Bundesverband IT-Sicherheit e.V.

TeleTrusT
Pioneers in IT security.

Kryptoagilität

Handreichung

2026

Danksagung

TeleTrusT bedankt sich bei den nachstehenden Personen für ihre Mitwirkung in der TeleTrusT-Arbeitsgruppe "Kryptoagilität" sowie für die aktive Mitgestaltung dieser Handreichung.

Projektleitung

Fehenberger, Dr. Tobias - Adva Network Security

Autoren und mitwirkende Experten (Auszug)

Abou Nasser, Morad - Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Demirel, Dr. Denise - Accenture
Klaußner, Jan - Bundesdruckerei
Kowol, Dominik - eperi
Minder, Daniel - evolutionQ
Mühlbauer, Holger - Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Rödiger, Jasper - Rohde & Schwarz Cybersecurity
Rosbach, Felix - comforte
Schröter, Jannes - Rohde & Schwarz Cybersecurity
Zügel, Werner - essendi it

Dieses Dokument dient als Anhaltspunkt und bietet einen Überblick. Er erhebt weder Anspruch auf Vollständigkeit noch auf die exakte Auslegung der bestehenden Rechtsvorschriften. Er darf nicht das Studium der relevanten Richtlinien, Gesetze und Verordnungen ersetzen. Des Weiteren sind die Besonderheiten der jeweiligen Produkte sowie deren unterschiedliche Einsatzmöglichkeiten zu berücksichtigen. Insofern sind bei den im Dokument angesprochenen Beurteilungen und Vorgehensweisen eine Vielzahl weiterer Konstellationen denkbar.

Impressum

Herausgeber:

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Chausseestraße 17
10115 Berlin
Tel.: +49 30 4005 4310
E-Mail: info@teletrust.de
https://www.teletrust.de

© 2026 TeleTrusT

Inhaltsverzeichnis

1 Executive Summary 4

2 Einleitung 6
2.1 Relevanz von Kryptografie 6
2.1.1 Allgegenwärtigkeit von kryptografischen Verfahren 6
2.1.2 Bedrohungen für kryptografische Verfahren 7
2.1.3 PQC ist eine Kryptorevolution 7
2.2 Definition Kryptoagilität 8
2.3 Anwendungsbereich der Handreichung 9
2.4 Hintergrundwissen 9
2.4.1 Regulatorische Vorgaben 9
2.4.2 Standards und Empfehlungen (Best Practices): 10

3 Umsetzung von Kryptoagilität für Anwender 12
3.1 Kryptoobjekt 12
3.2 Kryptostrategie 12
3.3 Interne Sicherheitsvorgaben und -prozesse 13
3.4 Kryptoinventar zur Verwaltung von Kryptoobjekten 14
3.4.1 Motivation 14
3.4.2 Ausprägungen und Kriterien 15
3.4.3 Auskunftsformate für Herstellerprodukte 16
3.4.4 Inventarprozesse 17
3.5 Kontinuierliche Verbesserung der Sicherheit der eingesetzten Kryptoobjekte 18
3.5.1 Identifizieren von Verbesserungspotentialen 18
3.5.2 Risikoorientierte Priorisierung von Verbesserungspotentialen 19
3.5.3 Planung der Umsetzung von Verbesserungspotentialen und Migrationen 20
3.5.4 Umsetzen von Verbesserungspotenzialen und Durchführen von Migrationen 20

4 Umsetzung von Kryptoagilität für Hersteller 22
4.1 Motivation 22
4.2 Anforderungen an Architektur 22
4.3 Update-Konzept 23
4.3.1 Update-Arten 23
4.3.2 Update-Aspekte 24
4.4 Weitere Anforderungen an den Hersteller 24
4.5 Abhängigkeitsbetrachtung 25
4.5.1 Fremdkomponenten 25
4.5.2 Externe/standardisierte Schnittstellen 25

5 Zusammenfassung 26

1 Executive Summary

Die vorliegende Handreichung ordnet Kryptoagilität als strategische Fähigkeit zur nachhaltigen Steuerung kryptografischer Risiken ein.

Sie adressiert die wachsende Notwendigkeit, kryptografische Verfahren unter veränderten Bedrohungslagen, regulatorischen Anforderungen und technologischen Entwicklungen kontrolliert und mit vertretbarem Aufwand anpassen zu können.

Relevanz
Kryptografie unterstützt die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität digitaler Geschäftsprozesse und ist damit unmittelbar geschäftskritisch.

Da kryptografische Verfahren durch Schwachstellen, neue Analyseverfahren, steigende Rechenleistung und insbesondere durch die Migration in Richtung Post-Quanten-Kryptografie an Wirksamkeit verlieren können, entsteht für Organisationen ein fortlaufender Anpassungsbedarf.

Vor diesem Hintergrund ist Kryptoagilität nicht als einmaliges technisches Vorhaben, sondern als dauerhafte organisatorische und technische Steuerungsfähigkeit zu verstehen.

Die Handreichung betont ausdrücklich, dass Migrationen nicht als singuläre Projekte behandelt werden sollten, sondern in belastbare Prozesse zu überführen sind, damit zukünftige Umstellungen beherrschbar bleiben.

Was ist Kryptoagilität
Kryptoagilität wird als Prozess verstanden, durch den Hersteller und Anwender sicherheitsrelevante kryptografische Bestandteile eines IT-Systems effizient austauschen können, ohne die Kernfunktionalitäten zu beeinträchtigen.

Diese Fähigkeit umfasst nicht nur Algorithmen, sondern sämtliche relevanten Kryptoobjekte wie Protokolle, Zertifikate, Schlüssel, Parameter, kryptografische Module und Bibliotheken.

Die Handreichung macht deutlich, dass Kryptoagilität nur dann wirksam ist, wenn organisatorische Verantwortlichkeiten, technische Umsetzbarkeit und belastbare Entscheidungsprozesse zusammenwirken. Sie ist damit ein Bestandteil moderner Sicherheitsarchitektur und kein isoliertes Software-Update-Thema.

Erforderliche Steuerungselemente
Für Anwenderorganisationen werden vier zentrale Steuerungselemente hervorgehoben: eine Kryptostrategie, eine (aktualisierte) Kryptorichtlinie, ein strukturiertes Kryptoinventar sowie ein kontinuierlicher Verbesserungs- und Migrationsprozess.

Die Kryptostrategie definiert Ziele, Handlungsfelder, Ressourcenbedarf, Abhängigkeiten und Prioritäten für die Entwicklung der Organisation in Richtung Kryptoagilität.

Die Kryptorichtlinie ist ein zentrales, internes Vorgabendokument, das u.a. festlegt, welche kryptografischen Verfahren zulässig sind und dokumentiert, auf Basis welcher Sicherheitsanforderungen sie ausgewählt wurden.

Das Kryptoinventar bildet die operative Grundlage für Transparenz und Steuerbarkeit, indem es eingesetzte Kryptoobjekte, ihre Relationen, ihre Compliance-Eigenschaften und ihren Migrationsbedarf sichtbar macht.

Auf dieser Basis können Risiken bewertet, Verbesserungsbedarfe priorisiert und Migrationsmaßnahmen planvoll umgesetzt werden.

Anforderungen an Hersteller und Lieferkette
Die Handreichung adressiert Kryptoagilität ausdrücklich auch als Herstellerverantwortung.

Produkte und Komponenten sollen so entworfen werden, dass kryptografische Funktionen abstrahiert, modular integriert, konfigurierbar oder kontrolliert austauschbar sind und durch sichere Standardeinstellungen, Update-Konzepte sowie geeignete Tests abgesichert werden.

Zusätzlich unterstreicht das Dokument die Bedeutung von Transparenz entlang der Lieferkette, insbesondere bei der Nutzung von Fremdkomponenten und kryptografischen Bibliotheken.

Herstellerseitige Informationen wie maschinenlesbare Auskunftsformate zu enthaltenen Krypto-Bausteinen können den Aufbau und die Pflege eines organisationsweiten Kryptoinventars wesentlich unterstützen.

Regulatorische Einordnung
Die Handreichung verortet Kryptoagilität im Kontext nationaler und europäischer Anforderungen sowie anerkannter Standards, unter anderem der DSGVO, des IT-Sicherheitsgesetzes, des Cybersecurity Acts, der MiCAR, DORA, NIS-2, BSI-Empfehlungen, NIST-Veröffentlichungen und ISO/IEC 27001. Aus dieser Perspektive ist Kryptoagilität als Ausdruck des Stands der Technik bzw. als notwendige Umsetzungsfähigkeit einzuordnen.

Für das Management ergibt sich daraus, dass Kryptoagilität nicht nur zur technischen Risikominimierung beiträgt, sondern auch die regulatorische Belastbarkeit, Auditierbarkeit und Zukunftsfähigkeit der Sicherheitsarchitektur stärkt.

Einordnung für Entscheidungen
Aus Managementsicht ist Kryptoagilität als dauerhaftes Transformations- und Governance-Thema zu behandeln.

Prioritär sind klare Verantwortlichkeiten, belastbare Beschaffungsanforderungen, ein risikoorientierter Migrationsansatz sowie die Verankerung kryptoagiler Prinzipien in Architektur, Betrieb und Sicherheitsvorgaben.

Die Handreichung liefert damit einen belastbaren Orientierungsrahmen, um kryptografische Abhängigkeiten systematisch transparent zu machen, regulatorische Anforderungen resilient zu erfüllen und die eigene Organisation auf die PQC-Transformation sowie weitere künftige Kryptografie-Migrationen vorzubereiten.

2 Einleitung

2.1 Relevanz von Kryptografie

2.1.1 Allgegenwärtigkeit von kryptografischen Verfahren

Kryptografie ist ein zentraler Baustein, um die grundlegenden Schutzziele der Informationssicherheit - Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität - zu gewährleisten, wie sie unter anderem vom BSI im IT-Grundschutz beschrieben werden. Durch Verschlüsselung, Signaturen, Zertifikate und die daraus abgeleiteten sicheren Protokolle und Anwendungen wird verhindert, dass Unbefugte Einsicht in sensible Informationen gewinnen oder diese unbemerkt manipulieren können.

Damit schützt Kryptografie sensible Daten wie Verträge, personenbezogene Daten oder interne Strategien vor Diebstahl und Manipulation, sowohl bei der Speicherung als auch bei der Übertragung und teilweise auch während der Verarbeitung.

Gespeicherte Daten finden sich in der Regel auf Datenträgern, die sich wiederum häufig in Geräten, wie beispielsweise Servern, Workstations und Laptops, aber auch in Smartphones und Tablets befinden. Dies kann auf mehreren Ebenen erfolgen. Eine Möglichkeit ist die komplette Verschlüsselung des Datenträgers auf Ebene der Hardware, bei der alle Daten verschlüsselt werden. Eine weitere Möglichkeit ist die Verschlüsselung einzelner Daten auf Anwendungs- oder Plattformebene, beispielsweise einzelner Einträge einer Datenbank. Entsprechende Möglichkeiten gibt es auch für die Speicherinfrastruktur der Cloudanbieter. Backups und Archive werden meist ebenfalls durch die entsprechende Verwaltungs-Software verschlüsselt.

Die Verschlüsselung von Daten während ihrer Übertragung kann auf verschiedenen Netzwerkebenen erfolgen: zwischen zwei direkt verbundenen Kommunikationspartnern auf einer niedrigen Ebene, z.B. mit MACsec oder WLAN-Verschlüsselung, zwischen weiter entfernten Partnern über einen Tunnel, z.B. mit IPSec, oder auch auf höheren Ebenen zwischen Anwendungen, zum Beispiel mit TLS oder E-Mail-Verschlüsselung. Bei der Vernetzung von Standorten oder der Anbindung an Rechenzentren wird der Schutz typischerweise auf niedrigeren Ebenen umgesetzt. Mobile Geräte werden häufig über Tunnel an feste Infrastrukturen angebunden. Anwendungen wie E-Mail, Browser, Instant Messaging, Videokonferenzen oder VoIP bringen ihre eigenen Schutzmechanismen mit.

