In Zusammenarbeit mit A-SIT Plus GmbH

Markus Kaiser, Graz

Migration auf Post-Quanten-Kryptographie im Anwendungsbereich der Electronic Machine Readable Travel Documents (eMRTD)

Stand: 07.05.2025

A-SIT Plus GmbH

Zusammenfassung

Die fortschreitende Entwicklung von Quantencomputern stellt bestehende kryptographische Systeme vor erhebliche Herausforderungen. Dies betrifft insbesondere asymmetrische Verfahren, die auf der Schwierigkeit mathematischer Probleme wie der Primfaktorzerlegung basieren, die mit Quantencomputern plötzlich einfacher, d.h., effizienter, lösbar werden. Dadurch ergibt sich die Notwendigkeit einer Migration auf Post-Quanten-Kryptographie, die auch bei Verfügbarkeit von Quantencomputern ausreichende Sicherheit bietet. Expertenmeinungen und Einschätzungen zum tatsächlichen Zeitpunkt der Verfügbarkeit praktisch relevanter Quantencomputer divergieren. Derartige Schätzungen sind auch stets mit einer gewissen Unsicherheit behaftet, die ihre Gründe in nicht vorhersehbaren disruptiven Entwicklungssprüngen oder auch der bewussten Geheimhaltung bereits erreichter Meilensteine haben kann. Weitgehend einig sind sich Experten, dass eine Migration auf Post-Quanten-Kryptographie jedenfalls schnellstmöglich vorbereitet werden muss, da dafür – je nach Anwendungsgebiet – mit langen Durchlaufzeiten zu rechnen ist.

Dieses Dokument bietet eine Einführung in die Post-Quanten-Kryptographie, stellt relevante Algorithmen und Ansätze vor und gibt einen Einblick in relevante Schlüssellängen und Signaturgrößen. Das Dokument zeigt auch auf, welche Herausforderungen sich für IT-Systeme, die aktuell noch auf klassischen kryptographischen Algorithmen beruhen, ergeben. Besonderes Augenmerk wird dabei auf den Anwendungsbereich der Electronic Machine Readable Travel Documents (eMRTD) gelegt. Für diesen werden spezifische Anforderungen, Herausforderungen und Fragestellungen analysiert.

Die in diesem Dokument zusammengefassten Analyseergebnisse zeigen, dass eine konkrete Umstellung auf Post-Quanten-Kryptographie derzeit (2025) u.a. aufgrund fehlender internationaler Normen und Standards und ihrer technischen Implementierungen praktisch oft noch nicht möglich ist. Während mittlerweile erste standardisierte Post-Quanten-Algorithmen verfügbar sind, wurden relevante Normen und Standards spezifischer Anwendungsbereiche oft noch nicht entsprechend nachgezogen. Dies betrifft u.a. auch den Anwendungsbereich der Electronic Machine Readable Travel Documents (eMRTDs) und die für die Ausgabe von eMRTDs verantwortlichen Stellen. Die Analyse zeigt jedoch auch, dass speziell im Bereich der eMRTD mit einer langen Durchlaufzeit für eine Migration auf Post-Quanten-Kryptographie zu rechnen sein wird, sodass mit jetzt schon möglichen vorbereitenden Schritten schnellstmöglich begonnen werden sollte. Daraus können folgende Empfehlungen abgeleitet werden.

Empfehlungen: *Es wird dringend empfohlen, mit vorbereitenden Tätigkeiten wie der Erarbeitung einer geeigneten Migrationsstrategie bereits jetzt zu starten. Dies ist insbesondere im Anwendungsbereich der eMRTDs wichtig, da durch deren lange Gültigkeit von bis zu 10 Jahren mit einer sehr langen Durchlaufzeit für eine vollständige Migration auf Post-Quanten-Kryptographie zu rechnen ist. Nur durch eine frühzeitige Auseinandersetzung mit dem Thema kann sichergestellt werden, dass notwendige Vorbereitungen für konkrete Migrationsprozesse bereits getroffen wurden, wenn alle für*

eine Migration notwendigen technischen und normativen Voraussetzungen geschaffen sind. Nur so kann die eigentliche Migration zu diesem künftigen Zeitpunkt effizient vorgenommen und rechtzeitig abgeschlossen werden, noch bevor erste praktisch relevante Quantencomputer verfügbar sind.

Über dieses Dokument

Dieses Dokument entstand in Zusammenarbeit der *A-SIT Plus GmbH* mit dem *Institute of Information Security (ISEC)* der *Technischen Universität Graz (TU Graz)*.

Dipl.-Ing. Dr.techn. Peter Teufl

A-SIT Plus GmbH

Univ.-Prof. Dipl.-Ing. Dr.techn. Christian Rechberger

Institute of Information Security (ISEC), TU Graz

Inhalt

1 Einleitung

Mit der fortschreitenden Entwicklung leistungsfähiger Quantencomputer geraten etablierte asymmetrische kryptographische Verfahren wie RSA (Rivest–Shamir–Adleman) oder Eliptic Curve Cryptography (ECC) zunehmend unter Druck. Diese asymmetrischen Algorithmen, deren Sicherheit auf der Schwierigkeit der Primfaktorzerlegung großer Zahlen oder dem diskreten Logarithmusproblem elliptischer Kurven beruhen, könnten künftig durch quantenbasierte Verfahren – allen voran Shor‘s Algorithmus[1] – in vertretbarer Zeit gebrochen werden. Damit steht langfristig die Sicherheit aller Lösungen der Informationstechnologie (IT), die aktuell über klassische asymmetrische Algorithmen wie RSA oder ECC gewährleistet wird, auf dem Spiel. Um dieser absehbaren Bedrohung wirksam zu begegnen, rückt die Post-Quanten-Kryptographie (PQC) in den Fokus. PQC-Verfahren basieren auf mathematischen Problemen, die nach heutigem Kenntnisstand weder von klassischen Computern noch von Quantenrechnern effizient gelöst werden können, und bieten so eine positive Zukunftsperspektive für sichere digitale Infrastrukturen.

Die weltweite Standardisierungsarbeit, unter anderem vorangetrieben durch anerkannte und renommierte Institutionen wie dem National Institute of Standards and Technology (NIST) in den USA, dem Bundesamt für Sicherheit in der Informationstechnik (BSI) in Deutschland oder auch dem European Telecommunications Standards Institute (ETSI) auf Ebene der Europäischen Union (EU), läuft bereits auf Hochtouren. Erste Auswahlverfahren haben Mitte der 2010er Jahre konkrete PQC-Algorithmen identifiziert, deren endgültige Standardisierung teilweise bereits erfolgt ist. Eine Umstellung aktueller IT-Systeme auf diese PQC-Algorithmen ist jedoch kein triviales Unterfangen. Während symmetrische Algorithmen wie der Advanced Encryption Standard (AES) vergleichsweise einfach durch eine Erhöhung der Schlüssellänge robust gegen Quantenangriffe gemacht werden können, müssen bei asymmetrischen Verfahren völlig neue Ansätze etabliert werden. Die Implementierung quantenresistenter Verfahren stellt hohe Anforderungen an Software-Stacks, Hardware Security Modules (HSM), Chipkarten und andere Komponenten. Hinzu kommt, dass etablierte Protokolle wie Transport Layer Security (TLS) oder auch ganze Zertifizierungsprozesse neu ausgerichtet werden müssen, um alternative Algorithmen, größere Schlüssel, umfassendere Signaturen und veränderte Sicherheitsmodelle abzubilden.

Darüber hinaus ergeben sich bei einer Migration auf PQC-Algorithmen auch praktische Herausforderungen, etwa in Bereichen, in denen Platz- oder Bandbreitenrestriktionen bestehen. Die teils deutlich größeren PQC-Schlüssel und Signaturen beeinflussen die Performance, erhöhen den Datenbedarf

[1] Mit dem Algorithmus von Shor können Primfaktorzerlegungen und diskrete Logarithmen effizient auf Quantencomputern berechnet werden. Während klassische Computer diese Aufgaben bisher nicht in polynomieller Zeit bewältigen konnten, können diese nun mittels quantenmechanischer Prinzipien wie der Quanten-Fourier-Transformation in polynomieller Laufzeit bewältigt werden. Da in den letzten Jahren zudem große Fortschritte im Bau von Quantencomputern erzielt wurden, stellt dies eine ernstzunehmende Bedrohung für asymmetrische kryptographische Verfahren wie RSA und ECC dar, deren Sicherheit auf der Schwierigkeit der Faktorisierung großer Zahlen und diskreten Logarithmen basieren.

und können die bisherigen Formfaktoren sprengen – etwa bei RFID[2]/NFC[3]-Karten, Chipkartenlesern oder auch bei QR[4]-Codes zur Offline-Verifikation, die heute u.a. bei digitalen Zertifikaten und Ausweisdokumenten zur Anwendung kommen. Die Frage, wie solche Umstellungen in der Praxis umgesetzt werden können, ohne dabei die Nutzbarkeit, Interoperabilität oder den Datenschutz zu gefährden, ist noch nicht abschließend geklärt. Insgesamt zeigt sich, dass der Übergang zur Post-Quanten-Kryptographie eine tiefgreifende Transformation für die aktuell etablierten technischen Standards, Infrastrukturen und Sicherheitsarchitekturen bedeutet. Diese notwendige Transformation muss frühzeitig strategisch adressiert werden, um zukünftige quantenbasierte Angriffe effektiv abwehren zu können.

Das vorliegende Dokument verfolgt das Ziel, ein grundlegendes Verständnis der Post-Quanten-Kryptographie zu vermitteln und dabei wesentliche Algorithmen und Ansätze vorzustellen. Neben dieser Einführung werden detaillierte Informationen zu relevanten Parametern wie Schlüssellängen und Signaturgrößen ausgewählter Algorithmen gegeben, um eine fundierte Basis für technische Analysen und Entscheidungen zu schaffen. Ein weiterer Schwerpunkt des Dokuments liegt in der Identifikation von Aspekten bestehender IT-Lösungen, die bei einer Migration auf Post-Quanten-Kryptographie berücksichtigt werden müssen. Darüber hinaus werden die spezifischen Herausforderungen einer solchen Migration herausgearbeitet, um potenzielle Hindernisse frühzeitig zu erkennen und Lösungsansätze entwickeln zu können. Besonders im Anwendungsbereich der Electronic Machine Readable Travel Documents (eMRTD) beleuchtet das Dokument spezifische Anforderungen und Fragestellungen, die für diesen Use-Case von Bedeutung sind. Abschließend wird ein Überblick über geeignete technische und organisatorische Mitigationsmaßnahmen gegeben, über die Risiken adressiert werden können. Ziel ist es, eine praxisorientierte Grundlage zu schaffen, die verantwortliche Organisationen bei der Vorbereitung auf den Übergang zur Post-Quanten-Kryptographie unterstützt.

2 Hintergrund

Dieser Abschnitt behandelt allgemeine Hintergrundinformationen zur Post-Quanten-Kryptographie. Dadurch schafft dieser Abschnitt ein notwendiges Grundverständnis relevanter technischer Konzepte und bildet damit die Basis für punktuelle Vertiefungen in den nachfolgenden Abschnitten.

2.1 Quantencomputer als Gefahr für klassische kryptographische Algorithmen

Quantencomputer nutzen quantenmechanische Effekte wie Superposition und Verschränkung, um Berechnungen bei geeigneten Problemstellungen in einer Art zu parallelisieren, die selbst modernste klassische Hochleistungsrechner nicht erreichen können. Die Möglichkeit, Berechnungen bestimmter

[2] RFID: Radio Frequency Identification
[3] NFC: Near Field Communication
[4] QR: Quick Response

Problemstellungen hochgradig zu parallelisieren, stellt vor allem für die Sicherheit klassischer, d.h. aktuell zum Einsatz kommender, kryptographischer Algorithmen ein Problem dar, die genau auf solchen für Quantencomputer speziell geeigneten Problemstellungen beruhen. Shors Algorithmus[5] gilt dabei als paradigmatisches Beispiel: Er ermöglicht es, große Zahlen und diskrete Logarithmen effizient zu faktorisieren beziehungsweise zu berechnen, was die mathematischen Grundlagen kryptographischer Algorithmen wie RSA und ECC fundamental erschüttert. Beide Verfahren – bislang u.a. wesentliche Stützen der heutigen Public-Key-Infrastrukturen (PKI) – verlieren damit langfristig ihre Sicherheit und Zuverlässigkeit, sobald ausreichend leistungsfähige Quantenrechner zur Verfügung stehen.

