisieren, reduziert spätere Retrofit-Kosten, schützt die installierte Basis und stärkt die langfristige Wettbewerbsfähigkeit. Maschinen- und Anlagenbauer sollten dies während der Entwicklung ihrer Produkte berücksichtigen.

Bei der Migration von Systemen muss die Interoperabilität zwischen unterschiedlichen Systemen sichergestellt werden. Altkomponenten in einer Verarbeitungskette können dazu führen, dass auf klassische kryptografische Verfahren zurückgegriffen werden muss. Dadurch können Schwachstellen entstehen.

Aufwand und Budget für die Umsetzung einer PQC-Migrationsstrategie können den Umfang einer Umstellung der gesamten IT-Infrastruktur auf eine neue Technologiegeneration erreichen. Manche Komponenten bringen PQC-Mechanismen unbemerkt über reguläre Updates mit, andere müssen ersetzt werden. Alle Komponenten müssen jedoch konfiguriert, integriert und gewartet werden. Beschäftigte benötigen Schulungen und Sensibilisierung; beides ist für die wirksame Anwendung von Sicherheitsmaßnahmen unerlässlich.

Die Umsetzung einer vollständigen Migrationsstrategie kann Aktivitäten über mehrere Jahre nach sich ziehen. Für ein so komplexes Vorhaben ist ein wirksames Programmmanagement erforderlich, und die Unterstützung durch die oberste Führungsebene ist unerlässlich. Der Fortschritt sollte transparent messbar sein. An sinnvollen Meilensteinen des Migrationspfads sollten Überprüfungen stattfinden, um die korrekte Nutzung der PQC-Mechanismen sicherzustellen. Besondere Aufmerksamkeit gilt kritischen Informationsobjekten, die noch mit klassischen Mitteln geschützt sind.

In diesem Papier geben wir eine kompakte Einführung in die Post-Quanten-Kryptografie: warum sie für die meisten Organisationen wichtig ist und wie man sich auf die Zeit vorbereitet, in der Quantencomputer ausreichend leistungsfähig und wirtschaftlich verfügbar sind, um die Sicherheit der Public-Key-Kryptografie ernsthaft zu bedrohen.

Das Thema wurde auf regulatorischer Ebene aufgegriffen, und es liegen Leitfäden für die Planung und Durchführung der Migration zu PQC-Mechanismen vor. Diese können für die Migration herangezogen werden, die in allen Organisationen zügig beginnen sollte.

Quellen

1. https://ec.europa.eu/newsroom/dae/redirection/document/117507
2. https://www.bsi.bund.de/EN/Service-Navi/Presse/Pressemitteilungen/Presse2024/241127_Post-Quantum_Cryptography.html
3. Google, „A timeline for cryptography migration", Google Blog, März 2026. [Online]. Verfügbar unter: https://blog.google/innovation-and-ai/technology/safety-security/cryptography-migration-timeline/. Google gehört zu den Unternehmen, die aktiv in den Bau eines Quantencomputers investieren. In diesem Beitrag hat Google den eigenen Zeitplan für die PQC-Migration auf 2029 vorgezogen und integriert PQC in eigene Produkte wie Android.
4. Thé, Jesse Van Griensven, Victor Oliveira Santos, and Bahram Gharabaghi. 2026. „A Novel Hybrid Quantum Circuit for Integer Factorization: End-to-End Evaluation in Simulation and Real Quantum Hardware" Journal of Cybersecurity and Privacy 6, no. 2: 71. https://doi.org/10.3390/jcp6020071
5. BSI – Technische Richtlinie, Kryptographische Verfahren: Empfehlungen und Schlüssellängen. BSI TR-02102-1, 23. Januar 2026. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile&v=15. Diese Technische Richtlinie beschreibt ausführlich den kryptografischen Hintergrund klassischer und post-quanten-kryptografischer Algorithmen. Sie richtet sich an Entwickler von Systemen, die kryptografische Algorithmen einsetzen.
6. NIST – Post-Quantum Cryptography FAQs https://csrc.nist.gov/projects/post-quantum-cryptography/faqs
7. NIST Releases First 3 Finalized Post-Quantum Encryption Standards. 13. August 2024. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
8. NIS Cooperation Group. A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography, 11. Juni 2025. https://ec.europa.eu/newsroom/dae/redirection/document/117507
9. Federal Office for Information Security (BSI) *et al.*, „Securing tomorrow, today: Transitioning to post-quantum cryptography", Partner aus 18 EU-Mitgliedstaaten, gemeinsame Erklärung, 27. November 2024. Online verfügbar: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/PQC-joint-statement.pdf
10. Quantum Technologies and Quantum-Safe Cryptography. https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/quantentechnologien-und-post-quanten-kryptografie_node.html
11. https://cyber.gouv.fr/en/technological-and-cybersecurity-challenges/post-quantum-cryptography/
12. A. Amadori *et al.*, „The PQC Migration Handbook: Guidelines for migrating to post-quantum cryptography", AIVD, CWI und TNO, Techn. Bericht, 2. Aufl., Dez. 2024. Online verfügbar: https://publications.tno.nl/publication/34643386/fXcPVHsX/TNO-2024-pqc-en.pdf. Dieses Buch bietet einen umfassenden Überblick über die Bestandteile einer organisatorischen Migrationsstrategie hin zu PQC. Es enthält zudem eine Fülle tiefgehender technischer Informationen, die für Sensibilisierung und Verständnis des Themas nützlich sind.

QUANTUM TECHNOLOGY AND
APPLICATION CONSORTIUM

QUTAC

www.qutac.de