Der Schutz von Daten während ihrer Verarbeitung kann durch Trusted Execution Environments unterstützt werden. Je nach Plattform kombinieren diese Ausführungsisolation, Zugriffskontrolle und gegebenenfalls Speicherverschlüsselung. Zusätzlich muss sichergestellt werden, dass nur autorisierter Code auf die geschützten Daten zugreifen kann. Digitale Signaturen können dabei die Integrität und Authentizität des ausgeführten Codes unterstützen.

Die Digitalisierung von Geschäftsprozessen wurde und wird durch Kryptografie aber auch erst möglich: Elektronische Rechnungen, digitale Unterschriften, Online-Banking, digitale Identitäten und Zugangskontrollsysteme funktionieren nur zuverlässig, wenn Vertraulichkeit und Integrität der Daten dauerhaft gewährleistet sind und die Authentizität von Absendern und Dokumenten belegt werden können.

Auch neue Geschäftsmodelle entstehen erst durch Kryptografie, beispielsweise Pay-TV oder Distributed-Ledger-Technologien wie Smart Contracts oder Kryptowährungen.

Wichtig ist bei allen Anwendungen die sichere Speicherung privater Schlüssel. Je nach Bedrohungsmodell, Schutzbedarf und Einsatzszenario können hierfür beispielsweise Trusted Platform Modules (TPMs), Hardware-Sicherheitsmodule (HSMs) oder geeignete Cloud-Schlüsseldienste eingesetzt werden.

2.1.2 Bedrohungen für kryptografische Verfahren

Der Blick in die Vergangenheit zeigt, dass kryptografische Verfahren nicht dauerhaft sicher bleiben müssen. Dies kann verschiedenste Gründe haben.

Zum einen kann die konkrete Implementierung fehlerhaft sein und beispielsweise Timing-Angriffe ermöglichen oder "schlechte" Zufallszahlen erzeugen. Darüber hinaus können präzisere Messmethoden oder neue Analyseverfahren neue Angriffsvektoren eröffnen. Zum anderen kann auch das Verfahren an sich durch Fortschritte in der Kryptoanalyse unsicherer werden, die z.B. zu einer Reduktion des Schlüsselraums führen. Auch Probleme in begleitenden Verfahren können für Angriffe genutzt werden. So wurden mehrere Padding-Varianten für das RSA-Kryptosystem entwickelt, um verschiedene Angriffe abzuwehren.

Gleichzeitig steigt die Leistungsfähigkeit von Angreifern kontinuierlich: Rechenleistung und spezialisierte Hardware verkürzen die Sicherheitsreserven klassischer Verfahren. So wurde DES zuerst durch Triple-DES und dann durch AES abgelöst, um Brute-Force-Angriffen entgegenzuwirken. Künftige Quantencomputer verstärken dieses Problem. Shors Algorithmus bedroht klassische asymmetrische Verfahren, während Grovers Algorithmus die effektive Sicherheit symmetrischer Verfahren reduziert.

Kryptografische Algorithmen erhalten somit ein "Ablaufdatum" und verlieren mit der Zeit an Schutzwirkung.

Um langfristig sichere Geschäftsprozesse zu gewährleisten, müssen Organisationen daher ihre Kryptografie regelmäßig prüfen, Schlüsselstärken anpassen und veraltete Algorithmen systematisch durch moderne, auch Post-Quanten-Verfahren ersetzen. Damit einher geht auch die Anpassung des notwendigen Schlüsselmaterials. Kryptoagile Architekturen schaffen für beides die Grundlage.

2.1.3 PQC ist eine Kryptorevolution

Mit der Einführung von Post-Quanten-Kryptografie (PQC) stehen Organisationen vor einem tiefgreifenden Umbruch, der über einen bloßen Algorithmuswechsel hinausgeht. Während klassische kryptografische Verfahren über Jahrzehnte hinweg analysiert und in stabilen Infrastrukturen verankert wurden, sind mit ML-KEM, ML-DSA und SLH-DSA seit 2024 erste zentrale PQC-Verfahren standardisiert. Ihre breite praktische Einführung und langfristige Betriebserfahrung befinden sich jedoch noch im Aufbau. Gleichzeitig verschärfen zwei Szenarien den Handlungsdruck: Zum einen können Angreifer bereits heute mit klassischen Methoden verschlüsselte, sensible Daten abschöpfen, um sie in Zukunft zu entschlüsseln ("Harvest Now, Decrypt Later" - HNDL). Zum anderen können mit klassischen Verfahren erzeugte digitale Signaturen in Zukunft gefälscht werden und so historische Daten geändert, gefälschte Zertifikate ausgestellt und zur Identifikation genutzt oder gefälschte bösartige Software installiert werden ("Trust Now, Forge Later" - TNFL). Daraus ergibt sich eine doppelte Unsicherheit: Bestehende Verfahren verlieren perspektivisch an Sicherheit, während neue Verfahren noch nicht in allen Einsatzszenarien umfassend betrieblich erprobt sind. In diesem Spannungsfeld wird Kryptoagilität zur zentralen Fähigkeit, um kryptografische Verfahren strukturiert, wiederholbar und mit vertretbarem Aufwand austauschen zu können.

Hybride Verfahren können den Übergang zu Post-Quanten-Kryptografie absichern, ersetzen jedoch nicht die dauerhafte Fähigkeit, kryptografische Komponenten kontrolliert auszutauschen. Die im Zuge der PQC-Migration etablierten Prozesse sollten daher verstetigt werden.

2.2 Definition Kryptoagilität

Die in Kapitel 2.1 "Relevanz von Kryptografie" dargestellte Bedeutung, Veränderlichkeit und Post-Quanten-Transformation kryptografischer Verfahren erfordern die Fähigkeit, kryptografische Bestandteile kontrolliert anzupassen. Diese Fähigkeit wird im Folgenden als Kryptoagilität definiert.

Kryptoagilität beschreibt einen Prozess bei Herstellern und Anwendern von IT-Systemen, bei dem als Reaktion auf externe Einflüsse sicherheitsrelevante kryptografische Bestandteile eines IT-Systems effizient angepasst werden können, ohne dessen Kernfunktionalitäten zu beeinträchtigen.

Kryptoagilität ist keine rein technische Eigenschaft eines IT-Systems, sondern eine gemeinsame, fortlaufende Fähigkeit von Herstellern und Anwendern, kryptografische Sicherheitsmechanismen unter veränderten Rahmenbedingungen kontrolliert anzupassen. Aus der oben genannten Definition ergeben sich fünf Kernelemente: die gemeinsame Verantwortung von Herstellern und Anwendern, kontinuierliche Prozesse, die Reaktion auf externe Einflüsse, die Einbeziehung aller sicherheitsrelevanten kryptografischen Bestandteile sowie der Erhalt der fachlichen Kernfunktionalität und Betriebsfähigkeit.

Die gemeinsame Verantwortung wird in Kapitel 3 "Umsetzung von Kryptoagilität für Anwender" für Anwender und Kapitel 4 "Umsetzung von Kryptoagilität für Hersteller" für Hersteller konkretisiert. Anwender sind hier als Organisationen zu verstehen, die kryptografische Produkte beziehungsweise Systeme beschaffen, konfigurieren und betreiben. Hersteller hingegen sind Organisationen, die solche Systeme oder Komponenten entwickeln und bereitstellen. Eine Organisation kann zugleich beide Rollen einnehmen, etwa wenn sie eigene Systeme entwickelt und hierfür Fremdkomponenten verwendet. Hersteller tragen daher die Verantwortung, kryptografische Sicherheitsmechanismen in Systemen, Produkten und Komponenten so zu entwerfen, dass diese grundsätzlich austauschbar oder konfigurierbar sind. Anwender wiederum müssen organisatorisch und technisch in der Lage sein, entsprechende Änderungen im Betrieb umzusetzen. Kryptoagilität ist damit keine isolierte Entwicklungsanforderung, sondern eine gemeinsame Aufgabe entlang des gesamten Lebenszyklus eines IT-Systems, vom Design bis zum End-of-Life.

Als Prozess ist Kryptoagilität nicht mit einer einzelnen Migration abgeschlossen. Kryptografische Abhängigkeiten sind vielmehr fortlaufend zu identifizieren, zu bewerten und bei Bedarf anzupassen. Die hierfür erforderlichen Steuerungs- und Migrationsprozesse werden in Kapitel 3 "Umsetzung von Kryptoagilität für Anwender" näher beschrieben.

Externe Einflüsse, die eine solche Anpassung erforderlich machen, sind insbesondere neue Schwachstellen, geänderte regulatorische Vorgaben und Standards sowie technologische Entwicklungen. Die maßgeblichen Bedrohungen und die PQC-Transformation wurden bereits in den Kapiteln 2.1.2 "Bedrohungen für kryptografische Verfahren" und 2.1.3 "PQC ist eine Kryptorevolution" näher erläutert.

Die Definition erfasst sämtliche sicherheitsrelevanten kryptografischen Bestandteile eines IT-Systems und nicht nur einzelne Algorithmen. In dieser Handreichung werden diese als Kryptoobjekte bezeichnet und in Kapitel 3.1 "Kryptoobjekt" konkretisiert.

Die Anpassung soll die fachliche Kernfunktionalität sowie die erforderliche Betriebsfähigkeit, Interoperabilität und Verfügbarkeit eines Systems erhalten. Daraus folgt, dass kryptografische Mechanismen möglichst von fachlichen Kernprozessen entkoppelt gestaltet werden sollten. Die daraus folgenden technischen Gestaltungsanforderungen behandelt Kapitel 4.2 "Anforderungen an Architektur".

Dieses Begriffsverständnis erweitert den vorwiegend technischen Fokus bestehender Definitionen von BSI, NIST und ETSI um die organisatorische Prozessperspektive. Gemeinsam ist den Ansätzen die kontrollierte Anpassungs- und Migrationsfähigkeit kryptografischer Bestandteile, ohne tiefgreifende Änderungen an der übrigen Systemarchitektur. Kryptoagilität schafft damit die Voraussetzung, kryptografische Sicherheit über den gesamten Lebenszyklus eines IT-Systems wirksam und anpassungsfähig zu erhalten.

2.3 Anwendungsbereich der Handreichung

Diese Handreichung zeigt, wie Organisationen Kryptoagilität organisatorisch und technisch aufbauen und dauerhaft in ihre Sicherheitsarchitektur sowie in bestehende Sicherheits- und IT-Prozesse integrieren können. Sie richtet sich an Anwender und Hersteller kryptografischer Systeme und beschreibt organisatorische wie technische Maßnahmen, mit denen kryptografische Komponenten bei neuen Bedrohungen, regulatorischen Anforderungen oder technologischen Entwicklungen effizient und mit vertretbarem Aufwand angepasst oder ausgetauscht werden können.

Voraussetzung hierfür sind etablierte grundlegende IT-Sicherheitsprozesse, darunter Best Practices bei der Produktentwicklung, etwa in den Bereichen Software-Architektur, Dokumentation und Tests, sowie ein geeignetes Konfigurationsmanagement beim Einsatz von Produkten, beispielsweise für Versionsmanagement einschließlich Abhängigkeiten, Update-Management und Assetmanagement. Darauf aufbauend behandelt die Handreichung die strategische Planung kryptografischer Verfahren, deren Verankerung in internen Vorgaben, die Schaffung von Transparenz durch ein Kryptoinventar sowie die kontinuierliche Bewertung, Verbesserung und Migration eingesetzter kryptografischer Komponenten.

Der Fokus dieses Dokuments liegt insbesondere auf der Fähigkeit, kryptografische Verfahren kontrolliert und mit vertretbarem Aufwand austauschen zu können: Dies wird durch die Entwicklung einer Kryptostrategie, die Anpassung interner Vorgaben, den Aufbau und Betrieb eines Kryptoinventars, die kontinuierliche Verbesserung der eingesetzten Kryptoobjekte sowie die Planung und Durchführung von Migrationen, etwa im Kontext der Post-Quanten-Kryptografie, ermöglicht. Dabei wird zwischen Anwendern und Herstellern unterschieden; für eine Organisation können beide Rollen gleichzeitig zutreffen.

