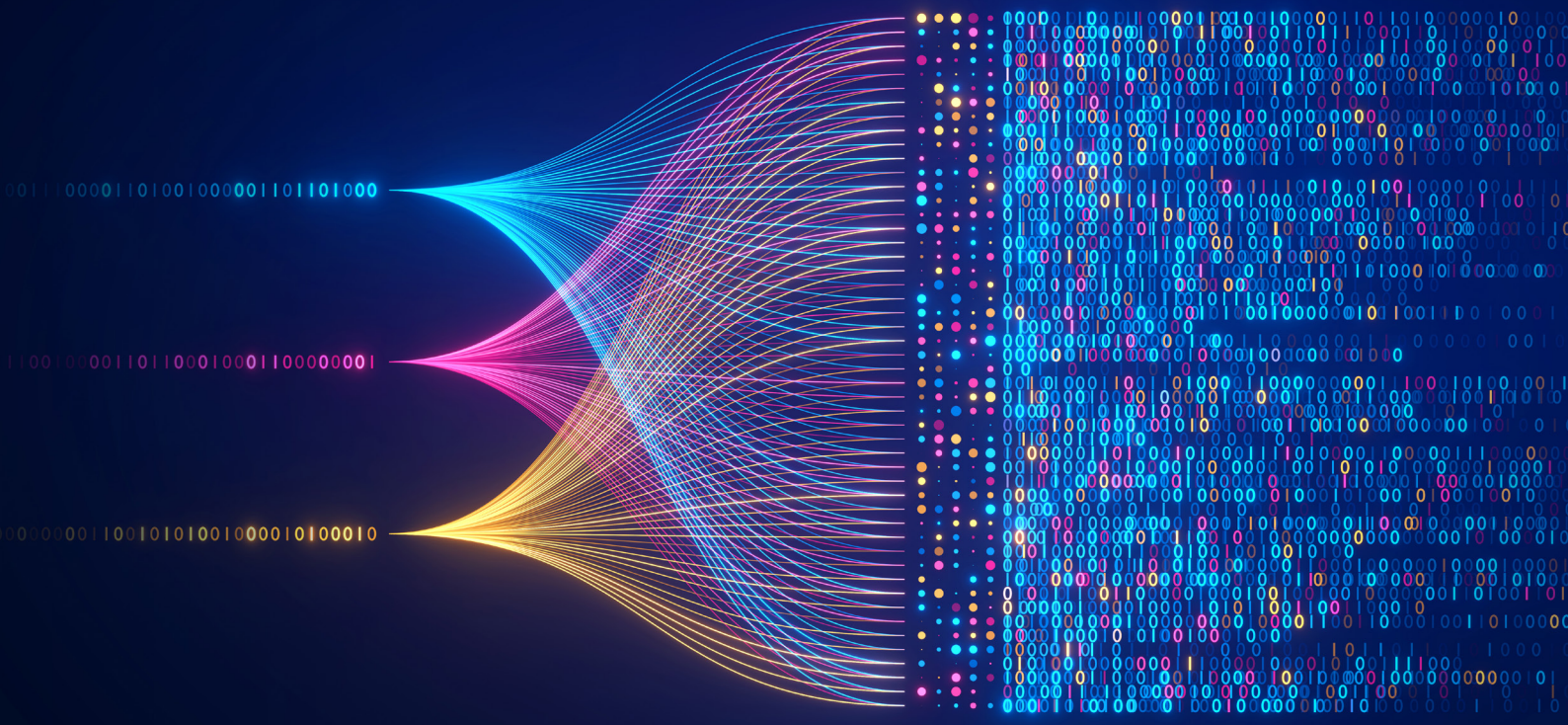
EVIDEN

Post-Quanten-Migration

So gelingt die Umstellung auf quantensichere Kryptografie

Neue Ausgabe 2024



Management Summary

Beunruhigt Sie die Vorstellung, dass ein Hacker in Ihr Unternehmensnetz eindringt, Ihre verschlüsselten E-Mails liest und auf die sensibelsten Daten Ihres Unternehmens zugreift? Dieses Szenario ist realistischer, als man denkt, wenn eines Tages kryptografisch relevante Quantencomputer zur Verfügung stehen werden. Dann sind alle Kryptosysteme, die auf RSA, Diffie-Hellman oder ECC basieren, leicht angreifbar. Diese kryptografischen Mechanismen stellen das aktuelle Sicherheitsfundament dar und werden milliardenfach in Web-Browsern, E-Mail-Clients, Smartphones, VPN-Lösungen und Betriebssystemen eingesetzt.

Zum Glück ist es noch nicht so weit. Zwar gibt es bereits Quantencomputer, aber die aktuellen Modelle sind viel zu schwach, um ein echtes kryptografisches System zu knacken. Aber die Technologie macht Fortschritte, und daher wird der Bedarf an quantenresistenten Alternativen immer offensichtlicher. Solche „Post-Quanten-Kryptografie"-Methoden (PQC) gibt es bereits. Nach jahrelanger akademischer Forschung sind einige von ihnen nun reif für die Normung. CRYTSTALS-Kyber (Schlüsselaustausch) und CRYSTALS-Dilithium (digitale Signaturen) gelten derzeit als die vielversprechendsten Verfahren.

Unabhängig von der Post-Quanten-Kryptografie wurden so genannte Quantenschlüsselverteilungsprotokolle (QKD) entwickelt. QKD-Protokolle beruhen selbst auf der Quantenmechanik selbst und können mit Quantencomputern nicht gebrochen werden. Die QKD-Technologie steckt jedoch noch in den Kinderschuhen und ist nicht geeignet, die derzeitigen Schlüsselaustauschsysteme in typischen IT-Umgebungen von Unternehmen oder Behörden zu ersetzen. Aus diesem Grund wird QKD in diesem Dokument nicht behandelt.

Jetzt, wo die Post-Quanten-Kryptografie praxisreif wird, stellt die Migration zu ihr eine der größten Herausforderungen in der IT-Welt dar. Protokollentwickler, Kryptografieanbieter, Systemintegratoren und Administratoren stehen in den kommenden Jahren vor einer großen Aufgabe.

Eine offensichtliche Herausforderung ist, dass Post-Quanten-Methoden mehr Rechenressourcen benötigen als die derzeit verwendeten RSA-, Diffie-Hellman- und ECC-Verfahren. Vorgeschlagene PQC-Methoden verwenden öffentliche und private Schlüssel, die wesentlich länger sind als die der aktuellen Systeme, während die Gesamtleistung geringer ist. Dies kann insbesondere für Plattformen mit begrenzten Ressourcen wie Smart Cards und Smart Token eine Herausforderung darstellen.

Da die derzeit vorgeschlagenen kryptografischen Post-Quanten-Algorithmen noch nicht so ausgereift sind wie ihre konventionellen Gegenstücke, sind sich die Experten einig, dass weitere Analysen erforderlich sind. Aus demselben Grund ist die Notwendigkeit von Krypto-Agilität, d. h. die Fähigkeit, schnell zu einer alternativen Methode überzugehen, ohne wesentliche Änderungen an der Umgebung vorzunehmen, von entscheidender Bedeutung. Unternehmen, die in der Lage sind, Änderungen zwischen kryptografischen Algorithmen in laufenden Systemen zu implementieren, sind am besten auf die Risiken vorbereitet, die sich aus dem Ausfall eines bestimmten Algorithmus in der Zukunft ergeben.

Migrationsstrategien, bei denen alle klassischen Kryptosysteme abgeschaltet und alle Post-Quanten-Alternativen auf einmal gestartet werden, sind natürlich nicht realistisch. Stattdessen wird empfohlen, ein schrittweises Migrationsprojekt zu planen, das in einer Übergangsphase auch hybride Kryptomethoden (d. h. eine Kombination aus Prä- und Post-Quanten-Algorithmen) umfassen kann. Eviden empfiehlt, ein solches Projekt wie folgt zu strukturieren:

- Projektaufbau
- Erstellung eines Krypto-Inventars
- Identifizieren
- Bewertung der Auswirkungen auf Organisation und Richtlinien
- Einbindung der Geschäftsführung
- Durchführung der Migration

Dieser Leitfaden skizziert die wichtigsten Schritte, um Ihre Unternehmens-IT-Umgebung quantenresistent zu machen, und zeigt, wie die größten Herausforderungen gelöst werden können. Darüber hinaus wird aufgezeigt, was Eviden für Ihr Unternehmen oder Ihre Behörde tun kann, um einen reibungslosen Übergang in die Post-Quanten-Welt zu ermöglichen. Für weitere Informationen können Sie uns gerne kontaktieren.

