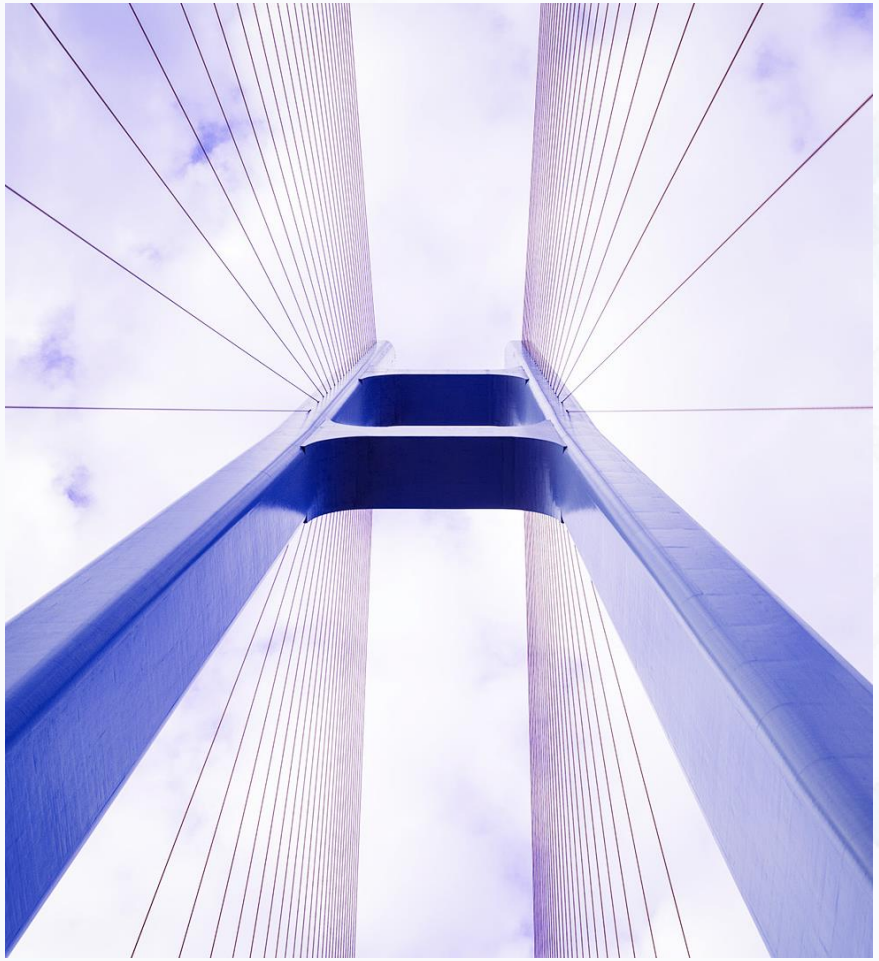
Quantum Ready oder regulatorisches Risko?

PQC, DORA und NIS-2 für kritische Infrastruktur

—

Wien, 10. Juni 2025



Contents

Einleitung

Worum geht es?

Die Bedrohung durch Quantencomputing, die EU-Regulierungslandschaft (DORA, NIS-2) und Post-Quanten-Kryptographie (PQC) als Lösung.

Warum dies jetzt (2025) relevant ist!

PQC nicht explizit gefordert...

... aber robustes Risikomanagement benötigt Stand der Technik & Resilienz.

-> Impliziert: Auseinandersetzung mit Quantenbedrohung (PQC) notwendig.

Die Rollen der Zielgruppe:

- CIO – Strategie/Budget
- CISO – Risiko/Compliance
- EA – Architektur/Machbarkeit

Die Quantenbedrohung für die Kryptographie

Was ist das Problem?

Fehlertolerante Quantencomputer werden die aktuelle Public-Key-Kryptographie (RSA, ECC, DH) brechen, die TLS, VPNs, digitalen Signaturen, Code-Signierung usw. zugrunde liegt.

AES ist wenig betroffen.

Wann kommt der Q-Day?

Der allgemeine Expertenkonsens zu Zeitplänen für kryptografisch relevanten Quanten-computern sieht das Potenzial etliche Jahre entfernt.
Entscheidend ist: Die Migration dauert länger.