Nicht betrachtet werden andere IT-Sicherheitsmaßnahmen rund um Angriffserkennung und -abwehr wie zum Beispiel Intrusion-Detection-Systeme oder Firewalls.

2.4 Hintergrundwissen

2.4.1 Regulatorische Vorgaben

Kryptografie allgemein und Kryptoagilität im Speziellen sind für die Erfüllung verschiedener nationaler und europäischer Anforderungen relevant, die im Folgenden aufgeführt werden. Kryptoagilität wird darin häufig nicht explizit genannt, kann jedoch als erforderliche Umsetzungsfähigkeit zur fortlaufenden Anpassung kryptografischer Maßnahmen an den Stand der Technik abgeleitet werden. Als Referenz für den Stand der Technik kann z.B. die Handreichung "Stand der Technik" von TeleTrusT[1] (Stand 2026, Kapitel 3.2.4) herangezogen werden, in der Kryptoagilität als zwingend erforderlich deklariert wird.

Gesetzliche Vorgaben (insbesondere in Deutschland und der EU):

- **Datenschutz-Grundverordnung (DSGVO):**
  Art. 32 DSGVO fordert "geeignete technische und organisatorische Maßnahmen" (TOMs) zum Schutz personenbezogener Daten. Dazu gehört auch der Einsatz von Kryptografie. "Geeignet" bedeutet hier, dass die Maßnahmen dem Stand der Technik entsprechen und kontinuierlich angepasst werden müssen. Dies impliziert die Notwendigkeit von Kryptoagilität, um auf neue Bedrohungen oder Schwachstellen reagieren zu können.

- **IT-Sicherheitsgesetz (ITSG) in Deutschland:**
  Das ITSG verpflichtet Betreiber kritischer Infrastrukturen (KRITIS) zur Implementierung angemessener Sicherheitsmaßnahmen, die dem Stand der Technik entsprechen. Auch hier ist die kontinuierliche Anpassung der Kryptografie ein impliziter Bestandteil. Für die Meldepflichten bei Sicherheitsvorfällen ist es von Vorteil, wenn Unternehmen durch Kryptoagilität in der Lage sind, schnell auf Schwachstellen zu reagieren und die Auswirkungen zu minimieren.

- **Cybersecurity Act (EU):**
  Der CSA schafft einen EU-weiten Rahmen für die Cyber-Sicherheitszertifizierung von IKT-Produkten, -Diensten und -Prozessen. Obwohl er keine direkten Anforderungen an die Kryptoagilität stellt, erleichtert Kryptoagilität die fortlaufende Aufrechterhaltung des im Rahmen einer

[1] https://www.teletrust.de/publikationen/broschueren/stand-der-technik/

Zertifizierung geforderten Sicherheitsniveaus, insbesondere wenn kryptografische Verfahren angepasst oder ersetzt werden müssen.

- **MiCAR (Markets in Crypto-Assets Regulation - EU):**
  Reguliert Krypto-Assets und die damit verbundenen Dienstleistungen in der EU. Auch wenn der Fokus auf Marktregulierung und Anlegerschutz liegt, sind Anbieter von Krypto-Dienstleistungen (CASPs) implizit angehalten, robuste Sicherheitsmaßnahmen - einschließlich aktueller kryptografischer Verfahren - umzusetzen, um Risiken für Nutzer und das System zu minimieren. Dies erfordert ebenfalls Kryptoagilität.

Des Weiteren gibt es verschiedene branchenspezifische Regulierungen, die die Anforderungen an Kryptoagilität für einen bestimmten Industriezweig weiter konkretisieren. So reguliert zum Beispiel die EU-Durchführungsverordnung 2024/2690 Cloudanbieter und andere Internetdienstleister und fordert von ihnen, soweit angemessen, einem "Krypto-Agilitätsansatz" zu folgen. DORA und nachgeordnete Verordnungen legen für die betroffene Finanzindustrie fest, dass kompromittierte oder nicht mehr geeignete kryptografische Verfahren kontrolliert ersetzt werden, was mit einer Forderung nach Kryptoagilität gleichzusetzen ist.

2.4.2 Standards und Empfehlungen (Best Practices):

Obwohl keine unmittelbaren Gesetze, gibt es einige Standards und Handlungsempfehlungen mit einem quasi-regulatorischen Charakter, da sie als "Stand der Technik" anerkannt werden und dadurch verpflichtende Anforderungen an Kryptografie und Kryptoagilität darstellen.

- BSI (Bundesamt für Sicherheit in der Informationstechnik) in Deutschland:
  - BSI IT-Grundschutz-Kompendium[2]**:**
    Enthält Bausteine und Empfehlungen für eine umfassende Informationssicherheit. Kryptografische Verfahren sind ein fester Bestandteil vieler Bausteine. Die Empfehlungen des BSI werden regelmäßig aktualisiert und berücksichtigen den aktuellen Stand der Technik, was die Anpassung der Kryptografie einschließt.
  - Technische Richtlinien (TR):
    Das BSI veröffentlicht spezifische Technische Richtlinien (z.B. TR-02102 "Kryptografische Verfahren: Empfehlungen und Schlüssellängen"[3]), die konkreten Empfehlungen zu Art und Stärke kryptografischer Verfahren geben. Diese werden regelmäßig überarbeitet, um neuen Erkenntnissen und Bedrohungen (z.B. Quantencomputing) Rechnung zu tragen. Die Fähigkeit, diese Empfehlungen umzusetzen, ist ein Kernaspekt der Kryptoagilität. Das BSI betont explizit die Bedeutung von Kryptoagilität, insbesondere im Hinblick auf Post-Quanten-Kryptografie.
  - Leitfäden zur Migration zur Post-Quanten-Kryptografie[4]:
    Das BSI gibt spezifische Handlungsempfehlungen für die Migration zu quantensicherer Kryptografie, was wiederum Kryptoagilität voraussetzt.

- NIST (National Institute of Standards and Technology) in den USA:
  - NIST spielt eine weltweit führende Rolle bei der Standardisierung kryptografischer Algorithmen. Ihre Veröffentlichungen (z.B. FIPS, SP 800-Reihe) sind international anerkannte Standards.
  - NIST SP 800-175B "Guidance for Using Cryptographic Standards in the Federal Government": Betont die Notwendigkeit, kryptografische Algorithmen flexibel einsetzen und bei Bedarf wechseln zu können.
  - NIST Post-Quantum Cryptography (PQC) Standardization Process:
    Die Standardisierung quantenresistenter Algorithmen ist ein Haupttreiber für die Kryptoagilität. Mit FIPS 203, FIPS 204 und FIPS 205 liegen seit 2024 erste finale Standards für ML-KEM, ML-DSA und SLH-DSA vor. Organisationen sollten daher deren risikoorientierte Einführung vorbereiten.

- ISO/IEC 27001 (Informationssicherheits-Managementsysteme):

[2] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html
[3] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html
[4] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Post-Quanten-Kryptografie.html

    - Obwohl ISO 27001 nicht direkt "Kryptoagilität" vorschreibt, fordert sie die Implementierung eines Informationssicherheits-Managementsystems (ISMS), das die kontinuierliche Verbesserung und Anpassung von Sicherheitsmaßnahmen (einschließlich Kryptografie) an neue Risiken und Technologien beinhaltet.
    - Anhang A Maßnahme 8.24 der ISO 27001:2024 verpflichtet, Richtlinien und Verfahren für kryptografische Techniken festzulegen, was ebenfalls die Notwendigkeit von Prozessen für den Umgang mit sich ändernden Anforderungen und der Aktualisierung von Kryptografie impliziert.

- Branchenstandards und Best Practices:
    - PCI DSS (Payment Card Industry Data Security Standard): Fordert den Schutz von Kreditkartendaten, was starke Kryptografie erfordert. Änderungen in den Anforderungen oder der Kryptografie-Landschaft müssen hier schnell umgesetzt werden können.
    - OWASP Top 10: Ein hersteller- und branchenübergreifender Leitfaden für die sichere Entwicklung von Webanwendungen. Die OWASP Top 10 führen regelmäßig kryptografiebezogene Schwachstellen - etwa den Einsatz fehlerhafter oder veralteter kryptografischer Verfahren - als wesentliche Sicherheitsrisiken auf. Kryptoagilität unterstützt dabei, solche Verfahren kontrolliert durch sichere Alternativen zu ersetzen.

3 Umsetzung von Kryptoagilität für Anwender

Das folgende Kapitel erläutert die wesentlichen Aspekte, die Anwender bei der Umsetzung von Kryptoagilität für kryptografische Lösungen berücksichtigen sollten. Kapitel 3.1 erläutert den Begriff Kryptoobjekt. Kapitel 3.2 beschreibt die zentralen Fragestellungen für die Entwicklung einer Kryptostrategie, die Kryptoagilität angemessen berücksichtigt. Anschließend behandelt Kapitel 3.3 die erforderlichen Anpassungen der Sicherheitsvorgaben und -prozesse einer Organisation. Kapitel 3.4 widmet sich der Auswahl, dem Aufbau und dem Betrieb eines Kryptoinventars. Kapitel 3.5 erläutert schließlich, wie daraus resultierende Handlungsbedarfe identifiziert, priorisiert, geplant und umgesetzt werden.

3.1 Kryptoobjekt

Ein zentraler Begriff dieser Handreichung ist das "Kryptoobjekt". Darunter wird ein inventarisierbares kryptografisches Asset oder Artefakt verstanden, das kryptografische Funktionen bereitstellt, konfiguriert, verwendet oder absichert. Dazu zählen insbesondere Algorithmen - etwa Hashfunktionen, symmetrische und asymmetrische Verschlüsselung, digitale Signaturen - einschließlich ihrer Parameter, geheime oder private Schlüssel mitsamt ihrer Metadaten, Zertifikate, Protokolle, kryptografische Bibliotheken zur Implementierung kryptografischer Verfahren, Zufallszahlengeneratoren sowie Hardware-Sicherheitsmodule und Smartcards. Eine kryptografische Komponente bezeichnet hingegen eine technische Software- oder Hardware-Einheit, die ein oder mehrere Kryptoobjekte implementiert oder verwendet. Einzelne Zufallswerte, Klartexte und Chiffretexte gelten nicht als eigenständige Kryptoobjekte.

3.2 Kryptostrategie

Der erste Schritt für Anwender besteht darin, eine entsprechende Kryptostrategie[5] zu entwickeln, in der Kryptoagilität als angestrebtes Ziel verankert wird. Die Strategie beschreibt die angestrebten Teilziele, die erforderlichen Schritte, einen möglichen Zeitplan sowie den entsprechenden Ressourcenbedarf. Die Inhalte sind mit allen relevanten Stakeholdern abzustimmen, zu kommunizieren und kontinuierlich zu konkretisieren.

Bei Erstellung des Strategiepapiers sind insbesondere die folgenden Fragen zu klären:

- Welche Motivation hat die Organisation, in Kryptoagilität zu investieren und welche Ziele sollen dadurch erreicht werden?
- Wie ist der aktuelle Reifegrad der Kryptoagilität, insbesondere im Hinblick auf den Wechsel zwischen verschiedenen kryptografischen Algorithmen und Lösungen?
- Welche Handlungsfelder ergeben sich aus der Strategie?
- Welche Teilziele sollen bis zu welchem Zeitpunkt erreicht werden?
- Welche Ressourcen werden benötigt, um die Teilziele innerhalb des vorgesehenen Zeitraums zu erreichen?
- Welche Stakeholder sind einzubeziehen und welche Abhängigkeiten müssen berücksichtigt und gesteuert werden?