Inhalt

Einführung

Quantencomputer

Quantencomputer sind anders aufgebaut als bisherige Computersysteme. Sie beruhen auf den Prinzipien der Quantenmechanik, was völlig neuartige Designs erlaubt. Quantencomputer sind eine vielversprechende Zukunftstechnologie, die unter anderem für die folgenden Anwendungen eingesetzt werden kann:

- Quantencomputer können die chemische Forschung unterstützen und damit Lösungen gegen den Klimawandel entwickeln[1];
- Quantencomputer können die Entwicklung von Medikamenten unterstützen[2];
- Quantencomputer können das autonome Fahren verbessern[3];
- Quantencomputer lassen sich für künstliche Intelligenz nutzen[4];

Es gibt auch interessante Anwendungen der Quantenmechanik in der Kryptografie. Dazu gehören die Quantenzufallszahlengenerierung (QRNG), die zur Erzeugung geheimer Schlüssel verwendet werden kann, und die Quantenschlüsselverteilung (QKD), die beweisbar sicher gegen viele Angriffe ist.

Darüber hinaus sind Quantensensoren für Radar, Navigation, Bildgebung und Teilchendetektion eine vielversprechende Technologie. Sie übertreffen herkömmliche Sensoren in Bezug auf Empfindlichkeit, räumliche Auflösung und Zeitauflösung erheblich und können unter anderem in Medizin und Technik eingesetzt werden.

Und schließlich können Quantencomputer aktuelle Krypto-Verfahren wie RSA, Diffie-Hellman und andere knacken.

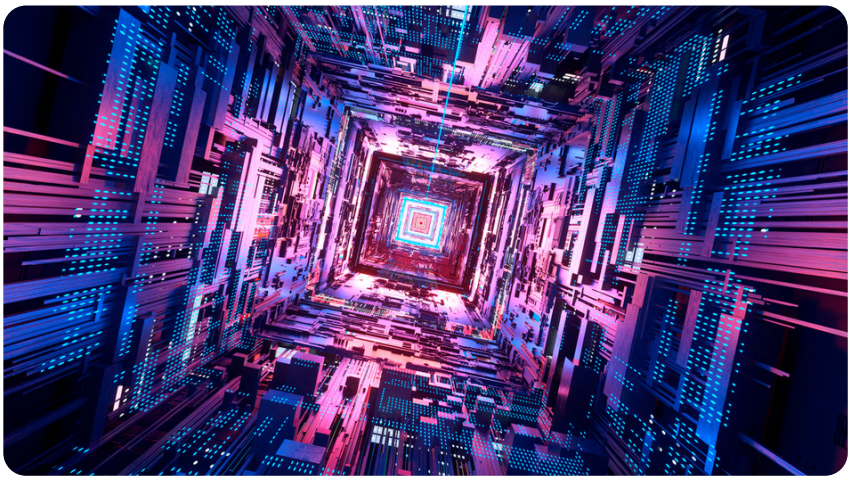
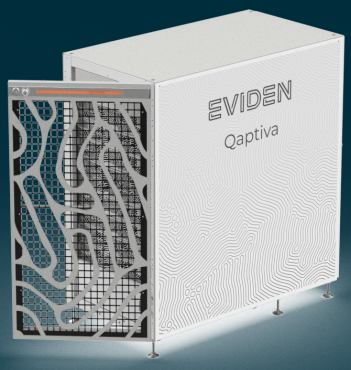


Abbildung 1: Quantencomputer sind eine vielversprechende Zukunftstechnologie. Mit ihnen lassen sich unter anderem bestimmte Krypto-Verfahren knacken.

Aus dem Eviden-Portfolio:

- Qaptiva, eine umfangreiche NISQ-Programmierumgebung für die Optimierung, Kompilierung und Emulierung von Code auf fehlerfreien und fehlerbehafteten Qubits und für die Code-Ausführung auf einer QPU
- Appliances, die mehrere Hundert Qubits emulieren
- Unterstützung beim Einsatz von Quantencomputern
- Quantenalgorithmen in Python auf einer beliebigen Plattform mit myQLM



1. https://www.weforum.org/agenda/2019/12/quantum-computing-applications-climate-change/
2. https://pharmafeatures.com/drug-discovery-quantum-computing/
3. https://www.newsweek.com/ibm-using-quantum-computing-help-automotive-industry-solve-ev-traffic-problems-1637827
4. https://www.researchgate.net/profile/V-Moret-Bonillo/publication/265642441_Can_artificial_intelligence_benefit_from_quantum_ computing/links/54f0b8090cf2b36214aae3a2/Can-artificial-intelligence-benefit-from-quantum-computing.pdf
5. https://atos.net/en/solutions/high-performance-computing-hpc/quantum-computing-qaptiva

Post-Quanten-Kryptografie

Wie wir in unserem Whitepaper „Einführung in die Post-Quanten-Kryptografie“[6] erläutert haben, stellen Quantencomputer eine ernsthafte Bedrohung für die IT-Sicherheit dar. Stellen Sie sich vor, dass ein Hacker in der Lage ist, in fast jedes Unternehmensnetzwerk einzudringen und es auszuspionieren. Stellen Sie sich außerdem vor, dass derselbe Hacker alle verschlüsselten E-Mails und jede gesicherte Netzwerkkommunikationen, auf die er stößt, lesen kann, als wäre es Klartext. Und stellen Sie sich schließlich vor, dass dieser Angreifer jede geschützte WWW- und VPN-Verbindung in seiner Reichweite kapern kann.

All dies könnte eines Tages passieren, wenn es Quantencomputer gibt, die in der Lage sind, große Primzahlenprodukte zu faktorisieren. In diesem Whitepaper werden solche Maschinen als „kryptografisch relevante Quantencomputer“ bezeichnet. Geräte dieser Art könnten mehrere wichtige kryptografische Algorithmen brechen, darunter RSA und Diffie-Hellman, zwei Systeme, die milliardenfach in Web-Browsern, Servern, E-Mail-Clients, Smartphones, Geldautomaten und in anderen Umgebungen verwendet werden. Eine digitale Apokalypse würde Realität werden.

Zum Glück ist es noch nicht so weit. Obwohl es bereits Quantencomputer gibt, können die aktuellen Modelle höchstens zweistellige Zahlen in ihre Faktoren zerlegen. Um aktuelle asymmetrische Systeme wie RSA oder Diffie-Hellman zu gefährden, müssten sie eine derartige Operation mit einer 700-stelligen Zahl durchführen können. Dies wird in naher Zukunft nicht machbar sein. Allerdings forschen derzeit zahlreiche Organisationen intensiv an Quantencomputern, und die Technik wird immer besser.

Aus den genannten Gründen ist es notwendig, auf quantensichere Alternativen zu RSA, Diffie-Hellman und einigen anderen Systemen umzustellen. Glücklicherweise gibt es diese Alternativen bereits. Sie werden unter dem Begriff Post-Quanten-Kryptografie zusammengefasst.

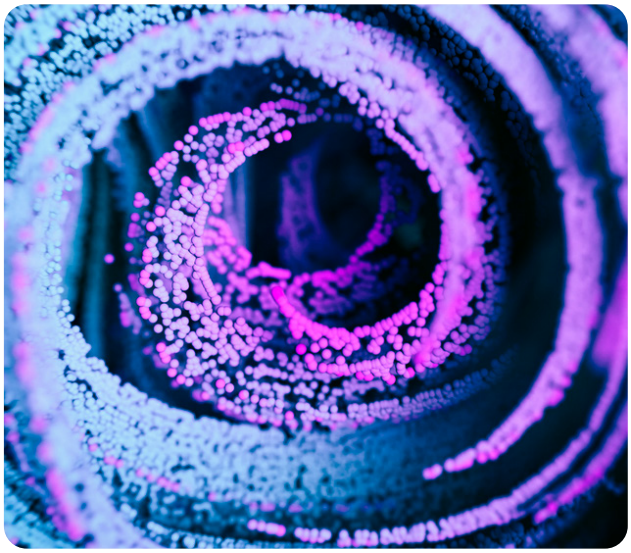
Bisher werden die Methoden der Post-Quanten-Kryptografie in der Praxis kaum eingesetzt. Viele davon befinden sich noch im Experimentierstadium. Es gibt jedoch Fortschritte. Einige Post-Quanten-Methoden gelten inzwischen als sicher und praktikabel, die Standardisierung ist im Gange.

Dieses Dokument konzentriert sich auf den Migrationspfad zur Post-Quanten-Kryptografie. Er stellt die wichtigsten Herausforderungen vor, die es zu bewältigen gilt, um Unternehmens-IT-Umgebungen quantenresistent zu machen, und zeigt auf, wie diese Herausforderungen gelöst werden können. Außerdem wird aufgezeigt, was Eviden für Ihr Unternehmen oder Ihre Behörde tun kann, um einen reibungslosen Übergang in die Post-Quanten-Welt zu ermöglichen.

Quanten-Schlüsselverteilung

Die Quantenschlüsselverteilung (QKD), manchmal auch als Quantenkryptografie bezeichnet, ist eine quantensichere kryptografische Technologie. QKD-Protokolle beruhen auf der Quantenmechanik selbst und können mit einem Quantencomputer nicht gebrochen werden. Es ist jedoch zu beachten, dass QKD spezielle Hardware erfordert und außerdem eine Sichtverbindung benötigt, was die Entfernung beschränkt. Außerdem deckt die QKD längst nicht alle kryptografischen Anwendungsfälle ab und gilt als noch nicht ausgereift.