"Harvest Now, Decrypt Later"

Verschlüsselte sensible Daten, die heute abgefangen werden, können entschlüsselt werden, sobald ein leistungsfähiger Quantencomputer existiert.

Auswirkungen vor dem Q-Day:

QC-Readiness für:

- Verschlüsselung langfristig vertraulicher Daten lange vor dem Q-Day
- Bereitschaft für Signaturen ab dem Q-Day

Prognosen und Maßnahmen

Org	Land	Zeit	Vorhersage des Q-Days oder Maßnahme
ANSSI	FR	2030	PQC soll in Sicherheitsprodukten ab 2030 verwendet werden
BSI	D	2041	CRQC verfügbar
DHS	US	-	Roadmap für Inventar, Priorisierung and Migrationsplanung empfohlen
ENISA	EU	-	Vorsichtshalber sollte man jetzt mit der Migration beginnen
IBM	US	2030+	Roadmap: CRQC frühestens 2030
MIT	US	2040+	CRQC frühestens 2040 verfügbar
NCSC	UK	2035	PQC-Migration soll bis 2035 abgeschlossen sein
NSA	US	2035	Nicht vorhersagbar, aber PQC soll bis 2035 umgesetzt sein

PQC: Post-Quantum Kryptographie

Was ist PQC?
Kryptographische Algorithmen, die resistent gegen Angriffe sowohl von klassischen als auch von Quantencomputern sind.
(Nicht: Quantenkryptographie)

Wichtige Merkmale

- Generell größere Schlüssel- und Signaturgrößen (Auswirkungen auf Bandbreite, Speicher, Protokolle).
- Unterschiedliche Leistungsmerkmale (potenzielle Auswirkung auf Latenz, Durchsatz).
- Notwendigkeit der "Krypto-Agilität" (Systeme so gestalten, dass zukünftige Krypto-Änderungen erleichtert werden). Dient sowohl PQC als auch Nicht-Quanten-Zwecken.

Stand der Standardisierung

Was ist der NIST PQC-Standardisierungsprozess?

1. Das National Institute of Standards and Technology (NIST) treibt die Post-Quanten-Kryptographie (PQC) maßgeblich voran.

2.hat NIST 2022 die ersten Siegeralgorithmen benannt, die bereits implementiert werden: für Schlüssel-austausch **Kyber** und für digitale Signaturen **Dilithium**.

3.Weitere Kandidaten für Signaturen und Key-Encapsulation-Mechanismen (KEMs) dienen als Optimierungs- und Backup-Optionen.

Function	Pre-Quantum	Post-Quantum
Key Exchange	RSA, DH, ECDH	Kyber, NTRU, BIKE
Signature	RSA, EdDSA	Dilithium, Falcon, SPHINCS+
Hash	SHA-2 (256+)	SHA2, SHA-3 (384+)
Encryption	AES 128+	AES (256+)

Was ist der Hybride Ansatz?

Konzept der gleichzeitigen Nutzung klassischer und PQC-Algorithmen während einer Übergangsphase.

Parallele Signaturen

- Rückwärtskompatibilität
- Vertrauen in quantum-safe Algorithmen?

Post-Quantum Performance vs. RSA/ECC

Wichtige Punkte

- PQC key exchange (e.g., Kyber) is ~2–5× langsamer als ECDH aber schneller als RSA/DH.
- Dilithium ist ca. 2–3× langsamer als ECDSA
- Hashing Overhead: SHA-3 und SHAKE haben minimale Auswirkungen (~1–2× Latenz vs. SHA-2).
- Hybrid Deployments: (zB. ECDH + Kyber, SHA-256 + SHAKE) haben kaum zusätzlichen Overhead.
- Legacy: SHA-1 and RSA-2048 sind auch ohne Quantum Computing in vielen Szenarion nicht mehr sicher.

Function	Algorithm	Memory	Pub Key Size	Ciphertext Size	Signature Size
Signature	Dilithium, Falcon	x5 - x8	x4 - x37	-	x2 - x63
Key Exchange	Kyber	x4 - x6	x3 - x28	x3 - x25	-

Regulatorische Anforderungen an Kryptographie

Relevante Rahmenwerke & Vorschriften:

DORA (Digital Operational Resilience Act)

Schwerpunkt auf IKT-Risikomanagement im Finanzsektor; verlangt Resilienz gegen neu entstehende Bedrohungen.

