10/2025

sopra steria

KRYPTOREGISTER

STARTPUNKT FÜR EINE POSTQUANTENRESILIENTE IT

VORWORT

Die Ära marktreifer Quantencomputer rückt näher. Eine Zeit, auf die sich Cyberkriminelle, aber auch ihre potenziellen Opfer – Unternehmen und Behörden – vorbereiten. Die einen wollen mithilfe der Technologie Algorithmen brechen, die anderen wollen das verhindern. Letztere müssen dafür ihre aktuellen Kryptoverfahren, IT-Systeme und Prozesse postquantenresilient gestalten. Hierzu gehören ein systematischer Aufbau und das Führen eines Kryptoinventars.

Mit der Standardisierung erster Post-Quanten-Schlüsselaustausch- und -Signaturverfahren durch das National Institute of Standards and Technology (NIST) beginnt für Wirtschaft und öffentliche Verwaltung die kritische Phase der Bestandsaufnahme. Denn die Mehrheit der Organisationen hat keinen lückenlosen und gepflegten Überblick darüber, welche kryptographischen Verfahren, Protokolle und Schlüssel derzeit im Einsatz sind – und an welchen Stellen.

Ein systematisches Kryptoregister ist allerdings Grundvoraussetzung für jede Post-Quanten-Migrationsstrategie. Wir zeigen mit diesem Paper, warum sich die Verantwortlichen in den Unternehmen und Behörden bereits jetzt mit einer Kryptoinventarisierung befassen sollten, welche Standards sich durchsetzen und wie Organisationen vom Forschungsstand profitieren.

KRYPTOREGISTER – DARUM JETZT

Was viele Organisationen verkennen: Post-Quanten-Kryptographie (englisch Post-Quantum Cryptography, PQC) ist kein reines Forschungsthema mehr. Die Entwicklungsschritte hin zu ersten allgemein gebrauchsfähigen und relevanten Quantencomputern werden kürzer. Für Unternehmen ist es eine strategische Notwendigkeit, sich schon heute eine praktikable Migrationsstrategie für eine quantensichere Kryptographie zu überlegen, um nicht zu spät zu kommen. Für die zuständigen staatlichen Stellen ist Post-Quanten-Kryptographie ebenfalls kein Zukunftsthema:

- Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt die Umstellung für Hochrisikoanwendungen bis Ende 2030 (BSI-Empfehlung PQC).
- Die NIS-Kooperationsgruppe gibt in der Veröffentlichung „A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography" der Europäischen Kommission eine Empfehlung, bis 2026 Post-Quanten-Migrationspläne zu entwickeln und ein Kryptoinventar zu erstellen (Roadmap EC).

Alles keine Termine, die nach ferner Zukunft klingen.

Das NIST hat bereits erste Post-Quanten-Verfahren standardisiert (FIPS 203 bis FIPS 205). Ein vierter Standard (FIPS 206) steht kurz vor der Veröffentlichung. Dies sind weitere klare Signale dafür, dass eine neue Ära der Kryptographie bereits begonnen hat. Drei Argumente sprechen dafür, dass der Aufbau von Post-Quanten-Resilienz kein Thema für die lange Bank ist:

1. **Die Gewissheit über die baldige Verwundbarkeit:** Es herrscht Konsens darüber, dass viele heute eingesetzte kryptographische Verfahren mittel- bis langfristig nicht mehr sicher sein werden. Dazu zählen insbesondere asymmetrische Verfahren der Kategorie „Public-Key-Kryptographie".
2. **Die Bedrohung durch „Harvest now, decrypt later"-Angriffe:** Heute abgefangene Daten können bei Verfügbarkeit eines leistungsfähigen Quantencomputers in wenigen Jahren entschlüsselt werden – wenn kryptographische Algorithmen eingesetzt werden, die auf den mathematischen Prinzipien der Primfaktorzerlegung (z. B. RSA) und des diskreten Logarithmus (z. B. DSA) basieren.
3. **Der fehlende Überblick über den eigenen Krypto-Status-quo:** Viele Organisationen können eine scheinbar einfache, aber strategisch hoch relevante Frage nicht beantworten: „Welche kryptographischen Verfahren setzen wir aktuell überhaupt ein und auf welchen IT-Systemen kommen diese zum Einsatz?" Ob RSA- oder DSA-Algorithmen, ob veraltete TLS-Protokollversionen oder verborgene Abhängigkeiten in IT-Komponenten von Drittanbietern: In großen IT-Landschaften fehlt oft ein strukturierter Überblick über kryptographische Assets – von Zertifikaten über Algorithmen bis hin zu Kryptobibliotheken oder zugehörigem Schlüsselmaterial.

