

KRYPTOAGILITÄT

Impulspapier | November 2024

Zusammenfassung

Die Kryptografie ist eine Schlüsseltechnologie für den Schutz in der digitalen Welt. Sie ermöglicht vertrauliche Kommunikation, Onlinebanking, die Geheimhaltung von persönlichen Daten und Geschäftsgeheimnissen, den Nachweis der Echtheit von Dokumenten und Medien, das Einspielen von authentischen Updates und Patches für Betriebssysteme und für Antivirenprogramme, Smart Home Automation, sicheres Cloud Computing, Smart Grids und vieles mehr.

Kryptoagilität bezeichnet die Fähigkeit, kryptografische Verfahren möglichst schnell und einfach auszutauschen. Damit kann die langfristige Sicherheit von Kryptografie gewährleistet werden, denn kryptoagile Systeme sind offen für Innovationen und verbessern die Widerstandsfähigkeit bei Angriffen auf einzelne Verfahren.

Jede Sicherheitsarchitektur, die Kryptographie verwendet, muss Kryptoagilität berücksichtigen, denn die Vergangenheit hat gezeigt, dass kryptografische Verfahren mit der Zeit – und manchmal sogar disruptiv – geschwächt oder gebrochen werden und dann zügig ersetzt werden müssen. Zugleich werden Sicherheitseigenschaften von Kryptografie fortlaufend verbessert und durch kryptografische Verfahren mit neuer (Schutz-)Funktionalität erweitert – auch hier ist Kryptoagilität unabdingbar.

Fazit: Kryptoagilität ist eine Voraussetzung für Innovationen in der Kryptografie und für langfristige Sicherheit. Sie fördert die technologische Souveränität und ihre kluge Umsetzung bringt Wettbewerbsvorteile.

Dieses Impulspapier gibt auf unterschiedlichen Ebenen und an verschiedene Stakeholder Empfehlungen zur Berücksichtigung, Umsetzung und Weiterentwicklung von Kryptoagilität.

Kryptografie und Kryptoagilität

Fortlaufende Innovationen und neue Bedrohungen für die Kryptografie treiben ihre Weiterentwicklung permanent voran und begründen gleichzeitig die Notwendigkeit von Kryptoagilität.

Die Forschung entwickelt neue kryptografische Verfahren mit verbesserter Sicherheit, neue (Sicherheits-)Features kommen zu bestehenden Primitiven und Verfahren hinzu und die Forschung findet neuartige Schutzkonzepte. Zugleich – und das macht Kryptoagilität so dringlich und wichtig – erodieren kryptografische Verfahren; sie werden langsam über Jahrzehnte oder sogar plötzlich unsicher. Da Kryptografie materielle und immaterielle Werte schützt, ist es für Kriminelle attraktiv, ihre Schwächen – beispielsweise in Implementierungen – zu suchen und für ihre Zwecke auszunutzen.

Die Notwendigkeit von Kryptoagilität ergibt sich darüber hinaus aufgrund inkompatibler Standards.

Im Folgenden wird auf diese drei Punkte näher eingegangen.

Innovationen in der Kryptografie

Innovationen in der Kryptografie adressieren nicht nur die Angriffsresistenz von Kryptoverfahren (z. B. durch Vorschläge für alternative Verfahren oder Härtung bestehender), sondern viele weitere Eigenschaften wie Performanz, Reduzierung des Speicherplatzbedarfs und anwendungsspezifische Optimierung. Beispielsweise hat die Kryptografie mit elliptischen Kurven (ECC) die Nutzung von Kryptografie auf Geräten mit geringem Speicherplatz oder Bandbreite im Vergleich zu den zu dieser Zeit gängigen Faktorisierungsverfahren erleichtert: Erst 1999 nahm die amerikanische Standardisierungsbehörde NIST (National Institute for Standards and Technology) die Innovation ECC auf und empfahl mit 15 Kurven ihre Verwendung.

Innovationen in der Kryptografie ermöglichen neuartige Schutzmöglichkeiten. Beispielsweise bietet *Perfect Forward Secrecy (PFS)* für Schlüsselaustauschprotokolle ein zusätzliches Sicherheitsfeature: Selbst bei Kompromittierung des privaten (Session-)Schlüssels wird die Sicherheit der Kommunikation früherer Sessions (d.h. solche, die vor der Kompromittierung durchlaufen wurden) nicht gefährdet. Diese Eigenschaft erhöht substanziell die Sicherheit und deswegen ist in der aktuellen Version 1.3 des am weitesten verbreiteten Protokolls für den Internetdatenaustausch *Transport Layer Security (TLS)* ein Schlüsselaustausch nur noch mit PFS möglich.