NIS2-Richtlinie

Fordert robustes Cyber-Risikomanagement mit Lieferkettensicherheit und modernster Kryptografie.

Allgemeine Cybersicherheits-Rahmenwerke (z. B. ISO 27001, NIST CSF):

Heben proaktive Risiko- und Bedrohungsanalysen sowie die fortlaufende Optimierung der Sicherheitskontrollen hervor.

Implikation für die Compliance

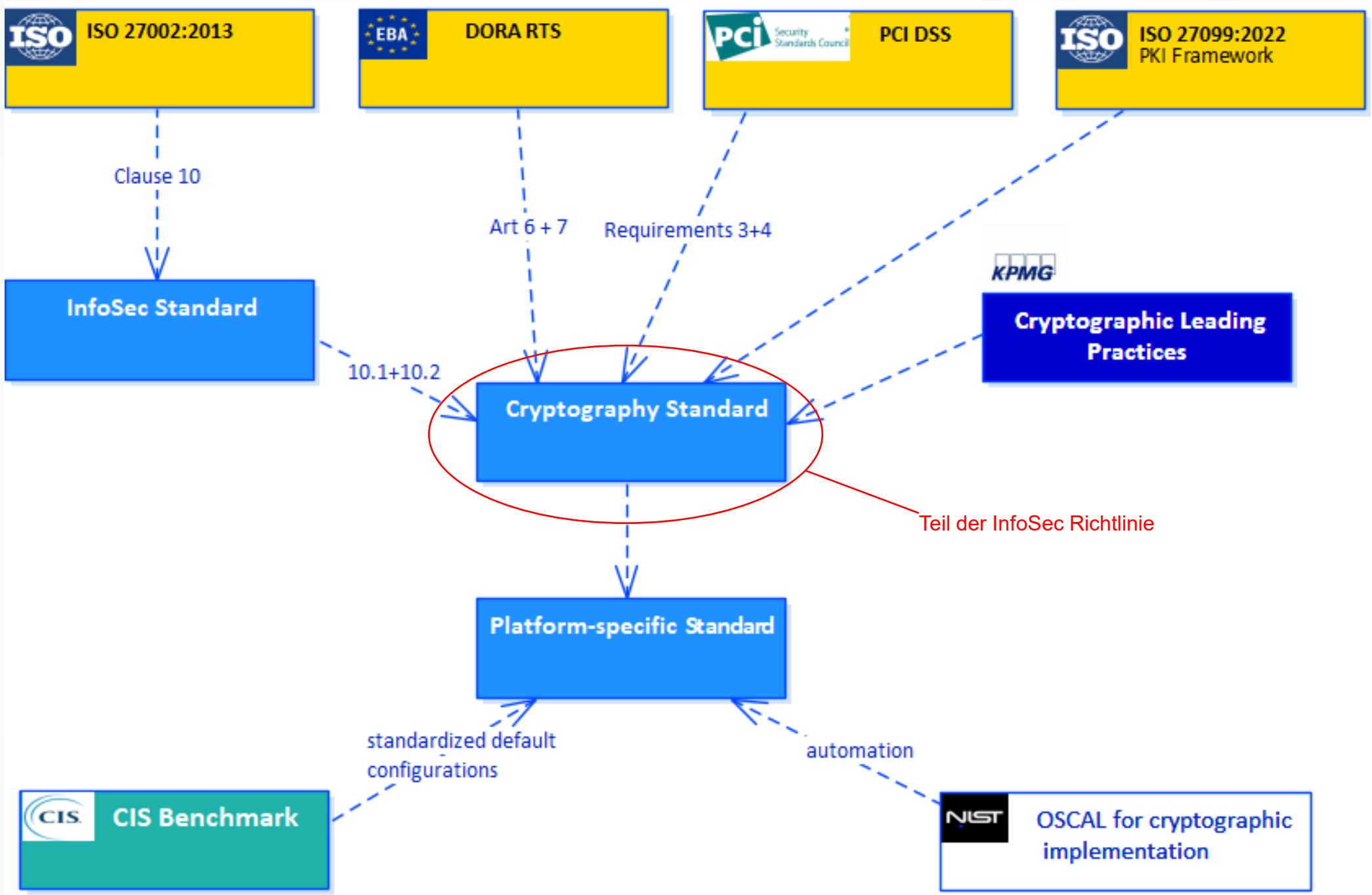
Während PQC nicht explizit genannt wird, erfordert die Anforderung an „aktuelle Sicherheit“ und "Resilienz" implizit die Auseinandersetzung mit der Quantenbedrohung.