Wer sich allerdings ernsthaft auf eine Migration der Kryptoverfahren vorbereiten will, muss wissen, wo er steht. Am Aufbau eines Kryptoregisters führt somit kein Weg vorbei.

KRYPTOGRAPHISCHE ASSETS – WAS DAMIT GEMEINT IST UND WARUM SIE SO SCHWER ZU ERFASSEN SIND

Wenn von einem „Kryptoinventar", einem „Kryptokataster" oder einem „Kryptoregister" die Rede ist, geht es nicht nur um Schlüsselmaterial oder Zertifikate. Die Realität kryptographischer Abhängigkeiten in IT-Systemen ist vielschichtiger und verbirgt sich oft tief in der IT-Infrastruktur oder in Softwarekomponenten anderer Hersteller.

Zu den zentralen kryptographischen Assets zählen unter anderem:

- Schlüsselmaterial (z. B. Private Keys, Shared Secrets)
- Zertifikate
- Algorithmen (z. B. RSA, ECDSA, AES, SHA-2)
- Bibliotheken & Krypto-Implementierungen (z. B. OpenSSL, Bouncy Castle, libsodium)
- Protokolle (z. B. TLS 1.2/1.3, SSH, S/MIME)

Die große Herausforderung bei der Erfassung besteht darin, dass all diese Assets in modernen Systemlandschaften nicht zentral abgelegt sind, sondern sich über viele Ebenen verteilen. Sie finden sich in

- Applikationen
- Middleware, Containern, Firmware
- CI/CD-Pipelines
- vorgefertigten Softwarekomponenten von anderen Unternehmen oder Entwicklern

Erschwerend kommt hinzu: Durch den Einsatz von Drittanbieterkomponenten wie externen Bibliotheken oder Frameworks ergeben sich viele indirekte kryptographische Abhängigkeiten. Unternehmen oder Behörden haben keine direkte Kontrolle über deren Konfiguration und Sicherheit.

Eine weitere Herausforderung betrifft das Thema Aktualität: Was heute als sicher gilt, kann morgen schon veraltet oder verwundbar sein. Mit einer einmaligen Erfassung des Status quo und einer Aktualisierung alle paar Jahre ist es nicht getan. Organisationen müssen eine granulare Kryptolandkarte zeichnen können und diese auf dem neusten Stand halten.

KRYPTOINVENTARISIERUNG HEUTE

Angesichts der komplexen IT-Landschaften braucht es eine systematische Erfassung von Krypto-Assets und Abhängigkeiten, sowie einen höheren Automatisierungsgrad. Unternehmen und Behörden haben hier einige Schritte zu gehen: Das aktuelle Vorgehen ist in vielen Fällen sehr personalintensiv, unvollständig und selten standardisiert.

Viele Organisationen führen klassische Excel-Listen, deren manuelle Pflege sehr aufwändig und fehleranfällig ist. Punktuell führen Unternehmen und Behörden Codeanalysen durch oder werten Einträge in Konfigurationsmanagementdatenbanken (CMDB) aus. Die verwendeten Quellen sind meist heterogen. Oft handelt es sich um Scan-Reports einzelner Systeme oder um Auditergebnisse aus spezifischen Teilbereichen der IT-Infrastruktur. Viele Krypto-Assets fallen durchs Raster. In sicherheitskritischen Umgebungen werden zumindest Zertifikate oder TLS-Konfigurationen an zentraler Stelle erfasst, dokumentiert und gemanagt. Andere Komponenten wie eingebettete Kryptobibliotheken oder die damit genutzten kryptographischen Algorithmen bleiben dagegen häufig unberücksichtigt.

Ein zentrales Problem ist der große Ressourcenbedarf. Gerade in komplexen IT-Systemen von Konzernen und großen Behörden kostet die manuelle oder halbautomatisierte Erfassung kryptographischer Abhängigkeiten viel Zeit und Personal. Das Führen eines vollständigen und aktuellen Kryptoregisters ist ohne automatisierte Unterstützung nicht wirtschaftlich.

