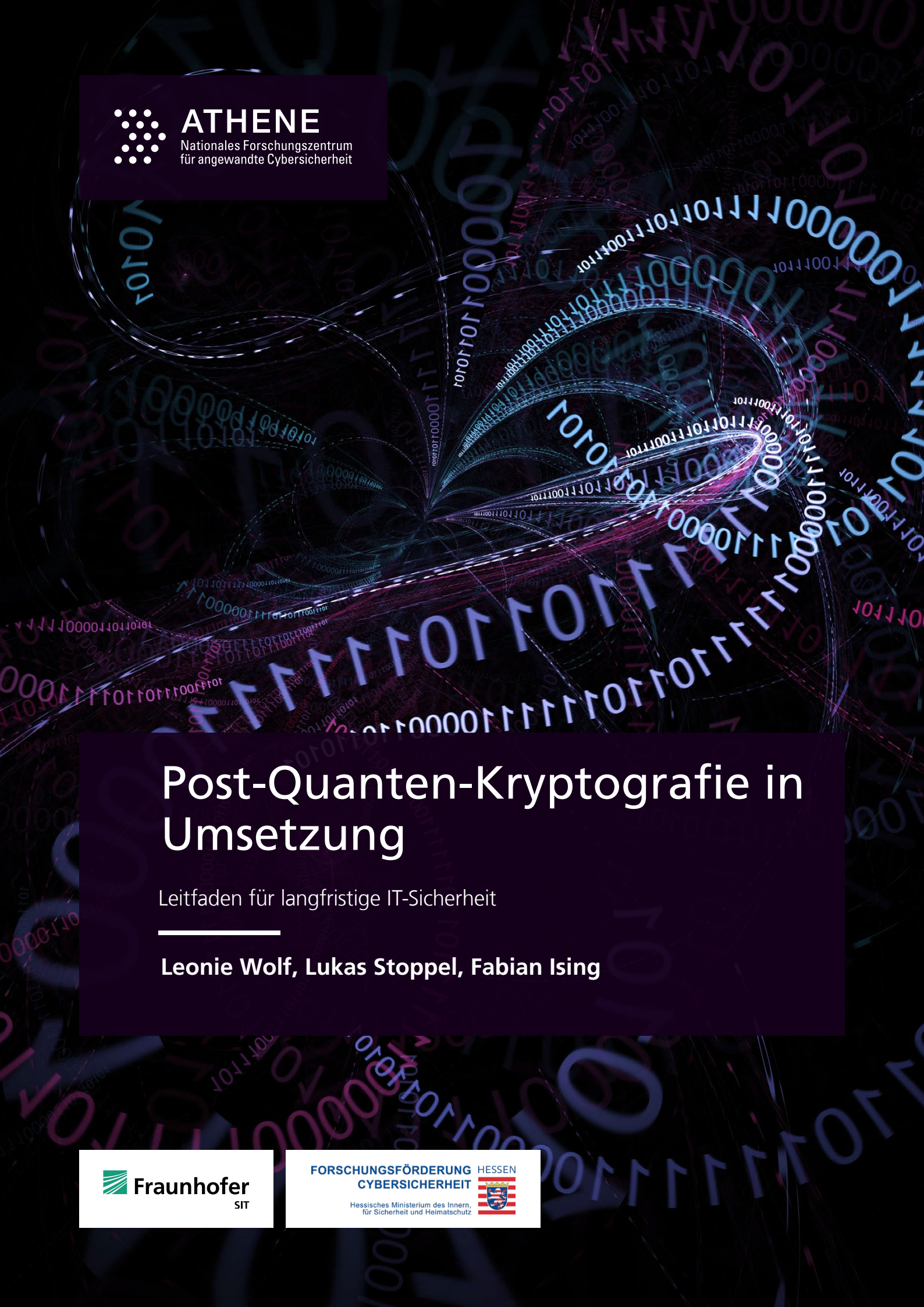


ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

Post-Quanten-Kryptografie in Umsetzung

Leitfaden für langfristige IT-Sicherheit

Leonie Wolf, Lukas Stoppel, Fabian Ising

Fraunhofer SIT

FORSCHUNGSFÖRDERUNG CYBERSICHERHEIT HESSEN
Hessisches Ministerium des Innern, für Sicherheit und Heimatschutz

Post-Quanten-Kryptografie in Umsetzung

Leitfaden für langfristige IT-Sicherheit

Impressum

Layout und Satz
Peggy Watzke

Kontakt
Nationales Forschungszentrum für angewandte Cybersicherheit ATHENE
c/o Fraunhofer-Institut für Sichere Informationstechnologie SIT
Rheinstraße 75
64295, Darmstadt

© Fraunhofer-Institut für Sichere Informationstechnologie SIT, Darmstadt, 2026

Hinweise
Dieser Beitrag entstand im Rahmen eines Projektes mit dem Hessischen Ministerium des Innern, für Sicherheit und Heimatschutz.

Titelbild: pixabay, insspirito

Die in diesem Beitrag enthaltenen Informationen sind sorgfältig erstellt worden, können eine Rechtsberatung jedoch nicht ersetzen. Eine Haftung oder Garantie dafür, dass die Informationen die Vorgaben der aktuellen Rechtslage erfüllen, wird daher nicht übernommen. Gleiches gilt für die Brauchbarkeit, Vollständigkeit oder Fehlerfreiheit, so dass jede Haftung für Schäden ausgeschlossen wird, die aus der Benutzung dieser Arbeitsergebnisse/Informationen entstehen können. Diese Haftungsbeschränkung gilt nicht in Fällen von Vorsatz.

Autoren

Leonie Wolf
ATHENE | Fraunhofer SIT

Lukas Stoppel
ATHENE | Fraunhofer SIT

Fabian Ising
ATHENE | Fraunhofer SIT

Liebe Leserin, lieber Leser,

Liebe Leserin, lieber Leser,

sichere Kommunikation ist die Grundlage für Vertrauen in unserer digital vernetzten Welt - sei es in Unternehmen, der Zivilgesellschaft oder der öffentlichen Verwaltung. Verschlüsselung und digitale Signaturen schützen diese Kommunikation vor unbefugtem Zugriff und Manipulation. Doch die Bedrohungslage entwickelt sich weiter, denn Quantencomputer könnten zukünftig viele der heute verwendeten Schutzmechanismen umgehen. Um langfristig die Sicherheit unserer digitalen Infrastruktur zu gewährleisten, ist die Umstellung auf quantenresistente Kryptografie ein unverzichtbarer Schritt.

Hessen setzt auf einen ganzheitlichen Ansatz für Cybersicherheit. Das Hessische Ministerium des Innern, für Sicherheit und Heimatschutz fördert gezielt Projekte, die diese Sicherheit stärken. Der vorliegende Leitfaden „Post-Quanten-Kryptografie in Umsetzung" ist das Ergebnis dieser Zusammenarbeit und baut auf dem vorherigen Leitfaden zur „Krypto-Agilität" auf. Er wurde unter Einbeziehung aktueller Forschungsergebnisse sowie der konkreten Bedürfnisse von Bürgern, Unternehmen und öffentlichen Einrichtungen entwickelt. Von Anfang an waren Vertreter der kommunalen Familie aktiv in die Erarbeitung eingebunden, um praxisnahe Lösungen zu schaffen.