Die EU-Regulierungslandschaft: Anforderungen von DORA & NIS-2

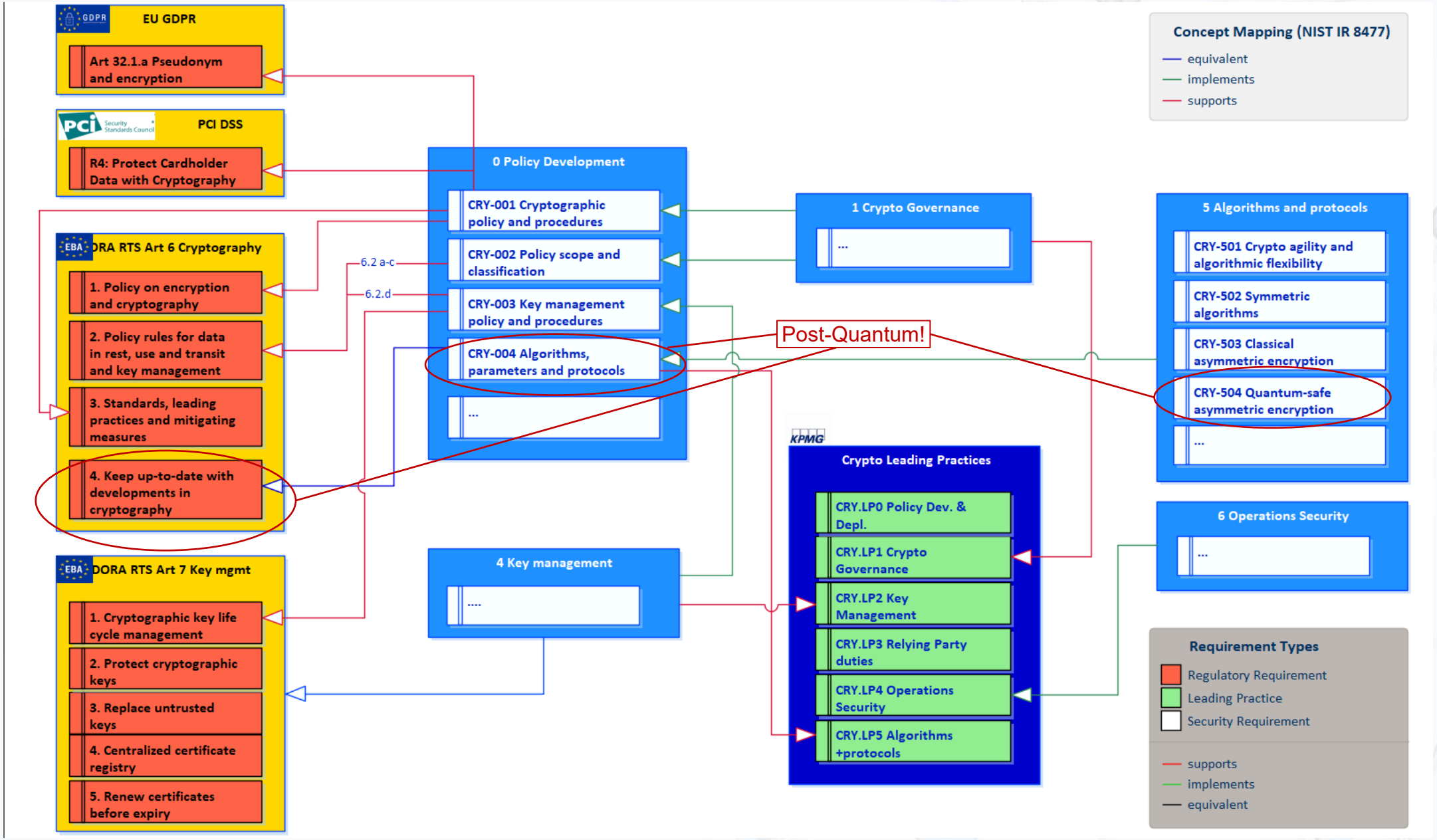
DORA	NIS2	DORA + NIS-2
DORA RTS Artikel 6.4: Aktualisierung oder Änderung der kryptographischen Technologie auf der Grundlage von Entwicklungen in der Kryptoanalyse.	NIS-2 Artikel 21: Schreibt angemessene und verhältnismäßige technische/organisatorische Sicherheitsmaßnahmen vor, basierend auf einem risikobasierten Ansatz und dem Stand der Technik.	Sicherheit der Lieferkette (NIS-2 Art 21, DORA Art 28+): Kritische Einrichtungen sind für das Risiko der Lieferkette verantwortlich. Sie müssen beginnen, Anbieter nach ihren PQC-Roadmaps und ihrer kryptographischen Flexibilität zu fragen, wie durch den Fokus auf Drittparteienrisiken vorgeschrieben.