Es wird allgemein erwartet, dass der Einsatz von QKD auf militärische und nationale Kommunikation in speziellen Netzen beschränkt bleiben wird. Eine von der ANSSI (Frankreich), dem BSI (Deutschland), der NLNCSA (Niederlande) und der SNCSA (Schweden) veröffentlichtes Stellungnahme bestätigt diese Ansicht.[7] Dies bedeutet, dass die QKD für ein aktuelles Post-Quanten-Migrationsprojekt nicht relevant ist. Aus diesem Grund wird die QKD in diesem Dokument nicht näher behandelt.



6. https://www.cryptovision.com/en/download-access

7. https://cyber.gouv.fr/sites/default/files/document/Quantum_Key_Distribution_Position_Paper.pdf

Standardisierung

Im Jahr 2017 startete das US-amerikanische National Institute of Standards and Technology (NIST) einen Wettbewerb, bei dem kryptografische Post-Quanten-Verfahren gegeneinander antraten.[8] Experten aus der ganzen Welt wurden aufgefordert, geeignete Algorithmen für ein Auswahlverfahren einzureichen, bei dem die besten Verfahren ermittelt und anschließend standardisiert werden sollten. Dieser Wettbewerb umfasste sowohl Signaturalgorithmen als auch Verschlüsselungs- bzw. Schlüsselaustauschverfahren. Das Ergebnis sollte ein Portfolio zuverlässiger Post-Quanten-Krypto-Verfahren sein, die für verschiedene Zwecke geeignet sind und auf unterschiedlichen mathematischen Grundlagen basieren.

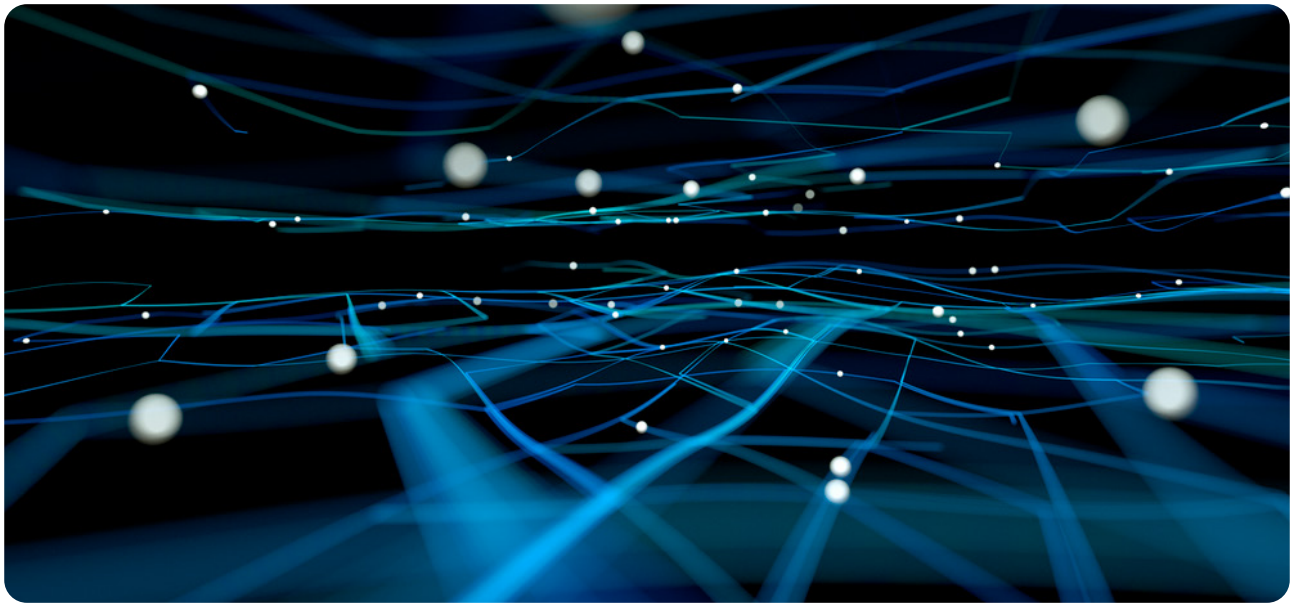
Das NIST nahm 69 der eingereichten Verfahren in den Wettbewerb auf. Im Juli 2022, nach drei Bewertungsrunden, wurden vier Gewinner bekannt gegeben: CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON und SPHINCS+. Es wird erwartet, dass die beiden CRYSTALS-Methoden in den nächsten Jahrzehnten die bevorzugten Algorithmen sein werden, wobei CRYSTALS-Kyber für den Schlüsselaustausch und CRYSTALS-Dilithium für digitale Signaturen verwendet wird.

Die NIST-Jury ermittelte außerdem vier weitere Kandidaten (die später auf drei reduziert wurden, da sich ein Algorithmus als unsicher erwies) zur weiteren Analyse und Bewertung in einer vierten Runde. Je nach Ausgang dieses Prozesses könnten in naher Zukunft weitere Gewinner bekannt gegeben werden.

Von den zahlreichen Algorithmen im Wettbewerb erwiesen sich nur wenige Signaturverfahren als sicher und praktikabel. Hinzu kommt, dass diese Verfahren relativ lange Signaturen erzeugen, die aufwendig zu überprüfen sind. Daher hat das NIST im Jahr 2022 einen weiteren Post-Quanten-Wettbewerb nur für Signaturverfahren ausgeschrieben, mit einem besonderen Aufruf zur Einreichung von Algorithmen mit kurzen und leicht zu verifizierenden Signaturen.[9] Derzeit werden in einer ersten Runde 40 Verfahren geprüft.

Es wird erwartet, dass die siegreichen Algorithmen aus diesen Post-Quanten-Wettbewerben in zahlreiche Standards und Produkte weltweit einfließen werden. Man kann davon ausgehen, dass das deutsche Bundesamt für Sicherheit in der Informations-technik (BSI) und die französische IT-Sicherheitsbehörde (ANSSI) ihre Algorithmen-Empfehlungen entsprechend anpassen werden.

Auch die Internet Engineering Task Force (IETF), das Standardisierungsgremium des Internets, wird die Gewinner des NIST-Wettbewerbs voraussichtlich übernehmen. Darüber hinaus hat die IETF zwei „Requests for Comments“ (RFCs) veröffentlicht, die Post-Quanten-Verfahren spezifizieren, die nicht an den NIST-Wettbewerben teilgenommen haben, nämlich die Signaturverfahren XMSS (RFC 8391)[10] und Leighton-Micali (RFC 8554)[11].



8. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography
9. https://csrc.nist.gov/projects/pqc-dig-sig/round-1-additional-signatures
10. https://www.rfc-editor.org/rfc/rfc8391.html
11. https://www.rfc-editor.org/rfc/rfc8554.html

Der Weg in die Post-Quanten-Welt

Wann leistungsfähige Quantencomputer Realität sein werden, weiß niemand. Daher müssen Annahmen getroffen werden. Die National Security Agency (NSA), die Cybersicherheitsbehörde der Vereinigten Staaten, schreibt den Betreibern von nationalen Sicherheitssystemen vor, spätestens ab 2035 Post-QuantenAlgorithmen zu verwenden.[12] Das deutsche BSI geht von der Arbeitshypothese aus, dass Prä-Quanten-Krypto-Verfahren in den frühen 2030er Jahren unsicher werden.[13]

Alle derzeit verfügbaren Post-Quanten-Verfahren unterscheiden sich in wesentlichen Punkten von RSA und Diffie-Hellman. Insbesondere sind die Schlüssel der Post-Quanten-Algorithmen oft wesentlich länger als die der herkömmlichen Verfahren. Beispielsweise benötigen die öffentlichen Schlüssel von CRYSTALS-Kyber und CRYSTALS-Dilithium um ein Vielfaches mehr an Speicherplatz als diejenigen von RSA und Diffie-Hellman (siehe Abbildung 2). Bei anderen Post-Quanten-Algorithmen ist der Unterschied sogar noch größer. Bei den privaten Schlüsseln ist die Situation nicht wesentlich anders. Darüber hinaus werden viele Schlüsselgenerierungs-, Signier- und Verifizierungsvorgänge langsamer, wenn Post-Quanten-Kryptografie verwendet wird.[14]

Die meisten Experten empfehlen für eine Übergangsphase hybride kryptografische Mechanismen. Ein hybrider kryptografischer Mechanismus kombiniert einen Prä-Quanten-Algorithmus wie RSA mit einer Post-Quanten-Methode wie CRYSTALS-Dilithium, so dass ein Angreifer beide Verfahren brechen muss, um erfolgreich zu sein. Diese Kombination bietet Schutz sowohl vor Quantencomputern als auch vor potenziellen Schwachstellen in Post-Quanten-Algorithmen.