Post-Quanten-Kryptografie umfasst Verfahren, die unsere digitale Kommunikation auch vor Angriffen durch Quantencomputer schützen. Sie wird bereits heute zur Sicherung eines Großteils des Internetverkehrs genutzt. Die flächendeckende Nutzung dieser Verfahren ist ein zentraler Baustein für unsere digitale Resilienz und gleichzeitig eine große Herausforderung angesichts der vielfältigen IT-Landschaft. Die EU-Kommission hat eine Roadmap für die Umsetzung vorgelegt. Dieser Leitfaden zeigt, welche strategischen Schritte in Hessen notwendig sind, um diese Roadmap umzusetzen und so die Sicherheit in der digitalen Welt zu erhöhen.

Prof. Dr. Roman Poseck

Hessischer Minister des Innern, für Sicherheit und Heimatschutz

Management Summary

Die Verfügbarkeit leistungsfähiger Quantencomputer wird die IT-Sicherheit grundlegend verändern. Die meisten heute eingesetzten kryptografischen Verfahren wären dann nicht mehr sicher. Das Risiko ist nicht hypothetisch, sondern bereits heute real: Nach dem „Harvest-now-Decrypt-Later"-Prinzip wird verschlüsselte Kommunikation bereits jetzt aufgezeichnet, um sie künftig zu entschlüsseln. Für Organisationen mit sensiblen oder langfristig schützenswerten Daten besteht damit unmittelbarer Handlungsbedarf.

Die zentrale Lösung für diese Herausforderung ist die Post-Quanten-Kryptografie (PQC). Die Migration ist jedoch keine rein technische Aufgabe, sondern eine strategische: Sie betrifft bestehende Systeme ebenso wie künftige Beschaffungen und muss angesichts langer IT-Lebenszyklen frühzeitig geplant werden. Maßnahmen, die erst getroffen werden, wenn Quantencomputer verfügbar sind, kommen zu spät.

Dieser Leitfaden unterstützt Kommunen, Behörden und andere Organisationen dabei, die PQC-Migration strukturiert anzugehen. Im Fokus stehen Maßnahmen, die bereits heute umgesetzt werden können und zugleich die allgemeine IT-Sicherheit stärken (sogenannte „No-Regret-Moves"), sowie strategische Weichenstellungen für bestehende Systeme und zukünftige Beschaffungen.

Die zentralen Empfehlungen dieses Leitfadens sind:

1. Transparenz durch Inventarisierung
Systematische Erfassung aller IT-Systeme, eingesetzter Kryptografie sowie ihrer Abhängigkeiten. Nur dokumentierte Systeme können gezielt migriert werden.

2. Risiken bewerten und priorisieren
Strukturierte Risikoanalyse nach Angreifbarkeit, Schadenspotenzial bei Kompromittierung und Migrationsaufwand, um Ressourcen gezielt einzusetzen.

3. Migration strategisch angehen
Viele Standardkomponenten und Kommunikationsprotokolle unterstützen bereits hybride oder quantenresistente Verfahren. Erste Migrationsschritte sind oft mit überschaubarem Aufwand möglich. Für Alt-Systeme stehen häufig Übergangslösungen zur Verfügung.

4. Beschaffungen zukunftssicher gestalten
PQC-Anforderungen sollten bereits heute in Vergaben einfließen: Dokumentationspflichten, Kryptoagilität und die Unterstützung hybrider Verfahren sind dabei zentrale Kriterien.

Die Migration zur Post-Quanten-Kryptografie ist ein langfristiger Prozess, der frühzeitig begonnen werden muss. Wer jetzt handelt, reduziert Risiken und sichert die IT-Infrastruktur nachhaltig ab. Wer wartet, muss später unter Zeitdruck und mit höheren Kosten reagieren.

Inhalt

Einleitung

Schon lange nutzen Menschen Kryptografie, um Nachrichten vor fremdem Zugriff und Veränderungen zu schützen. Durch die aktuelle Entwicklung von Quantencomputern, die bestimmte mathematische Probleme sehr effizient lösen, sind jedoch weit verbreitete kryptografische Prinzipien gefährdet. Nicht nur in Zukunft, sondern bereits jetzt – nach dem Harvest-Now-Decrypt-Later-Prinzip können verschlüsselte Daten heute gespeichert und später mithilfe von Quantencomputern entschlüsselt werden.

Eine Lösung für dieses Problem liegt in der Post-Quanten-Kryptografie (PQC), die auf neuen kryptografischen Prinzipien basiert, die sowohl vor klassischen als auch vor Quantencomputern schützen. Eine zentrale Herausforderung besteht darin, diese in die Fläche zu bringen, bevor langfristig zu schützende Daten in Gefahr geraten. Die Migration ist keine rein technische Aufgabe. Sie betrifft gewachsene IT-Landschaften ebenso wie Zuständigkeiten, Prozesse und Vergaben. Ohne ein strukturiertes Vorgehen lässt sich eine sichere Migration nicht gewährleisten.

Die Herausforderungen sind bekannt – so hat die Europäische Union im Juni 2025 einen Fahrplan für die Migration zur Post-Quanten-Kryptografie in den Mitgliedstaaten veröffentlicht [1]. Dieser Fahrplan ist ambitioniert und macht deutlich, dass die Migration schnell erfolgen muss. Allerdings werden keine Aussagen dazu getroffen, wie die Migration auf operativer Ebene erfolgen soll.

Dieser Leitfaden soll Kommunen, Landesbehörden und weitere Interessierte dabei unterstützen, die Migration auf PQC zu planen und umzusetzen. Ziel ist die Verknüpfung des aktuellen Forschungsstands mit praktischen Empfehlungen. Der Leitfaden richtet sich explizit auch an Entscheidungsträgerinnen und -träger, die (noch) keine Expertinnen und Experten in diesem Themenbereich sind, aber die Migration aktiv vorantreiben möchten. Dazu geben wir Empfehlungen für erste Schritte, die die IT-Sicherheit allgemein verbessern und zugleich die Migration unterstützen. Hinweise zur Auswahl von kryptografischen Standards und zur Migration bestehender Systeme sind ebenso wichtig wie Empfehlungen zur Auftragsvergabe für neue Systeme.

Erstellt wurde dieser Leitfaden vom Fraunhofer-Institut für Sichere Informationstechnologie SIT in Darmstadt in Zusammenarbeit mit dem Hessischen Ministerium des Innern, für Sicherheit und Heimatschutz sowie Vertreterinnen und Vertretern der kommunalen Familie Hessen. Das Fraunhofer SIT ist eine herausragende Einrichtung für angewandte IT-Sicherheitsforschung und als Teil des Nationalen Forschungszentrums ATHENE hervorragend in der hessischen Spitzenforschung vernetzt.

Kapitel 1 – Sichere Kommunikation im Quantenzeitalter

Quantencomputer werden in absehbarer Zukunft viele der heute eingesetzten asymmetrischen kryptografischen Verfahren brechen können. In der Praxis bedeutet das: Mit klassischen kryptografischen Verfahren verschlüsselte Daten könnten künftig entschlüsselt werden. Die Lösung ist die Post-Quanten-Kryptografie (PQC).

Kapitel 1.1: Risiko durch Quantencomputer

Quantencomputer funktionieren grundlegend anders als klassische Computer. Etablierte Leistungsbegriffe greifen daher zu kurz: Ihr Vorteil liegt nicht in einer höheren Abarbeitungsgeschwindigkeit, sondern in der drastischen Reduktion der Rechenschritte bei hochkomplexen Aufgaben.