Beide Verordnungen fordern proaktives, risikobasiertes Management aller relevanten IKT-Bedrohungen und die Sicherstellung, dass die Sicherheit die aktuelle technologische Landschaft und vorhersehbare Risiken widerspiegelt.

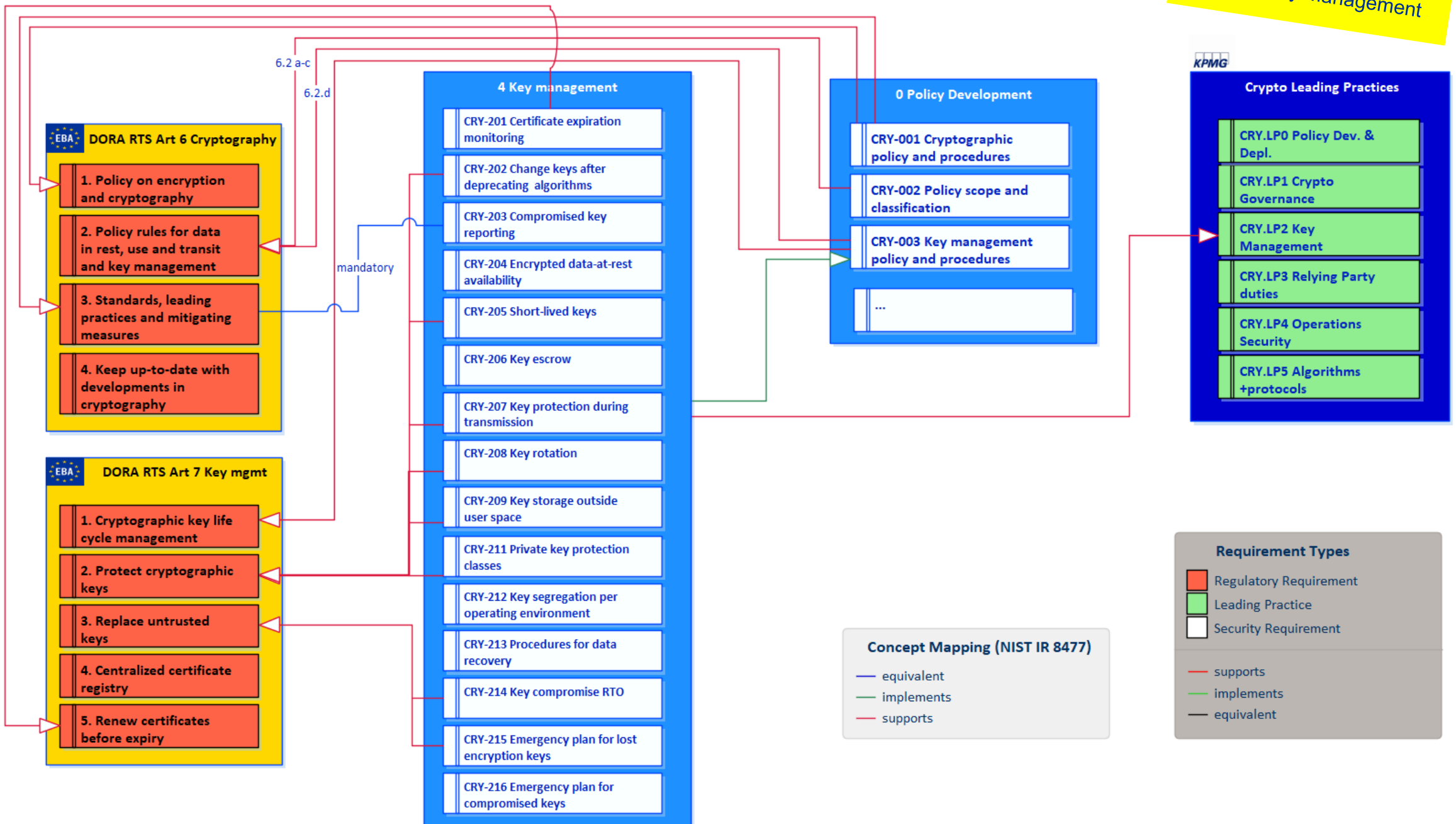
Beispiel für einen Kryptographie-Standard (1: Ableitung)