Zur Erreichung von Kryptoagilität sind verbindliche Grundsätze festzulegen. Ein zentraler Grundsatz ist die Etablierung eines kontinuierlichen Verbesserungsprozesses, der die Kryptoagilität von Assets und Prozessen bewertet und Verbesserungspotenziale identifiziert. Ziel ist es insbesondere, Aufwand und Dauer von Aktualisierungen kritischer Systeme fortlaufend zu reduzieren. Zugleich umfasst der Prozess die regelmäßige Bewertung, Priorisierung und Aktualisierung der eingesetzten Kryptoobjekte, um ein angemessenes Sicherheitsniveau zu gewährleisten und zeitnah auf Veränderungen in der Bedrohungslage reagieren zu können.

Ein weiterer Grundsatz betrifft die Integration neuer kryptografischer Verfahren. Sobald diese standardisiert und für den jeweiligen Einsatzzweck geeignet sind, sollten sie in bestehende Lösungen integriert

[5] In Abgrenzung zum vom BSI im IT-Grundschutz-Baustein CON.1 explizit erwähnten Kryptokonzept definiert eine Kryptostrategie die übergeordneten Ziele, Grundsätze und Rahmenbedingungen für den Einsatz kryptografischer Verfahren im Unternehmen, während das Kryptokonzept deren konkrete Umsetzung in Form festgelegter Algorithmen, Protokolle, Schlüssellängen und Prozesse in den jeweiligen Systemen beschreibt.

werden, um eine ausreichende Vielfalt an kryptografischen Primitiven bereitzustellen. Weiterhin müssen modular auswählbare kryptografische Verfahren mit unterschiedlichen Sicherheitseigenschaften bereitgestellt werden. Neben klassischen asymmetrischen und symmetrischen Verfahren sollten auch Post-Quanten- sowie hybride Verfahren unterstützt werden, um auf unterschiedliche zukünftige Bedrohungsszenarien reagieren zu können. Darüber hinaus ist eine Diversifizierung nach den zugrunde liegenden mathematischen Problemklassen anzustreben. So sollten beispielsweise sowohl gitterbasierte als auch codebasierte Post-Quantum-Verfahren auswählbar sein.

Weitere Grundsätze richten sich insbesondere an Hersteller von Produkten, die Kryptografie einsetzen. Anwender sollten deren Einhaltung im Beschaffungsprozess verbindlich einfordern und überprüfen. Dazu gehört unter anderem die Trennung von Implementierung und Konfiguration: Lösungen sind so zu gestalten, dass die eingesetzte Kryptografie - beispielsweise Algorithmen, Protokolle und Parameter - in möglichst hohem Maß konfigurierbar und austauschbar und damit anpassbar bleibt (weitere Details siehe Kapitel 4.2 "Anforderungen an Architektur".

3.3 Interne Sicherheitsvorgaben und -prozesse

Die für die Organisation relevanten Kryptoobjekte sind verbindlich zu definieren sowie kontinuierlich zu vervollständigen und zu aktualisieren. Sicherheitsanforderungen an die Auswahl und den Einsatz von Kryptoobjekten werden üblicherweise in einer Kryptorichtlinie oder einem Kryptokonzept gemäß BSI IT-Grundschutz-Kompendium CON.1.A10 dokumentiert. Dieses zentrale Vorgabendokument legt fest, welche Verfahren zulässig sind und wie sie verwaltet werden. Darauf aufbauend können ergänzende Dokumente für spezifische Anwendungsfelder ergänzt werden, beispielsweise Certificate Policies (CPs) oder Certification Practice Statements (CPS) für Public-Key-Infrastrukturen.

Bei der Definition und Dokumentation der Sicherheitsvorgaben ist sicherzustellen, dass diese zur Umsetzung der in der Kryptostrategie festgelegten Grundsätze beitragen. Im Hinblick auf Kryptoagilität sind insbesondere die folgenden kryptografiebezogenen Vorgaben anzupassen und aktuell zu halten:

- Eine Liste aller zulässigen kryptografischen Algorithmen, Cipher-Suiten und Protokolle, einschließlich der erlaubten Parameter, um einen flexiblen Wechsel auf alternative Verfahren zu ermöglichen. Die Liste sollte neben klassischen auch zulässige Post-Quanten- und hybride Verfahren umfassen.
- Anforderungen an Lösungen, die einen flexiblen Wechsel zwischen verschiedenen kryptografischen Algorithmen und Cipher-Suiten ermöglichen, einschließlich der hierfür erforderlichen Prozesse.
- Anforderungen an hybride Lösungen, bei denen ein Angreifer mehr als ein kryptografisches Primitiv kompromittieren müsste.
- Vorgaben für eine Ablösungsrichtlinie (engl. deprecation policy) für kryptografische Verfahren, die klare Kriterien für den Wechsel kryptografischer Verfahren, verbindliche Übergangsfristen sowie definierte Prozesse zur Überwachung und Migration auf sichere Alternativen umfasst.

Darüber hinaus sind die Dokumente zum **Schlüsselmanagement** wie folgt anzupassen:

- Prozesse für den flexiblen Wechsel der in einer bestehenden Public-Key-Infrastruktur (PKI) unterstützten kryptografischen Algorithmen.
- Vorgaben zur Nutzung geeigneter Übergangsmechanismen in der PKI, beispielsweise hybrider Schlüsselaushandlungsverfahren.

Ergänzend zu den allgemeinen Sicherheitsvorgaben für Kryptografie ist Kryptoagilität als verbindliche Anforderung in der Beschaffung neuer Produkte zu verankern. Anwender sollten im Beschaffungsprozess sicherstellen, dass die ausgewählten Lösungen den Vorgaben der Kryptostrategie entsprechen (siehe Kapitel 3.2 "Kryptostrategie").

Im **Schwachstellenmanagement** sind insbesondere die folgenden Aspekte zu berücksichtigen und in den entsprechenden Vorgabedokumenten festzuhalten:

- Die Aufgabenbereiche des Kryptoinventars und des Schwachstellenscanners[6] sind eindeutig voneinander abzugrenzen. Dabei ist insbesondere festzulegen, welche Lösungen unsichere Kryptoobjekte identifizieren und wie diese in die Prozesse zur Behebung von Schwachstellen überführt werden.
- Aufgrund des dynamischen Umfelds sind neue Angriffe, unsichere kryptografische Verfahren und aktuelle Sicherheitsanalysen bestehender Algorithmen anhand geeigneter Quellen kontinuierlich zu beobachten. Hierzu zählen beispielsweise Veröffentlichungen von NIST und BSI. Schwachstellenscanner sind fortlaufend an neue Angriffsmethoden und daraus resultierende Erkenntnisse zu unsicheren Verfahren anzupassen.
- Wird ein automatisiertes Werkzeug zur Erstellung des Kryptoinventars eingesetzt, sollte dieses mit dem Schwachstellenscanner synchronisiert werden.

Ein unsicher gewordenes Kryptoobjekt begründet zunächst eine Schwachstelle oder ein erhöhtes Risiko, jedoch nicht zwangsläufig einen Sicherheitsvorfall. Ein solcher liegt in der Regel erst vor, wenn ein sicherheitsrelevantes Ereignis eingetreten ist oder unmittelbar bevorsteht und dadurch Schutzziele wie Vertraulichkeit, Integrität, Authentizität oder Verfügbarkeit beeinträchtigt werden. Wird ein Verfahren beispielsweise durch leistungsfähige Quantencomputer praktisch angreifbar, lassen sich Zertifikate technisch weiterhin verifizieren, obwohl ihre Authentizitätsaussage nicht mehr hinreichend belastbar ist. Auch der Wechsel zwischen Kryptoobjekten kann infolge unvorhergesehener Kompatibilitätsprobleme Betriebsstörungen verursachen und damit die Verfügbarkeit beeinträchtigen.

Um bei einem Sicherheitsvorfall schnell reagieren zu können, müssen geeignete Kryptoobjekte als Ersatz für unsichere Objekte verfügbar sein. Zudem muss transparent sein, welche Assets - beispielsweise Anwendungen, IT-Systeme, Kommunikationsnetze - auf welche Kryptoobjekte agil migriert werden können. Diese Transparenz kann insbesondere durch ein Kryptoinventar geschaffen werden. Ergänzend müssen organisatorische Prozesse, etwa durch verkürzte Freigabeverfahren, eine zügige Reaktion ermöglichen.

Zur Umsetzung von Kryptoagilität sind daher auch die **Vorgaben zur Sicherheitsvorfallbehandlung** wie folgt anzupassen:

- Ergänzung bestehender Reaktionsstrategien um kryptoagile Maßnahmen, insbesondere zur Austauschbarkeit und Konfigurierbarkeit kryptografischer Objekte.
- Festlegung der Voraussetzung und des Prozesses für den Wechsel auf alternative sichere Kryptoobjekte im Falle eines Sicherheitsvorfalls.

3.4 Kryptoinventar zur Verwaltung von Kryptoobjekten

3.4.1 Motivation

Die zentrale Verwaltung kryptografiebezogener Informationen innerhalb einer Organisation ist eine wesentliche Voraussetzung für Kryptoagilität. Nur wenn die Kryptoobjekte und ihre Einsatzkontexte bekannt sind, können sie gezielt aktualisiert oder ausgetauscht werden. Ein **Kryptoinventar** ist eine Übersicht über alle kryptografischen Objekte einschließlich relevanter Metainformationen, beispielsweise ihrer Konformität mit internen Vorgaben und ihre Beziehungen untereinander. Die Inventarisierung von Kryptoobjekten schafft insbesondere folgende Mehrwerte:

- Transparenz über die eingesetzten Verfahren und - abhängig von der jeweiligen Lösung - über ihre Abhängigkeiten,
- leichtere Identifikation von Sicherheitslücken, beispielsweise aufgrund veralteter Verfahren,
- frühzeitige Erkennung und Priorisierung von Migrationsbedarfen, beispielsweise auf Post-Quanten- oder hybride Lösungen,
- Überprüfung der Einhaltung interner Richtlinien und Standards sowie externer Compliance-Anforderungen und
- effizientere Verwaltung und bedarfsgerechte Aktualisierung von Kryptoobjekten.

[6] Ein Schwachstellenscanner scannt bspw. die Infrastruktur und identifiziert alle Schwachstellen, auch solche, die durch den Einsatz unsicherer Kryptoverfahren entstehen. Diese müssen hinsichtlich der Definition, welche Kryptoverfahren als unsicher gelten, aktuell gehalten werden.

Die Erstellung und Pflege eines Inventars werden zudem durch rechtliche Vorgaben und Standards gefordert (siehe Kapitel 2.4 "Hintergrundwissen"). Für Kryptoinventare sind insbesondere die folgenden Anforderungen relevant:

- **BSI IT-Grundschutz-Kompendium:**
  BSI CON.1 Anforderung A19 fordert die Erstellung eines Krypto-Katasters, in welchem für jede Gruppe von IT-Systemen die Einsatzzwecke, Zuständigen, eingesetzten kryptografischen Verfahren, eingesetzte Hard- oder Software mit kryptografischen Funktionen sowie eingesetzte sicherheitsrelevante Parameter (z.B. Schlüssellängen) festzuhalten sind.

- **Payment Card Industry Data Security Standard (PCI DSS):**
  PCI DSS 4.0 fordert in Anforderung 12.3.3 ein aktuelles und dokumentiertes Inventar aller verwendeten Chiffren und Protokolle.

- **Digital Operational Resilience Act (DORA):**
  Die Delegierte Verordnung (EU) 2024/1774 der Europäischen Kommission fordert in Artikel 7 Absatz 4, dass die Finanzunternehmen zumindest für IKT-Assets, die kritische oder wichtige Funktionen unterstützen, ein Register aller Zertifikate und Zertifikatspeicher erstellen und führen.

- **NIS-2:**
  Die Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates fordert von wesentlichen und wichtigen Einrichtungen angemessene Maßnahmen zum Cyber-Sicherheitsrisikomanagement, darunter Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung. Eine ausdrückliche Verpflichtung zur Pflege eines Kryptoinventars ergibt sich daraus nicht. Ein Inventar stellt jedoch eine zweckmäßige Umsetzungs- und Nachweismaßnahme dar.