Das zeigt sich besonders bei kryptografischen Problemen: Quantencomputer können bestimmte mathematische Aufgaben, auf denen heute viele kryptografische Verfahren beruhen, wesentlich effizienter lösen. Konkret bedroht der Shor-Algorithmus das Faktorisierungsproblem (und damit Verfahren wie RSA) sowie das diskrete Logarithmusproblem (und damit Verfahren wie ECC). Der entscheidende Punkt ist dabei nicht „schnelleres Rechnen" im klassischen Sinn, sondern dass Quantencomputer die zugrunde liegenden Probleme mit deutlich weniger Rechenschritten lösen [2].

Für die Praxis heißt das: Klassische asymmetrische Verschlüsselungs- und Signaturverfahren wie Diffie-Hellman, RSA und ECC müssen ersetzt werden.

Symmetrische Verfahren wie der Advanced Encryption Standard (AES) oder ChaCha20 sind ebenfalls betroffen, allerdings in deutlich geringerem Ausmaß [3]. Hier spielt vor allem der Grover-Algorithmus eine wichtige Rolle: Er beschleunigt eine reine Brute-Force-Suche „quadratisch", was vereinfacht gesagt dem Halbieren des Sicherheitsniveaus in Bit entspricht (z. B. 128 Bit → 64 Bit). Eine robuste Gegenmaßnahme ist daher, die Schlüssellänge zu verdoppeln. So würde ein Wechsel von AES-128 auf AES-256 (und entsprechend auch der Einsatz von 256-Bit-Schlüsseln wie bei ChaCha20) selbst unter Grover weiterhin ein Sicherheitsniveau von 128 Bit bieten und damit dem vom BSI geforderten Sicherheitsniveau von 120 Bit entsprechen.

Für die Praxis heißt das: Bei symmetrischen Verschlüsselungsverfahren genügt eine Erhöhung der Schlüssellänge.

Der Quantum Threat Timeline Report 2024 [4] befragte 32 Expertinnen und Experten dazu, wie wahrscheinlich sie es einschätzen, dass kryptografisch relevante Quantencomputer in den nächsten 5, 10, 15, 20 oder 30 Jahren einen 2048-Bit-RSA-Schlüssel in weniger als 24 Stunden faktorisieren können. Die in Tabelle 1 dargestellten Ergebnisse zeigen, dass bereits für den Zeithorizont von zehn Jahren mehr als die Hälfte der befragten Expertinnen und Experten von einer Eintrittswahrscheinlichkeit von mindestens 50 Prozent ausgeht.

Vor diesem Hintergrund ist, obgleich Quantencomputer gegenwärtig noch keine operative Bedrohung darstellen, davon auszugehen, dass das sogenannte Harvest-Now-Decrypt-Later-Angriffsszenario bereits aktiv angewendet wird.

Im Rahmen dieses Szenarios werden durch ressourcenstarke Akteure – sowohl staatliche als auch nichtstaatliche – verschlüsselte Kommunikationsdaten systematisch erfasst und gespeichert. Zu einem späteren Zeitpunkt könnten diese Daten, bei Verfügbarkeit eines hinreichend leistungsfähigen Quantencomputers, retrospektiv entschlüsselt werden.

Diese Bedrohungslage betrifft bereits heute sämtliche Kommunikationsformen, wobei insbesondere Daten mit langfristigem Schutzbedürfnis einem erhöhten Risiko ausgesetzt sind. Hierzu zählen unter anderem:

- Personenbezogene Daten (gesundheitsbezogene Daten, biometrische Informationen, politische Zugehörigkeiten)
- Politisch sensible Informationen (diplomatische Korrespondenz, strategische Dokumente)
- Rechtlich schützenswerte Daten (gerichtliche oder anwaltliche Kommunikation, Vertragswerke)

Angesichts der Tatsache, dass eine Migration von klassischen kryptografischen Verfahren zu PQC je nach Systemkomplexität einen erheblichen zeitlichen Aufwand erfordert, empfehlen staatliche Institutionen einen sofortigen Migrationsbeginn. Sowohl die Europäische Union in ihrer Roadmap als auch die niederländische Organisation für angewandte Naturwissenschaften (TNO) haben entsprechende Handlungsempfehlungen zur proaktiven Implementierung von PQC-Verfahren formuliert [1] [5]. In Deutschland benennt das BSI in seiner Technischen Richtlinie konkrete Empfehlungen für standardisierte Verfahren [6].

Tabelle 1 – Experteneinschätzung: Wann wird ein Quantencomputer einen 2048-Bit-RSA-Schlüssel in weniger als 24 Stunden faktorisieren können?

Wahrscheinlichkeit	5 Jahre	10 Jahre	15 Jahre	20 Jahre	30 Jahre
> 99% Ausgesprochen wahrscheinlich	0%	0%	3%	12%	19%
> 95% Ausgesprochen	0%	6%	12%	22%	31%
> 70% Eher wahrscheinlich	3%	9%	19%	25%	38%
~ 50% Unentschieden	6%	16%	31%	31%	9%
< 30% Eher unwahrscheinlich	19%	22%	22%	6%	0%
< 5% Unwahrscheinlich	16%	34%	9%	3%	3%
< 1% Sehr unwahrscheinlich	56%	12%	3%	0%	0%

Kapitel 1.2: Grundlagen Post-Quanten-Kryptografie

Der Kern der symmetrischen Kryptografie ist die Verwendung desselben Schlüsselmaterials für die Ver- und Entschlüsselung. Etablierte Verfahren sind beispielsweise AES und ChaCha20.

Vorteile der symmetrischen Kryptografie:

- Effizient berechenbar, daher auch für größere Datenmengen geeignet.
- Durch die Verdoppelung der Schlüssellänge lässt sich das ursprüngliche Sicherheitsniveau gegenüber Quantencomputern beibehalten.

Nachteile der symmetrischen Kryptografie:

- Für den Schlüsselaustausch ist ein sicherer Kanal erforderlich.

Der Kern der asymmetrischen Kryptografie besteht in der Verwendung eines öffentlichen und eines privaten Schlüssels. Werden Nachrichten mit dem öffentlichen Schlüssel verschlüsselt, können sie ausschließlich mit dem privaten Schlüssel wieder entschlüsselt werden.

Vorteile der asymmetrischen Kryptografie:

- Es ist kein sicherer Kanal für den Schlüsselaustausch erforderlich.
- Signaturen können (privat) erzeugt und (öffentlich) verifiziert werden.

Nachteile der asymmetrischen Kryptografie:

- Die Berechnungen sind langsam und ineffizient für große Nachrichten.
- Die Echtheit des öffentlichen Schlüssels muss geprüft werden.
- Klassische asymmetrische Verfahren sind nicht quantenresistent und müssen durch PQC-Verfahren ersetzt werden.

Moderne kryptografische Kommunikationssysteme basieren grundlegend auf drei kryptografischen Bausteinen:

- Ein symmetrisches Verschlüsselungsverfahren zur Verschlüsselung von Daten.
- Ein asymmetrisches Schlüsselkapslungsverfahren (Key Encapsulation Mechanism, KEM), bei dem ein symmetrischer Schlüssel zwischen den Kommunikationsparteien ausgetauscht wird.
- Ein asymmetrisches Signaturverfahren zur Gewährleistung der Identität der Parteien.

Symmetrische Verschlüsselungsverfahren wie AES oder ChaCha20 sind durch quantencomputerbasierte Angriffe nur in begrenztem Umfang angreifbar. Vor diesem Hintergrund konzentriert sich die PQC primär auf das Feld der asymmetrischen Kryptografie, da etablierte Verfahren wie RSA und elliptische Kurven (ECC) durch den Shor-Algorithmus vollständig kompromittierbar sind. PQC betrifft hauptsächlich die asymmetrische Kryptografie.