Die Sicherheit symmetrischer Kryptosysteme wie AES ist von Quantencomputern hingegen weniger stark betroffen. Zwar kann Grovers Algorithmus[6] die Schlüsselsuche in diesen Kryptosystemen im Prinzip beschleunigen, doch sinkt die effektive Sicherheit hier nur um den Faktor zwei[7]. Eine einfache Anpassung, etwa die Verwendung von AES-256 anstelle von AES-128 und damit eine Erhöhung der Schlüssellänge, reicht aus, um ein angemessenes Schutzniveau zu bewahren. Somit entsteht ein klarer Unterschied zwischen asymmetrischen und symmetrischen Verfahren: Während erstere vollständig neu konzipiert und ausgerichtet werden müssen, um gegen künftige Quantenangriffe gewappnet zu sein, lassen sich letztere mit vergleichsweise geringem Aufwand über eine Anpassung der Schlüssellänge auf ein quantenresistentes Niveau heben.

Die Tatsache, dass aktuell noch keine Quantencomputer existieren, die etwa RSA- oder ECC-Schlüssel praktisch brechen können, bedeutet lediglich eine zeitliche Atempause. Internationale Institutionen wie das NIST, das BSI und die ETSI haben bereits damit begonnen, Standards für Post-Quanten-Kryptographie zu definieren. Durch dieses vorausschauende Vorgehen wird die Grundlage geschaffen, rechtzeitig auf quantenresistente Verfahren umzusteigen – noch bevor Quantencomputer die Größe und Stabilität erreichen, um klassische Kryptographie tatsächlich zu kompromittieren.

2.2 Erwartete Verfügbarkeit praxisrelevanter Quantencomputer

Auch wenn die Verfügbarkeit praktisch verwendbarer Quantencomputer intensiv erforscht wird, bleibt der genaue Zeitpunkt ihrer Verfügbarkeit ungewiss. Aktuelle Schätzungen von Experten gehen davon aus, dass großskalige, fehlerkorrigierte Quantencomputer, die reale Anwendungen unterstützen, in den nächsten 10 bis 20 Jahren entwickelt werden könnten. Das BSI geht von höchstens 16 Jahren aus, bis ein entsprechender Quantencomputer verfügbar sein wird[8]. Die tatsächliche Zeitleiste hängt

[5] Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS), pp. 124–134. IEEE.
[6] Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. In Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC), pp. 212–219. ACM.
[7] Streng genommen sinkt die effektive Sicherheit sogar etwas weniger als um den Faktor zwei, da Grover-Implementierungen in der Praxis teuer sind und sich wenig gut parallelisieren lassen.
[8] BSI: Entwicklungsstand Quantencomputer: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/Entwicklungsstand_QC_Zusammenfassung_V_2_1.pdf?__blob=publicationFile&v=3

von technologischen Durchbrüchen ab, insbesondere in den Bereichen Qubit-Stabilität, Skalierbarkeit und effiziente Fehlerkorrektur.

Aktuell existieren Quantencomputer in experimentellen Umsetzungen. Unternehmen wie IBM[9], Google und andere konnten bereits Prototypen vorstellen, die jedoch meist auf wenige Dutzend, bis knapp über 1.000 Qubits beschränkt sind. Von einer praxisnahen Anwendung zur Kompromittierung aktueller kryptographischer Verfahren sind diese Prototypen noch weit entfernt.

Die Entwicklung praktisch nutzbarer Quantencomputer wird aktuell noch durch mehrere Faktoren erschwert, u.a.:

- **Fehlerkorrektur:** Aktuelle Quantencomputer sind anfällig für Rauschen und Fehler. Um daraus resultierende Quantenfehler zu minimieren, sind Fehlerkorrekturverfahren erforderlich, die zusätzliche Qubits beanspruchen.
- **Skalierung:** Die physikalische Größe und Komplexität von Quantencomputern wächst mit der Anzahl der Qubits. Systeme mit Millionen von Qubits wären notwendig, um komplexe Probleme (fehlerkorrigiert) zu lösen.
- **Kryogene Umgebung:** Quantenprozessoren erfordern in der Regel extrem niedrige Temperaturen (nahe dem absoluten Nullpunkt), was die Konstruktion und den Betrieb teuer und schwierig macht.

An den aktuellen Herausforderungen in der Realisierung praktischer Quantencomputer wird weltweit auch von führenden Technologieunternehmen wie IBM, Google oder Microsoft geforscht und gearbeitet. Wann entscheidende Durchbrüche erzielt werden können, ist schwer prognostizierbar. Dies auch, weil tatsächliche Entwicklungsstände und Forschungsresultate z.B. aus geschäftlichen Interessen nicht notwendigerweise immer gleich veröffentlicht werden. Im Allgemeinen scheint die Schätzung des BSI, dass praxisrelevante Quantencomputer spätestens ab dem Jahr 2040 verfügbar sein werden, aus aktueller Sicht plausibel.

2.3 Ansätze zur Erreichung von Post-Quanten-Kryptographie

Post-Quanten-Kryptographie basiert auf Problemklassen, die unter den derzeit bekannten quanten- und klassisch-algorithmischen Methoden als schwer lösbar gelten. Ziel ist es, Verfahren bereitzustellen, die selbst gegenüber zukünftigen Quantenangriffen standhaft bleiben. Diese neuen Algorithmen stützen sich daher auf mathematische Probleme, die weder durch klassische noch durch bekannte Quantenalgorithmen effizient gelöst werden können. In der aktuellen Forschung und Standardisierung haben sich dabei mehrere geeignete Problemfelder herauskristallisiert:

[9] IBM: International Business Machines Corporation

- **Gitterprobleme (Lattice-Based):** Verfahren wie CRYSTALS-Kyber[10] (Key Encapsulation Mechanism) oder CRYSTALS-Dilithium[11] (Signaturen) basieren auf der Schwierigkeit von Problemen wie „Learning With Errors“ (LWE) oder dem „Shortest Vector Problem“ (SVP). Diese gelten als besonders robust, da bislang kein effizienter Algorithmus bekannt ist, der sowohl klassisch als auch mit Quantenrechnern diese Gitterprobleme in praktikabler Zeit lösen könnte. Gleichzeitig bieten Lattice-basierte Verfahren meist ein ausgewogenes Verhältnis zwischen Sicherheit und Performance.
- **Code-basierte Verfahren:** Ein prominentes Beispiel ist der McEliece-Kryptoschlüssel[12], der seine Sicherheit aus der Schwierigkeit des Dekodierens zufälliger linearer Codes bezieht. Trotz meist sehr großer öffentlicher Schlüssel galt McEliece seit Jahrzehnten als sehr widerstandsfähig gegen alle bekannten Angriffe. Aktuelle Forschungsergebnisse stellen diese Einschätzung jedoch seit kurzem in Frage. Ein weiteres Beispiel für ein Code-basiertes Verfahren ist der HQC-Algorithmus[13], der von NIST auch bereits für eine weitere Standardisierung ausgewählt wurde.
- **Hash-basierte Signaturen:** Verfahren wie SPHINCS+[14] nutzen ausschließlich kryptographische Hashfunktionen zur Signaturerzeugung. Hashfunktionen gelten als fundamental robuste primitive Bausteine, wobei SPHINCS+ jedoch einen hohen Preis in Form sehr großer Signaturen zahlt. Dennoch bietet diese rein hashbasierte Sicherheit ein zusätzliches Maß an Vertrauen, da sich die Stabilität von Hashfunktionen bereits über lange Zeiträume in der Praxis bewährt hat.
- **Isogenien-basierte Verfahren:** Diese Algorithmen basieren auf komplexen Problemen, die in der Struktur bestimmter elliptischer Kurvenisogenien verankert sind. Isogenien-basierte Verfahren sind in der Regel jedoch deutlich rechenintensiver als gitter- oder code-basierte Alternativen. Einzelne Algorithmen aus dieser Klasse wurden auch bereits erfolgreich gebrochen[15].

2.4 Aktivitäten zur Standardisierung von PQC-Algorithmen

Die Bedeutung der Post-Quanten-Kryptographie führte dazu, dass internationale Gremien und Institutionen bereits vor einiger Zeit begannen, entsprechende Standards voranzutreiben. Das NIST[16] leitete 2016 einen umfangreichen Evaluierungs- und Auswahlprozess ein, um aus einer Vielzahl von Vorschlägen diejenigen Algorithmen zu identifizieren, die ein hohes Maß an Sicherheit, Effizienz und Umsetzbarkeit bieten. Mitte 2022 wurden mit CRYSTALS-Kyber (für Schlüsselvereinbarungen/Key

[10] https://pq-crystals.org/kyber/
[11] https://pq-crystals.org/dilithium/
[12] Robert J. McEliece: A Public-Key Cryptosystem Based on Algebraic Coding Theory. In: Deep Space Network Progress Report. Band 42, Nr. 44, 1978, S. 114–116
[13] Anthony Boucher, Slim El Heddi, Philippe Gaborit, Gilles Zémor: HQC: a Code-Based KEM. In IACR Cryptology ePrint Archive, 2017/360. Online verfügbar unter: https://eprint.iacr.org/2017/360
[14] https://sphincs.org/
[15] Wouter Castryck und Thomas Decru: An Efficient Key Recovery Attack on SIDH (Preliminary Version). In IACR Cryptology ePrint Archive, 2022/975. Online verfügbar unter: https://eprint.iacr.org/2022/975
[16] https://csrc.nist.gov/projects/post-quantum-cryptography

Encapsulation Mechanism), CRYSTALS-Dilithium, FALCON und SPHINCS+ (für Signaturen) erste Favoriten bekanntgegeben, die sich durch ihre unterschiedlichen Sicherheits- und Performanceprofile auszeichnen. Im August 2024 wurden vom NIST schließlich mit FIPS 203[17] („Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM)“), FIPS 204[18] („Module-Lattice-Based Digital Signature Standard (ML-DSA)“) und FIPS 205[19] („Stateless Hash-Based Digital Signature Standard (SLH-DSA)“) drei PQC-Algorithmen standardisiert, die auf den im folgenden Abschnitt beschriebenen Algorithmen CRYSTALS-Kyber (Grundlage für FIPS 203), CRYSTALS-Dilithium (Grundlage für FIPS 204) und SPHINCS+ (Grundlage für FIPS 205) basieren. Die finale Standardisierung von FIPS 206 („FFT (Fast-Fourier Transform) over NTRU-Lattice-Based Digital Signature Algorithm (FN-DSA)“) basierend auf dem Algorithmus FALCON wird für 2025 erwartet.

Parallel prüft NIST weitere Kandidaten („Round 4“), um langfristig eine vielseitige und belastbare Standardbasis bereitzustellen. Europäische und deutsche Institutionen wie die ETSI und das BSI werden auf diesen Ergebnissen aufbauen, um eigene Empfehlungen für den europäischen und nationalen Einsatz zu formulieren. So entsteht ein global koordiniertes Vorgehen, das frühzeitig die Weichen für eine künftige, quantenresistente Kryptolandschaft stellt.

3 PQC-Algorithmen

Dieser Abschnitt stellt einige aktuell relevante PQC-Algorithmen näher vor. Insbesondere werden die zugehörigen Schlüssellängen und Signaturgrößen im Detail diskutiert und gegenübergestellt, um so einen direkten Vergleich wichtiger Kerneigenschaften dieser Algorithmen zu ermöglichen.