3.4.2 Ausprägungen und Kriterien

Kryptoinventare können sowohl manuell als auch teilautomatisiert erstellt werden. Für manuelle Inventare werden häufig Tabellen (z.B. in Excel) eingesetzt, in denen die wesentlichen Informationen zu jedem Kryptoobjekt erfasst werden. Ein Nachteil dieses Ansatzes besteht darin, dass in der Regel nur bereits bekannte Kryptoobjekte erfasst werden. Objekte aus Schattenarchitekturen bleiben häufig unberücksichtigt. Zudem bildet ein manuelles Inventar oftmals lediglich den erwarteten Soll-Zustand und nicht die tatsächlich im Betrieb eingesetzten Kryptoobjekte ab. Die Datenerhebung und -pflege ist darüber hinaus zeitaufwendig und erfordern üblicherweise eine enge Abstimmung mit Asset-Verantwortlichen oder Herstellern.

Automatisierte Lösungen, beispielsweise Scanner zur Untersuchung verschiedener Infrastrukturbereiche, unterstützen die Identifikation tatsächlich eingesetzter Kryptoobjekte. Dadurch verringert sich der manuelle Erfassungsaufwand. Darüber hinaus stehen Inventarlösungen zur Verfügung, die erweiterte Scan-Funktionen mit einer benutzerfreundlichen Oberfläche verbinden und dadurch auch die Verwaltung der Objekte vereinfachen. Nachteil solcher Lösungen ist insbesondere der zusätzliche Kostenfaktor durch die Anschaffung und den Betrieb. Zudem lassen sich derzeit nicht alle Einsatzbereiche automatisiert erfassen, weshalb lediglich eine Teilautomatisierung erreicht werden kann. Dies betrifft insbesondere nicht-scanbare Hardware wie USB-Sticks oder externe Festplatten sowie teilweise auch IoT- oder OT-Geräte. Ebenso können proprietäre Kryptoimplementierungen außerhalb des Erkennungsumfangs liegen, wenn sie nicht auf Standardbibliotheken oder Referenzimplementierungen basieren. Ergänzend ist daher eine Strategie zur Ermittlung von Schattenkryptografie zu etablieren. Sie sollte sicherstellen, dass auch nicht scanbare Assets und proprietäre Kryptoimplementierungen risikoorientiert erkannt und adressiert werden.

Unabhängig vom gewählten Erhebungsansatz sollte das Kryptoinventar mindestens die folgenden Anforderungen erfüllen:

- **Vollständigkeit:** Das Inventar sollte die relevanten Arten von Kryptoobjekten und deren Attribute möglichst vollständig und aussagekräftig erfassen.

- **Aktualität:** Das Inventar sollte den aktuellen Stand möglichst zeitnah abbilden und mit vertretbarem Aufwand aktualisierbar sein.

- **Lebensdauer / Schutzdauer:** Für Objekte mit langfristigem Schutzbedarf, beispielsweise Archive, Backups, Schlüsselspeicher, ist die verbleibende Schutzdauer zu bewerten. Bei Daten mit langfristigem Vertraulichkeitsbedarf kann aufgrund von "Harvest Now, Decrypt Later"-Angriffen unmittelbarer Handlungsbedarf zur Migration auf Post-Quanten- oder hybride Verfahren bestehen.

- **Transparenz:** Das Inventar sollte Abhängigkeiten und Beziehungen zwischen Kryptoobjekten nachvollziehbar abbilden. In Verbindung mit der Configuration Management Database (CMDB) sollte das Datenmodell erkennen lassen, in welchem fachlichen Anwendungskontext ein Kryptoobjekt eingesetzt wird und welche Abhängigkeiten bestehen, beispielsweise bei verschlüsselter B2B-Kommunikation zwischen zwei Organisationen. Ergänzend sollten geeignete Taxonomien eine einheitliche Klassifizierung und Strukturierung der Objekte ermöglichen.

- **Sicherheit:** Informationen zu Kryptoobjekten sind in einem zentralen, angemessen geschützten und kontrolliert zugänglichen Ort zu verwalten. Im Inventar sollten grundsätzlich nur Referenzen und Metadaten gespeichert werden. Sensible Informationen, insbesondere private Schlüssel, dürfen nicht darin abgelegt werden.

- **Benutzerfreundlichkeit:** Das Inventar sollte übersichtlich, leicht verständlich und intuitiv nutzbar sein.

- **Skalierbarkeit:** Das Inventar sollte die erwartete Anzahl an Kryptoobjekten sowie wachsende Datenmengen zuverlässig verarbeiten können.

Soll eine automatisierte Lösung eingesetzt werden, können insbesondere die folgenden Fragen die Auswahl eines geeigneten Herstellers beziehungsweise Produkts unterstützen:

- Welche integrierten Scanner stellt die Lösung bereit und welche Bereiche der Infrastruktur können damit auf Kryptoobjekte untersucht werden?
- Wie wird die Aktualität des Inventars sichergestellt? Erfolgen Scans kontinuierlich oder in festgelegten Intervallen? Welche Intervalle sind konfigurierbar und können einzelne Infrastrukturbereiche gezielt aktualisiert werden?
- Welche Schnittstellen bietet die Lösung zur Anbindung externer Datenquellen, insbesondere von Schwachstellenscannern und Schlüsselmanagementsystemen? Inwieweit können Informationen aus Bestandsmanagementsystemen, Herstellerauskünften, wie beispielsweise im CBOM-Format (siehe Kapitel 3.4.3 "Auskunftsformate für Herstellerprodukte"), sowie manuellen Erhebungen importiert werden? Welche bereits eingesetzten Scanner und sonstige Quellen, etwa bestehende Kryptoinventare, können als Datenquellen eingebunden werden?
- Welche Arten von Kryptoobjekten, beispielsweise Primitive, Algorithmen, Protokolle, Zertifikate, Schlüssel und Bibliotheken, kann die Lösung erkennen?
- Wie ist das Datenmodell aufgebaut und welche Attribute werden für die verschiedenen Arten von Kryptoobjekten erfasst und verwaltet, beispielsweise Algorithmen, Protokolle, Schlüsselmetadaten, Parameter, Lokationen, Historie, Verantwortlichkeiten sowie Zeitpunkt der Inbetriebnahme und Änderung?[7] Welche zusätzlichen Informationen, etwa Beiziehungen, Konformitätsstatus und Post-Quanten-Sicherheit, lassen sich darstellen?
- Werden eingelesene Kryptoobjekte normalisiert, sodass gleiche Primitive, Algorithmen, Protokolle und Bibliotheken einheitlich bezeichnet werden?
- Welche Exportfunktionen bietet die Lösung?
- Welche Betriebsmodelle unterstützt die Lösung, beispielsweise On-Prem oder Cloud?
- Welche Leistungsfähigkeit weist die Lösung auf und welche Datenmengen kann sie verarbeiten und auswerten?

3.4.3 Auskunftsformate für Herstellerprodukte

Eine Bill of Materials (BOM) eines Systems beschreibt in standardisierter und maschinenlesbarer Form, welche Komponenten ein System enthält.

Dabei werden verschiedene Ausprägungen unterschieden, beispielsweise Hardware Bill of Materials (HBOMs) und Software Bill of Materials (SBOMs). Eine SBOM dokumentiert die in einem Produkt

[7] Siehe dazu auch BSI Dokument CON.1.A19 "Erstellung eines Krypto-Katasters"

enthaltenen Software-Komponenten einschließlich ihrer Versionen und Abhängigkeiten. Der Einsatz von SBOMs wird bereits von TeleTrusT empfohlen, siehe TeleTrusT-Leitfaden "Software Bill of Materials"[8].

Eine Cryptography Bill of Materials (CBOM) geht noch einen Schritt weiter und beschreibt die in den Komponenten enthaltenen kryptografischen Bestandteile. Dazu zählen insbesondere Algorithmen, Schlüsselmetadaten, Zertifikate und Protokolle. Das zugrunde liegende Datenmodell strukturiert die zu erfassenden Kryptoobjekte und schafft Transparenz über die in einem Produkt enthaltenen kryptografischen Verfahren. Da CBOMs den Aufbau und die Pflege des Kryptoinventars wesentlich unterstützen, sollten Anwender entsprechende Informationen von ihren Zulieferern beziehungsweise Herstellern einfordern.

Eine CBOM verfügt jedoch in der Regel nicht über alle Funktionalitäten, die mit einem Kryptoinventar angestrebt werden und ersetzt dadurch kein vollständiges Kryptoinventar. Während eine CBOM primär die in Herstellerprodukten enthaltenen kryptografischen Bestandteile beschreibt, soll das Kryptoinventar alle Kryptoobjekte einer Organisation abdecken, einschließlich der beim Anwender erzeugten Objekte, beispielsweise Zertifikate. Darüber hinaus können die tatsächlich eingesetzten Kryptoobjekte aufgrund individueller Konfigurationen von den durch das Herstellerprodukt grundsätzlich unterstützten Objekten abweichen. Beispielsweise kann ein Herstellerprodukt mehrere Verfahren und Schlüssellängen anbieten, während der Anwender diese auf bestimmte Verfahren und Schlüssellängen beschränkt, um interne Vorgaben einzuhalten. Im Kryptoinventar werden daher die tatsächlich eingesetzten Kryptoobjekte geführt. Darüber hinaus sollte das Kryptoinventar die Konformität mit internen Vorgaben sowie die Beziehungen zwischen den Kryptoobjekten abbilden.

3.4.4 Inventarprozesse

3.4.4.1 Vorstudie

Ein Kryptoinventar ist kein Selbstzweck. Vor seiner Einführung sind die Anforderungen, Ziele und der erforderliche Datenumfang festzulegen. Hierzu empfiehlt sich eine Anforderungsanalyse, die sicherstellt, dass das Kryptoinventar die wesentlichen Anforderungen angemessen erfüllt.

Ergänzend sollte ein Grobkonzept die für den Aufbau und Betrieb des Kryptoinventars erforderlichen Prozesse sowie die durch das Inventar unterstützten Prozesse beschreiben. Dazu zählen insbesondere die initiale Erhebung und kontinuierliche Aktualisierung des Datenbestandes, dessen Auswertung und Priorisierung sowie die Ableitung von Handlungsbedarfen und Maßnahmen aus den bereitgestellten Informationen und Kennzahlen.

Für das Kryptoinventar und die flankierenden Prozesse ist eine verantwortliche Person oder Organisationseinheit zu benennen.

3.4.4.2 Aufbau und flankierende Prozesse

Aufbauend auf der Vorstudie werden die organisatorischen Einbindungen und flankierenden Prozesse konkretisiert. Dazu gehören insbesondere die Erhebung und laufende Analyse des Datenbestandes sowie die Ableitung daraus resultierender Handlungsbedarfe.

Das Kryptoinventar sollte stufenweise aufgebaut werden. Ausgangspunkt sind vorhandene Quellen, beispielsweise manuell geführte Listen, PKIs, das IT-Asset-Management und bestehende Scan-Ergebnisse. Dabei sind insbesondere die folgenden Empfehlungen zu berücksichtigen:

1. Geschäftskritische Anwendungen und Systeme mit hohem Sicherheitsbedarf priorisieren.
2. Festlegen, welche Arten von Kryptoobjekten erfasst werden sollen.
3. Einbeziehen aller relevanten Stakeholder in die Inventarisierung und Kategorisierung und Sicherstellen des Zugangs zu den erforderlichen Informationen.
4. Mitarbeitende regelmäßig über die Bedeutung von Kryptoagilität, Post-Quanten-Kryptografie und des Kryptoinventars sowie über ihren Beitrag zur Genauigkeit und Aktualität der Daten informieren und schulen.
5. Sichten vorhandener Informationsquellen, beispielsweise Sicherheitsvorgaben zum Schlüsselmanagement und zum Einsatz von Kryptografie sowie Verzeichnisse über Schlüssel und Zertifikate.
6. Festlegung einer einheitlichen Taxonomie für die Daten des Inventars.