Hinsichtlich ihrer grundsätzlichen Funktionsweisen weisen PQC-Verfahren strukturelle Analogien zu klassischen asymmetrischen Verfahren auf. Die Sicherheit dieser Verfahren beruht auf mathematischen Problemen, für die bisher keine effizienten Quantenangriffe bekannt sind – im Gegensatz zur Primfaktorzerlegung oder zum diskreten Logarithmus, die durch den Shor-Algorithmus in relevanter Zeit lösbar sind.

Standardisierte PQC-Verfahren

Die potenzielle Gefahr durch Quantencomputer ist seit 1994 durch den Shor-Algorithmus bekannt. Mit neuen Erfolgen im Bereich der Quantencomputer startete das NIST im Jahr 2016 einen Prozess zur Standardisierung von PQC.

Über drei Evaluierungsrunden (2017–2022) wurden die Kandidaten durch öffentliche Analyse, Sicherheitsbewertungen und Performance-Tests reduziert, wobei die Krypto-Community aktiv beteiligt war. Im August 2024 veröffentlichte das NIST die ersten drei finalen Standards für digitale Signaturen und KEM. Weitere Standards (wie FALCON und HQC) befinden sich zur Zeit der Recherche noch im Standardisierungsprozess.

Bereits heute sind einige quantenresistente, also gegen Quantencomputer gesicherte, Algorithmen standardisiert und sowohl für den Einsatz in Deutschland als auch international freigegeben. Tabelle 2 zeigt eine Übersicht über diese Algorithmen und deren Standardisierungsstand. Im Rahmen des Standardisierungsprozesses der US-amerikanischen Standardisierungsbehörde NIST wurden mehrere PQC-Verfahren für den produktiven Einsatz spezifiziert:

- Der Key-Encapsulation-Mechanismus ML-KEM (FIPS 203).
- Das Signaturverfahren ML-DSA (FIPS 204).
- Das Signaturverfahren SLH-DSA (FIPS 205).

Tabelle 2 – Standardisierte quantenresistente Algorithmen sowie zugehörige Standards des NIST und BSI (Stand Februar 2026)

Algorithmus	Verwendung	NIST	BSI
ML-KEM	KEM (Verschlüsselung)	FIPS 203	TR-02102
FRODO-KEM	KEM (Verschlüsselung)	-	TR-02102
Classic McEliece	KEM (Verschlüsselung)	-	TR-02102
HQC	KEM (Verschlüsselung)	-	TR-02102
ML-DSA	Signaturen	FIPS 204	TR-02102
SLH-DSA	Signaturen	FIPS 205	TR-02102
XMSS	Signaturen	SP 800-208	TR-02102
LMS	Signaturen	SP 800-208	TR-02102

Gemäß BSI TR-02102 [6] sind für alle eingesetzten Algorithmen Parameter zu wählen, die einem Mindestsicherheitsniveau von 120 Bit entsprechen. Die empfohlenen Parameter aller in Tabelle 2 aufgeführten Algorithmen erfüllen dieses Sicherheitsniveau.

Ein Spezialfall sind symmetrische Verschlüsselungsverfahren wie AES oder ChaCha20, die grundsätzlich quantenresistent sind. Ihr effektives Sicherheitsniveau kann jedoch durch den Grover-Algorithmus auf einem Quantencomputer halbiert werden [3]. Daher wird für symmetrische Verfahren eine Schlüssellänge von 256 Bit empfohlen [6, p. 42], um dennoch das erforderliche 120-Bit-Sicherheitsniveau zu gewährleisten.

Während ML-KEM und ML-DSA auf der Komplexität von Gitterproblemen basieren (insbesondere auf dem Shortest-Vector-Problem), leitet SLH-DSA seine Sicherheit aus der Hash-Funktion ab, konkret aus der Schwierigkeit, Urbilder (Preimages) zu finden oder Kollisionen zu erzeugen.

Kapitel 1.3: Hybride Verfahren

Da die heute standardisierten PQC-Verfahren im Vergleich zu RSA und ECC noch relativ neu sind, empfehlen sowohl das NIST als auch das BSI den Einsatz hybrider KEM- und Signaturverfahren. Alle vorgestellten hybriden Verfahren basieren darauf, zwei oder mehr unterschiedliche kryptografische Algorithmen zu kombinieren.

Es geht hier darum, möglichst ein PQC-Verfahren mit einem etablierten Verfahren zu kombinieren. Daraus ergibt sich ein Verfahren, das so lange als sicher gilt, wie mindestens eines der eingesetzten PQC-Verfahren oder eines der klassischen Kryptografieverfahren als sicher gilt.

Derzeit werden hybride Verfahren nicht nur von den genannten Institutionen, sondern auch in Anwendungen, Standards und von Herstellern bevorzugt eingesetzt. Details hierzu finden sich in Kapitel 2.3.

Hybride Signaturen & KEMs

Bei hybriden Signaturverfahren erfolgt die Kombination der Algorithmen entweder parallel oder seriell. Die Gegenseite muss die resultierenden Signaturen entsprechend der gewählten Methode entweder gemeinsam oder sequenziell verifizieren.

Im Gegensatz dazu basieren hybride KEM-Verfahren auf dem Einsatz spezieller Schlüsselableitungsfunktionen (Key Derivation Functions, KDFs). Diese ermöglicht es, aus den durch verschiedene Algorithmen erzeugten Einzelschlüsseln einen einheitlichen kombinierten Schlüssel abzuleiten [16].

Kapitel 2: Migration zur Post-Quanten-Kryptografie: No-Regret-Moves und weitere Schritte

No-Regret-Moves sind Maßnahmen, die die allgemeine IT-Sicherheit verbessern, unabhängig davon, ob die Bedrohung durch Quantencomputer Realität wird. Dazu gehören sowohl die Sofortmaßnahmen als auch die Risikoanalyse.

?

EU-Roadmap [1]:

Many of the steps [...] for the PQC transition constitute "no-regret" moves; they improve cybersecurity in general [...]

»

Leistungsfähige Quantencomputer könnten zukünftig ein riesiges Potential bieten. Gleichzeitig bedrohen sie aber auch die Sicherheit unserer gesamten digitalen Infrastruktur. Deshalb müssen wir jetzt handeln und Schutzmaßnahmen ergreifen.

Claudia Plattner, Präsidentin des BSI

Kapitel 2.1: Sofortmaßnahmen

Einige unterstützende Maßnahmen lassen sich schnell umsetzen und stärken zugleich die allgemeine Cybersicherheit.

Identifikation und Zusammenarbeit mit Betroffenen
Der Umstieg von der etablierten zur Post-Quanten-Kryptografie kann nur erfolgreich sein, wenn alle Beteiligten zusammenarbeiten. Es gilt daher zuallererst zu identifizieren, wer in welchem Zusammenhang von der Migration betroffen sein wird. Diese Beteiligten sollten auf die Gefahren durch Quantencomputer hingewiesen werden. Gemeinsam können dann die weiteren Schritte durchgeführt werden.