3.1 Auswahl relevanter Algorithmen

Die Auswahl der in dieser Analyse betrachteten Post-Quanten-Kryptographie-Algorithmen wurde basierend auf dem NIST-Standardisierungsprozess und den über diesen Prozess ausgewählten und bereits standardisierten Algorithmen getroffen[20]. Dieser Prozess stellt die führende Grundlage für die Evaluierung und Auswahl von PQC-Algorithmen dar und gewährleistet, dass die betrachteten Verfahren den aktuellen wissenschaftlichen und technischen Standards entsprechen. Dementsprechend werden in den nachfolgenden Abschnitten dieses Dokuments die folgenden Algorithmen einbezogen:

- **CRYSTALS-Kyber:** CRYSTALS-Kyber[21] ist ein Schlüsselvereinbarungsalgorithmus, der auf Gitter-basierten mathematischen Problemen beruht. Er zeichnet sich durch hohe

[17] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.pdf
[18] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.pdf
[19] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.205.pdf
[20] Bereits ausgewählte aber zum Zeitpunkt der Dokumenterstellung (April 2025) noch nicht final standardisierte Algorithmen wie HQC werden nicht näher betrachtet.
[21] Bos, J. W., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., Schwabe, P., Seiler, G., & Stehlé, D. (2018). CRYSTALS – Kyber: A CCA-Secure Module-Lattice-Based KEM. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS), pp. 353–367. ACM.

Effizienz und geringe Schlüssellängen aus, was ihn besonders für Anwendungen mit begrenzten Ressourcen attraktiv macht. CRYSTALS-Kyber bietet zudem starke Sicherheitsgarantien gegen Quantencomputer und wurde im NIST-Standardisierungsprozess unter FIPS 203 und dem Namen „Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM)“ standardisiert.

- **CRYSTALS-Dilithium:** CRYSTALS-Dilithium[22] ist ein digitaler Signaturalgorithmus, der ebenfalls auf Gitter-basierten Problemen basiert. Der Algorithmus kombiniert Sicherheitsstärke mit Effizienz in der Berechnung und moderaten Signaturgrößen, was ihn ideal für Szenarien macht, in denen sowohl Sicherheit als auch Performanz entscheidend sind. CRYSTALS-Dilithium ist bekannt für seine einfache Struktur und starke theoretische Fundierung. Im Rahmen des NIST-Standardisierungsprozesses wurde dieser Algorithmus unter FIPS 204 und dem Namen „Module-Lattice-Based Digital Signature Standard (ML-DSA)“ standardisiert.
- **FALCON:** FALCON[23] ist ein weiterer digitaler Signaturalgorithmus, der auf Gitter-basierten Problemen aufbaut, allerdings mit einem Fokus auf besonders kleine Signaturgrößen und hohe Verifikationsgeschwindigkeiten. Diese Eigenschaften machen FALCON zu einer geeigneten Wahl für Anwendungen mit strikten Anforderungen an die Bandbreite und Speicherplatznutzung, wie sie häufig bei maschinenlesbaren Dokumenten auftreten. Im Rahmen des NIST-Standardisierungsprozesses wird dieser Algorithmus voraussichtlich 2025 unter FIPS 206 und dem Namen „FFT (Fast-Fourier Transform) over NTRU-Lattice-Based Digital Signature Algorithm (FN-DSA)“ standardisiert werden.
- **SPHINCS+:** SPHINCS+[24] ist ein hashbasierter digitaler Signaturalgorithmus, der ohne Annahmen über spezielle mathematische Probleme auskommt. Er bietet besonders robuste Sicherheitsgarantien, da seine Sicherheit ausschließlich auf gut verstandenen Hash-Funktionen beruht. Obwohl SPHINCS+ größere Signaturen erzeugt, bietet der Algorithmus eine einzigartige Resilienz gegen zukünftige kryptographische Angriffe, was ihn für hochkritische Anwendungen interessant macht. Im Rahmen des NIST-Standardisierungsprozesses wurde dieser Algorithmus unter FIPS 205 und dem Namen „Stateless Hash-Based Digital Signature Standard (SLH-DSA)“ standardisiert.

3.2 Schlüssellängen und Signaturgrößen

Für eine praktische Anwendung kryptographischer Algorithmen sind vor allem die für eine ausreichende Sicherheit notwendige Schlüssellänge und – bei Signaturalgorithmen – die Größe

[22] Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., & Stehlé, D. (2018). CRYSTALS – Dilithium: A Lattice-Based Digital Signature Scheme. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS), pp. 356–373. ACM.
[23] Fouque, P.-A., Hoffstein, J., Kirchner, P., Léo, Y., Nguyen, D. T., Persichetti, E., Prest, T., & Vergnaud, D. (2018). FALCON: Fast-Fourier Lattice-Based Compact Signatures Over NTRU. Submission to the NIST Post-Quantum Cryptography Standardization Project.
[24] Bernstein, D. J., Hülsing, A., Kölbl, S., Niederhagen, R., Rijneveld, J., & Schwabe, P. (2019). SPHINCS+: Submission to the NIST Post-Quantum Cryptography Standardization Project.

resultierender Signaturen relevante und ihre praktische Tauglichkeit beeinflussende Parameter. Dies gilt für klassische Algorithmen ebenso wie für PQC-Algorithmen. Dieser Abschnitt gibt einen Überblick über notwendige Schlüssellängen und Signaturgrößen relevanter PQC-Algorithmen und setzt diese in Relation zu jenen klassischer Algorithmen.

3.2.1 Empfehlungen zu Schlüssellängen

Im Allgemeinen empfiehlt es sich, sich bei der Wahl von Schlüssellängen an gängigen Empfehlungen renommierter Institutionen zu orientieren. Diese werden unter anderem von internationalen Organisationen wie der ENISA (European Union Agency for Cybersecurity)[25], dem BSI (Bundesamt für Sicherheit in der Informationstechnik)[26] und – speziell im Anwendungsbereich der eMRTD – der ICAO (International Civil Aviation Organization)[27] bereitgestellt. Diese Institutionen geben regelmäßig Empfehlungen zu Schlüssellängen und kryptographischen Parametern heraus, um ein angemessenes Sicherheitsniveau für verschiedene Anwendungsbereiche zu gewährleisten.

- **ENISA-Empfehlungen:** Die ENISA legt in ihren Berichten Empfehlungen[28] für die Mindestschlüssellängen basierend auf der erwarteten Lebensdauer der Daten fest. Für asymmetrische Verfahren wird beispielsweise RSA-3072 oder ECC-P256 für ein 128-Bit-Sicherheitsniveau empfohlen. Für langfristig kritische Daten oder Anwendungen, die ein höheres Sicherheitsniveau benötigen, sollten RSA-15360 oder ECC-P521 verwendet werden, um ein Sicherheitsniveau von 256 Bit zu gewährleisten.
- **BSI-Empfehlungen:** Das BSI stellt in der Technischen Richtlinie TR-02102[29] detaillierte Vorgaben zu kryptographischen Verfahren bereit. Für ein Sicherheitsniveau von 128 Bit werden ECC-Kurven wie P-256 und RSA-Schlüssellängen von 3000 bis 4000 Bit empfohlen. Für Anwendungen mit sehr hohen Sicherheitsanforderungen ist AES-256 für symmetrische Verschlüsselung und ECC-P521 für asymmetrische Anwendungen vorgesehen.
- **ICAO-Empfehlungen:** Die ICAO, die Standards für maschinenlesbare Reisedokumente (z.B. elektronische Reisepässe) setzt, empfiehlt den Einsatz von ECC-Kurven für die digitale Signatur und die Verschlüsselung, speziell P-256 oder P-384 für mittelfristige Sicherheit. Diese Algorithmen werden in internationalen Standards wie dem Extended Access Control (EAC) Framework genutzt.

Empfehlungen zu Schlüssellängen für die Verwendung von PQC-Algorithmen sind noch weniger verbreitet. Erste Richtwerte zu geeigneten Schlüssellängen finden sich unter anderem in den einschlägigen Vorgaben des BSI.

[25] https://www.enisa.europa.eu/
[26] https://www.bsi.bund.de/
[27] https://www.icao.int/
[28] https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014
[29] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.html

3.2.2 Empfohlene Schlüssellängen zur Erreichung definierter Sicherheitsniveaus

Empfohlene Schlüssellängen hängen neben dem Algorithmus selbst primär von dem zu erreichenden Sicherheitsniveau ab. Gängige Sicherheitsniveaus sind 128 Bit bzw. 256 Bit. Letzteres gewährleistet eine längerfristige Robustheit gegen Angriffe. Tabelle 1 zeigt empfohlene Schlüssellängen und Signatur-/Chiffratgrößen für kryptographische Algorithmen abhängig vom avisierten Sicherheitsniveau und identifiziert diesbezügliche Unterschiede zwischen klassischen und PQC-Algorithmen[30].

Algorithmus	Typ	Schlüssellänge des privaten Schlüssels [Bit]	Schlüssellänge des öffentlichen Schlüssels [Bit]	Signatur-/ Chiffratgröße [Bit]
Klassische Algorithmen – 128-Bit Sicherheitsniveau				
RSA-3072	Asymmetrische Verschlüsselung Klassisch	3.072	3.072	Variabel (mind. 3.072)
ECC-P256	Asymmetrische Verschlüsselung Klassisch	256	256	512
AES-128	Symmetrische Verschlüsselung Klassisch	128	N/A	N/A
Klassische Algorithmen – 256-Bit Sicherheitsniveau				
RSA-15360	Asymmetrische Verschlüsselung Klassisch	15.360	15.360	Variabel (mind. 15.360)
ECC-P521	Asymmetrische Verschlüsselung Klassisch	521	521	Variabel
AES-256	Symmetrische Verschlüsselung Klassisch	256	N/A	N/A
PQC-Algorithmen – 128-Bit Sicherheitsniveau				
ML-KEM-512 CRYSTALS-Kyber-512 FIPS-203	PQC-KEM[31]	13.056	6.400	6.144
ML-DSA-44 CRYSTALS-Dilithium FIPS 204	PQC-Signatur	20.480	10.496	19.360

[30] Mit „N/A“ gekennzeichnete Einträge sind nicht anwendbar/nicht relevant.
[31] KEM: Key Encapsulation Mechanism

FN-DSA-512 **FALCON-512** **FIPS-206**	PQC-Signatur[32]	10.240	7.176	5.328
SLH-DSA-*-128s **SPHINCS+-128s** **FIPS-205**	PQC-Signatur[33]	768	256	62.848

Tabelle 1. Schlüssellängen und Signatur-/Chiffratgrößen für kryptographische Algorithmen abhängig vom avisierten Sicherheitsniveau.

Tabelle 1 zeigt, dass sich in Bezug auf Schlüssellängen und Signatur-/Chiffratgrößen teils signifikante Unterschiede zwischen klassischen und PQC-Algorithmen ergeben. Die folgenden Abbildungen stellen diese Unterschiede auch graphisch dar.

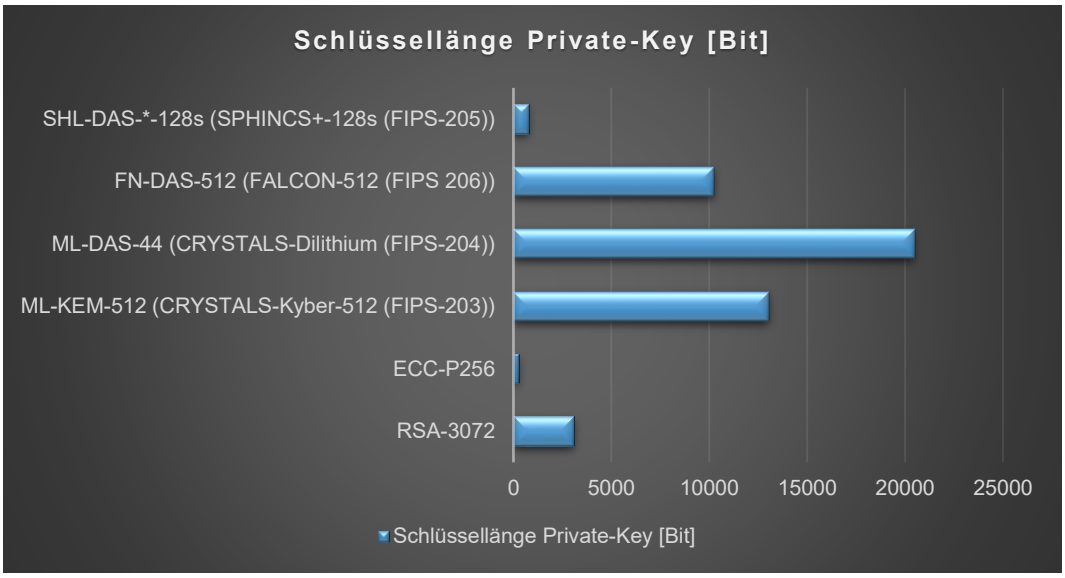

Abbildung 1. Vergleich der empfohlenen Schlüssellängen des Private-Keys für ein Sicherheitsniveau von 128 Bit.