[8] https://www.teletrust.de/publikationen/broschueren/cloud-security/

7. Auswahl und Einführung geeigneter Werkzeuge sowie automatisierter Lösungen, beispielsweise zur Zertifikats- und Schlüsselverwaltung sowie zur Erhebung von Kryptoobjekten.
8. Das Kryptoinventar durch geeignete Prozesse regelmäßig aktualisieren (siehe Kapitel 3.4.4.3 "Betrieb").
9. Die Erhebungsmethoden des Kryptoinventars schrittweise erweitern. Dazu gehören Scans von Netzwerken, Endpunkten, Dateisystemen, Anwendungen, Datenbanken, Containern und Hardware-Komponenten sowie die Anbindung von Drittsystemen, beispielsweise des IT-Asset-Managements oder der CMDB.

3.4.4.3 Betrieb

Ziel ist ein den Anforderungen der Organisation entsprechendes, möglichst vollständiges und aktuelles Kryptoinventar. Neue Produkte, Konfigurationsänderungen und Außerbetriebnahmen verändern den Bestand der Kryptoobjekte. Daher ist das Inventar kontinuierlich zu aktualisieren. Bei automatisierten Lösungen kann dies durch regelmäßige Scans relevanter Infrastrukturbereiche erfolgen. Die Häufigkeit richtet sich nach Kritikalität und erwarteter Änderungshäufigkeit.

Nach jeder Aktualisierung sind die Ergebnisse auszuwerten und daraus Handlungsbedarfe abzuleiten und zu priorisieren. Die weitere Behandlung und Umsetzung beschreibt Kapitel 3.5 "Kontinuierliche Verbesserung der Sicherheit der eingesetzten Kryptoobjekte".

3.5 Kontinuierliche Verbesserung der Sicherheit der eingesetzten Kryptoobjekte

Das in Kapitel 3.4 "Kryptoinventar zur Verwaltung von Kryptoobjekten" beschriebene Kryptoinventar ermöglicht die Erfassung und Verwaltung von Kryptoobjekten. Dieses Kapitel behandelt die kontinuierliche Verbesserung ihrer Sicherheit. Dazu gehören die Identifikation und priorisierte Behandlung von Verbesserungspotentialen.

3.5.1 Identifizieren von Verbesserungspotentialen

Das Kryptoinventar liefert Hinweise auf mögliche Verbesserungspotentiale des aktuellen Sicherheitsniveaus. Dazu gehören insbesondere die folgenden Kriterien:

- Unsichere kryptografische Algorithmen, Betriebsmodi oder Schlüssellängen (z.B. gemäß BSI TR 02102-1)
- Veraltete Protokolle, beispielsweise SSLv2 und SSLv3 (gemäß BST TR 02102-2, -3 und -4)
- Kryptobibliotheken mit bekannten Schwachstellen
- Schlüssel unzureichender Qualität, beispielsweise aufgrund von Zufallsgeneratoren mit mangelhafter Zufälligkeit
- Kompromittierte Schlüssel, beispielsweise infolge einer versehentlichen Veröffentlichung oder eines Diebstahls durch Cyber-Kriminelle

Zusätzlich kann sich das aktuelle Sicherheitsniveau durch Veränderungen der Bedrohungslandschaft ändern. Dazu gehören die folgenden Faktoren:

- Neue Angriffsvektoren: Ständig werden neue Methoden entwickelt, um Verschlüsselungen zu umgehen oder zu brechen, sei es durch die Entdeckung von grundlegenden kryptografischen Schwachstellen (z.B. Bleichenbacher-Attacke oder das Brechen von SIKE) oder den Einsatz neuer Technologien wie Quantencomputer oder KI-Verfahren. Veraltete kryptografische Verfahren bieten hier schnell Angriffsflächen und erfordern daher raschen Handlungsbedarf.
- Zunehmende Rechenleistung: Die Rechenleistung steigt exponentiell (Stichwort: Mooresches Gesetz). Was heute sicher ist, kann zukünftig durch Brute-Force-Angriffe kompromittiert werden.
- Veränderter Schutzbedarf: Der Schutzbedarf von Informationen und Geschäftsprozessen kann sich im Zeitverlauf ändern.

3.5.2 Risikoorientierte Priorisierung von Verbesserungspotentialen

Neben den bereits diskutierten Priorisierungskriterien, beispielsweise Aufwand und Zeit für eine Umstellung oder Anpassung zur Erhöhung der Agilität, ist das zu adressierende Risiko ein entscheidender Faktor.

Eine Risikoanalyse ermöglicht es, das Risiko für die Organisation anhand der Eintrittswahrscheinlichkeit eines Angriffs infolge einer Schwachstelle und der möglichen Schadenshöhe zu bestimmen. Dies ist insofern auch für Kryptoagilität relevant, da ein solches Risiko eintritt, sobald eine kryptografische Lösung unsicher wird und bestehen bleibt, bis eine sichere Lösung etabliert oder das Risiko anderweitig behandelt wurde. Je agiler die eingesetzten technischen Lösungen sind, desto kürzer ist der Zeitraum, in dem das Risiko besteht. Risikoanalysen können daher genutzt werden, um das potenzielle Risiko bei einem Verlust kryptografischer Sicherheit zu ermitteln und die Transformation hin zu agilen Lösungen zu priorisieren. Die Bereiche mit den höchsten potenziellen Risiken sollten bei der Umsetzung von Kryptoagilität priorisiert werden.

Im Folgenden wird zunächst anhand eines Beispiels dargestellt, wie Risikoanalysen methodisch durchgeführt werden können, um Risiken durch unsichere kryptografische Lösungen zu ermitteln. Die Grundlagen der Risikoanalyse werden an dieser Stelle nicht im Detail erläutert. Einen guten Einstieg bietet der Standard 200-3 des BSI. Mögliche Angriffsvektoren und Szenarien mit Handlungsbedarf können Kapitel 2.1.2 "Bedrohungen für kryptografische Verfahren" entnommen werden. Das Beispiel zeigt jedoch, dass solche Analysen zeitaufwendig sein können. Daher wird anschließend skizziert, wie alternativ Risikoindikatoren ermittelt werden können. Diese können auch als Vorstufe dienen, um detaillierte Risikoanalysen auf bestimmte Risikohöhen, beispielsweise erhöhte Risiken, zu begrenzen.

Als Beispiel dient die Kommunikation von vertraulichen Daten über das Internet. Das betrachtete Objekt - im Folgenden gemäß BSI als Asset bezeichnet - ist das Netzwerk beziehungsweise eine konkrete Kommunikationsverbindung. Die Kryptoobjekte, die diese Kommunikationsverbindung schützen, können dem Kryptoinventar entnommen werden (siehe Kapitel 3.4 "Kryptoinventar zur Verwaltung von Kryptoobjekten"). In einem ersten Schritt werden alle Angriffe identifiziert, die möglich wären, wenn die eingesetzten Kryptoobjekte unsicher würden. Eine mögliche Gefährdung ist das Abhören und damit der Bruch der Vertraulichkeit der Daten. Anschließend wird das Risiko gemäß der BSI-Methode anhand der Eintrittswahrscheinlichkeit und der Schadenshöhe ermittelt.

Bei einem bereits gebrochenen Verfahren ist die Eintrittswahrscheinlichkeit sehr hoch, da insbesondere über das Internet übertragene Daten von einem Angreifer vergleichsweise einfach abgehört werden können. Ist das eingesetzte Verfahren noch sicher, hängt die Eintrittswahrscheinlichkeit davon ab, wie lange der Schutz voraussichtlich bestehen bleibt beziehungsweise aufrechterhalten werden muss. Bei Verschlüsselung richtet sich dies in der Regel nach Art und Klassifizierung der Daten. Als Beispiel werden Daten betrachtet, deren Übertragung durch ein klassisches Schlüsselaustauschverfahren abgesichert ist und die daher künftig von einem hinreichend leistungsfähigen Quantencomputer entschlüsselt werden könnten. Müssen die Daten über Jahrzehnte vertraulich bleiben, ist die Eintrittswahrscheinlichkeit aufgrund eines "Harvest Now, Decrypt Later"- Angriffs (siehe Kapitel 2.1.2 "Bedrohungen für kryptografische Verfahren") als hoch einzuschätzen. Bei Steuersignalen hingegen, deren Schutzbedarf nur wenige Tage umfasst, ist die aktuelle Eintrittswahrscheinlichkeit als gering einzustufen.

Als zweiter Faktor ist die erwartete Schadenshöhe zu bestimmen. Sie ist gering, wenn ausschließlich Informationen übertragen werden, deren Offenlegung unkritisch ist. Bei vertraulichen oder streng vertraulichen Informationen ist hingegen von einer hohen Schadenshöhe auszugehen.

Sind beide Faktoren ermittelt, wird anhand der Risikomatrix der Organisation das erwartete Risiko bestimmt. Ist dieses gering, ist in der Regel keine Behandlung erforderlich. Bei einem hohen oder sehr hohen Risiko besteht hingegen unmittelbarer Handlungsbedarf. Ist eine unverschlüsselte Kommunikation zu keinem Zeitpunkt vertretbar, kann Kryptoagilität dazu beitragen, durch den schnellen Austausch kryptografischer Verfahren einen nahezu lückenlosen Schutz sicherzustellen. Bei Informationen mit langfristigem Schutzbedarf reicht Kryptoagilität allein jedoch nicht aus, da Angreifer die Kommunikation bereits heute aufzeichnen und speichern können und kryptoagile Maßnahmen in der Regel reaktiv erfolgen.

Die Durchführung von Risikoanalysen ist zeitaufwendig und erfolgt meist gemeinsam mit den Verantwortlichen des jeweiligen Assets, um die Schadenshöhe sachgerecht zu bestimmen. Daher kann es

sinnvoll sein, zunächst orientierende Risikoindikatoren für die Assets zu erheben und nur Assets mit erhöhtem Risikoindikator im Hinblick auf ihre Kryptoobjekte detailliert zu analysieren. Hierfür kann eine vereinfachte Analyse auf Basis einer Liste aller Assets, beispielsweise aus der Configuration Management Database (CMDB), durchgeführt werden. Zur Einschätzung der Eintrittswahrscheinlichkeit können Asset-Attribute, etwa die Kommunikation von Daten über das Internet, herangezogen werden. Für die Bewertung der Schadenshöhe eignen sich insbesondere die Schutzbedarfsfeststellung sowie Informationen aus dem Business Continuity Management (BCM).

Dieses Vorgehen konzentriert sich auf den Verlust der Sicherheit bereits eingesetzter Kryptoobjekte. Risiken, die aus dem fehlenden Einsatz von Kryptografie entstehen, sind für die Betrachtung der Kryptoagilität nicht relevant und werden daher in dieser Handreichung nicht behandelt.

3.5.3 Planung der Umsetzung von Verbesserungspotentialen und Migrationen

Anwender dürfen sich nicht ausschließlich auf die vom Hersteller bereitgestellten Updates verlassen, die ohne Unterbrechung des Betriebs der eingesetzten IT-Systeme eingespielt werden, sondern müssen auch eigene Maßnahmen und Überlegungen einbeziehen. Die Update-Strategien von Software-Lieferanten sollten nachvollzogen werden. Dazu gehört, wie häufig Updates bereitgestellt werden und welche Arten von Updates - Sicherheits-Updates, Funktions-Updates oder Fehlerbehebungen - zu erwarten sind.

Anwender können zugleich Hersteller eigener Software-Systeme sein. Daher sind auch interne Software-Entwicklungs- und Deployment-Prozesse im Hinblick auf Kryptoagilität weiterzuentwickeln.