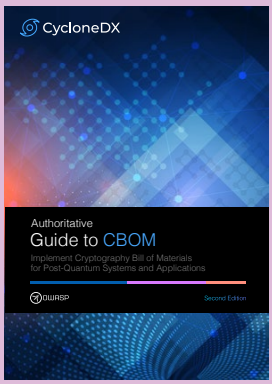
Inventarisierung
Der Einstieg in den Aufbau einer PQC-abgesicherten IT-Infrastruktur beginnt mit einer systematischen Inventarisierung der bestehenden Systeme und Dienste. Ein solches IT-Inventar strukturiert nicht nur den Übergang zu PQC-Verfahren, sondern bildet zugleich eine grundlegende Voraussetzung für eine wirksame Ermittlung des tatsächlichen Handlungsbedarfs für die organisationseigene IT-Landschaft. Auf dieser Basis lassen sich weitere Migrationsmaßnahmen effizient planen und umsetzen.

Eine solche Inventarisierung umfasst neben IT-Systemen und -Anwendungen auch die verwendete Kryptografie und Schnittstellen, konkret:

- Kommunikationsprotokolle: TLS, SSH, VPN, E-Mail etc. inkl. Versionsnummer
- Softwarebibliotheken für Kryptografie: Bezeichnung und Versionsnummer
- Kryptografische Verfahren: Algorithmen und Parameter (insb. Schlüssellängen)
- Externe Kommunikationsabhängigkeiten: Diensteanbieter, Entwickler und vergleichbare Akteure

So kann etwa eine gezielte Suche nach Diensten, die RSA nutzen, alle betroffenen Systeme zuverlässig identifizieren und damit den Handlungsbedarf unmittelbar sichtbar machen. Bereits existierende Security-Scanner können bei diesem Schritt helfen. Standards, wie die Cryptographic Bill of Materials (CBOM), bieten eine strukturierte Vorgehensweise, Anleitungen und Tools für die Inventarisierung.

An dieser Stelle zeigt sich die unmittelbare Verbindung zwischen der Inventarisierung und dem Konzept der Kryptoagilität. Eine kryptoagile Infrastruktur ermöglicht, kryptografische Verfahren mit minimalem Anpassungsaufwand zu ersetzen.



Kapitel 2.2: Risikoanalyse

Die Migration zur Post-Quanten-Kryptografie erfordert Zeit und Ressourcen. Nicht alle Systeme können gleichzeitig umgestellt werden. Um Prioritäten festzulegen, empfiehlt sich eine strukturierte Risikoanalyse. Eine solche Analyse ist nicht nur für die PQC-Migration sinnvoll. Sie unterstützt generell dabei, IT-Sicherheitsmaßnahmen dort umzusetzen, wo sie den größten Nutzen erzielen.

Die EU-Roadmap [1] schlägt hierfür drei zentrale Bewertungsdimensionen vor:
1. Angreifbarkeit der verwendeten Verfahren
2. Schadenspotenzial bei Kompromittierung
3. Migrationsaufwand des Systems

Diese drei Faktoren werden jeweils auf einer Skala bewertet und anschließend zu einem Gesamtrisiko zusammengeführt.

Angreifbarkeit der verwendeten Verfahren
Bei diesem Faktor geht es darum, welche kryptografischen Algorithmen derzeit verwendet werden und wie anfällig sie gegenüber Quantencomputern sind. Weitere Details dazu finden sich im TNO-Dokument zur Quantumrisikoanalyse [8], das Bewertungen zu einigen häufig verwendeten Algorithmen enthält.

Als Orientierung können folgende Faustregeln [5] dienen:

0 – explizit quantenresistente Verfahren

1 – Verfahren, die (nach aktuellem Wissensstand) nicht direkt durch Quantencomputer gebrochen werden (z. B. symmetrische Verfahren mit ausreichender Schlüssellänge)

2 – Algorithmen, die nicht quantenresistent sind (z. B. RSA und ECC)

Da in den meisten IT-Systemen mehrere Algorithmen verwendet werden (z. B. AES in Kombination mit RSA), muss eine Gesamtbewertung erfolgen. Werden mehrere Algorithmen in einem hybriden Verfahren genutzt, so müssen alle verwendeten Algorithmen gebrochen werden, bevor die Sicherheit des Systems gefährdet ist. In diesem Fall entspricht die Gesamtbewertung der niedrigsten Bewertung eines Einzelalgorithmus. Wenn Algorithmen parallel verwendet werden, genügt es, einen Algorithmus mit einem Quantencomputer zu brechen, um das Gesamtsystem unsicher zu machen. In diesem Fall entspricht die Gesamtbewertung der höchsten Einzelbewertung [5].

Schadenspotenzial

Dieser Faktor bewertet die Folgen eines Versagens des kryptografischen Systems. Besonders relevant ist hier im Hinblick auf das Harvest-Now-Decrypt-Later-Prinzip die Schutzdauer der betroffenen Daten.

Eine solche Bewertung ist sehr anwendungsspezifisch; für eine genauere Bewertung verweisen wir hier auf Abbildung 2.6 des „PQC Migration Handbook" [5]. Es gibt allerdings auch hier einige Faustformeln:

1 – Es werden keine sensiblen Daten oder Systeme geschützt.

2 – Die betroffenen Daten und Systeme sind voraussichtlich nicht mehr relevant, wenn das System gebrochen wird.

3 – Die Schutzbedürftigkeit der Daten ist hoch oder die Schutzdauer beträgt zehn oder mehr Jahre.

Die PQC-Roadmap der EU [1] nennt eine Schutzdauer von zehn Jahren als relevante Schwelle. Ein Beispiel hierfür sind Personendaten, die im Meldewesen anfallen könnten.

Migrationsaufwand

Der letzte Faktor ist die Zeit, die benötigt wird, um das System von klassischer auf quantenresistente Kryptografie umzustellen. Auch hier definiert [5] einige Faustformeln:

1 – Die Migration innerhalb von zwei Jahren ist realistisch.
2 – Die Migration ist zwar nicht trivial, aber absehbar (in bis zu acht Jahren) umsetzbar.
3 – Die Migration ist sehr komplex und schwer einschätzbar. Die erwartete Migrationsdauer liegt bei mehr als acht Jahren.

Ein hoher Migrationsaufwand spricht dafür, frühzeitig mit der Planung zu beginnen.

Sollte ein nicht quantenresistentes System absehbar (innerhalb von zwei Jahren) durch ein neues ersetzt werden, muss ggf. keine Migration mehr erfolgen. In diesem Fall muss allerdings darauf geachtet werden, dass das neue System quantenresistent ist.

Gesamtbewertung und Konsequenz

Aus der Kombination der drei Faktoren ergibt sich eine Risikokategorie: kein Risiko, niedriges Risiko, mittleres Risiko oder hohes Risiko. Bei keinem Risiko (also in der Praxis ausschließlich bei der Verwendung quantenresistenter Algorithmen) besteht kein Handlungsbedarf. Für die anderen Risikoklassen gibt die EU-Roadmap klare Zeitvorgaben:

- **Hohes Risiko:**
  Migration **bis Ende 2030**, Planungsbeginn spätestens Ende 2026
- **Mittleres Risiko:**
  Migration **bis Ende 2035**, Planungsbeginn spätestens Ende 2026
- **Niedriges Risiko:**
  Migration, so weit möglich, bis **Ende 2035**

Tabelle 2 –Bewertungsmatrix Risikomanagement

Angreifbarkeit	Schadenspotenzial	Migrationsaufwand	Gesamtrisiko [1]
0	1 2 3	1 2 3	Kein Risiko
1	1 2	1 2 3	Niedriges Risiko
1	3	1	Niedriges Risiko
1	3	2 3	Mittleres Risiko
2	1	1 2	Niedriges Risiko
2	1	3	Mittleres Risiko
2	2	1 2	Mittleres Risiko
2	2	3	Hohes Risiko
2	3	1 2 3	Hohes Risiko

Kapitel 2.3: Migration von bestehenden Produkten und Protokollen

Spezialsoftware für kommunale Fachverfahren lässt sich in der Regel weder kurzfristig noch eigenständig auf PQC umstellen. Die technische Verantwortung hierfür liegt beim jeweiligen Softwarehersteller. Der zentrale Hebel zur Durchsetzung einer PQC-Fähigkeit liegt daher insbesondere in den Vergaben (siehe Abschnitt 2.4 dieses Leitfadens).