Hinzu kommt ein grundlegendes Strukturdefizit: Kryptographische Artefakte werden in den wenigsten Organisationen systematisch inventarisiert, versioniert oder mit einem definierten Lifecycle versehen. Damit fehlt die Grundlage für eine Migrationsplanung in Richtung Post-Quanten-Verfahren.

DIE IDEE EINES MODERNEN KRYPTOREGISTERS

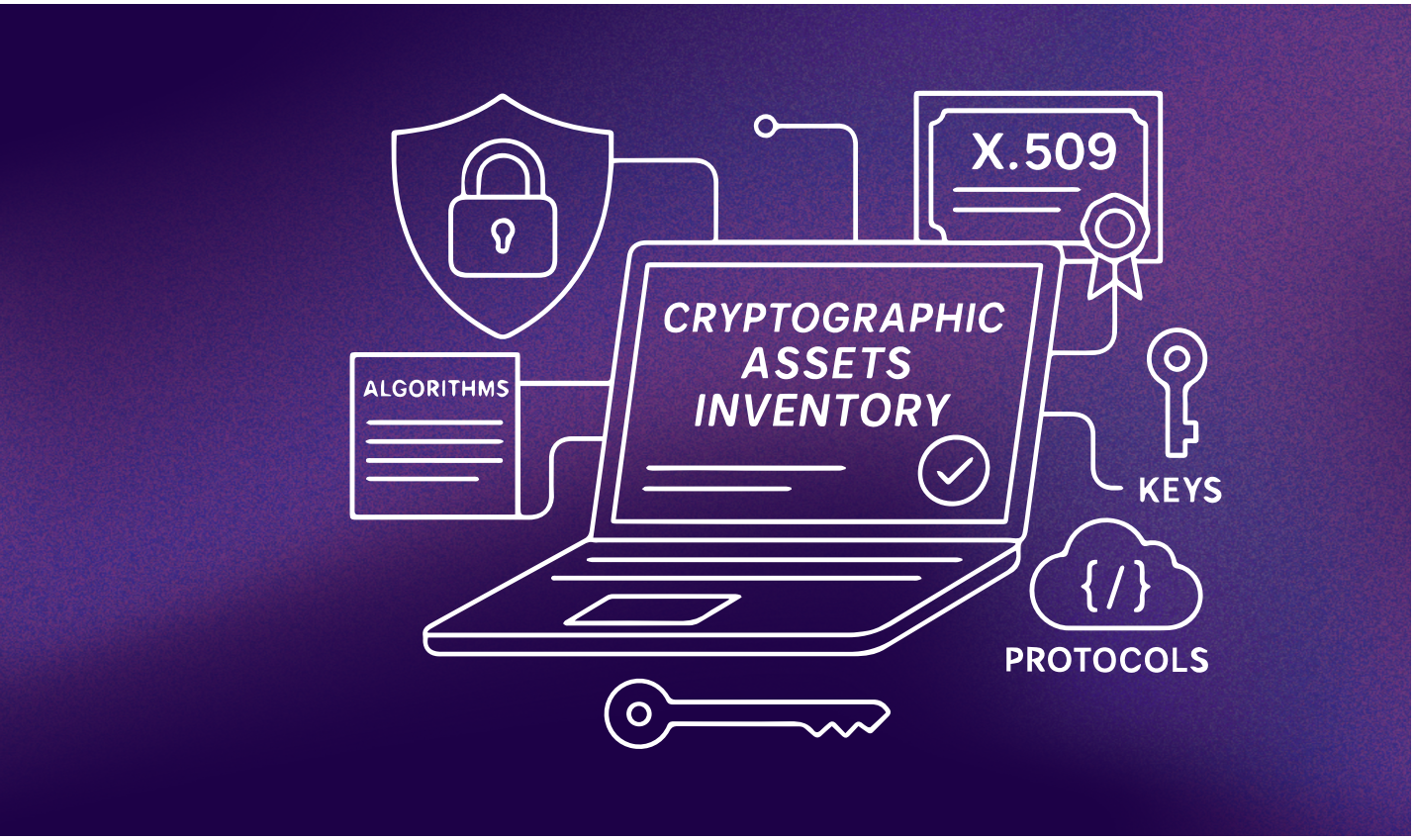
Die zunehmende Bedeutung kryptographischer Verfahren für die funktionale und regulatorische Sicherheit moderner IT-Systeme erfordert eine strukturiertere Form der Dokumentation. Als Analogie zur Software Bill of Materials (SBOM) etabliert sich das Konzept einer Cryptographic Bill of Materials (CBOM).