Hybride Signaturen gibt es in zwei Varianten. Der komposite Ansatz sieht vor, dass eine hybride Signatur (bestehend aus zwei Signaturen) in einem Signaturfeld gespeichert wird. Der komposite Ansatz hat den Vorteil, dass die bestehenden Formate, die fast alle nur für eine Signatur ausgelegt sind, nicht geändert werden müssen. Der nicht-komposite Ansatz hingegen sieht vor, dass bei Verwendung eines hybriden Schemas zwei Signaturfelder verwendet werden. Die nicht-komposite Methode erfordert in der Regel eine Erweiterung des Nachrichtenformats, da die meisten Spezifikationen auf der Annahme beruhen, dass nur eine Signatur verwendet wird.

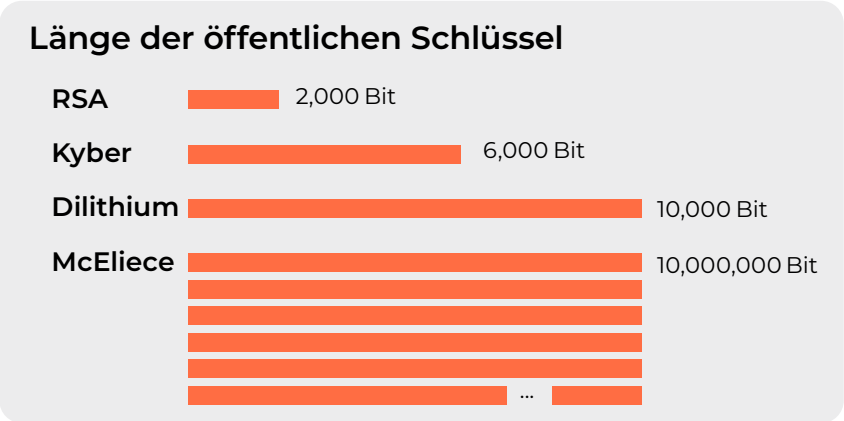


Abbildung 2: Die öffentlichen Schlüssel der meisten Post-Quanten-Algorithmen sind länger als die von herkömmlichen Krypto-Algorithmen wie RSA.

Mehrere hybride kryptografische Netzwerkprotokolle werden derzeit standardisiert. Zu den wichtigsten gehören die hybriden Varianten von S/MIME, OpenPGP, TLS und IKEv2. Public-Key-Infrastrukturen (PKI), einschließlich digitaler Zertifikate, werden ebenfalls angepasst.

Leider gehen die Meinungen über den Einsatz hybrider Krypto-Mechanismen auseinander.[14] Während das deutsche BSI und die französische ANSSI den Einsatz dieses Ansatzes klar empfehlen, raten andere IT-Sicherheitsbehörden davon ab. Die EU-Organisationen ETSI und ENISA lassen den Einsatz hybrider Systeme zu, geben aber keine Empfehlung dafür oder dagegen ab. Es bleibt zu hoffen, dass weitere Analysen zu einer Einigung unter den Experten führen werden. Die Migration zu Post-Quanten-Algorithmen wird einfacher, wenn die in einem IT-System verwendeten Krypto-Algorithmen leicht austauschbar sind. Dieses Paradigma wird als Krypto-Agilität bezeichnet. Im Idealfall erlaubt eine Krypto-Lösung den Wechsel der verwendeten Algorithmen per Mausklick. Darüber hinaus sollte es möglich sein, neue Kryptoverfahren einzuführen, ohne den Code neu kompilieren zu müssen.

Der Übergang zur Post-Quanten-Kryptografie ist untrennbar mit dem Paradigma der Krypto-Agilität verbunden. Nur mit kryptoagilen Lösungen wird ein einfacher und schneller Wechsel zu quantensicheren Methoden möglich. Zweifellos wird die Nachfrage der Verbraucher die Entwicklung kryptoagiler Lösungen vorantreiben, und die Hersteller werden sich bemühen, dieser Schwerpunktverlagerung gerecht zu werden. Standards, Benchmarks und Zertifizierungen werden sich weiterentwickeln. Die Pläne für die Migration nach der Quantenumstellung werden stark von der Kryptoagilität der beteiligten Komponenten abhängen.

12. https://fedscoop.com/nsa-sets-2035-deadline-for-adoption-of-post-quantum-cryptography-across-natsec-systems/
13. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Kryptografie-quantensicher-gestalten.html
14. https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study

Gesetzgebung

Die Umstellung auf Post-Quanten-Kryptografie ist in vielen Ländern ein wichtiges Thema für die Politik. Es wird erwartet, dass Staaten, die Quantentechnologien frühzeitig adaptieren, Vorteile in Bezug auf Produktivität, Wirtschaftswachstum, Gesundheit, Nachhaltigkeit sowie nationale Sicherheit und Widerstandsfähigkeit haben. Unter anderem beschäftigen sich die Behörden in den USA (CISA, NSA, NIST), Großbritannien (DSI&T), Deutschland (BSI), Frankreich (ANSSI) und auf EU-Ebene (ENISA) mit Post-Quanten-Strategien.[15]

Besonders aktiv sind die USA. So veröffentlichte das US-Ministerium für Innere Sicherheit zusammen mit dem NIST im Jahr 2021 einen Leitfaden mit dem Titel „Post-Quantum Cryptography".[16] Im Jahr 2022 unterzeichnete US-Präsident Biden den Quantum Computing Cybersecurity Preparedness Act[17] , der Bundesbehörden auffordert, Technologien zum Schutz vor Quantencomputer-Angriffen einzuführen. Die US-Regierungsbehörden wurden angewiesen, bis Mai 2023 ein vollständiges Inventar aktiver kryptografischer Systeme vorzulegen.

15. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Kryptografie-quantensicher-gestalten.html
16. https://www.dhs.gov/quantum
17. https://www.forbes.com/sites/forbestechcouncil/2023/01/25/what-the-quantum-computing-cybersecurity-preparedness-act-means-for-national-security/#:~:text=7535%2C%20the%20Quantum%20Computing%20Cybersecurity,and%20deploy%20quantum%2Dresilient%20cybersecurity

Die Migration zu Post-Quanten-Verfahren

Allgemeines

Jetzt, da neue Standards in greifbare Nähe rücken und Krypto-Anbieter ihre Produkte anpassen, ist es für Unternehmen und Behörden an der Zeit, sich ebenfalls mit Post-Quanten-Kryptografie zu beschäftigen. Aus heutiger Sicht ist eine Umstellung auf die neuen Methoden innerhalb der nächsten zehn Jahre erforderlich. Es sollte ein schrittweises Projekt geplant werden, das sich mit dieser Aufgabe befasst. In Anbetracht der Tatsache, dass große Unternehmen in der Regel Dutzende, wenn nicht Hunderte von Krypto-Anwendungen verwenden, wird ein erheblicher Ressourcenaufwand erforderlich sein.

Nicht alle kryptografischen Implementierungen sind in gleicher Weise von kryptografisch relevanten Quantencomputern betroffen. Symmetrische Algorithmen, wie AES oder Triple-DES, müssen nicht durch neue kryptografische Systeme ersetzt werden. Stattdessen reicht es aus, diese Chiffren mit geeigneten Schlüssellängen zu verwenden. Man geht davon aus, dass 256 Bit selbst den leistungsfähigsten kryptografisch relevanten Quantencomputern standhalten werden.

In vielen Systemen sind bereits 256-Bit-Schlüssel in Gebrauch. Wenn dies nicht der Fall ist, erlauben Hardware- und Software-Implementierungen oft eine Änderung der Schlüssellänge per Mausklick. Wenn dies nicht unterstützt wird, muss der Programmcode geändert werden. Es ist jedoch nicht notwendig, eine völlig neue Verschlüsselungstechnologie einzuführen, um die symmetrische Kryptografie quantensicher zu machen.

Anders verhält es sich mit RSA und Diffie-Hellman, die durch neuartige Algorithmen ersetzt werden müssen. Dies gilt auch für andere asymmetrische Krypto-Systeme, einschließlich Fiat-Shamir, DSA und Algorithmen, die auf elliptischen Kurven (ECC) basieren.

Da nicht alle Anwendungen der asymmetrischen Kryptografie auf die gleiche Weise angegriffen werden können, sollten die folgenden Unterscheidungen getroffen werden:

1. Verschlüsselung und Schlüsselaustausch: Asymmetrische Algorithmen, die zu diesem Zweck verwendet werden, können nicht nur zum Zeitpunkt ihrer Verwendung, sondern auch später angegriffen werden („Store now, decrypt later“). So kann ein Angreifer beispielsweise versuchen, eine verschlüsselte E-Mail zu entschlüsseln, die Jahre zuvor versandt wurde. Wegen dieser Bedrohung sollte der Übergang zur Post-Quanten-Verschlüsselung so schnell wie möglich vollzogen werden.

2. Datensignaturen: Signierte Nutzdaten können ebenfalls Ziel eines „Store now, decrypt later“-Angriffs sein. So könnte ein Angreifer signierte Informationen manipulieren, die Jahre zuvor erstellt wurden. Dies lässt sich jedoch verhindern, indem die Daten zu einem späteren Zeitpunkt mit einem Post-Quanten-Verfahren signiert werden.