Trotzdem lassen sich in vielen Fällen konkrete Schritte zur Migration unternehmen. Viele eingesetzte Standardkomponenten und Übertragungsprotokolle unterstützen bereits heute quantenresistente oder hybride Verfahren und lassen sich unabhängig von den jeweiligen Fachanwendungen anpassen. Insbesondere wenn kommunale Fachverfahren auf Standardtechnologien wie Webkomponenten oder gesicherte Transportprotokolle (z. B. TLS oder VPN) aufsetzen, lassen sich bereits heute sinnvolle und wirksame Migrationsschritte umsetzen, ohne bestehende Anwendungen abzulösen.

Es empfiehlt sich folgende Priorisierung, da hier mit vergleichsweise geringem Aufwand ein hoher Sicherheitsgewinn erzielt werden kann:

1. Externe Kommunikation, insbesondere VPN-Verbindungen zu Rechenzentren, Dienstleistern und anderen Partnern.
2. Zentrale Basisdienste, wie Webserver und -Portale, insbesondere, wenn darüber sicherheitsrelevante Daten übertragen werden.

Allgemein sollte der Fokus zunächst auf Übertragungswegen liegen, da hier bereits heute die Gefahr von Harvest-Now-Decrypt-Later-Angriffen besteht. Maßnahmen zur quantenresistenten Verschlüsselung ruhender Daten sowie der Einsatz von PQC-Signaturverfahren können in vielen Fällen zu einem späteren Zeitpunkt erfolgen.

Virtual Private Networks (VPNs)

Für den weit verbreiteten VPN-Standard OpenVPN existiert bereits eine quantenresistente Implementierung [9]. Das neuere Wireguard-Protokoll hingegen bietet derzeit nur eine Übergangslösung, die einen deutlich höheren Konfigurationsaufwand mit sich bringt [10]. Für IPsec-VPNs existieren derzeit nur ein vorläufiger Standard sowie Maßnahmen zur Vorbereitung auf eine PQC-Migration [11].

OpenVPN setzt im Hintergrund auf das TLS-Protokoll (siehe unten) und unterstützt daher direkt PQC-Verfahren, die von der jeweiligen TLS-Bibliothek unterstützt werden. Entsprechende Anleitungen zur Konfiguration von OpenVPN sind online verfügbar [9].

Das VPN-Protokoll WireGuard bietet zum Zeitpunkt der Forschung keinen direkten Migrationspfad zu quantenresistenten Verfahren. Die von den Entwicklern vorgeschlagene Übergangslösung [10] ist mit hohem Konfigurationsaufwand verbunden und derzeit nur eingeschränkt für den breiten kommunalen Einsatz geeignet.

Das IPsec-Protokoll unterstützt hybride Schlüsselaustauschverfahren und kann dabei bis zu acht verschiedene Verfahren kombinieren. Obwohl momentan noch keine PQC-Verfahren direkt unterstützt werden, lohnt sich der Einsatz des hybriden Verfahrens bereits heute:
Eine zukünftige Erweiterung um unterstützte PQC-Verfahren im Sinne der Kryptoagilität ist somit jederzeit möglich. Erste Arbeiten an einer direkten PQC-Unterstützung für IPsec laufen bereits [11].

Transport Layer Security (TLS)

Bereits heute zeigt TLS 1.3, dass PQC-gehärtete Verbindungen im Internet möglich sind – auch ohne vollständig verabschiedeten Standard.
So zeigt eine Statistik von Cloudflare (eines der größten Internet-Traffic-Unternehmen), dass bereits über 58 Prozent des durch Cloudflare gerouteten HTTPS-Traffics PQC-gesichert ist [15].

Das TLS-Protokoll ist eines der am häufigsten verwendeten verschlüsselten Übertragungsprotokolle im Internet. TLS in Version 1.3 wird derzeit um PQC-Verfahren erweitert, auch wenn der zugehörige Standard [12] sich noch in einer Vorabversion befindet. Insbesondere im Webbereich (HTTPS) werden quantenresistente Schlüsselaushandlungsverfahren bereits in den gängigsten Browsern und Servern standardmäßig unterstützt [13]. Auch aktuelle Versionen von TLS-Bibliotheken wie OpenSSL unterstützen bereits PQC-Verfahren [14]. Ein Update der verwendeten Serverkomponenten und Bibliotheken kann also ein einfacher Weg sein, um beispielsweise verwendete Webanwendungen zu migrieren.

SSH, insbesondere OpenSSH

SSH als zentrales Werkzeug für die Remoteadministration ist ein wichtiger Faktor beim Schutz von Daten vor Harvest-Now-Decrypt-Later-Angriffen. Die weit verbreitete Software OpenSSH verwendet standardmäßig bereits quantenresistente, hybride Verfahren für den Schlüsselaustausch. Kommunen sollten daher sicherstellen, dass eingesetzte OpenSSH-Versionen aktuell sind (mindestens Version 10.0), sodass die entsprechenden Algorithmen genutzt werden können.

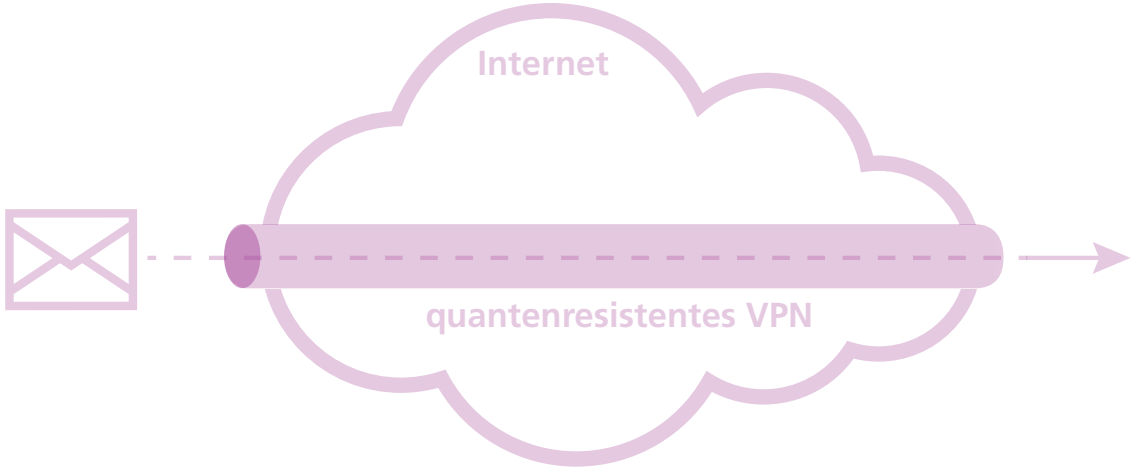
Empfehlungen zur Migration von Produkten ohne Migrationspfad

Bei Software-Produkten, für die absehbar keine oder nur sehr langfristig PQC-Unterstützung zu erwarten ist, empfiehlt sich eine Schichtenstrategie als zeitlich begrenzte Übergangslösung. Hierbei wird die nicht quantenresistente Kommunikation in eine quantenresistente Transportschicht gekapselt, um bestehende Anwendungen auf dem Kommunikationsweg vor Harvest-Now-Decrypt-Later-Angriffen zu schützen, bis eine native PQC-Unterstützung verfügbar ist oder eine Ablösung erfolgt.