Eine CBOM beschreibt sämtliche kryptographischen Komponenten eines Systems. Dazu gehören die eingesetzten Algorithmen, das Schlüsselmaterial sowie die Protokolle, Zertifikate und Bibliotheken. Ziel ist es, kryptographische Abhängigkeiten transparent darzustellen und im Sinne eines sicheren Systemdesigns nachvollziehbar zu dokumentieren.

Durch eine CBOM schaffen Organisationen die Basis für eine Migration aktueller Verfahren in Richtung Post-Quanten-Kryptographie. Nur wer die eingesetzte Kryptographie systematisch erfasst hat, kann fundiert entscheiden, welche Komponenten durch PQC-geeignete Alternativen ersetzt oder angepasst werden müssen.

Darüber hinaus erlaubt eine CBOM eine risikobasierte Bewertung. Veraltete Verfahren oder fehlerhafte Konfigurationen lassen sich gezielt identifizieren und priorisieren. Damit wird die technische und zudem die organisatorische Handlungsfähigkeit im Umgang mit kryptographischen Risiken gestärkt. Zudem erfüllen Unternehmen und Behörden, die der Umsetzung des IT-Grundschutzes unterliegen, zwei zentrale Anforderungen aus dem Baustein CON.1 – Kryptokonzept (CON.1.A15 und CON.1.A19).

Das Konzept ist prinzipiell etabliert. In vielen Organisationen fehlte allerdings bislang die methodische Umsetzung. Hier helfen standardisierte Formate wie CycloneDX. Sie vereinfachen den Informationsaustausch und ermöglichen automatisierte Prozesse.



CYCLONEDX: DER DE-FACTO-STANDARD

Beispielhafte Darstellung einer CBOM im CycloneDX-Format

Wer kryptographische Komponenten im Sinne einer CBOM systematisch erfassen möchte, nutzt dafür am besten ein geeignetes maschinenlesbares Format. CycloneDX, ursprünglich als Standard zur Beschreibung von Software-Stücklisten (SBOM) entwickelt, hat sich auch beim Aufbau und Führen eines Kryptoinventars bewährt.

Seit Version 1.6 unterstützt CycloneDX eine dedizierte Modellierung kryptographischer Komponenten. Dazu zählen Algorithmen, Protokolle, Zertifikate und kryptographisches Material, wie z. B. Schlüssel. Die Erweiterung wurde gezielt eingeführt, um CBOM-Anforderungen abzubilden und bestehende Strukturen aus der SBOM-Welt wiederzuverwenden.

CycloneDX besitzt einige wichtige Vorzüge. Einer ist die Kompatibilität mit anderen IT-Werkzeugen und Ökosystemen. Das technische Format lässt sich in CI/CD-Pipelines, Container-Scans oder Software-analyse-Tools integrieren. Organisationen können damit die Erfassung kryptographischer Komponenten in bestehende Prozesse einbinden, ohne Parallelstrukturen aufbauen zu müssen. Darüber hinaus trägt das strukturierte Datenmodell zur Standardisierung und Vergleichbarkeit von CBOMs bei. Für die Weitergabe an Partnerunternehmen, Aufsichtsbehörden oder interne Governance-Prozesse ist das von großer Bedeutung.

CycloneDX ist damit mehr als ein technisches Format. Es ist ein strategisches Werkzeug zur Operationalisierung kryptographischer Transparenz.

KRYPTOREGISTER – VON DER FORSCHUNG PROFITIEREN

Unternehmen und Behörden müssen beim Aufbau eines Kryptoregisters nicht bei null beginnen. Es gibt bereits zahlreiche Institute und Forschende, die sich mit dem Thema Inventarisierung wissenschaftlich und praktisch befassen.