[32] Die Schlüssellänge des privaten Schlüssels wird in der Regel mit 10.240 Bit (1280 Byte) angegeben. In der offiziellen Spezifikation findet sich jedoch keine explizite Angabe der Schlüssellänge.
[33] Die Schlüssellänge des privaten Schlüssels hängt davon ab, welche Komponenten in den privaten Schlüssel einbezogen werden. In der NIST-Spezifikation FIPS 205 besteht der private Schlüssel aus mehreren Bestandteilen (SK.seed, SK.prf, PK.seed). Daraus ergibt sich die in der Tabelle angeführte Gesamtlänge. Anderen Quellen betrachten nur den Bestandteil SK.seed als privaten Schlüssel, wodurch sich in der Literatur mitunter unterschiedliche Längenangaben finden.

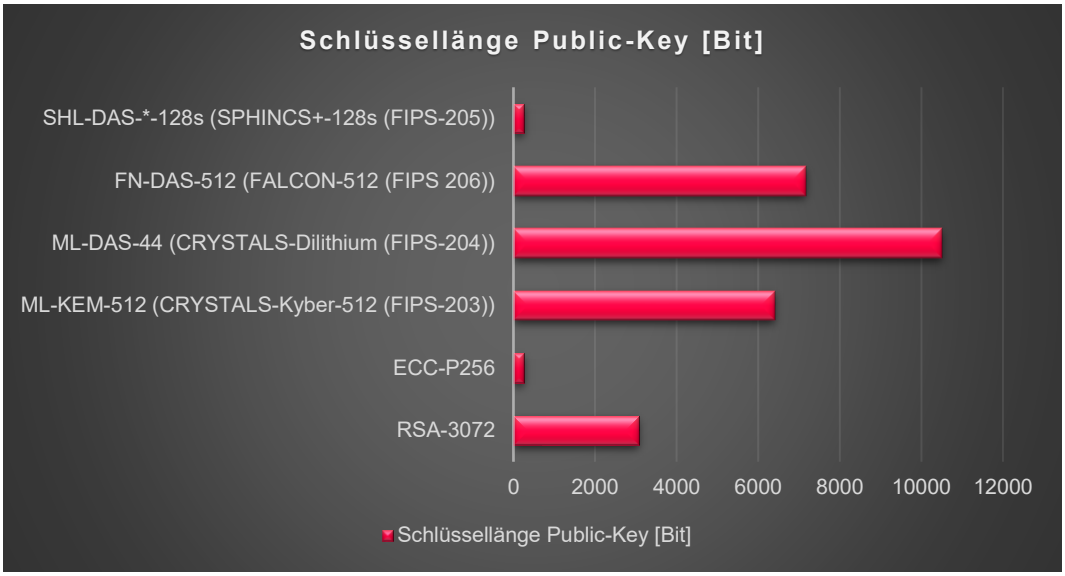

Abbildung 2. Vergleich der empfohlenen Schlüssellängen des Public-Keys für ein Sicherheitsniveau von 128 Bit.

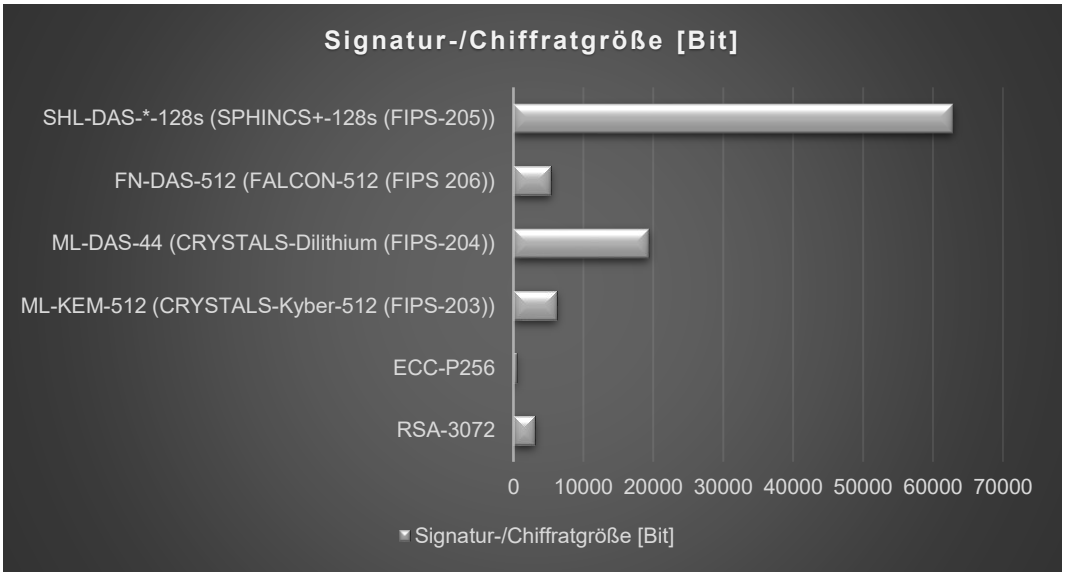

Abbildung 3. Vergleich der resultierenden Signatur-/Chiffratgrößen für ein Sicherheitsniveau von 128 Bit.

Die Größe resultierender Signaturen/Chiffrate kann insbesondere dann eine technische Herausforderung sein, wenn diese aufgrund applikationsspezifischer Anforderungen in QR-Codes kodiert werden müssen. Beispielsweise führen größere Signaturen hier unmittelbar zu größeren QR-Codes, was je nach Anwendungsfall praktische Probleme aufwerfen kann, z.B. dann, wenn diese QR-Codes

ausgedruckt oder auf mobilen Geräten mit eingeschränkten Bildschirmgrößen dargestellt werden müssen[34].

Herausforderungen in Bezug auf große Schlüssellängen und ausufernde Signaturgrößen sind jedoch nicht auf die Verwendung von QR-Codes beschränkt. Auch andere Technologien (Chipkarten, RFID-Chips, etc.) können dadurch vor praktische Probleme gestellt werden. Dies vor allem auch dann, wenn mit größeren Schlüssellängen und Signaturgrößen auch eine langsamere Verarbeitung einhergeht. In Anwendungsfällen, in denen Performanz von Bedeutung ist (z.B. Grenzkontrolle auf Flughäfen), kann dies negative praktische Auswirkungen haben.

3.3 Schlussfolgerungen

In Bezug auf Schlüssellängen und Signaturgrößen können für die betrachteten klassischen und PQC-Algorithmen folgende erste Schlussfolgerungen gezogen werden. Für häufig zum Einsatz kommende klassische Algorithmen stellt sich die Situation wie folgt dar:

- **RSA** benötigt für höhere Sicherheitsstufen stark steigende Schlüssellängen, was die Praktikabilität bei 256-Bit Sicherheitsniveau stark einschränkt.
- **ECC** bietet bei kleineren Schlüssellängen ein vergleichbares Sicherheitsniveau und bleibt auch für 256-Bit Sicherheitsanforderungen effizient.
- **AES** ist für symmetrische Verschlüsselung weiterhin ein robuster Standard. Für 256-Bit Sicherheit ist lediglich eine entsprechende Erhöhung der Schlüssellänge erforderlich.

Dem gegenüber kann die Situation für aktuell relevante PQC-Algorithmen wie folgt zusammengefasst werden:

- **ML-KEM** (CRYSTALS-Kyber) nach FIPS 203 ist ein KEM (Key Encapsulation Mechanism), daher wird durch diesen Algorithmus keine Signatur generiert. Der Algorithmus bietet eine effiziente Schlüsselvereinbarung, der resultierende Schlüssel ist aber deutlich größer als bei klassischen Verfahren.
- **ML-DSA** (CRYSTALS-Dilithium) nach FIPS 204 und **FN-DSA** (FALCON) nach FIPS 206 sind Signaturlösungen mit einem Kompromiss zwischen Schlüssellänge und Signaturgröße. FN-DSA hat kleinere Signaturen, ist jedoch rechenintensiver.
- **SHL-DSA** (SPHINCS+) nach FIPS 205 setzt vollständig auf Hash-basierte Sicherheit und erzeugt die größten Signaturen, gilt aber als besonders sicher.

[34] Als plakatives Beispiel kann hier die, während der COVID19-Pandemie breit verwendete Grüner-Pass-App dienen, die ebenfalls stark auf der Verwendung von QR-Codes beruhte. In diesen QR-Codes kodierte Daten durften aus praktischen Gründen eine Größe von ca. 1.500 Byte nicht übersteigen, um auf mobilen Geräten und Ausdrucken noch vernünftig dargestellt und verarbeitet werden zu können. Wollte man z.B. eine ML-DSA-Signatur (Signatur, öffentlicher Schlüssel, etc.) in einem QR-Code kodieren, bräuchte man dafür mehr als 10 QR-Codes der Größe, wie sie die Grüner-Pass-App verwendete.

4 Betroffene Bereiche von IT-Lösungen

Die bevorstehende Ära der Quantencomputer wirft nicht nur grundlegende Fragen zur Sicherheit klassischer kryptographischer Verfahren auf, sondern hat auch weitreichende Auswirkungen auf IT-Infrastrukturen und darauf aufbauende IT-Lösungen, für die Kryptographie ein essenzieller Baustein ist. Ob sichere Kommunikation im Internet, digitales Bezahlen, Zugriffskontrollsysteme oder Machine-2-Machine-Kommunikation: Klassische asymmetrische Kryptosysteme wie RSA oder ECC sind integraler Bestandteil diverser aktuell im Einsatz befindlicher Protokolle und Lösungen. Vor dem Hintergrund der bevorstehenden Ära der Quantencomputer müssen nahezu alle Bereiche, in denen Verschlüsselung, digitale Signaturen oder Authentifizierung eingesetzt werden, langfristig überdacht und angepasst werden – von Web-Protokollen über Hardwarekomponenten bis hin zu komplexen Zertifizierungsprozessen.