Es bieten sich dafür im Wesentlichen zwei Möglichkeiten an:

1. Falls es sich um eine Software handelt, die über das HTTP(S)-Protokoll kommuniziert oder sogar als Webseite angeboten wird, kann die nicht PQC-fähige Software hinter einem PQC-fähigen HTTPS-Reverse-Proxy betrieben werden. Insbesondere für Software, die als Webseite in einem Browser genutzt wird, funktioniert dies meist ohne großen Aufwand.
2. Für andere Protokolle bietet es sich an, die Software über eine quantenresistente VPN-Verbindung zu nutzen. Alle Verbindungen über das Internet werden dabei nicht direkt, sondern über eine IP-Adresse im VPN-Netzwerk aufgebaut und damit geschützt.

In beiden Fällen wird eine quantensichere Verbindung bis zum Netzübergang ins Betreibernetz hergestellt. Die Verbindungen innerhalb des Betreibernetzes bleiben weiterhin anfällig für Angriffe durch Quantencomputer und müssen entsprechend, genau wie ruhende Daten, vor Fremdzugriff geschützt werden.



Kapitel 2.4:
Empfehlungen für Vergaben

IT-Systeme, die heute beschafft werden, bleiben häufig über viele Jahre – teils Jahrzehnte – im Einsatz. Vergaben sind daher ein zentraler Hebel, um die zukünftige Resilienz gegenüber Quantencomputern zu stärken – unabhängig von der Migration bestehender Systeme.

Gerade bei spezialisierter Fachsoftware können nicht immer alle Anforderungen unmittelbar erfüllt werden. Abhängig vom Systemtyp und vom Risiko der verarbeiteten Daten sollten daher unterschiedliche Qualitätsstufen definiert und eingefordert werden.

Stufe 1: Dokumentationspflicht

Eine strukturierte Migration zur Post-Quanten-Kryptografie (PQC) setzt Transparenz voraus. Ohne Kenntnis der eingesetzten Verfahren ist weder eine Risikoanalyse noch eine priorisierte Migrationsplanung möglich.

Deshalb sollte von Anbietern eine vollständige Dokumentation eingefordert werden, insbesondere zu:

- Kommunikationsschnittstellen und eingesetzten Protokollen,
- verwendeten kryptografische Algorithmen,
- verwendeten kryptografischen Parametern und deren Konfigurationsmöglichkeiten
- und eingesetzten kryptografischen Bibliotheken.

Diese Transparenz bildet die Grundlage für alle weiteren Anforderungen.

Stufe 2: Migrationsfähigkeit (Kryptoagilität und hybride Verfahren)

Kryptoagilität stellt sicher, dass ein System künftig auf neue kryptografische Verfahren umgestellt werden kann, ohne grundlegend neu entwickelt werden zu müssen. Sie ist damit eine zentrale Voraussetzung für eine nachhaltige PQC-Strategie. Weiterführende Hinweise hierzu finden sich im Leitfaden „Krypto-Agilität" des Fraunhofer SIT [7].

Anbieter sollten daher belegen, dass:

- kryptografische Komponenten modular austauschbar sind,
- ein Algorithmuswechsel ohne Anpassung der Anwendungslogik möglich ist
- und sicherheitsrelevante Parameter (z. B. Schlüssellängen oder Cipher Suites) zentral verwaltbar sind.

Ein entsprechender Nachweis kann etwa durch Architekturdokumentationen, API-Beschreibungen oder dokumentierte Konfigurationsschnittstellen erbracht werden.

Neben der strukturellen Austauschbarkeit sind hybride Verfahren ein wichtiger Übergangsmechanismus. Sie kombinieren klassische Kryptografie mit PQC-Verfahren und stellen sicher, dass das Gesamtsystem weiterhin geschützt bleibt, solange mindestens eines der eingesetzten Verfahren sicher ist.

Anbieter sollten daher belegen, dass ihre Systeme hybride Verfahren für den Schlüsselaustausch und/oder für Signaturen unterstützen.

Stufe 3: Quantenresistenter Schlüsselaustausch

Zur wirksamen Absicherung gegen das Harvest-Now-Decrypt-Later-Szenario ist insbesondere der Schlüsselaustausch entscheidend. Ein quantenresistentes Verfahren schützt bereits heute vor einer zukünftigen Entschlüsselung gespeicherter Kommunikationsdaten. Insbesondere bei Systemen mit hohem Schadenspotenzial oder langer Schutzdauer sollte dieses Schutzniveau verlangt werden.

Anbieter sollten belegen, dass ihre Systeme mindestens ein quantenresistentes Schlüsselaustauschverfahren (KEM) unterstützen, das in der jeweils aktuellen Fassung der BSI TR-02102-1 [6] aufgeführt ist.

Stufe 4: Quantenresistente Kommunikation

Für ein vollständig quantenresistentes System müssen neben dem Schlüsselaustausch auch digitale Signaturen quantenresistent ausgestaltet sein. Signaturen schützen nicht nur die Vertraulichkeit indirekt, sondern sichern auch Integrität und Authentizität – etwa bei Systemupdates oder Verwaltungsprozessen.

Nach aktuellem Stand existieren noch keine kryptografisch relevanten Quantencomputer. Diese Stufe ist daher derzeit nicht in allen Szenarien zwingend erforderlich. Für besonders schutzbedürftige Systeme – etwa mit sicherheitskritischen Update-Mechanismen – kann sie jedoch bereits heute notwendig sein.

Anbieter sollten belegen, dass ihre Systeme mindestens ein quantenresistentes Signaturverfahren unterstützen, das in der jeweils aktuellen Fassung der BSI TR-02102-1 [6] aufgeführt ist.

Fazit und Checklisten

Langfristig ist die Migration auf Post-Quanten-Kryptografie unvermeidbar, bringt jedoch operative und organisatorische Herausforderungen mit sich. Deshalb erfordert sie eine sorgfältige Planung und frühzeitiges Handeln. Durch konkrete Maßnahmen wie die Inventarisierung der verwendeten Kryptografie, den Einbau von Kryptoagilität und die Verwendung einheitlicher Standards lässt sich bereits heute viel erreichen, was zugleich die Cybersicherheit an sich unterstützt.

Um die Migration langfristig voranzutreiben, sollte die Post-Quanten-Kryptografie insbesondere bei neuen Beschaffungen und bei der Vergabe von Aufträgen in den Fokus genommen werden. Hierbei sollen die folgenden Checklisten helfen.

Checkliste: No-Regret-Moves

1. IT-Systeme und Anwendungen inventarisieren (Fokus: Kryptografie)

- ☐ Verwendete Kommunikationsprotokolle (z. B. TLS, VPN)
- ☐ Genutzte kryptografische Algorithmen und Parameter
- ☐ Eingesetzte kryptografische Bibliotheken
- ☐ Relevante Kommunikationsschnittstellen und externe Abhängigkeiten

2. Risikobewertung pro IT-System durchführen

- ☐ Angreifbarkeit der eingesetzten Kryptografie bewerten
- ☐ Schadenspotenzial bei Kompromittierung einschätzen
- ☐ Migrationsaufwand abschätzen

3. Migration vorbereiten

- ☐ Priorisierung der Systeme auf Basis der Risikoanalyse
- ☐ Erstellung eines strukturierten Migrationsplans
- ☐ Identifikation kurzfristig umsetzbarer Maßnahmen („Quick Wins“)

Checkliste: Kriterien für Vergaben

Für Ausschreibungen und Beschaffungen lassen sich vier Qualitätsstufen definieren, die sich am Risiko des jeweiligen Systems und der verarbeiteten Daten orientieren. Jede Stufe setzt voraus, dass die Anforderungen der vorherigen Stufe erfüllt sind.