Die Autorinnen und Autoren des Papers „On Criteria and Tooling for Cryptographic Inventories" (Schmitt et al., Prof. Wiesmaier u. a., Hochschule Darmstadt; researchgate.net, UCS) formulieren konkrete Kriterien, die ein Kryptoregister erfüllen muss, z. B. in Bezug auf Vollständigkeit, Aktualisierbarkeit, Nutzbarkeit und Wiederverwendbarkeit. Ein Inventar berührt demnach fünf zentrale Domänen:

- Softwareanwendungen,
- vernetzte Hardware,
- Netzwerkkommunikation,
- gespeicherte Daten sowie den
- Anwendungsquellcode.

Prototypen zur teilautomatisierten Inventarisierung werden ebenfalls vorgestellt (researchgate.net).

Die aktuelle Arbeit Cryptoscope (Moffie et al., 2025) widmet sich der statischen Analyse von Quellcode, um kryptographische Assets automatisiert zu identifizieren und zu klassifizieren. In mehr als 92 Prozent der getesteten Projekte gelingt das zuverlässig, einschließlich Algorithmen, Schlüsselmaterial und Nonces (arXiv). Damit ist ein klarer technologischer Trend erkennbar: Das Führen eines Kryptoinventars ist immer seltener ein manueller Akt.

Die Forschenden Hohm, Heinemann und Wiesmaier bieten zudem ein Crypto Agility-Maturity Modell (CAMM). Es hilft Organisationen, den Stand ihrer Kryptomigrationsplanung strukturiert zu bewerten und weiterzuentwickeln (researchgate.net, CAMM).

LEITPLANKEN FÜR EIN KRYPTOREGISTER:

- Ein Kryptoregister sollte systematisch alle kryptographischen Assets in allen Teilbereichen erfassen (Software, Hardware, Protokolle usw.).
- Die Nutzung standardisierter Formate wie CycloneDX ermöglicht Automatisierung und Integration in bestehende Risk- und Compliance-Prozesse.
- Bewertungsmethoden wie das Capability Maturity Model (CMM) bieten Governance-Mechanismen und helfen bei der Priorisierung von Migrationsmaßnahmen.

NÄCHSTE STUFE:
KRYPTOREGISTER-AGENTEN

Das vollständige und systematische Vorgehen beim Erstellen eines Kryptoregisters ist ein wichtiger Schritt in Richtung einer postquantenresilienten IT. Standardisierte Formate wie CycloneDX und erste Werkzeuge zur Analyse kryptographischer Abhängigkeiten vereinfachen die Arbeit.

Das Ziel sollte allerdings die vollständig automatisierte Erhebung der Krypto-Assets in Echtzeit und über Systemgrenzen hinweg sein. Insbesondere in heterogenen IT-Umgebungen, die sich aus Eigenentwicklungen, Open-Source-Komponenten, Legacy-Systemen und Drittanbieterprodukten zusammensetzen, stößt jede manuelle oder halbautomatisierte Erfassung an Grenzen. Die Komplexität, Dynamik und fehlende Durchgängigkeit technischer Schnittstellen machen eine kontinuierliche, systemweite Transparenz derzeit schwer realisierbar.

Ein möglicher nächster Entwicklungsschritt liegt daher in der Konzeption und Entwicklung eines agentenbasierten Ansatzes: ein intelligenter Dienst, der kryptographische Artefakte laufend erkennt, klassifiziert, mit Kontext anreichert und direkt in eine CBOM überführt – idealerweise mit Integrationspunkten zu DevSecOps-Prozessen, Systemmanagement oder ISMS-Strukturen.

Ein solches Projekt befindet sich derzeit in einem frühen Planungsstadium. Es schafft methodisch tragfähige Grundlagen, um eine automatisierte, anwendungsnahe Kryptoinventarisierung zu entwickeln – mit Fokus auf Umsetzbarkeit im Alltag von Unternehmen und Behörden.

Um das Potenzial in der Praxis zu nutzen, braucht es die Zusammenarbeit zwischen Forschung, Tech-Playern und den anwendenden Unternehmen und öffentlichen Verwaltungen. Die Richtung ist jedenfalls klar: Kryptographische Transparenz sollte zukünftig stärker von Technik gestützt geschaffen werden und Teil der operativen Arbeit sein.

ANSPRECHPARTNER

SEBASTIAN KAVALIR
Senior Consultant Cybersecurity
Sopra Steria

Sopra Steria SE
Hans-Henny-Jahnn-Weg 29
22085 Hamburg
T. 040 22703-0
E. info.de@soprasteria.com

www.soprasteria.com