Eine Migration von Kryptoobjekten ist eine Verbesserung, die über reine System-Updates hinausgeht. Dabei sind mehrere Aspekte zu berücksichtigen, um einen reibungslosen Übergang zu gewährleisten. Zunächst sollten die Systemverantwortlichen die bestehenden Systeme eingehend analysieren, um potenzielle Herausforderungen und Abhängigkeiten zu identifizieren. Für die Priorisierung und Festlegung der Migrationsreihenfolge sind insbesondere folgende Einflussfaktoren zu berücksichtigen:

- Das Risiko, das besteht, solange keine Migration durchgeführt wurde. Zur Erhebung der Risiken siehe Kapitel 3.5.2 "Risikoorientierte Priorisierung von Verbesserungspotentialen".
- Die Migrationskomplexität, insbesondere der geschätzte Aufwand und die Dauer der Umstellung eines Prozesses beziehungsweise der betroffenen Kryptoobjekte. Bei der Aufwandsschätzung sind insbesondere die Abhängigkeiten von Herstellern, anderen Kryptoobjekten und externen Nutzern, etwa B2B-Kommunikationspartnern, zu berücksichtigen.
- Die für die Migration erforderlichen und verfügbaren internen und externen Ressourcen.

Auf dieser Grundlage lassen sich Prioritäten und Reihenfolgen für Migrationspläne festlegen. Für die Migration sind klare Ziele zu definieren. Dabei sind neben Sicherheitsaspekten auch funktionale Anforderungen zu berücksichtigen, die für den laufenden Betrieb der Organisation wesentlich sind.

Es ist ein detaillierter Zeitplan zu erstellen, der alle Phasen der Migration von Kryptoobjekten umfasst, einschließlich der Planung, Implementierung und Tests. Eine sorgfältige Planung und Umsetzung reduzieren die damit verbundenen Risiken. Schulungen und Informationen zu neuen kryptografischen Standards und Verfahren fördern zudem die Akzeptanz bei den Mitarbeitenden. Ergänzend sollte ein Monitoring- und Feedbacksystem eingerichtet werden, um Leistung und Sicherheit der Kryptoobjekte nach der Migration kontinuierlich zu überwachen. So lassen sich potenzielle Probleme frühzeitig erkennen und erforderliche Anpassungen vornehmen.

3.5.4 Umsetzen von Verbesserungspotenzialen und Durchführen von Migrationen

Kryptoagilität umfasst die kontinuierliche Überwachung und Aktualisierung der Kryptoobjekte in den IT-Systemen. Bei Migrationen sind insbesondere die folgenden Aspekte zu berücksichtigen und in einem entsprechenden Vorgabedokument festzuhalten:

- Abschätzung der Seiteneffekte und Auswirkungen auf betroffene Anwendungen, beispielsweise bei B2B-Kommunikation und Datenarchivierung.
- Festlegen des Lösungswegs je Kryptoobjekt und Anwendung.
- Treffen von Entscheidungen über die notwendigen Systemanpassungen.
- Erprobung des Vorgehens in einer Testumgebung anhand eines Testplans je Kryptoobjekt, einschließlich der Interaktionen zwischen Systemen. Um einen zeitnahen Wechsel zwischen verschiedenen Kryptoobjekten zu ermöglichen, sind alle vorgesehenen Kryptoobjekte vor der Produktivsetzung im Rahmen der Software-Tests zu prüfen. Dabei sind insbesondere ihre Kompatibilität und Abhängigkeiten von anderen Software-Komponenten zu berücksichtigen.
- Bewertung der Testergebnisse und Entscheidung über den produktiven Einsatz.

Migrationen werden üblicherweise durch einen Change-Prozess begleitet. Daher ist festzulegen, welche Schritte und Verfahren für die Änderungen erforderlich sind. Der Prozess sollte so schlank gestaltet sein, dass ein effizienter Wechsel möglich bleibt.

Ein schneller Austausch von Kryptoobjekten beziehungsweise eine Anpassung ihrer Konfiguration kann je nach Verfahren Änderungen an verschiedenen Stellen erfordern, beispielsweise in Systemkonfigurationen, Schlüssel- und Zertifikatsspeichern oder Backups.

Beim Austausch von Kryptoobjekten sind gegebenenfalls auch Schlüssel oder weitere zugehörige Objekte zu ersetzen. Dabei ist zu prüfen, an welchen Stellen dies erforderlich ist. Bei kommunizierenden Systemen müssen die Änderungen zeitlich abgestimmt erfolgen, sowohl organisationsintern als auch organisationsübergreifend.

Bei der Konfiguration ist darauf zu achten, dass Kryptoagilität möglichst wenige Eingriffe in bestehende Systeme erfordert. Zudem sind die betroffenen Stellen und Artefakte zu dokumentieren. Nach Möglichkeit sollten keine Code-Änderungen erforderlich sein, Änderungen ausschließlich durch berechtigte Rollen und Personen vorgenommen werden und globale Kryptografieparameter zentral bereitgestellt und angepasst werden können.

4 Umsetzung von Kryptoagilität für Hersteller

4.1 Motivation

Anwender sind darauf angewiesen, dass ein Hersteller nach einem Sicherheitsvorfall, der auf Schwachstellen der Kryptografie beruht, unverzüglich Updates bereitstellt oder das Produkt durch den Anwender selbst umkonfiguriert werden kann. Daraus folgen Anforderungen an den Hersteller hinsichtlich der Produktarchitektur und der Update-Verfahren. Außerdem ist zu beachten, dass ein Hersteller selbst wieder Fremdkomponenten wie kryptografische Bibliotheken einsetzt und damit gleichzeitig in die Anwenderrolle schlüpft. Dieses Kapitel geht auf diese Aspekte näher ein.

4.2 Anforderungen an Architektur

Herstellerseitige Kryptoagilität basiert auf gutem **Softwaredesign** des Systems. Voraussetzung ist zuerst, dass kryptografische Funktionalität (Algorithmen und Protokolle) hinter **Schnittstellen** abstrahiert wird. Dabei ist es insbesondere wichtig, dass die Schnittstelle dem Aufrufer nicht die Wahl der konkreten Algorithmen, Protokolle oder Parameter wie Schlüssellängen überlässt. Wird unterschiedliche Kryptofunktionalität benötigt, sollte vielmehr **nach ihrem Zweck abstrahiert** und beispielsweise Funktionen zur Verschlüsselung von zu persistierenden Daten oder zur Signatur von Kommunikationspaketen bereitgestellt werden.

Die so abstrahierte Kryptofunktionalität sollte dann **durch möglichst wenige, zentrale Module oder Services gekapselt** sein, die sich unabhängig vom Rest des Systems austauschen lassen. Entwurfsmuster wie Dependency Injection helfen dabei. Durch Plugin-Konzepte ist es sogar möglich, dass Dritte ihre eigenen Kryptografiemodule einbringen. Dabei sollten aber nur (evtl. zentral) erlaubte/bekannte Module geladen werden können, um Sideloading-Attacken vorzubeugen (s.u. zu Konfigurationsmanagement).

Des Weiteren kann ein **Schichtenmodell** helfen, die Aufrufe der so gekapselten Kryptofunktionalität nicht über die ganze Codebasis zu verteilen. Dadurch kann auch leichter erkannt werden, welche Daten wann und wie kryptografisch behandelt werden, u.a. bei der Erstellung des Kryptoinventars.

Die Kryptografiemodule können **fest definierte Algorithmen, Protokolle und ihre Parameter** vorsehen **oder konfigurierbar** sein. Feste Definitionen können den Vorteil besitzen, dass sie besser getestet werden können, insbesondere auch hinsichtlich der Interoperabilität innerhalb des Gesamtsystems. Typischerweise kommen sie auch in zertifizierten Produkten zum Einsatz. Ein Hersteller sollte jedoch sicherstellen, dass er zeitnah neue Versionen mit neuer Kryptografie liefern kann, sollte sich die bisherige als unzureichend oder gar gebrochen herausstellen.

Bei konfigurierbarer Funktionalität kann der Anwender in solchen Fällen, auch nach Herstellervorgabe, sehr schnell reagieren und selbst auf andere Kryptografie umstellen. In jedem Fall muss herstellerseitig eine nach dem Stand der Technik **sichere Standardkonfiguration** vorgegeben sein und mit neuen Systemversionen aktualisiert werden. Die Konfiguration ist nach Möglichkeit **gegen versehentliche oder absichtliche Änderung zu schützen**, z.B. durch Rollenkonzepte. Die herstellerseitige Unterstützung von Konfigurationsmanagementsystemen ist wünschenswert, da damit eine andauernde Überwachung und Auditierung der Änderungen sichergestellt ist.

Die Auswahl der Algorithmen, Protokolle und ihrer Parameter soll **Industriestandards und behördlichen Empfehlungen** insbesondere des BSI und des NIST entsprechen, weshalb sie auch regelmäßig anzupassen ist. Hier ist auch zu beachten, dass die Lebensdauer eines Schlüssels (Langzeitsicherung vs. temporäre Signatur) andere Parameter und/oder Algorithmen bedingt. Hinsichtlich der Implementierung von kryptografischen Algorithmen und Protokollen sollte auf standardisierte und gut getestete, evtl. sogar **zertifizierte Bibliotheken**[9] zurückgegriffen werden, die regelmäßig aktualisiert werden sollten.

[9] Botan (https://botan.randombit.net/) -BSI-Empfehlung
Bouncycastle (http://bouncycastle.org/) - FIPS validated
Dell BSAFE (dell.com) - FIPS validated
libgcrypt (https://gnupg.org/software/libgcrypt/) - FIPS validated
NSS (https://developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS) - FIPS validated
OpenSSL (https://www.openssl.org/) - FIPS validated
wolfCrypt (http://www.wolfssl.com/) - FIPS validated

Wo dies nicht möglich ist, sollte sich die Implementierung eng an die veröffentlichten Standards halten, die insbesondere bei Algorithmen auch meist Pseudocode enthalten. Die konkrete Implementierung muss jedoch besonders auf mögliche Seitenkanalangriffe untersucht werden.

Aus Kompatibilitätsgründen kann es in manchen Fällen (z.B. zur Unterstützung eines gestaffelten Updates) notwendig sein, schwächere Algorithmen oder Parameter zuzulassen. Hierbei sollten aber für den Anwender Hürden eingebaut werden, z.B. indem solche Algorithmen oder Parameter nicht in den Standard-Listen zu finden sind, sondern auf besondere Weise aktiviert werden müssen. Auch sollte der Anwender auf die Verwendung von schwacher Kryptografie hingewiesen werden, wobei aber zu beachten ist, dass die Warnungen bei absichtlicher Verwendung die Nutzung des Produkts nicht wesentlich beeinträchtigen.

Damit verschiedene Versionen oder unterschiedliche Konfigurationen eines Produkts miteinander kommunizieren oder auf persistierte Daten zugreifen können, ist es notwendig, dass die **Produktversion** (bei fest codierter Kryptofunktionalität pro Version) oder die verwendeten **Algorithmen und Protokolle** (bei konfigurierbarer Kryptofunktionalität) mit den Daten als kryptografische **Metadaten** gemeinsam mit den geschützten Daten gespeichert oder übertragen werden, sodass jeweils die passende Kryptografie ausgewählt werden kann. Protokolle können auch eine **Aushandlung** der zu verwendenden Kryptografie vorsehen (siehe beispielsweise TLS). Da damit jedoch auch Fallback- und Downgrade-Attacken möglich werden, ist insbesondere bei der absichtlichen Aktivierung von schwacher Kryptografie (s.o.) durch geeignete Maßnahmen (z.B. Whitelists und Logging) sicherzustellen, dass dies nur zwischen definierten und bekannten Endpunkten geschieht.

Die Länge von Schlüsseln und von verschlüsselten oder signierten Daten kann sich bei verschiedenen kryptografischen Algorithmen oder Parametern teilweise deutlich unterscheiden. Insbesondere bei PQC-Algorithmen ist mit einer Längenerhöhung zu rechnen. Daher sollten **Längenfelder in Daten nicht zu klein** gewählt werden oder ein **Encoding** gewählt werden, das (fast) **beliebige Größen** zulässt. Falls feste Puffergrößen aufgrund von Programmierstandards vorgeschrieben sind, müssen die **Puffer** für Daten in ihrer **Länge angepasst** werden oder Daten in mehreren Segmenten einer bestimmten Maximalgröße übergeben werden können. Werden die Puffer **dynamisch alloziert**, bietet es sich an, dass die API nach der benötigten Größe für einen Rückgabepuffer gefragt werden kann.