Beispiel für einen Kryptographie-Standard (2: PQC)



Exkurs Key Management



Beispiel für einen Kryptographie-Standard (4: Prozesslandkarte)

Exkurs Key Management

1 CA Management	2 Certificate Life Cycle Management			3 Certificate usage		4 PKI Governance	5 Service Life Cycle	
1.1 CA Management	2.1 Initial	2.2 Ongoing	2.3 Termination	3.1 Authentication	3.2 Validation	4.1 PKI Governance	5.1 Service Stages	5.1 Service Operation
1.1.1 HSM Verwaltung	2.1.1 Registrierung	2.2.1 Zertifikat-Rollover	2.3.1 Zertifikat widerrufen	3.1.1 Session Authentifizierung	3.2.1 Validierung der Unterschrift	4.1.1 Definition und Überprüfung von Rollen und Verantwortlichkeiten	5.1.1 Service-Strategie	5.2.1 Störungsmanagement
1.1.2 Root Key Verwaltung	2.1.2 Automatische Registrierung	2.2.2 Schlüssel-Rollover	2.3.2 Schlüssel deaktivieren	3.1.2 Erstellung von Signaturen	3.2.2 Validierung des Widerrufsstatus	4.1.2 Verwaltung der Trust List	5.1.2 Dienstgestaltung	5.2.2 Änderungsmanagement
1.1.3 Zertifikatablauf Überwachung	2.1.3 Archivierung von Schlüsseln	2.2.3 Schlüssel ersetzen			3.2.3 Verwendung der Vertrauensliste	4.1.3 Genehmigung kryptografischer Mechanismen	5.1.3 Dienstübergang	5.2.3 Management von Serviceanfragen
1.1.4 Zertifikatstemplate Verwaltung	2.1.4 Schlüsselerstellung					4.1.4 Abstimmung von Schutzbedarf und Zertifikatsrichtlinie	5.1.4 Kontinuierliche Serviceverbesserung	5.2.4 Ereignis- und Problem-Management
1.1.5 Root Zertifikats-Rollover	2.1.5 Schlüsselverteilung					4.1.5 Kryptografische Agilität		5.2.5 Verfügbarkeits- und Kontinuitätsmanagement
	2.1.6 BYOK für Cloud Dienste					4.1.6 Metadaten mit ITSM-Assets verknüpft		5.2.6 Betriebskontrolle
								5.2.7 Konfigurationsmanagement
								5.2.8 Freigabe- und Bereitstellungsmanagement
								5.2.9 Verwaltung des privilegierten Zugriffs