3. Authentifizierungssignaturen: Die zur Authentifizierung verwendeten Signaturen, wie sie von Protokollen wie TLS oder IKE verwendet werden, werden sofort überprüft. Ist die Signatur korrekt, wird dem Signierer Zugang gewährt, andernfalls wird er abgewiesen. Solche Signaturen sind zu einem späteren Zeitpunkt wertlos. Aus diesem Grund ist die Migration von Authentifizierungssignaturverfahren weniger zeitkritisch als die zuvor genannten Anwendungen.

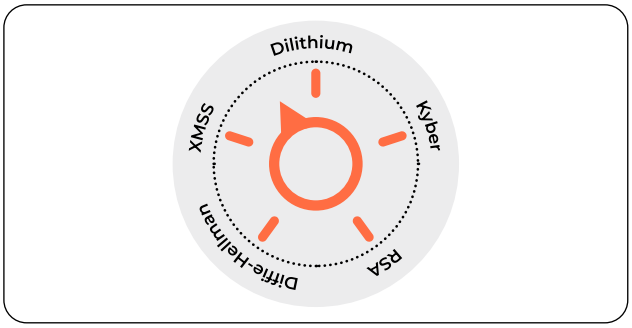


Abbildung 3: Krypto-Implementierungen sollten eine einfache Änderung der verwendeten Algorithmen ermöglichen. Dieses Prinzip wird als „Kryptoagilität“ bezeichnet.

Wie bereits erwähnt, empfehlen einige Experten hybride Krypto-Mechanismen für eine Übergangsphase. Wenn Sie diesem Rat folgen, müssen Ihre IT-Systeme nicht nur für die Post-Quanten-Zeit aktualisiert werden, sondern auch für die Nutzung hybrider Verfahren. Dies ist oft eine Herausforderung, da es meist einfacher ist, einen Algorithmus zu ersetzen, als die Unterstützung mehrerer Algorithmen gleichzeitig einzuführen.

Was die Migration einfacher macht

Die Migration zur Post-Quanten-Kryptografie wird einfacher, wenn die verwendete Krypto-Technik folgende Anforderungen erfüllt:[18]

- Der Betreiber ist mit den relevanten Compliance-Anforderungen vertraut.
- Der Betreiber verfügt über ein Krypto-Inventar.
- Ein Certificate Lifecyle Management (CLM) ist in Verwendung.
- Ein Schlüssel-Management-System (KMS) wird verwendet.
- Die verwendeten Krypto-Algorithmen sind nicht fest kodiert, Krypto-Agilität ist gegeben.
- Der Betreiber ist in der Lage, auf Krypto-Algorithmen umzustellen, die langsamer sind und längere Schlüssel verwenden als die derzeit genutzten.
- Die verwendeten Krypto-Bibliotheken werden auf dem neuesten Stand gehalten. Software, die nicht mehr unterstützt wird, wird ausgemustert.

Ablauf des Migrationsprozesses

Die Migration zur Post-Quanten-Kryptografie in einer Organisation sollte nach einem strukturierten Konzept erfolgen. Der ETSI-Bericht über Migrationsstrategien[19] legt die typischen Schritte eines solchen Projekts fest. In Anlehnung an diesen Leitfaden hat Eviden ein detailliertes Migrationsschema entwickelt. Dieser geschäfts- und praxisorientierte Prozess besteht aus sechs Schlüsselschritten:

1. Projektplanung
2. Erstellung eines Krypto-Inventars
3. Risikobewertung
4. Folgenabschätzung
5. Einbindung der Führungskräfte
6. Migrationsausführung

Projekt-Planung

Ein Unternehmen oder eine Behörde, die eine Migration zur Post-Quanten-Kryptografie plant, muss zunächst eine Analyse durchführen. Eine solche umfasst in der Regel die Auswirkungen und den potenziellen Schaden von Sicherheitsvorfällen, die durch quantenanfällige Komponenten verursacht werden, sowie die Gefahr von Ausfallzeiten und Verstößen gegen die Vorschriften. Auch die Budgetierung sollte in diesem Schritt ein Thema sein. Die Ergebnisse der Analyse helfen der Organisation, die Quantenbedrohung und ihre Auswirkungen auf die IT-Infrastruktur besser zu verstehen. Sie müssen der Geschäftsleitung vorgelegt werden, um die notwendige Unterstützung zu erhalten. Wenn die Geschäftsleitung zustimmt, wird ein größeres Migrationsprojekt in Angriff genommen.

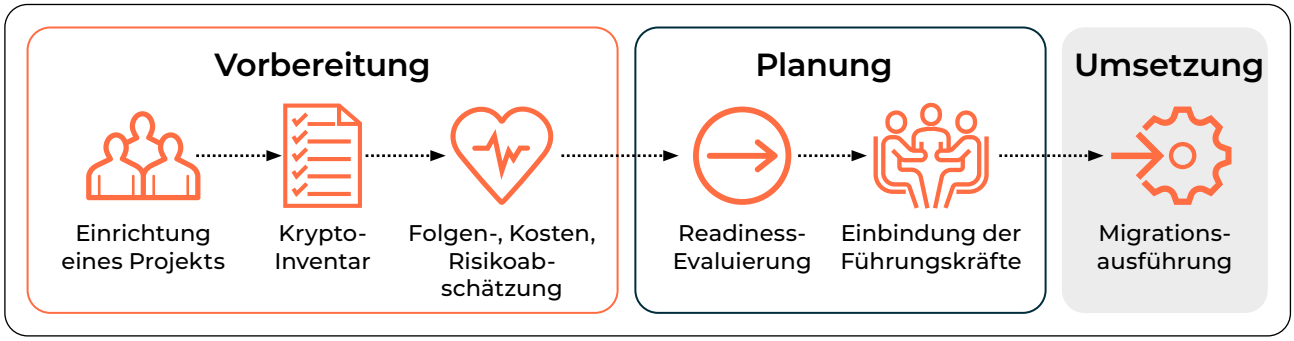


Abbildung 4: Die von Eviden definierten Schritte einer Post-Quanten-Migration

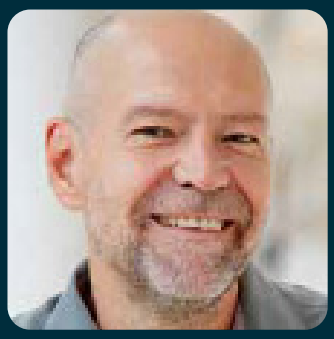
18. Paul van Brouwershaven, PKI Consortium Chair, at the PQC Conference in March 2023

19. https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf

> Die Post-Quanten-Migration ist eine wichtige Aufgabe für die kommenden Jahre. Ein Krypto-Inventar liefert einem Unternehmen wertvolle Erkenntnisse und zeigt oft Risiken auf, die bereits jetzt angegangen werden müssen.

Simon Ulmer, Eviden

Die Zeit drängt	Vorsicht ist angebracht
• Quantencomputer-Technik macht Fortschritte • Migration ist langwierig • Manche Daten müssen langfristig geschützt werden • Angreifer speichern Daten jetzt, um sie später zu entschlüsseln	• Es gibt noch keine Standards • Netzwerkprotokolle sind noch nicht angepasst • Migration ist komplex • Know-how muss aufgebaut werden • Interoperabilität ist nicht immer gegeben • Es gibt noch keine Sicherheitszertifizierungen



> Post-Quanten-Algorithmen unterscheiden sich in vielerlei Hinsicht von herkömmlichen Krypto-Verfahren. Die Post-Quanten-Migration erfordert daher ein hohes Maß an Fachwissen und Erfahrung.

Markus Hoffmeister, Eviden

Das Krypto-Inventar

Bevor eine Organisation auf Post-Quanten-Kryptografie umstellen kann, muss sie wissen, wo in ihrer IT-Landschaft überall Kryptografie eingesetzt wird. Typische Anwendungen, die Kryptografie nutzen, sind PC-Betriebssysteme, Web-Browser, VPN-Lösungen und Smartphone-Apps. Es gibt unzählige weitere. In vielen Fällen sind sich die Benutzer nicht einmal bewusst, dass sie Kryptografie einsetzen.

Um dieser Herausforderung zu begegnen, muss eine Organisation einen Katalog aller kryptografischen Anwendungen und Infrastrukturkomponenten, also ein Krypto-Inventar, erstellen. Das Krypto-Inventar enthält Informationen über jede Komponente (Krypto-Asset), die Kryptografie einsetzt, darunter:

- Hersteller
- Handelt es sich um eine Hardware- oder Softwarelösung?
- Wo wird die Komponente eingesetzt?
- Verwendete kryptografische Algorithmen (asymmetrisch und symmetrisch)
- Schlüssel und Schlüsselspeicher
- Digitale Zertifikate
- Protokolle
- Krypto-Anbieter und Bibliotheken

Darüber hinaus sollte ein Krypto-Inventar Infrastruktur-komponenten wie eine Public-Key-Infrastruktur (PKI) und Verweise auf Certificate Policies und Certification Practice Statements enthalten.