Neben der Größenänderung ist insbesondere bei PQC-Algorithmen auch eine Änderung des Laufzeitverhaltens zu beachten. Bei **zeitkritischen Operationen** müssen daher die zu verwendenden Algorithmen und Parameter sorgfältig ausgewählt werden.

4.3 Update-Konzept

4.3.1 Update-Arten

Software-Updates: Neben dem Beheben von Fehlern oder dem Schließen von Sicherheitslücken sind regelmäßige Updates für Software, Firmware und Hardware insbesondere im Rahmen der Kryptoagilität von entscheidender Bedeutung, um neue kryptografische Algorithmen, Protokolle und/oder unterstützte Parameter auszurollen und so Systeme an neue Bedrohungen anzupassen. Software-Updates sind dabei am flexibelsten und lassen sich schnell, häufig und teilweise auch automatisiert bereitstellen.

Firmware-Updates: Firmware-Updates sind seltener und komplexer, da sie tiefer in die Hardware integriert sind. Neben dem klassischen manuellen Firmware-Update, das physischen Zugriff auf das Gerät erfordert, ermöglichen Over-the-Air (OTA)-Methoden, Updates remote durchzuführen. Während manuelle Updates schon allein wegen des physischen Zugriffs weniger Angriffspotential bieten, sind sie in Fällen von zahlreichen und/oder räumlich weit verteilten Geräten unpraktikabel. Dann gilt abzuwägen, ob das angestrebte Sicherheitsniveau ein OTA-Firmware-Update zulässt.

Hardware-Updates: Hardware-Updates werden seltener durchgeführt, da sie oft den physischen Austausch von Komponenten oder ganzen Geräten erfordern. In einigen Fällen können Sicherheitsprobleme durch Microcode-Updates behoben werden, die software-basiert sind. Hardware-Updates sind vergleichsweise kostspielig und aufwendig.

4.3.2 Update-Aspekte

In Kapitel 4.2 "Anforderungen an Architektur" wurden bereits einige Aspekte ausführlicher besprochen, die aus Sicht der Software-Entwicklung für Updates zu beachten sind, nämlich die Kompatibilität verschiedener Versionen oder Konfigurationen bei gleichzeitiger Vermeidung von Fallback- und Downgrade-Angriffen.

Für persistente Daten spielen **Konvertierungsprozeduren** eine zentrale Rolle, die die Verschlüsselung oder Signatur der Daten auf die aktuelle Version umstellen. Dies geschieht durch Umschlüsselung bzw. durch Neu- oder Mehrfachsignaturen. Diese Konvertierungsprozeduren können auch verwendet werden, um ohne Updates Schlüsselrotation durchzuführen. Einen Sonderfall stellen Geheimnisse (z.B. Passwörter) dar, die als Hashwerte gespeichert sind. Ein Umschlüsseln ist in diesem Fall nicht möglich. Nach einer Umstellung des Passwort-Hash-Verfahrens sollten gespeicherte Hash-Werte daher möglichst bei der nächsten erfolgreichen Anmeldung auf das neue Verfahren migriert werden. Eine verpflichtende zeitnahe Passwortänderung ist insbesondere dann zu erwägen, wenn eine Kompromittierung oder konkrete Schwäche des bisherigen Verfahrens anzunehmen ist.

Die Implementierung von **Test- und Validierungsprozessen** ist ein weiterer kritischer Aspekt. Zu den vorausgesetzten Tests von Funktionalität und Sicherheit der neuen Algorithmen oder Protokolle kommen umfassende Tests der Kompatibilitäten zwischen verschiedenen Software-Versionen und der Update-Prozedur selbst hinzu. Eine definierte und dem Anwender kommunizierte Kompatibilitätsmatrix hilft beim Design dieser Tests, insbesondere wenn bei Updates und damit zusammenhängenden Datenkonvertierungen (s.o.) Versionen übersprungen werden können.

Ein weiterer Punkt ist die Einrichtung von **Rollback-Strategien**, die Mechanismen enthalten, die es ermöglichen, bei einem fehlerhaften Update schnell auf eine vorherige Version zurückzukehren. Für Software-Updates kann das z.B. durch die Möglichkeit von Downgrades erfolgen. Firmware-Updates können durch Dual-Firmware-Systeme eine Rückfallebene bei Fehlern erhalten. Wenn sich die Formate persistenter Daten bei einem Update ändern, sollte ein Backup erfolgen.

Absicherung von Updates: Software und ihre Updates sind typischerweise digital signiert, zum einen, um die Integrität der Software sicherzustellen, zum anderen, um die sichere Herkunft gegenüber dem Anwender nachzuweisen. Diese digitalen Signaturen unterliegen der gleichen Problematik wie die in der Software selbst eingesetzte Kryptografie. Signaturen der Software werden meist vom Betriebssystem oder einem Bootloader überprüft, weshalb hier der Einfluss des Herstellers auf die verwendete Kryptografie begrenzt ist. Signaturen von Firmware oder Microcode sind oft sicherheitskritisch, weshalb sowohl die dazu verwendete Kryptografie als auch die öffentlichen Schlüssel nicht per Update änderbar sind - und damit im Sinne dieser Handreichung nicht kryptoagil. Daher ist es hier umso wichtiger, langzeitsichere Verfahren einzusetzen, am besten hybridisiert.

4.4 Weitere Anforderungen an den Hersteller

Eine **umfassende Dokumentation** und ggf. Schulungen sind ebenfalls unerlässlich. Klar strukturierte und detaillierte Dokumentationen helfen Administratoren und Benutzern, die neue Software oder Hardware korrekt zu nutzen. Zudem sollten Benutzer über die Änderungen informiert und entsprechend geschult werden, um die neuen Funktionen und Sicherheitseinstellungen effektiv anwenden zu können.

Wie in Kapitel 3.4 "Auskunftsformate für Herstellerprodukte" besprochen, sollen vollständige und maschinenlesbare **CBOMs** durch die Hersteller bei der Entwicklung von Produkten erstellt und mitgeliefert werden. Die Hersteller sind jedoch angeraten, diese Information um weitere Informationen, wie bspw. die konkreten Anwendungsfelder der identifizierten Kryptoalgorithmen sowie die Beziehungen der Kryptoobjekte untereinander und zu den Zielsystemen zu ergänzen.

4.5 Abhängigkeitsbetrachtung

4.5.1 Fremdkomponenten

Häufig werden Fremdkomponenten in einem Produkt verwendet, welche kryptografische Funktionen bereitstellen. Prominentes Beispiel hierfür sind Kryptobibliotheken. Bei der Integration ist darauf zu achten, dass die Komponente die Anforderungen an Architektur, Update-Konzept, Kompatibilität und Dokumentation wie in den vorangegangenen Kapiteln ebenso unterstützt.

Zusätzlich sollte die Zuverlässigkeit des Herstellers eine Rolle spielen, damit zum entsprechenden Zeitpunkt auch Updates bereitgestellt werden können, am besten abgesichert durch entsprechende Verträge.

Kann die Komponente nicht aktualisiert werden, sollte sie auf eine Weise eingebettet werden, welche den Austausch der Komponente selbst erlaubt, wie in Kapitel 4.2 "Anforderungen an Architektur" zu Modularität beschrieben. In diesem Fall sollte darauf geachtet werden, dass standardisierte, interoperable Schnittstellen verwendet werden, um auch Komponenten anderer Hersteller einsetzen zu können. Beispiel hierfür sind Smartcards.

Information über die kryptografischen Fähigkeiten einer Komponente kommt im besten Fall durch eine CBOM wie in Kapitel 4.4 "Weitere Anforderungen an den Hersteller" beschrieben. Andernfalls sollte diese selbst erstellt werden.

4.5.2 Externe/standardisierte Schnittstellen

Wird Kommunikation mit anderen Komponenten kryptografisch geschützt, sollten die verwendeten Protokolle so gewählt werden, dass Kryptoagilität unterstützt wird.

So sollte ein Protokoll bereits verschiedene Kryptoverfahren für den gleichen Zweck einsetzen können. Für umfassende Agilität ist die Möglichkeit zur Aushandlung der verwendeten Kryptoverfahren im Protokoll selbst von großem Vorteil.

Da neue Kryptoverfahren meist höhere Anforderungen an Bandbreite und Laufzeit haben, sollte auch geprüft werden, ob das Protokoll Größenbeschränkungen für Daten oder Timeouts vorsieht, welche eine Verwendung verhindern. In diesem Fall sollte ein Wechsel auf eine andere Protokollversion oder sogar ein anderes Protokoll erwogen werden.

5 Zusammenfassung

In der heutigen digitalen Welt ist die Fähigkeit, kryptografische Verfahren flexibel anzupassen, von zentraler Bedeutung - insbesondere im Hinblick auf die bevorstehende Migration zu Post-Quanten-Algorithmen.

Kryptoagilität bezeichnet in diesem Kontext einen strukturierten Prozess, mit dem Hersteller und Anwender kryptografische Bausteine - etwa Algorithmen, Protokolle, Schlüssel, Zertifikate oder Bibliotheken - schnell und ohne Beeinträchtigung der Kernfunktionalität eines IT-Systems austauschen können. Dabei handelt es sich nicht nur um eine rein technische Fähigkeit, sondern um eine übergreifende Kompetenz, die organisatorische Klarheit, technische Entkopplung und kontinuierliche Anpassungsmechanismen vereint. Externe Einflüsse wie neu entdeckte Schwachstellen, geänderte regulatorische Vorgaben, aktualisierte Standards, neue Bedrohungsszenarien oder technologische Entwicklungen (z.B. Quanten-Computing) müssen zeitnah und strukturiert adressiert werden, sodass das System stets dem aktuellen Sicherheitsniveau entspricht.

Um kryptoagile Prozesse zu ermöglichen, müssen klare organisatorische Strukturen etabliert werden. Hersteller sind für das Design und die Bereitstellung austauschbarer Schnittstellen verantwortlich, während die Anwender im Betrieb die Umsetzung und das Monitoring übernehmen. Eine **Kryptostrategie** legt Grundsätze wie Austauschbarkeit und Konfigurierbarkeit fest und verankert sie in internen Richtlinien. Zentral ist zudem das **Kryptoinventar** (oder Krypto-Kataster), das transparent aufzeigt, welche kryptografischen Objekte wo eingesetzt werden. Auf Basis dieses Inventars können Risiko- und Migrationsanalysen durchgeführt sowie Abhängigkeiten, Verantwortlichkeiten und Entscheidungsprozesse definiert werden.

Die technische Realisierung kryptoagiler Systeme beruht auf einer konsequenten **Abstraktion** kryptografischer Funktionen. Statt Algorithmen fest im Produkt zu verankern, werden **Schnittstellen** definiert, die nur den Zweck (z.B. "Daten verschlüsseln", "Nachricht signieren") beschreiben. Implementierungen können dann die zugrunde liegenden kryptografischen Algorithmen austauschen, beispielsweise über **Updates**, ohne dass das übrige System angepasst werden muss. Durch diese Entkopplung bleibt die Fachlogik des Systems unverändert, während kryptografische Komponenten flexibel und kontrolliert ersetzt werden können.

Durch diese strukturierten Prozesse können Unternehmen sicherstellen, dass ihre Kryptografie stets den aktuellen Bedrohungen und regulatorischen Anforderungen gewachsen ist.

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Fachleute, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Personenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie der Vertrauenszeichen "IT Security made in Germany" und "IT Security made in EU". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Kontakt:

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Dr. Holger Mühlbauer
Chausseestraße 17
10115 Berlin
Telefon: +49 30 4005 4306
E-Mail: holger.muehlbauer@teletrust.de
https://www.teletrust.de

TeleTrusT
Pioneers in IT security.