Dieser Abschnitt betrachtet das Thema Post-Quanten-Kryptographie auf einer höheren Abstraktionsebene und zeigt auf, welche Bereiche und Komponenten aktueller IT-Lösungen von einer Migration von klassischer auf Post-Quanten-Kryptographie prinzipiell betroffen wären. Eine vollständige Betrachtung würde den Rahmen dieses Dokuments sprengen. Es soll vielmehr verdeutlicht werden, dass eine Migration auf Post-Quanten-Kryptographie weitreichende Auswirkungen haben kann, die weit über eine reine Anpassung einzelner Softwarekomponenten hinausgeht. Insbesondere müssen folgende Bereiche einer IT-Lösung durch eine geeignete Migrationsstrategie berücksichtigt werden:

- **Software-Implementierungen:** Bestehende Applikationen, Protokoll-Stacks, Libraries und Firmware müssen aktualisiert werden. Hierbei geht es nicht nur um das Ersetzen von klassischen Algorithmen wie z.B. RSA oder ECC durch PQC-Algorithmen wie ML-DSA. Es müssen auch neue API[35]-Standards definiert und Software-Entwickler:innen in der korrekten Verwendung von PQC-Algorithmen geschult werden.
- **Hardware Security Modules (HSM) und Chipkarten:** Spezialisierte Hardware, die zur Schlüsselgenerierung, -speicherung und -verwendung genutzt wird, ist aktuell oft eng auf klassische Algorithmen zugeschnitten. Die Integration von PQC-Algorithmen erfordert neue Hardware-Designs, größere Speicherkapazitäten und angepasste Sicherheitszertifizierungen. HSMs und Smartcards (z.B. Bank-Karten, SIM[36]-Karten, elektronische Identitätskarten (eID-Karten), etc.) müssen dann größere Schlüssel oder Signaturen verarbeiten können (siehe Abschnitt 3.2.2 zu empfohlenen Schlüssellängen). Das kann Auswirkungen auf Lese- und Schreibgeschwindigkeit, Stromverbrauch und Chipflächenbedarf haben. In jedem Fall ist ein Tausch aktuell im Feld befindlicher Hardware notwendig.
- **Zertifizierungsmaßnahmen:** Sowohl Software als auch Hardware müssen nach neuen Kriterien zertifiziert werden. Nationale und internationale Behörden und Gremien wie BSI, NIST oder ENISA müssen Prüfverfahren anpassen, um die Sicherheit von PQC-

[35] API: Application Programming Interface
[36] SIM: Subscriber Identification Module

Implementierungen sicherzustellen. Dazu gehören Testverfahren für die korrekte Implementierung, Resistenz gegen physikalische Angriffe (Side-Channel-Attacken) sowie der Nachweis, dass die eingesetzten PQC-Verfahren tatsächlich die angestrebte Sicherheit bieten.

- **Interoperabilitätstests:** Interoperabilitätstests sind bei der Migration auf Post-Quanten-Kryptographie insbesondere in großen verteilten Systemen von entscheidender Bedeutung. Dies vor allem dann, wenn verschiedene Parteien unabhängig voneinander PQC-fähige Komponenten als Teil dieser Systeme entwickeln oder implementieren. Ziel ist es sicherzustellen, dass diese Komponenten miteinander kompatibel sind und nahtlos zusammenarbeiten können. Dies betrifft in Zukunft beispielsweise auch PQC-fähige Reisepässe: Diese werden, wie aktuelle Reisepässe auch, von unterschiedlichen Staaten ausgestellt, müssen bei Grenzkontrollsystemen jedoch weltweit fehlerfrei gelesen und validiert werden können. Ohne gründliche Interoperabilitätstests könnte es zu Problemen wie Inkompatibilitäten bei Schlüsselformaten, Protokollvarianten oder kryptografischen Parametern kommen, was die Funktionalität des Gesamtsystems gefährden würde.

Diese erste rudimentäre Liste von Bereichen und Aspekten, die bei einer Migration auf Post-Quanten-Kryptographie berücksichtigt werden müssen, macht deutlich, dass eine solche Migration kein rein technisches Unterfangen ist und nicht nur von der Verfügbarkeit entsprechender von der Industrie bereitgestellter PQC-fähiger Produkte abhängt. Notwendige technische Umstellungen müssen ergänzt und begleitet werden durch diverse organisatorische Maßnahmen und Tätigkeiten (Zertifizierungen, Bereitstellung entsprechend geschulten Personals, etc.). Diese notwendigen Maßnahmen und Tätigkeiten erhöhen sowohl Aufwand als auch Durchlaufzeit einer geplanten Migration. In Bezug auf Durchlaufzeit sind auch Abhängigkeiten zu externen Entitäten zu beachten. Dies betrifft insbesondere Abhängigkeiten im Zusammenhang mit der Zertifizierungen von Produkten. Dabei ist zu beachten, dass entsprechende Zertifizierungen einerseits vollständig und erfolgreich durchgeführt werden müssen, darüber hinaus aber auch die dafür notwendigen Voraussetzungen gegeben sein müssen. Insbesondere müssen geeignete Prüfinstitute verfügbar sein.

5 Herausforderungen einer PQC-Migration

Im vorherigen Abschnitt wurde bereits verdeutlicht, dass eine Migration auf Post-Quanten-Kryptographie ein umfangreiches Unterfangen ist, das weit über die Ersetzung einzelner kryptographischer Algorithmen hinausgeht. Ausgehend von dieser Erkenntnis beschreibt dieser Abschnitt weitere Details zu ausgewählten Aspekten, die bei einer Migration beachtet werden müssen, und identifiziert konkrete diesbezügliche Herausforderungen.

5.1 Anpassung existierender Standards und Protokolle

In Bezug auf die notwendige Anpassung existierender Standards und Protokolle müssen u.a. folgende Herausforderungen gemeistert werden:

- **Weiterentwicklung bestehender Standards:** Viele etablierte Standards (z.B. TLS für den sicheren Datentransport im Web oder IKE[37] im VPN[38]-Kontext) sind bislang eng mit bestimmten klassischen Schlüssel- und Signaturalgorithmen verknüpft. Bei TLS wurden in der Vergangenheit z.B. Cipher Suites explizit auf RSA, ECDHE[39] oder ECDSA[40] abgestimmt. Diese Standards müssen nun erweitert werden, um PQC-KEMs und PQC-Signaturen zu unterstützen.
- **Neuerstellung von Standards:** Einige Spezifikationen sind stark auf ein bestimmtes Verfahren fokussiert. Wenn diese Algorithmen nicht einfach durch PQC-Varianten ausgetauscht werden können, sind teilweise vollkommen neue Standards erforderlich. Dies kann bedeuten, dass bestimmte Sicherheitsprotokolle, die aus historischen Gründen auf ECC beruhen, komplett neu konzipiert werden müssen, um PQC-Verfahren effizient einzubinden.

5.2 Herausforderungen in Bezug auf Schlüssellängen und Signaturgrößen

Wie in Abschnitt 3 beschrieben, haben PQC-Algorithmen häufig deutlich größere private und öffentliche Schlüssel und Signaturen/Chiffrate als klassische Verfahren. Dies beeinflusst verschiedene Bereiche und führt in diesen u.a. zu folgenden Herausforderungen:

- **Performance und Bandbreite:** Längere Schlüssel und größere Signaturen bedeuten mehr Daten, die übertragen, gespeichert und verarbeitet werden müssen. Das führt zu längeren Ladezeiten, höherem Bandbreitenverbrauch und möglicherweise spürbaren Performanceeinbußen, insbesondere auf ressourcenschwachen Geräten.
- **NFC-/Chipkarten-Kommunikation:** Auf Smartcards, NFC-Tags oder NFC/RFID-Chipkarten, die nur sehr begrenzte Speicher- und Rechenkapazitäten haben, kann die Implementierung von PQC-Verfahren problematisch werden. Die Lesezeit von Karten, die an Lesegeräten etwa an Zutrittskontrollen, Grenzkontrollen (z.B. bei Reisepässen) oder im öffentlichen Personennahverkehr (ÖPNV) – etwa bei NFC-Tickets – genutzt werden, könnte ansteigen. Neue Kompromisse zwischen Sicherheit, Verarbeitungsdauer und Komfort müssen gefunden werden.

[37] IKE: Internet Key Exchange
[38] VPN: Virtual Private Network
[39] ECDHE: Elliptic Curve Diffie-Hellman Ephemeral
[40] ECDSA: Elliptic Curve Digital Signature Algorithm

- **Visuelle Datenträger wie QR-Codes:** Bekannte Verfahren wie z.B. der „Grüne Pass“ (digitale COVID19-Zertifikate) oder Personalausweise mit QR-Codes, deren Signaturen auf kleinen ECC-Schlüsseln beruhen, stoßen an Kapazitätsgrenzen. Mit deutlich größeren PQC-Signaturen passt die gesamte Information möglicherweise nicht mehr in einen einzigen QR-Code. Alternativen wie das Aufteilen der zu kodierenden Information auf mehrere QR-Codes, Kompression oder Verweise auf externe Datenquellen sind denkbar, bringen jedoch neue Risiken mit sich. Beispielsweise könnte die externe Speicherung von Signaturinformationen Privacy-Bedenken aufwerfen, da Verweis- und Abrufmechanismen theoretisch Rückschlüsse auf Benutzerverhalten und Bewegungsmuster zulassen.

5.3 Herausforderungen in der Infrastruktur und Protokollunterstützung

PQC-Algorithmen müssen auf allen Ebenen der IT-Infrastruktur unterstützt werden. So müssen auch Betriebssysteme, Browser, Mobilgeräte oder Anwendungsbibliotheken entsprechend kompatibel sein. Dies erfordert folgende Maßnahmen bzw. führt zu den folgenden Herausforderungen (beispielhafte, nicht taxative Aufzählung):

- **Bereitstellung auf Plattformebene:** Betriebssysteme brauchen aktualisierte Kryptographie-Bibliotheken. Browser müssen neue Cipher-Suites in TLS unterstützen. Mobilgeräte (Smartphones, Tablets) benötigen Firmware-Updates, um neue Zertifikatstypen verarbeiten zu können.
- **Interoperabilität:** Verschiedene Anbieter und Ökosysteme müssen zusammenarbeiten, um sicherzustellen, dass z.B. ein auf PQC angehobener Webserver auch von aktuellen, aber noch nicht aktualisierten Clients erreicht werden kann. Es ergibt sich ein Bedarf an Hybrid-Ansätzen, bei denen klassische und PQC-Verfahren parallel unterstützt werden.
- **Metadaten und Protokollerweiterungen:** Sämtliche Metadaten, Protokoll-Header und Zertifikatsformate müssen angepasst oder erweitert werden, um die größeren Schlüssel und Signaturen handhaben zu können. Standardisierungsgremien stehen vor der Aufgabe, diese Änderungen international abzustimmen.

5.4 Schlussfolgerungen

Die bereits in Abschnitt 4 erhaltenen Erkenntnisse werden durch eine detailliertere Betrachtung einzelner Themenfelder untermauert: Die Umstellung auf Post-Quanten-Kryptographie ist weitaus mehr als ein reines Austauschen eines Algorithmus. Sie betrifft ein komplexes Ökosystem aus Hardware, Software, Protokollen, Zertifizierungsregeln, Standards und Benutzerumgebungen. Größere Schlüssel, komplexere Signaturen, geänderte Anforderungen an Speicher, Bandbreite und Rechenleistung treffen auf eine enorm diverse IT-Landschaft mit bestehenden Prozessen, zertifizierten HSMs, Millionen bereits verteilter Smartcards und zahlreichen Standards, die teils eng mit bestimmten

kryptographischen Primitiven verknüpft sind. Die Anpassung wird Zeit, Ressourcen und internationale Zusammenarbeit erfordern, um auch in der Post-Quanten-Ära die Vertraulichkeit, Integrität und Verfügbarkeit digitaler Systeme gewährleisten zu können.

6 Use-Case: Electronic Machine Readable Travel Documents (eMRTD)

Die bisherigen Betrachtungen in diesem Dokument erfolgten weitgehend generisch und unabhängig von konkreten Anwendungsfällen oder Use-Cases. Dadurch wurde eine solide Grundlage geschaffen, die allgemeine Prinzipien, Ansätze und Erkenntnisse aufzeigt. Im folgenden Abschnitt soll der Fokus auf den spezifischen Use-Case "Electronic Machine Readable Travel Documents" (eMRTD) gelegt werden. Dieser Use-Case birgt besondere Herausforderungen, die aus den spezifischen Anforderungen und Bedingungen elektronischer maschinenlesbarer Dokumente resultieren. Ziel dieses Abschnitts ist es, diese Herausforderungen klar zu benennen und ein besseres Verständnis für die damit verbundenen technischen und konzeptionellen Fragestellungen zu schaffen.