Der Detaillierungsgrad, den jeder Vermögenswert in einem Krypto-Inventar aufweisen muss, sollte ein klares Gleichgewicht zwischen Vollständigkeit und der Fähigkeit, die Migration rechtzeitig zu beginnen, herstellen. Betriebliche Zwänge können einen kontinuierlichen Verbesserungsansatz rechtfertigen, der die Aktualisierung oder das Hinzufügen neuer Informationen zum Inventar im Laufe der Zeit beinhaltet.

Eviden und seine Partner bieten Tools an, die die Erstellung und Pflege eines Krypto-Inventars unterstützen. Trotz des Automatisierungspotenzials müssen einige Aufgaben nach wie vor von Hand erledigt werden, da sie institutionelles Wissen und Verständnis für die IT- und Geschäftsaspekte einer Organisation erfordern. Die Identifizierung der Komponenten, die Kryptografie verwenden, ist bei Inventarisierungsprüfungen möglicherweise nicht ohne weiteres möglich und könnte übersehen werden.

Da nicht alle Bestände auf einmal entdeckt werden können, sollte die Erstellung und Aktualisierung des Krypto-Inventars ein kontinuierlicher Prozess im Unternehmen sein, der nicht unterbrochen werden darf. Darüber hinaus kann jedes neue Anwendungsprojekt das Krypto-Inventar verändern, indem es mit der Nutzung von Kryptografie beginnt oder aufhört, seine Infrastrukturebenen ändert oder sein Risikoprofil modifiziert.

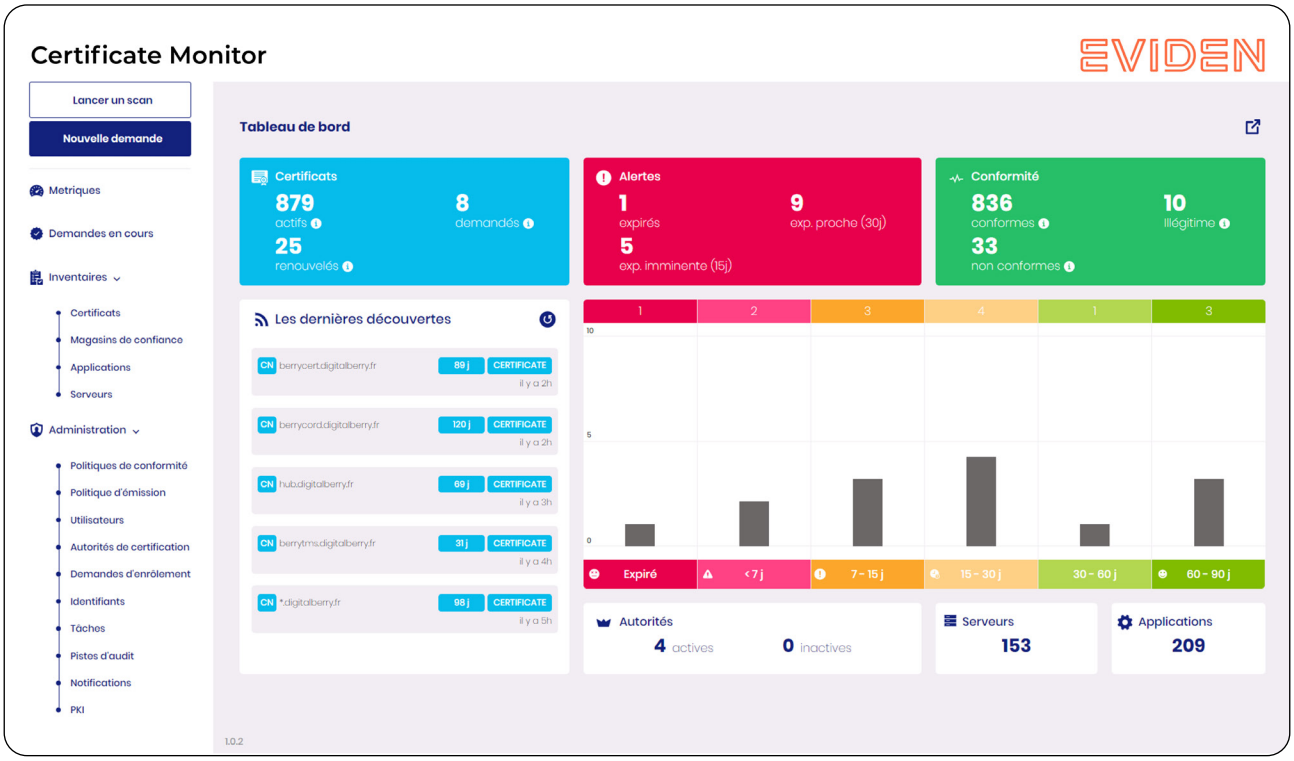


Abbildung 5: Eviden und seine Partner verwenden Tools, die die Erstellung und Pflege eines Krypto-Inventars ermöglichen.

Wussten Sie, dass Eviden “Strategic Cybersecurity Advisory”, eine Methode für die „First Level Business Risk Analysis“ entwickelt hat?

Erfahren Sie mehr im Kapitel “Was Eviden für Sie tun kann” am Ende des Dokuments.

Folgen-, Risiko- und Kostenabschätzung

In diesem Schritt muss jeder Eintrag des Krypto-Inventars im Hinblick auf seine Auswirkungen und das damit verbundene Risiko bewertet werden, wenn es nicht rechtzeitig quantenresistent gemacht wird. Zu diesem Schritt sollte auch eine Überprüfung bestehender Verträge gehören – idealerweise sollten diese Verträge einen Hinweis darauf enthalten, ob eine Lösung quantenfähig gemacht wird oder werden muss.

Andererseits müssen auch die Risiken der Verwendung von Post-Quanten-Kryptografie berücksichtigt werden. Die Umstellung auf Post-Quanten-Algorithmen könnte zu Inkompatibilitäten führen und unerwartete Ausfallzeiten zur Folge haben. Darüber hinaus müssen die Migrationsrisiken einer fehlerhaften Implementierung berücksichtigt werden.

Um eine Post-Quanten-Risikobewertung durchzuführen, muss man das Rad nicht neu erfinden. Stattdessen ist es möglich, einer allgemeinen Risikobewertung gemäß ISO 27005, NIST SP 800 30 oder OCTAVE einen Post-Quanten-Teil hinzuzufügen.[20] Darüber hinaus werden derzeit mehrere Post-Quanten-spezifische Risikobewertungsmethoden genutzt:

- CARAF (Crypto Agility Risk Assessment Framework),[21]
- Mosca’s Quantum Risk Assessment,[22]
- Wells Fargo PQC Risk Model.[23]

Auf Grundlage dieser Methoden hat Eviden seine eigene Vorgehensweise entwickelt, und zwar das PQC Risk Based Awareness Assessment (RBA2), das die folgenden Schritte umfasst:

- Ermitteln des Kontextes: Identifizieren von PQC-Anwendungsfällen, Zielen und Assets
- Identifizierung der Risiken: Identifizierung von PQC-Bedrohungen, Schwachstellen, Kontrollen und Souveränitätsstufen
- Risikoanalyse: Bestimmen der Wahrscheinlichkeit und der Auswirkungen für den gegebenen Zeitrahmen
- Risikobewertung: Berechnung der PQC-Priorität

Abbildung 6: Die Schritte einer Risikobewertung, wie sie von Eviden durchgeführt wird

20. https://www.sisainfosec.com/blogs/comparison-between-iso-27005-octave-nist-sp-800-30-sisa-blog/
21. https://academic.oup.com/cybersecurity/article/7/1/tyab013/6289827
22. https://globalriskinstitute.org/publication/gri-quantum-risk-assessment-report-part-1/
23. https://www.youtube.com/watch?v=sP0DsBZWpLs

Wussten Sie, dass Eviden mit dem „Strategic Cybersecurity Advisory“ eine Methode entwickelt hat, die Sie bei der Erstellung, Pflege und ständigen Verbesserung Ihres Krypto-Inventars unterstützt?

Erfahren Sie mehr im Kapitel “Was Eviden für Sie tun kann” am Ende des Dokuments.

Quantum-Readiness-Evaluierung

Die Migration der Anwendungen, die im Krypto-Inventar aufgeführt sind, gestaltet sich meist unterschiedlich schwierig. Um einen Überblick zu erhalten, sollte man die Kryptolösungen nach folgendem Schema bezüglich der Migrationsbe-reitschaft klassifizieren:

1. PQC-ready: Die Anwendung unterstützt bereits (asymmetrische) Post-Quanten-Methoden oder ausreichende (symmetrische) Schlüssellängen.
2. Krypto-Agilität: Die Anwendung ist nicht PQC-ready, ist aber kryptoagil.
3. PQC-Bereitschaftsplan: Die Anwendung ist zwar nicht kryptoagil, aber der Anbieter hat einen Plan, um dies zu ändern.
4. Bereitschaftsoption: Es gibt noch keinen PQC-Bereit-schaftsplan für diese Anwendung, aber es besteht die Möglichkeit, dass er in naher Zukunft erstellt wird.
5. Keine Bereitschaftsoption: Die Anwendung wird möglicherweise nie PQC-ready sein.