Herausforderungen

Lange Migrationszeiten

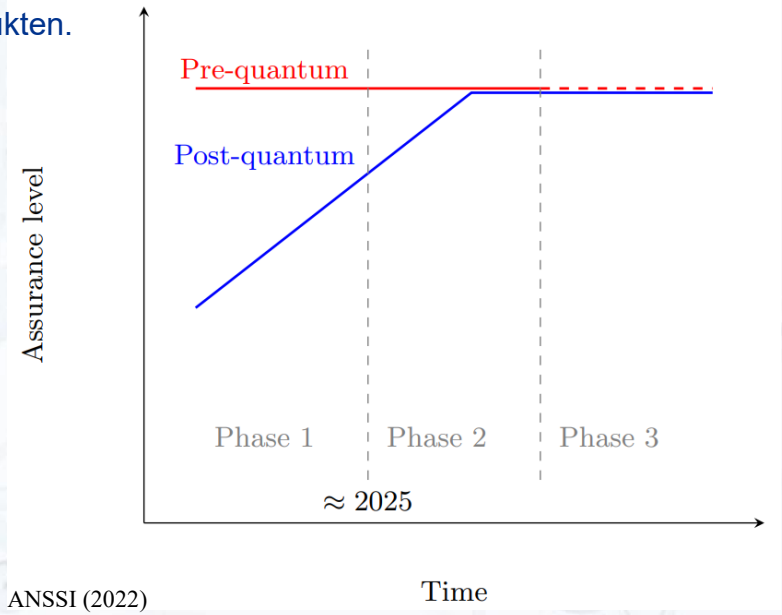
Inventarisierung der Kryptographie, Bewertung von Risiken, Testen von PQC, Aktualisieren/Patchen von Systemen, Koordination mit Anbietern dauert Jahre, potenziell ein Jahrzehnt oder länger für komplexe Systeme.

Agilität ist aufwändig

Das Entwerfen und Implementieren von Systemen, die kryptographische Algorithmen leicht austauschen können, erfordert Planung und Änderungen von Architektur und Produkten.

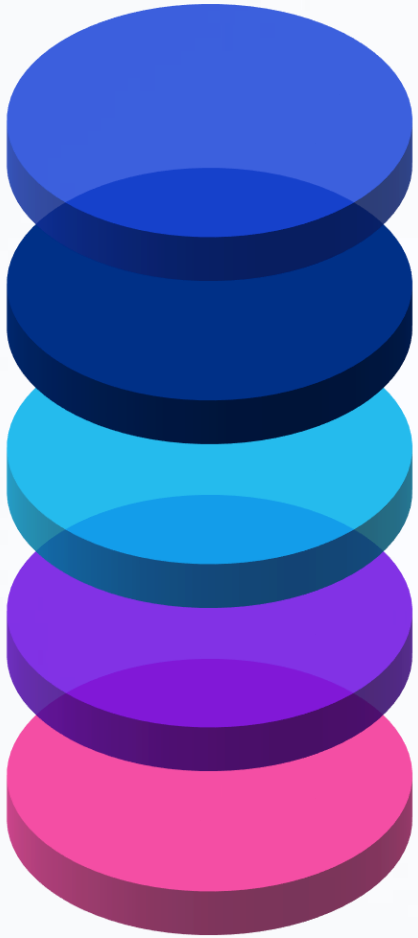
Lieferkette einbeziehen

Unternehmen müssen ihren Einfluss jetzt nutzen, um sicherzustellen, dass ihre kritischen Lieferanten rechtzeitig PQC-fähige Produkte und Dienstleistungen entwickeln



ANSSI (2022)

Fazit und Schlussfolgerung



01

Strategie

Haben Sie eine klar definierte Strategie, damit die Verschlüsselung Algorithmus-agnostisch ist. Produkte müssen flexibel sein, indem sie bekannte kryptographische Bibliotheken verwenden, die regelmäßige Updates für Algorithmen und Protokolle anbieten.

02

Perspektive

Es ist nicht nur ein Krypto-Upgrade; es ist fundamental für langfristiges Risikomanagement, regulatorische Compliance und operationale Resilienz für kritische Infrastrukturen.

03

Planung und Zusammenarbeit

Die Notwendigkeit von Planung und funktionsübergreifender Zusammenarbeit (PKI-Team, Anwendungsteams, Sicherheit, Architektur, Beschaffung), um die Reise zur Quanten-Bereitschaft ("Quantum-Readiness") zu beginnen.

04

OT-Strategie

Beziehen Sie die Bewertung der Gerätefähigkeiten in Ihre OT-Strategie (Operational Technology) mit ein, ziehen Sie kompensierende Kontrollen in Betracht.

05

PQC-Migration

Die PQC-Migration wird sowohl durch das IKT-Risikomanagement (die Quantenbedrohung) als auch durch Vorschriften wie DORA und NIS-2 (die aktuellen kryptographischen Algorithmen erfordern) vorangetrieben.

Rainer Hörbe

Senior Manager
IT Advisory / Cyber Security

KPMG Advisory GmbH
Porzellangasse 51
1090 Wien

M +43 664 859 59 11
E rhoerbe@kpmg.at
W kpmg.at/cyber

kpmg.at