Ein spezieller Schwerpunkt wird auf die von österreichischen Behörden ausgegebenen elektronischen Dokumente wie Reisepässe, Personalausweise oder Aufenthaltstitel gelegt. Für diese ergibt sich die spezielle Herausforderung, dass diese ausgegebenen elektronischen Dokumente eine Gültigkeit von bis zu 10 Jahren haben können und einmal ausgegebene elektronische Dokumente im Feld nicht mehr mit Sicherheitsupdates versorgt werden können. Im Kontext der Post-Quanten-Kryptographie bedeutet dies, dass entsprechende Maßnahmen wie die Verwendung kryptographischer Post-Quanten-Algorithmen, die in 10 Jahren absehbar notwendig sein werden, bereits jetzt in neu ausgegebenen elektronische Dokumenten berücksichtigt sein müssten.

6.1 Relevante Normen und Standards

Technische Lösungen im Bereich der eMRTD basieren auf den entsprechenden Normen und Standards. Die relevante Standardisierungsorganisation ist dabei die ICAO (International Civil Aviation Organization). Diese definiert die Standards für elektronische maschinenlesbare Reisedokumente (eMRTD) wie elektronische Reisepässe, Personalausweise, Aufenthaltstitel oder andere Identitätsnachweise. Diese Standards gewährleisten weltweit eine einheitliche Interoperabilität und Sicherheit, sowohl bei der maschinellen Verarbeitung der Daten als auch bei ihrer kryptographischen Absicherung. Die wichtigsten technischen Standards und Protokolle für ICAO-konforme Dokumente sind im ICAO Doc 9303[41] festgelegt.

[41] https://www.icao.int/publications/pages/publication.aspx?docnum=9303

6.2 Technologische Grundlagen und Sicherheitsmechanismen

Die Sicherheit elektronischer maschinenlesbarer Reisedokumente (eMRTD) beruht in der Regel auf zwei Komponenten:

- **Physische Sicherheit:** Dazu gehört die Verwendung sicherer Materialien, Hologramme und anderer Sicherheitsmerkmale auf dem Dokument.
- **Elektronische Sicherheit:** Dies betrifft den eingebetteten Chip (RFID), der die auf dem Dokument ersichtlichen Daten (außer Unterschrift und Körpergröße), einschließlich Bilder von Fingerabdrücken, und kryptographische Signaturen enthält.

Eine Migration auf Post-Quanten-Kryptographie würde sich primär auf die elektronische Sicherheit von eMRTDs auswirken. Diese soll daher im Folgenden näher betrachtet werden.

Bereits heute werden für die elektronische Sicherheit elektronischer maschinenlesbarer Dokumente mehrere kryptographische Verfahren genutzt:

- **Passive Authentication (PA):** Verwendet digitale Signaturen, um sicherzustellen, dass die auf dem Chip gespeicherten Daten nicht manipuliert wurden. RSA-2048 oder ECC-P256 sind hier die am häufigsten zum Einsatz kommenden Algorithmen.
- **Active Authentication (AA):** Ergänzt PA durch eine Challenge-Response-Authentifizierung, um sicherzustellen, dass der Chip nicht geklont wurde. ECC-basierte Verfahren wie P-256 sind üblich.
- **Chip Authentication (CA):** Ersetzt zunehmend Active Authentication und nutzt Elliptic Curve Diffie-Hellman (ECDH) für die Schlüsselvereinbarung.
- **Extended Access Control (EAC):** Wird bei hochsensiblen Daten (z.B. Fingerabdrücke) verwendet und basiert auf einer Kombination von Schlüsselvereinbarungen und Zertifikaten, häufig mit RSA oder ECC.
- **Basic Access Control (BAC):** Dient dem Schutz von drahtloser Kommunikation und basiert auf Triple Data Encryption Standard (3DES) und AES. Wird jedoch zunehmen durch PACE ersetzt.
- **Password Authenticated Connection Establishment (PACE):** Ersetzt zunehmend BAC und beruht auf ECC bzw. AES.

Aus dieser Auflistung wird ersichtlich, dass die elektronische Sicherheit von eMRTDs aktuell sehr stark von klassischen kryptographischen Algorithmen (RSA, ECC, AES, etc.) abhängt. Tabelle 2 fasst dies nochmal zusammen.

Kryptographisches Verfahren	Funktion	Verwendete Kryptographie	Bemerkungen
Passive Authentication (PA)	Validierung, dass die Daten auf dem Chip nicht verändert wurden	RSA-2048, ECC-P256	Signaturen müssen klein sein und schnell geprüft werden können
Active Authentication (AA)	Schutz gegen Klonen des Chips	ECC-P256	Challenge-Response, zunehmend ersetzt durch CA
Chip Authentication (CA)	Sicherstellung der Chip-Authentizität	ECDH mit ECC-P256	Effizienter und sicherer als AA
Extended Access Control (EAC)	Schutz des Zugriffs auf sensible Daten (z.B. Fingerabdrücke)	RSA-2048, ECC-P256	Starke Kryptographie für Schlüsselvereinbarung und Signaturen
Basic Access Control (BAC)	Schutz der drahtlosen Kommunikation	3DES, AES-128	Zunehmend ersetzt durch PACE
Password Authenticated Connection Establishment (PACE)	Sicherer Zugang zum Chip und Schutz der Daten	ECC-P256, AES-128	Moderne Alternative zu BAC

Tabelle 2. Überblick der bei eMRTDs zum Einsatz kommenden kryptographischen Verfahren.

6.3 Allgemeine Herausforderungen einer PQC-Migration

Aufgrund des aktuell weitverbreiteten und hohen Einsatzes von klassischen kryptographischen Algorithmen ist eine künftige Migration auf Post-Quanten-Kryptographie auch für eMRTDs unumgänglich. Dabei ergeben sich prinzipiell dieselben allgemeinen Herausforderungen, die bereits in Abschnitt 5 diskutiert wurden.

Für eMRTDs existieren aber noch zusätzliche Use-Case-spezifische Herausforderungen, die sich aus den Besonderheiten des gegebenen Anwendungsfalls ergeben. Dazu zählen die folgenden Aspekte:

- **Größere Schlüssel und Signaturen bei PQC:** Viele ICAO-Protokolle sind auf Effizienz und kleine Schlüsselgrößen von RSA und ECC optimiert. Die Integration von PQC-Algorithmen mit potenziell größeren Schlüssellängen und Signaturen erfordert Anpassungen bei der Chip-Hardware, der Datenübertragung und den Lesegeräten.

- **Abwärtskompatibilität:** Weltweit existieren Milliarden von eMRTDs, die mit bestehenden Standards kompatibel bleiben müssen, auch wenn PQC in neuen Dokumenten eingeführt wird.
- **Speicher- und Bandbreitenlimits:** Die Größe von PQC-Schlüsseln und Signaturen könnte zu Problemen bei der NFC-Kommunikation und der Datenspeicherung in Chips führen.

Aufgrund dieser Herausforderungen wird die Migration zu PQC eine langfristige, international koordinierte Aufgabe sein müssen, bei der Abwärtskompatibilität und Effizienz entscheidend bleiben.

6.4 Detailbetrachtung anhand eines hypothetischen eMRTD-Lifecycles

Der vorangegangene Abschnitt zeigte, dass für eMRTDs im Zuge einer Migration zu PQC neben den bekannten allgemeinen Herausforderungen auch spezifische Hürden genommen werden müssen. Um diese Hürden greifbarer zu machen, werden im Folgenden relevante Schritte innerhalb eines hypothetischen und vereinfachten Lebenszyklus eines eMRTD dargestellt. Für jeden Schritt werden relevante technische Komponenten und Standards identifiziert und es wird eine Abschätzung gegeben, wie sich eine PQC-Migration auf den jeweiligen Schritt auswirken würde. Die einzelnen betrachteten Schritte werden über die nachfolgenden Unterabschnitte repräsentiert.

6.4.1 Erstellung der Daten

In diesem Schritt, der Teil des Ausstellungprozesses eines eMRTD ist, werden die persönlichen Daten des eMRTD-Inhabers (z.B. Name, Geburtsdatum, Passnummer) sowie biometrische Daten (z.B. Gesicht, Fingerabdrücke) gesammelt und digitalisiert.

Involvierte Komponenten und relevante Standards:

- **Datenerfassungssysteme:** Kameras, Fingerabdruckscanner, Formulareingabesysteme
- **Datenformate:** ICAO Logical Data Structure (LDS) für die standardisierte Speicherung der Daten
- **Klassische Algorithmen:** Keine direkte kryptographische Anwendung in der Erfassungsphase

Erwartbare Auswirkungen bei einer Migration auf Post-Quanten-Kryptographie:

Die Struktur der LDS muss angepasst werden, um größere Schlüssellängen und Signaturgrößen zu berücksichtigen, da PQC-Signaturen mehr Speicherplatz benötigen.

6.4.2 Aufbereitung der Daten

In diesem Schritt werden die gesammelten Daten in ein standardisiertes Format überführt, um später kryptographisch signiert zu werden. Auch dieser Schritt ist Teil des Ausstellungsprozesses.

Involvierte Komponenten und relevante Standards:

- **Middleware:** Software zur Integration der verschiedenen Dateneingabesysteme
- **Datenformate:** LDS 2.0 oder zukünftige PQC-kompatible Erweiterungen
- **Klassische Algorithmen:** Noch keine direkten kryptographischen Schritte in dieser Phase

Erwartbare Auswirkungen bei einer Migration auf Post-Quanten-Kryptographie:

Middleware und Datenformate müssen auf PQC-Schlüssellängen und Signaturgrößen abgestimmt werden, um eine reibungslose Verarbeitung zu ermöglichen.

6.4.3 Einsatz der Public Key Infrastructure (PKI)

Hierbei handelt es sich um einen zentralen und wichtigen Schritt, über den die gesammelten Daten durch eine Zertifizierungsstelle signiert werden, um Integrität und Authentizität dieser Daten sicherzustellen.

Involvierte Komponenten und relevante Standards:

- **PKI-Software:** Managementsysteme für Zertifikate und Schlüssel (z.B. OpenSSL, EJBCA[42])
- **Standards:**
  - X.509 für Zertifikate
  - ICAO Public Key Directory (PKD) für den internationalen Austausch von Zertifikaten
- **Klassische Algorithmen:**
  - RSA (2048 oder 3072 Bit) für Signaturen
  - ECC-P256 für effizientere Signaturen und Schlüsselvereinbarungen

Erwartbare Auswirkungen bei einer Migration auf Post-Quanten-Kryptographie:

PKI-Systeme müssen aktualisiert werden, um PQC-Algorithmen wie ML-DSA (CRYSTALS-Dilithium) oder SLH-DSA (SPHINCS+) für Signaturen zu unterstützen. Die X.509-Zertifikate müssen größer werden, um die neuen PQC-Schlüssel und Signaturen aufzunehmen.

[42] EJBCA: Enterprise JavaBeans Certificate Authority

6.4.4 Aufbringen der Daten auf den Chip

In diesem Schritt, der auch Teil des Ausstellungsprozesses ist, werden die signierten Daten auf den Chip des eMRTD geschrieben.

Involvierte Komponenten und relevante Standards:

- **Protokolle:** Passive Authentication (PA) und Extended Access Control (EAC) für Authentifizierung und Zugriffskontrolle
- **Klassische Algorithmen:**
  - RSA-2048 oder ECC-P256 für die Signaturprüfung
  - ECDH[43] für Schlüsselvereinbarung bei EAC

Erwartbare Auswirkungen bei einer Migration auf Post-Quanten-Kryptographie:

Die Schreibprozesse auf den Chip müssen angepasst werden, um die größeren Signaturen und Schlüssellängen von PQC-Algorithmen zu unterstützen. NFC-Kommunikation könnte durch die höheren Datenvolumina langsamer werden, was neue Protokolloptimierungen erfordert.

6.4.5 Verwendung von Hardware Security Modules (HSMs)

HSMs erzeugen, speichern und verwalten kryptographische Schlüssel und führen die mit diesen Schlüsseln verbundenen Operationen sicher aus. Bei der Verwendung eines HSM handelt es sich nicht um einen eigenen abgegrenzten Schritt, eine solche kann vielmehr Bestandteil anderer Schritte sein. Aufgrund der für eMRTDs zentralen Wichtigkeit von HSMs soll deren Verwendung hier jedoch explizit betrachtet werden.