Stufe 1: Dokumentationspflicht

Das System

- ☐ stellt eine vollständige und aktuelle Dokumentation der verwendeten kryptografischen Verfahren, Parameter, Bibliotheken und Kommunikationsschnittstellen bereit.

Stufe 2: Migrationsfähigkeit

Das System

- ☐ ermöglicht den Austausch kryptografischer Algorithmen ohne Änderung der Anwendungslogik (Kryptoagilität).
- ☐ unterstützt hybride Verfahren als Übergangsmechanismus zwischen klassischen und quantenresistenten Verfahren.

Stufe 3: Quantenresistenter Schlüsselaustausch

Das System

- ☐ unterstützt den Einsatz von mindestens einem quantenresistenten Schlüsselaustauschverfahren (KEM), das in der jeweils aktuellen Fassung der BSI TR-02102-1 [6] aufgeführt ist.

Stufe 4: Quantenresistente Kommunikation

Das System

- ☐ unterstützt den Einsatz von mindestens einem quantenresistenten Signaturverfahren gemäß der jeweils aktuellen Fassung der BSI TR-02102-1 [6].

Glossar

Begriff	Erklärung
Grover-Algorithmus	Quantenalgorithmus, der die Suche in großen Datenmengen beschleunigt. Für kryptografische Verfahren bedeutet dies, dass sich die effektive Sicherheit symmetrischer Verfahren etwa halbiert (z. B. von 128 Bit auf 64 Bit), weshalb längere Schlüssel empfohlen werden.
Harvest-Now-Decrypt-Later-Prinzip	Angriffsszenario, bei dem verschlüsselte Daten heute gespeichert und zu einem späteren Zeitpunkt – etwa mit Quantencomputern – entschlüsselt werden.
Hybride Verfahren	Kombination aus klassischen und PQC-Verfahren zur Absicherung in der Übergangsphase.
KEM (Key Encapsulation Mechanism)	Verfahren zum sicheren Austausch von kryptografischen Schlüsseln.
Kryptoagilität	Fähigkeit eines Systems, kryptografische Verfahren flexibel auszutauschen, ohne grundlegende Änderungen im restlichen System vornehmen zu müssen.
Quantencomputer	Computer, die auf quantenmechanischen Prinzipien basieren und bestimmte mathematische Probleme deutlich effizienter lösen können als klassische Computer.
Quantenresistente / Post-Quanten-Kryptografie (PQC)	Bezeichnung für Verfahren, die nach aktuellem Stand als sicher gelten, auch gegenüber Angriffen durch Quantencomputer.
Shor-Algorithmus	Quantenalgorithmus, der es ermöglicht, bestimmte mathematische Probleme (z. B. Faktorisierung großer Zahlen) effizient zu lösen. Dadurch werden viele heute verwendete kryptografische Verfahren wie RSA oder ECC unsicher.

Literaturverzeichnis

[1] NIS Cooperation Group, „A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography," 11. Juni 2025. [Online]. Verfügbar unter: https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography. [Zugriff am 19. August 2025].

[2] J. D. Hidary, Quantum Computing: An Applied Approach, Springer International Publishing, 2019.

[3] S. D. und P. C., „On the practical cost of Grover for AES key recovery," November 2024. [Online]. Verfügbar unter: https://csrc.nist.gov/presentations/2024/practical-cost-of-grover-for-aes-key-recovery. [Zugriff am 31. März 2026].

[4] M. Mosca und M. Piani, „Quantum Threat Timeline Report 2024," 2024. [Online]. Verfügbar unter: https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/. [Zugriff am 10. Februar 2026].

[5] A. Amadori, T. Attema, M. Bombar, J. D. Duarte, V. Dunning, S. Etinski, D. v. Gent, M. Lequesne, W. v. d. Schoot, M. Stevens und A. C. a. Advisors, „The PQC Migration Handbook," Dezember 2024. [Online]. Verfügbar unter: https://publications.tno.nl/publication/34643386/fXcPVHsX/TNO-2024-pqc-en.pdf.

[6] Bundesamt für Sicherheit in der Informationstechnik (BSI), „BSI Technische Richtlinie TR-02102-1 - Kryptographische Verfahren: Empfehlungen und Schlüssellängen," Januar 2026. [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.html?nn=129156.

[7] L. Wolf, „Krypto-Agilität: Leitfaden für langfristige IT-Sicherheit," Fraunhofer SIT, 2024. [Online]. Verfügbar unter: https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Kryptoagilitaet-Studie_final.pdf.

[8] M. de Vries, S. E. Bootsma, V. A. Dunning und M. J. van Vliet, TNO 2024 R10707 - Quantum risicomethodologie voor cryptografie, TNO, 2024.

[9] OpenVPN, „Quantum Computing and the Future of Cybersecurity," 2026. [Online]. Verfügbar unter: https://blog.openvpn.net/quantum-safe-vpn. [Zugriff am 20. Januar 2026].

[10] J. A. Donenfeld, „Wireguard - Known Limitations: Post-Quantum Secrecy," [Online]. Verfügbar unter: https://www.wireguard.com/known-limitations/#post-quantumsecrecy. [Zugriff am 30. Januar 2026].

[11] P. Kampanakis, „Post-quantum Hybrid Key Exchange with ML-KEM in the Internet Key Exchange Protocol Version 2 (IKEv2)," Oktober 2025. [Online]. Verfügbar unter: https://datatracker.ietf.org/doc/draft-ietf-ipsecme-ikev2-mlkem/.

[12] K. Kwiatkowski, P. Kampanakis, B. E. Westerbaan und D. Stebila, „Post-quantum hybrid ECDHE-MLKEM Key Agreement for TLSv1.3," August 2024. [Online]. Verfügbar unter: https://datatracker.ietf.org/doc/draft-ietf-tls-ecdhe-mlkem/. [Zugriff am 20. Januar 2026].

[13] Cloudflare, Inc., „PQC support," 2024. [Online]. Verfügbar unter: https://developers.cloudflare.com/ssl/post-quantum-cryptography/pqc-support/#x25519mlkem768. [Zugriff am 20. Januar 2026].

[14] OpenSSL Foundation, „The Features of 3.5: Post-quantum cryptography," April 2025. [Online]. Verfügbar unter: https://openssl.foundation/news/the-features-of-3-5-post-quantum-cryptography. [Zugriff am 31. Januar 2026].

[15] Cloudflare, Inc., „Post-quantum encryption," 2026. [Online]. Verfügbar unter: https://radar.cloudflare.com/adoption-and-usage#post-quantum-encryptionadoption. [Zugriff am 20. Januar 2026].

[16] N. Waller, G. Alagic, E. Barker, L. Chen, D. Moody, A. Robinson und H. Silberg, „NIST Special Publication (SP) 800-227 Recommendations for Key-Encapsulation Mechanisms," 18 September 2025. [Online]. Verfügbar unter: https://csrc.nist.gov/pubs/sp/800/227/final. [Zugriff am 04. Februar 2026]