Da die Erstellung eines Krypto-Inventars und dessen Bewertung nach den aufgeführten Kriterien eine umfangreiche Aufgabe ist, sollte man einen solchen Katalog von einer dritten Partei prüfen lassen. Man kann sogar davon ausgehen, dass eine solche externe Quantum-Readiness-Evaluierung in naher Zukunft standardisiert und gesetzlich vorgeschrieben wird.

Einbindung der Führungskräfte

Wenn die bisher beschriebenen Schritte abgeschlossen sind, muss die Leitung des jeweiligen Unternehmens oder der Behörde einbezogen werden. Die Fachverantwortlichen müssen dem Management vermitteln, warum die Post-Quanten-Migration notwendig ist und welche Risiken bestehen, wenn sich dieser Prozess verzögert. Darüber hinaus müssen sie einen Budgetplan für das Migrationsprojekt erstellen. Auf dieser Basis ist dann eine Entscheidung der Unternehmens- bzw. Behördenleitung notwendig.

Migrationsausführung

Wenn der Nutzen und die Risiken der Post-Quanten-Migration abgeschätzt sind und das Projekt geplant und genehmigt ist, kann die Ausführung beginnen. Da es nicht praktikabel ist, alle betroffenen Krypto-Verfahren auf einmal zu ersetzen, ist eine Priorisierung erforderlich.

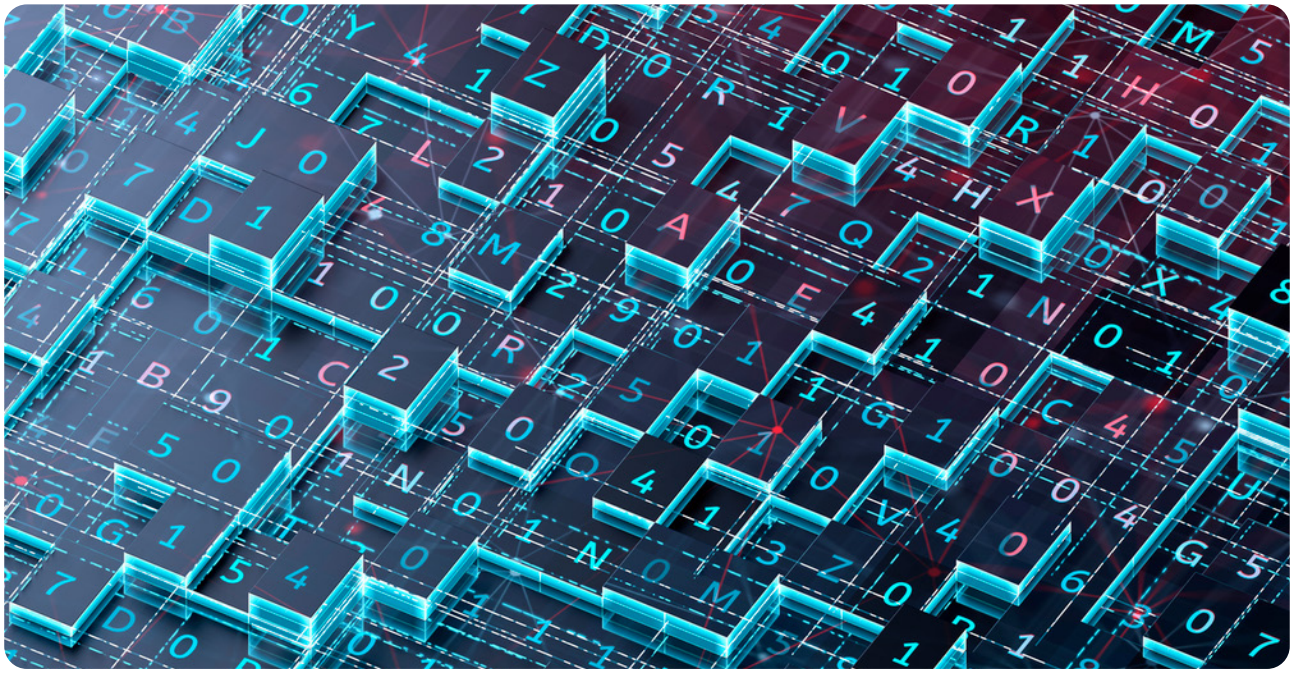
Als erstes sollte die Infrastruktur migriert werden. Dies gilt insbesondere für die PKI, da zuerst Post-Quanten-Zertifikate eingeführt werden müssen, bevor eine zertifikatsbasierte Anwendung Post-Quanten-fähig gemacht werden kann.

Der Zeitplan für die Migrationsausführung muss auf Grundlage der folgenden Kriterien erstellt werden:

- Stand der Technik von Quantencomputern: Vor 2030 werden leistungsfähige Quantencomputer kaum verfügbar sein. Die Fortschritte in dieser Technologie müssen dennoch beobachtet und der Migrationsprozess gegebenenfalls beschleunigt werden.
- Stand der Technik der Post-Quanten-Kryptografie: Die Post-Quanten-Kryptografie hat in den letzten Jahren beträchtliche Fortschritte gemacht, und auch zukünftig wird es neue Entwicklungen geben. So ist zum Beispiel keiner der drei vom NIST im Rahmen des Wettbewerbs ausgewählten Signaturalgorithmen für alle Anwendungen geeignet, weshalb derzeit neue Verfahren entwickelt werden. Mit dem Aufkommen weiterer Algorithmen muss der Projektplan möglicherweise geändert werden.
- Abhängigkeit von der Infrastruktur: Asymmetrische Krypto-Verfahren verwenden in der Regel digitale Zertifikate, die von einer PKI bereitgestellt werden. Es liegt auf der Hand, dass solche Komponenten nur dann aktualisiert werden können, wenn die Infrastruktur, auf die sie angewiesen sind, bereits migriert wurde. Umgekehrt können eigenständige Systeme, wie z. B. eine Komponente, die symmetrische Kryptografie ohne externe Schlüsselverwaltung verwendet, unabhängig von der Infrastruktur bearbeitet werden.
- PQC-Readiness: Natürlich können nur PQC-fähige Komponenten migriert werden.
- Risiko: Komponenten mit einem hohen Risiko, angegriffen zu werden, oder mit einem hohen Schadenspotenzial müssen eine hohe Priorität erhalten.

Es ist klar, dass die für die Migrationsausführung erforderlichen Ressourcen geplant werden müssen. Das Personal muss bereitgestellt und geschult werden. Das Projektmanagement sollte stets den aktuellen Stand der Quantencomputer-Technik und der Post-Quanten-Unterstützung der Komponenten im Krypto-Inventar umfassen. Im Idealfall wird das Krypto-Inventar während der Migration und bei der Einführung neuer Anwendungen ständig aktualisiert.

Jede Ergänzung des Krypto-Inventars sollte dazu führen, dass die Schritte 3 bis 6 des oben beschriebenen Prozesses für die neuen Assets durchlaufen werden.



Post-Quanten-Kryptografie

Die Umstellung auf Post-Quanten-Kryptografie wird nur gelingen, wenn sich Entwickler, Berater, IT-Manager, Administratoren und IT-Führungskräfte mit ihr auseinandersetzen. Dies ist nicht einfach, denn die Mathematik hinter den Post-Quanten-Verfahren ist komplex und unterscheidet sich erheblich von dem, was bisher in der Kryptografie eine Rolle spielt. So ist es beispielsweise deutlich schwieriger, CRYSTALS-Kyber und CRYSTALS-Dilithium zu verstehen als Systeme wie RSA und Diffie-Hellman.

Eviden ist daher an vielen Aktivitäten beteiligt, die die Post-Quanten-Kryptografie für Nicht-Mathematiker erklären. Viele der von Eviden entwickelten Erklärungsmodelle basieren auf Alltagsanalogien und nutzen Cartoons. Diese Comic-Illustrationen wurden in Whitepapers und Zeitschriftenartikeln veröffentlicht[24] und werden immer wieder bei führenden Sicherheitsveranstaltungen auf der ganzen Welt präsentiert.