Involvierte Komponenten und relevante Standards:

- **Hardware:** Zertifizierte HSMs (z.B. zertifiziert nach FIPS 140-2/3).
- **Klassische Algorithmen:**
  - RSA-2048 oder ECC-P256 zur Schlüsselsignierung und -verwaltung.

Erwartbare Auswirkungen bei einer Migration auf Post-Quanten-Kryptographie:

HSMs müssen aktualisiert oder durch neue Modelle ersetzt werden, die PQC-Algorithmen unterstützen. Dies betrifft nicht nur die Software, sondern auch die physische Architektur, da größere Schlüssel und Signaturen mehr Speicherplatz und Rechenleistung benötigen.

6.4.6 Sicherung der Übertragungsprotokolle

Die Kommunikation zwischen den Systemen erfolgt über sichere Protokolle wie TLS, um die Integrität und Vertraulichkeit der übertragenen Daten zu gewährleisten. Auch hier handelt es sich streng

[43] ECDH: Elliptic Curve Diffie-Hellman

genommen nicht um einen eigenständigen Schritt, sondern um einen wichtigen Teilaspekt anderer Schritte.

Involvierte Komponenten und relevante Standards:

- **Standards:** TLS 1.2 oder TLS 1.3
- **Klassische Algorithmen:**
  - RSA oder ECDHE für den Schlüsselaustausch
  - AES für symmetrische Verschlüsselung

Erwartbare Auswirkungen bei einer Migration auf Post-Quanten-Kryptographie:

TLS muss für hybride Schlüsselvereinbarungen angepasst werden, die klassische und PQC-Algorithmen kombinieren. Die Erweiterung der Cipher Suites um PQC-KEMs wie ML-KEM (CRYSTALS-Kyber) ist erforderlich.

6.4.7 Applikationen zur Verwaltung und Überprüfung der eMRTDs

Die ausgestellten eMRTDs werden von Grenzkontrollsystemen, Behörden und Applikationen überprüft. Dieser Schritt repräsentiert also die Verwendung eines eMRTDs durch dessen Inhaber.

Involvierte Komponenten und relevante Standards:

- **Software:** Grenzkontrollsysteme, Chipkartenleser
- **Protokolle:** PA, CA, EAC, PACE
- **Klassische Algorithmen:**
  - RSA-2048, ECC-P256 für Authentifizierung und Signaturprüfung

Erwartbare Auswirkungen bei einer Migration auf Post-Quanten-Kryptographie:

Applikationen und Lesegeräte müssen aktualisiert werden, um PQC-Signaturen validieren zu können. Die Chipkartenleser müssen zudem die mit PQC-Algorithmen einhergehenden größeren Schlüssel und Signaturen effizient verarbeiten können.

7 Mitigationsmaßnahmen

Die bisher in dieser Analyse angestellten Betrachtungen und insbesondere die in Abschnitt 6 vorgenommene Detailbetrachtung des Use-Cases der Electronic Machine Readable Travel Documents (eMRTD) zeigen, dass eine künftige Migration auf PQC einerseits unumgänglich ist, andererseits jedoch aus diversen Gründen unmittelbar noch nicht in Angriff genommen werden kann. Daraus stellt sich unmittelbar die Frage, welche Aktionen bereits jetzt gesetzt werden können, um eine spätere Migration (zu einem Zeitpunkt, an dem alle dafür notwendigen Rahmenbedingungen gegeben sind)

möglichst effektiv und effizient vornehmen zu können bzw. welche Mitigationsmaßnahmen bereits jetzt umgesetzt werden könnten. Solche Maßnahmen und Aktionen werden in diesem Abschnitt näher beschrieben.

Grundsätzlich kann zwischen technischen und organisatorischen Mitigationsmaßnahmen unterschieden werden. Erstere umfassen unter anderem die Auswahl geeigneter PQC-Algorithmen, deren Umsetzung und Integration in bestehende Lösungen oder auch die Einführung der resultierenden post-quanten-resistenten Lösungen im operativen Umfeld. Aufgrund der noch fehlenden Rahmenbedingungen (z.B. domainspezifische Normen, Spezifikationen, etc.) ist die Umsetzung solcher technischer Maßnahmen aktuell noch weitgehend unrealistisch.

Organisatorische Maßnahmen ergänzen die notwendigen technischen Maßnahmen bzw. bereiten diese vor. Einige dieser organisatorischen Maßnahmen können bereits jetzt in Angriff genommen werden. Solche Maßnahmen und Aktionen werden in diesem Abschnitt näher beschrieben.

7.1 Technische Maßnahmen

Die Umsetzbarkeit konkreter technischer Mitigationsmaßnahmen im Sinne einer vollständigen Migration auf PQC ist aktuell noch beschränkt, da dafür notwendige Rahmenbedingungen (Verfügbarkeit entsprechender domainspezifischer Normen und Spezifikationen, etc.) noch nicht ausreichend gegeben sind. An dieser Stelle sei jedoch beispielhaft ein grundsätzlicher Ansatz erwähnt, der bei Kompromittierung von im Feld befindlichen Dokumenten zumindest teilweise Abhilfe schaffen und bereits jetzt umgesetzt werden könnte.

Im Anwendungsbereich der eMRTDs wie z.B. Reisepässen liegt eine Bedrohung darin, dass die Authentizität der Dokumente bei Verfügbarkeit eines entsprechenden Quantencomputers nicht mehr zuverlässig verifiziert werden kann. Am konkreten Beispiel der Reisepässe bedeutet dies, dass für einen Reisepass nicht mehr zuverlässig festgestellt werden kann, ob dieser Reisepass tatsächlich von einer legitimen Ausgabestelle ausgestellt wurde, da die zugrundeliegenden klassischen kryptographischen Mechanismen nicht mehr als sicher und zuverlässig angesehen werden können. Um hier entgegenzuwirken, könnte im Zuge des Ausstellungsprozesses über eine sichere Hash-Funktion ein Hash-Wert über alle relevanten Daten des elektronischen Dokuments berechnet werden. Dieser Hashwert könnte am Dokument selbst aufgebracht und zusätzlich auch an einer sicheren zentralen Stelle hinterlegt werden. Die Authentizität und Integrität des Dokuments könnten dann zu einem beliebigen späteren Zeitpunkt über diesen zentral abgelegten Hashwert verifiziert werden.

Während dieser Ansatz prinzipiell eine praktikable Lösung darstellt, ergeben sich daraus auch einige Einschränkungen. So ist für die Zuverlässigkeit dieser Lösung die Integrität und Verfügbarkeit der zentral gespeicherten Hash-Werte entscheidend. Eine Speicherung dieser Daten in Distributed Ledgers („Blockchain“) kann hierfür ein möglicher Lösungsansatz sein. Im Allgemeinen bedingt der beschriebene Ansatz für die Prüfung der Korrektheit und Authentizität eines eMRTD das Vorhandensein

und die Nutzung einer zuverlässigen externen Datenquelle. Dies stellt eine zusätzliche Anforderung dar und verunmöglicht vollständig dezentrale Offline-Prüfungen.

Während einzelne technische Maßnahmen also prinzipiell jetzt schon denkbar sind, ist deren Umsetzbarkeit aktuell noch limitiert. Im Gegensatz dazu können geeignete organisatorische Maßnahmen bereits jetzt geplant und auch ergriffen werden. Einige Ansätze dazu werden im folgenden Unterabschnitt diskutiert.

7.2 Organisatorische Maßnahmen

Während mögliche Umsetzungen technischer Mitigationsmaßnahmen aufgrund fehlender Rahmenbedingungen aktuell noch stark limitiert sind, können bereits jetzt diverse organisatorische Maßnahmen ergriffen werden, um eine spätere notwendige Migration auf PQC bestmöglich vorzubereiten. Diese Maßnahmen sind im Folgenden kurz beschrieben.

7.2.1 Entwicklung einer PQC-Migrationsstrategie

Die Migration auf PQC ist ein hochkomplexer und aufwändiger Prozess, der langfristige Planung erfordert. Aktuell kann eine vollständige Umstellung noch nicht erfolgen, da viele Voraussetzungen – insbesondere im Bereich der domainspezifischen Standardisierung und Implementierung – noch fehlen. Insbesondere ist die Integration sicherer PQC-Algorithmen in bestehende Hard- und Software-Ökosysteme noch in Entwicklung. Dennoch ist es essenziell, sich bereits jetzt mit geeigneten Migrationsstrategien auseinanderzusetzen, um den Wechsel so effizient, kontrolliert und sicher wie möglich zu gestalten. Durch eine frühzeitige Planung können bereits jetzt Abhängigkeiten identifiziert, technische und organisatorische Herausforderungen erkannt und konkrete Maßnahmen vorbereitet werden. So wird sichergestellt, dass die tatsächliche Migration, sobald sie technisch und regulatorisch möglich ist, reibungslos und ohne unnötige Risiken umgesetzt werden kann.

Es wird daher empfohlen, bereits jetzt mit der Ausarbeitung einer detaillierten Migrationsstrategie zu starten. Diese Strategie sollte unter anderem folgende Aspekte berücksichtigen:

- **Analyse des aktuellen Systems:** Eine präzise und umfassende Bestandsaufnahme ist der erste Schritt für eine erfolgreiche Migration. Hierbei müssen sowohl technische, organisatorische als auch rechtliche Aspekte betrachtet werden, wie z.B.:
    - Welche kryptographischen Verfahren sind aktuell im Einsatz, und wo besteht Handlungsbedarf?
    - Welche Systeme, Prozesse und Schnittstellen sind von einer Umstellung betroffen?
    - Welche regulatorischen Vorgaben müssen erfüllt werden (rechtliche Anforderungen, Compliance-Anforderungen, etc.)?

- **Identifizierung offener Rahmenbedingungen und Abhängigkeiten:** Eine zentrale Herausforderung ist, dass notwendige Rahmenbedingungen für eine vollständige PQC-Migration derzeit noch nicht erfüllt sind. Daher ist es wichtig zu identifizieren:
    - **Standardisierung:** Welche für den Anwendungsbereich der eMRTDs relevanten Normen und Standards sind bereits festgelegt? Wo gibt es diesbezüglich noch Lücken?
    - **Software-Unterstützung:** Inwieweit sind relevante Software-Komponenten bereits kompatibel mit PQC und für eine entsprechende Migration vorbereitet? Gibt es Hersteller oder Softwareanbieter, die noch Anpassungen vornehmen müssen und zu denen Abhängigkeiten bestehen?
    - **Hardware- und Infrastrukturabhängigkeiten:** Gibt es bestehende Hardware-Komponenten, die nicht einfach auf PQC umgestellt werden können? Welche Übergangslösungen sind möglich?
    - **Externe Faktoren:** Gibt es zusätzliche Abhängigkeiten von Zulieferern, Partnern oder regulatorischen Vorgaben, die erst noch geklärt werden müssen, bevor eine Umstellung erfolgen kann?
- **Erstellung einer Roadmap:** Eine gut strukturierte Roadmap ist entscheidend für eine effiziente, sichere und kontrollierte Migration, sobald alle dafür notwendigen Rahmenbedingungen gegeben sind. Die Roadmap baut auf den zuvor identifizierten Handlungsbedarfen und Abhängigkeiten auf und sollte folgende Aspekte beinhalten:
    - **Priorisierung der Maßnahmen:** Welche Bereiche müssen zuerst umgestellt werden, um kritische Sicherheitsrisiken zu vermeiden?
    - **Schrittweise Implementierung:** Wenn möglich sollte die Migration schrittweise erfolgen, um Risiken im Zusammenhang mit unvorhergesehenen Ereignissen im Zuge der Migration zu beschränken.
    - **Übergangslösungen:** Wenn möglich sollten zeitlich beschränkte Übergangslösungen angedacht werden, über die eine parallele Verwendung klassischer Algorithmen und PQC-Algorithmen ermöglicht wird, sodass die Migration auf PQC fließend vonstattengehen kann. Insbesondere sollen hier auch Möglichkeiten (und Limitierungen) hybrider Verfahren im Detail geprüft werden, auch wenn dieses Thema aktuell noch durchaus kontrovers diskutiert wird.
    - **Validierung und Sicherheitstests:** Kontinuierliche Tests und Überprüfungen zur Sicherstellung der Kompatibilität und Sicherheit der neuen Verfahren.
    - **Fallback-Strategien:** Entwicklung von Notfallplänen für den Fall, dass Probleme im Zuge der Migration auftreten.
    - **Monitoring und kontinuierliche Anpassung:** Die Migration zu PQC ist kein einmaliger Prozess – neue Bedrohungen oder technologische Entwicklungen müssen kontinuierlich beobachtet und die Strategie entsprechend angepasst werden.

Die Erarbeitung einer Migrationsstrategie basierend auf den oben erwähnten Punkten ist zum aktuellen Zeitpunkt eine der wichtigsten Maßnahmen. Mit der Umsetzung dieser Maßnahme sollte unverzüglich gestartet werden.

7.2.2 Internationale Zusammenarbeit

Bereits jetzt kann das Engagement in internationale Zusammenarbeit etwa mit anderen Staaten oder Organisationen wie der ICAO intensiviert werden, um aktiv an der Erarbeitung der für eine PQC-Migration im Bereich der eMRTDs relevanten Standards und Spezifikationen mitwirken zu können. Über ein Engagement in diesem Bereich kann sichergestellt werden, dass eigene spezifische Anforderungen in den Standardisierungsprozess eingebracht und Entwicklungen im Bereich relevanter Standardisierungen frühzeitig erkannt werden können.

7.2.3 Gesetzliche und regulatorische Anpassungen

Eine PQC-Migration kann auch die Anpassung gesetzlicher und regulatorischer Grundlagen notwendig machen. Prinzipiell ist die Identifikation rechtlicher Handlungsbedarfe einer der relevanten Aktionspunkte im Zuge der Erarbeitung einer Migrationsstrategie. Aufgrund der in der Regel langen Durchlaufzeiten von Gesetzesänderungen können entsprechende notwendige Anpassungen, sofern diese bereits jetzt absehbar sind, schon frühzeitig in die Wege geleitet werden, noch bevor die Migrationsstrategie vollständig erarbeitet wurde.

7.2.4 Schulung von Mitarbeitenden

Ein entscheidender Erfolgsfaktor für eine PQC-Migration ist die Schulung und Sensibilisierung der Mitarbeitenden, damit das System nach der Umstellung sicher und korrekt betrieben sowie genutzt werden kann. Neue kryptographische Verfahren bringen veränderte Anforderungen an Konfiguration, Schlüsselverwaltung und Sicherheitsprozesse mit sich, die in der Organisation verstanden und konsequent umgesetzt werden müssen. Technische Teams benötigen spezifische Schulungen zur Implementierung, Wartung und Fehleranalyse der neuen kryptographischen Algorithmen, während administrative und operative Mitarbeitende im sicheren Umgang mit den neuen Mechanismen unterwiesen werden sollten. Ebenso ist es essenziell, Awareness-Programme zu etablieren, um ein Bewusstsein für die veränderten Sicherheitsanforderungen zu schaffen – insbesondere im Hinblick auf etwaige hybride Lösungen, Übergangsphasen und potenzielle Angriffsvektoren. Ein umfassendes Schulungskonzept stellt sicher, dass die Belegschaft frühzeitig mit den neuen Prozessen vertraut wird und die Sicherheit sowie Effizienz der Gesamtlösung langfristig gewährleistet bleibt.

Während Schulungen für administrative und operative Mitarbeitende zu adaptierten Prozessen wohl erst zu einem späteren Zeitpunkt sinnvoll und möglich sind, können technische Teams über entsprechende Schulungsangebote schon jetzt frühzeitig an die relevanten PQC-Technologien herangeführt werden.

7.2.5 Risikoanalyse und Erarbeitung von Notfallszenarien

Aktuelle Schätzungen gehen davon aus, dass ein relevanter Quantencomputer in spätestens 16 Jahren (d.h. bis 2040) realisierbar sein wird. Experten weisen jedoch darauf hin, dass derartige Schätzungen etwaige disruptive Entwicklungssprünge oder auch die bewusste Geheimhaltung erreichter Meilensteine nicht berücksichtigen. Es kann daher nicht gänzlich ausgeschlossen werden, dass Quantencomputer, die in der Lage sind, klassische kryptographische Algorithmen zu brechen, bereits früher verfügbar sein könnten.

Trotz dieses potenziellen Risikos ist eine kurzfristige PQC-Migration im Bereich der eMRTDs aus den mehrfach genannten Gründen aktuell noch nicht möglich. Im Worst-Case kann somit eine Situation entstehen, in der bereits ausgegebene und aktuell im Feld befindliche eMRTDs (Reisepässe, etc.) schlagartig als unsicher anzusehen sind.

Es wird empfohlen, sich auch auf dieses – wenn auch unwahrscheinliche – Szenario bestmöglich vorzubereiten. Über geeignete Methoden der Risikoanalyse sollten Risiken, die sich aus dem Szenario einer plötzlichen Verfügbarkeit eines relevanten Quantencomputers ergeben, identifiziert und bewertet werden. Zudem sollten geeignete Vorgehensweise für entsprechende Notfallszenarien entwickelt werden, sodass das plötzliche Eintreten eines solchen Szenarios die für eMRTDs verantwortlichen Organisationen nicht gänzlich unvorbereitet trifft.

7.2.6 Verkürzung der Gültigkeitsdauer klassischer Reisepässe

Eine große Herausforderung bei der PQC-Migration von eMRTDs ist die relative lange Gültigkeitsperiode dieser Dokumente. Reisepässe werden beispielweise oft mit einer Gültigkeitsdauer von bis zu 10 Jahren ausgegeben. Dies bedeutet auch, dass eine vollständige PQC-Migration von Reisepässen frühestens nach 10 Jahren abgeschlossen sein kann, sofern man bereits ausgegebene eMRTDs nicht vorzeitig als ungültig deklarieren möchte. Das ist potenziell problematisch, da in so einem langen Zeitraum disruptive Entwicklungsschritte im Bereich der Quantencomputer nicht gänzlich ausgeschlossen werden können.

Eine Möglichkeit hier gegenzusteuern ist es, die Gültigkeit von neu ausgegebenen eMRTDs, die nach wie vor auf klassischer Kryptographie beruhen, auf einen kürzeren Zeitraum zu beschränken. Die Vorteile einer Verkürzung des Gültigkeitszeitraums liegen auf der Hand. Allerdings würde eine solche Maßnahme auch diverse Nachteile mit sich bringen. Zum einen würde eine solche Maßnahme wohl eine Anpassung zugrundeliegender rechtlicher Grundlagen erfordern, zum anderen könnten durch eine kürzere Gültigkeitsdauer auch höhere Kosten entstehen.

8 Fazit

Die Migration auf Post-Quanten-Kryptographie ist ein hochrelevantes Thema, insbesondere im Bereich der eMRTDs. Angesichts der zunehmenden Aktivitäten und Fortschritte in diesem Bereich zeigt

sich, dass die Bedeutung dieses Themas kontinuierlich wächst. Aktuelle Schätzungen gehen davon aus, dass bis zum Jahr 2040 mit der Verfügbarkeit praktisch einsetzbarer Quantencomputer zu rechnen ist, die in der Lage sein werden, klassische kryptographische Algorithmen zu brechen. In Anbetracht der oft langen Gültigkeitsdauer von eMRTDs scheint ein zeitnahes Handeln daher angebracht. Gleichzeitig bestehen jedoch noch viele offene Fragen, insbesondere auch in Bezug auf fehlende domainspezifische Normen und Standards, die für eine flächendeckende und zuverlässige Umsetzung erforderlich sind.

Auch wenn eine vollständige Migration auf PQC derzeit aufgrund fehlender Rahmenbedingungen noch nicht möglich ist, können bereits jetzt erste Mitigationsmaßnahmen gesetzt werden. Eine der zentralsten Maßnahmen ist dabei die Erarbeitung einer fundierten Migrationsstrategie. Diese gewährleistet, dass notwendigen Tätigkeiten rasch und effektiv vorgenommen werden können, sobald die dafür nötigen Rahmenbedingungen gegeben sind. Die Erarbeitung einer Migrationsstrategie als zentrale Mitigationmaßnahme kann von weiteren, vor allem organisatorischen, Maßnahmen flankiert werden. Diese umfassen unter anderem entsprechende Schulungsaktivitäten, gesetzliche und regulatorische Anpassungen oder auch die aktive Mitwirkung in relevanten Standardisierungsaktivitäten.

Auch wenn eine vollständige technische PQC-Migration aktuell noch nicht möglich ist, können also bereits jetzt durch eine proaktive Herangehensweise diverse Risiken minimiert und Vorbereitungen auf eine möglichst effiziente künftige Migration getroffen werden. Die Erarbeitung einer Migrationsstrategie ist dabei das zentrale Element. Es wird dringend empfohlen, mit der Ausarbeitung einer solchen Migrationsstrategie ehestmöglich zu beginnen.

ANHANG A: Abkürzungsverzeichnis

3DES	Triple Data Encryption Standard
AA	Active Authentication
AES	Advanced Encryption Standard
API	Application Programming Interface
BAC	Basic Access Control
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Chip Authentication
EAC	Extended Access Control
COVID19	Coronavirus Disease 2019
ECC	Eliptic Curve Cryptography
eMRTD	Electronic Machine Readable Travel Document
ECDHE	Elliptic Curve Diffie–Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
eID	Elektronische Identität
EJBCA	Enterprise JavaBeans Certificate Authority
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute
EU	Europäische Union
FIPS	Federal Information Processing Standard
FN-DSA	FFT (Fast-Fourier Transform) over NTRU-Lattice-Based Digital Signature Algorithm
HSM	Hardware Security Module

HQC	Hamming Quasi-Cyclic
KEM	Key Encapsulation Mechanism
IBM	International Business Machines Corporation
ICAO	International Civil Aviation Organization
IKE	Internet Key Exchange
IT	Informationstechnologie
LDS	Logical Data Structure
LWE	Learning With Errors
ML-DSA	Module-Lattice-Based Digital Signature Standard
ML-KEM	Module-Lattice-Based Key-Encapsulation Mechanism Standard
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
N/A	Not Available / Nicht verfügbar bzw. unzutreffend
OpenSSL	Open Secure Sockets Layer
ÖPNV	Öffentlicher Personennahverkehr
PA	Passive Authentication
PACE	Password Authenticated Connection Establishment
PKD	Public Key Directory
PKI	Public Key Infrastruktur
PQC	Post Quantum Cryptography
QR	Quick Response
RFID	Radio Frequency Identification
RSA	Rivest–Shamir–Adleman

SIM	Subscriber Identity Module
SLH-DSA	Stateless Hash-Based Digital Signature Standard
SVP	Shortest Vector Problem
TLS	Transport Layer Security
USA	United States of America
VPN	Virtual Private Network

SIGNATURINFORMATIONEN	**Unterzeichner**	Christian Rechberger
	Datum/Zeit-UTC	2025-05-07T11:04:14+02:00
	Prüfinformation	Informationen zur Prüfung der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at
Hinweis	Dieses mit einer qualifizierten elektronischen Signatur versehene Dokument hat gemäß Art. 25 Abs. 2 der Verordnung (EU) Nr. 910/2014 vom 23. Juli 2014 ("eIDAS-VO") die gleiche Rechtswirkung wie ein handschriftlich unterschriebenes Dokument.	

SIGNATURE INFORMATION	**Signatory**	Peter Franz Teufl
	Date/Time-UTC	2025-05-07T11:16:25+02:00
	Verification	Information about the verification of the electronic signature can be found at: https://www.signaturpruefung.gv.at
Note	This document is signed with a qualified electronic signature. According to Art. 25 para. 2 of the Regulation (EU) No 910/2014 of 23. July 2014 ("eIDAS-Regulation") it shall have the equivalent legal effect of a handwritten signature.	