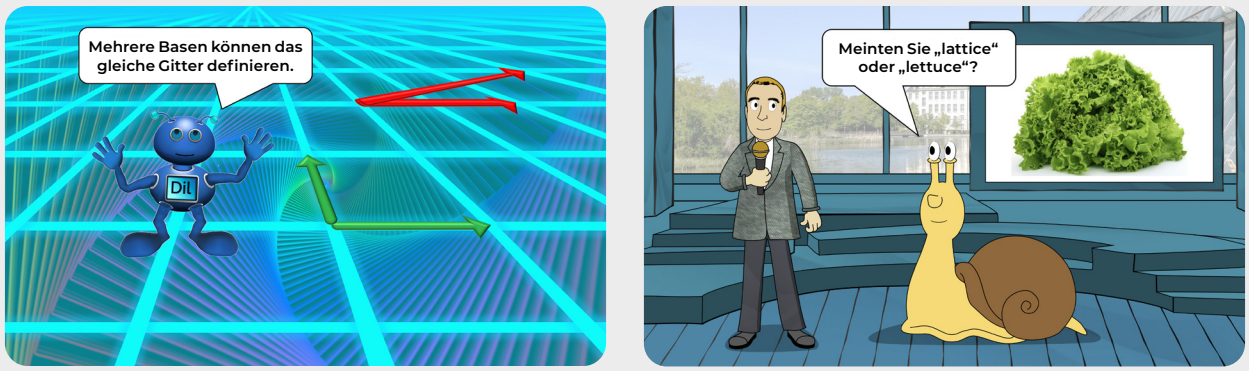


Abbildung 7: Mit solchen Grafiken, die auch für Nicht-Mathematiker verständlich sind, erklärt Eviden die Post-Quanten-Kryptografie.

Abbildung 8: Eviden-Mitarbeiter halten Vorträge zum Thema Post-Quanten-Kryptografie bei Konferenzen und Messen weltweit.

24. https://www.cryptovision.com/wp-content/uploads/2021/06/VAULT_Post-Quantum-Cryptography_062021.pdf

Was Eviden für Sie tun kann

Beratung

Eviden ist ein führender Spezialist für Consulting zur Post-Quanten-Migration. Wir stehen für einen schrittweisen Migrationsansatz, für den bei Bedarf unsere quantenresistenten Security-Produkte zur Verfügung stehen. Wir unterstützen Sie unter anderem bei den folgenden Aufgaben:

- Erstellung einer ersten Risikoanalyse, um den Umfang der notwendigen Maßnahmen abschätzen zu können,
- Erstellung, Pflege und kontinuierliche Verbesserung eines Krypto-Inventars,
- Bewertung der mit einer Quantenmigration verbundenen Risiken mit dem PQC Risk-Based Awareness Assessment (RBA2) von Eviden,
- Prüfen der Quanten-Readiness Ihrer Krypto-Lösungen und Auswahl der gegebenenfalls notwendigen Alternativen,
- Awareness-Maßnahmen in Form von Präsentationen und Veröffentlichungen.

Eviden ist an mehreren europäischen Forschungs- und Entwicklungsprojekten beteiligt, z. B. an der Erprobung des pragmatischen Einsatzes von Post-Quanten-Kryptografie in PKI-Smartcards.

Unsere Krypto-Produkte

IDnomic PKI
IDnomic PKI ist eine leistungsstarke, vielseitig einsetzbare PKI-Software-Suite, die den höchsten Sicherheitsstandards entspricht. IDnomic PKI ist kryptoagil konzipiert und in der Lage, hybride Zertifikate (komposit und nicht-komposit) auszustellen. Sie ermöglicht einen reibungslosen Migrationspfad von herkömmlichen Krypto-Verfahren zu Post-Quanten-Algorithmen. Die IDnomic PKI lässt sich leicht mit anderen Eviden-Lösungen erweitern, was unter anderem eine benutzerseitige Schlüsselverwaltung und komplexe Workflows ermöglicht.

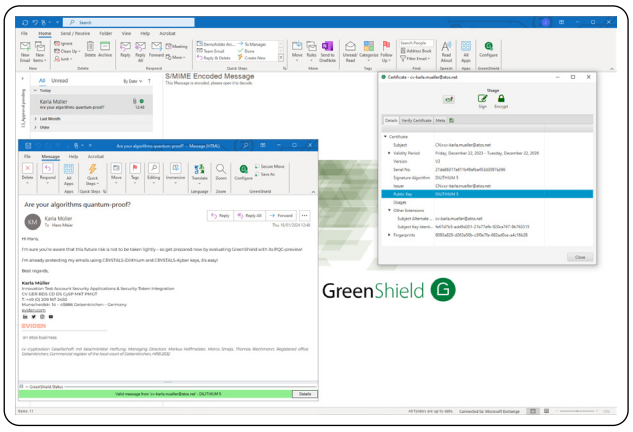


Abbildung 9: Cryptovision GreenShield verschlüsselt und signiert E-Mails und Dateien. Es verfügt über ein PQC-Vorschau-Modul, das die Verwendung von Post-Quanten-Algorithmen ermöglicht.

CardOS
CardOS ist ein hochsicheres, multi-funktionales Smartcard-Betriebssystem, das alle Funktionen zur Abdeckung verschiedener Anwendungen über kontaktbasierte und kontaktlose Schnittstellen bietet. CardOS wird in naher Zukunft Post-Quanten-Algorithmen unterstützen.

Evidian IAM
Evidian IAM ist eine Produktreihe, die Unternehmen vor Angriffen durch nichtautorisierte Benutzer schützt. Evidian IAM unterstützt zahlreiche Sicherheitsprotokolle und Krypto-Mechanismen. Diese werden in naher Zukunft die Post-Quanten-Signatur- und Verschlüsselungsstandards umfassen, die derzeit von der NIST entwickelt werden.

cryptovision Greenshield
Cryptovision GreenShield von Eviden ist eine Softwarelösung zum Verschlüsseln und Signieren von E-Mails und Dateien. Sie ist für den Austausch von Verschlusssachen (EU restricted, NATO restricted und VS-NfD) zugelassen und vom deutschen BSI und dem EU-Rat akkreditiert. Cryptovision GreenShield ist vollständig kryptoagil. Es verfügt über ein PQC-Vorschau-Modul, das Post-Quanten-und Komposit-Signaturen mit CRYSTALS-Dilithium und Post-Quanten-Verschlüsselung mit CRYSTALS-Kyber ermöglicht.

IDnomic Certificate Monitor
IDnomic Certificate Monitor ermöglicht die Überwachung der im Einsatz befindlichen digitalen Zertifikate. Diese Lösung ist daher ideal für die Erstellung eines Krypto-Inventars. Darüber hinaus bietet sie eine zentrale Schnittstelle für das Certificate Lifecycle Management und ermöglicht die automatische Erneuerung digitaler Zertifikate.

Trustway
Die Trustway Proteccio Produktlinie besteht aus mehreren zertifizierten Hardware-Security-Modul-Appliances. Trustway Proteccio hat die Post-Quantuen-Signaturverfahren CRYSTALS-Dilithium (Signatur) und CRYSTALS-Kyber (Schlüsselaustausch) integriert und wird in der ersten Hälfte des Jahres 2024 auf den Markt kommen.

Die VPN-Lösung Trustway IP Protect wird CRYSTALS-Kyber (Schlüsselaustausch) zwischen zwei Trustway IP Protect VPNs unterstützen.

Fazit

Eviden ist ein Experte auf dem Gebiet des Quantencomputings und der Kryptografie. Aufgrund dieser einzigartigen Expertise ist Eviden Ihr idealer Partner in allen Fragen der Post-Quanten-Kryptografie. Evidens Kryptografieprodukte, darunter HSMs, E-Mail-Verschlüsselungssoftware, Smartcards und PKI-Lösungen, werden derzeit quantensicher gemacht. Einige davon haben bereits Post-Quanten-Algorithmen implementiert.

Vor allem aber unterstützt Eviden Ihr Unternehmen bei der Post-Quanten-Migration. Wir stehen für einen umfassenden, schrittweisen Ansatz, der Ihnen dabei hilft, Ihre Migrationsziele rechtzeitig und im Rahmen des Budgets zu erreichen. Wir beraten Sie gerne bei der Krypto-Inventarisierung, Risikobewertung, Sensibilisierung, Produktauswahl, beim Projektmanagement und bei allen anderen Fragen der Post-Quanten-Migration.

Sie wollen mehr wissen? Wir informieren Sie gerne: cybersecurity@eviden.com

Autoren

Redaktionsleitung:
Klaus Schmeh
Chief Editor Marketing
klaus.schmeh@eviden.com

Kryptografie, PKI, Certificate Lifecycle Management:
Markus Hoffmeister
BDS Cyberproducts – Digital ID – Strategic Advisor
Managing Director cv cryptovision GmbH
markus.hoffmeister@eviden.com

Krypto-Inventare, Certificate Lifecycle Management, Risikobewertung:
Simon Ulmer
Group VP - Head of Digital ID – BDS Cyberproducts
Eviden Scientific Community member
simon.ulmer@eviden.com

Post-Quanten-Produkte:
Vasco Gomes
Cybersecurity Products CTO
Digital Security Offerings Technology Lead
Eviden Scientific Community member Cybersecurity Distinguished Expert
vasco.gomes@eviden.com

Risikobewertung:
Sławomir Pijanowski, Ph.D.
Global GRC Practice Leader, Global Cybersecurity Consulting
Eviden Distinguished Expert
slawomir.pijanowski@eviden.com

Post-Quanten-Organisation und -Koordination:
Anastazija Zivkovic
Security Advisor
Global Cybersecurity Consulting
anastazija.zivkovic@eviden.com

Connect with us

eviden.com