Bedrohungen

Eine noch bedeutsamere Notwendigkeit für Kryptoagilität stellen die nachfolgenden vier Bedrohungen dar.

1. Steigerung der Rechenleistung

Nach dem sogenannten Mooreschen Gesetz, einer Faustregel, verdoppelt sich die Anzahl von Rechenoperationen, die auf einem Chip pro Zeiteinheit stattfinden, alle ein bis zwei Jahre. Zwar ist umstritten, wie lange diese Faustregel noch zutrifft¹, doch es ist zu erwarten, dass die verfügbare Rechenleistung auch in den kommenden Jahren weiter anwachsen wird. So können Daten heute deutlich schneller signiert und verschlüsselt werden, aber auch Angriffe auf diese kryptografischen Verfahren sind dadurch beschleunigt worden. Um dem entgegenzuwirken, müssen beispielsweise die Schlüssellängen angepasst werden.²

2. Protokoll- und Implementierungsfehler

Immer wieder werden sicherheitsrelevante Fehler und Schwachstellen in Software³ und Protokollen⁴ gefunden. Die Zahl von Anwendungen, die obsoletere kryptografische Implementierungen einsetzen, nimmt selbst mehrere Jahre nach dem Bekanntwerden ihrer Schwäche bzw. Schwachstellen weiter zu.^{5,6}

Die Möglichkeiten kryptografische Implementierungen zu aktualisieren und Patches einspielen zu können, müssen bereits beim Entwurf von (Software-)Systemen vorgesehen werden. Wenn die Softwarearchitektur bezüglich der verwendeten Kryptografie und ihrer Schnittstellen modular aufgebaut ist, gibt es sogar eine Chance, ganze Kryptoverfahren agil austauschen zu können. In diese Richtung geht beispielsweise die *Java Cryptography Architecture (JCA)*⁷, die eine code-level-Erweiterbarkeit und -Austauschbarkeit zur Verfügung stellt. Mit JCS ist allerdings noch keine unterbrechungsfreie Austauschbarkeit im laufenden Betrieb gegeben. Eine weitere Möglichkeit besteht darin, von Beginn an mehrere Kryptoverfahren in Systeme einzubauen.

Beim Update, dem Anwenden von Patches, dem Umschalten und dem Austausch von Verfahren handelt es sich um Facetten von Kryptoagilität, die in der Schnittmenge von Kryptografie und (Software-)Engineering angesiedelt sind.

3. Mathematische Fortschritte

Die heute verwendete Kryptografie basiert auf mathematischen Problemen, die schwierig zu lösen sind – schwierig bedeutet aber nicht unmöglich. Es existiert kein Beweis, dass es nicht doch einfache Lösungen für diese Probleme gibt. Je länger erfolglos danach gesucht wird, umso größer wird das Vertrauen in die Schwierigkeit der mathematischen Probleme und damit in die Sicherheit der kryptografischen Verfahren. Dass dieses Vertrauen brüchig sein kann, daran erinnerte 2022 der Fall des isogeniebasierten Verfahrens SIKE. Nach jahrelanger Untersuchung wurde ein neuer einfacher Lösungsweg für das zugrunde liegende mathematische Problem gefunden und damit eine ganze Familie von kryptografischen Verfahren gebrochen. Mithilfe der öffentlich übertragenen Daten während des Diffie-Hellman-Schlüsselaustauschs konnte in wenigen Stunden der eigentlich geheime Schlüssel berechnet werden.⁸ Glücklicherweise war SIKE noch im Stadium der Voruntersuchung und nicht bereits standardisiert. Dem mathematischen Brechen des grundlegenden Problems eines Kryptoverfahrens kann in der Praxis nur begegnet werden, wenn kryptoagil auf ein anderes kryptografisches Verfahren gewechselt werden kann, dem andere mathematische Probleme zugrunde liegen.

4. Quantencomputer

Bereits seit der Erfindung von Shor's Algorithmus 1994 ist in der Theorie bekannt, welche grundlegende Bedrohung Quantencomputer insbesondere für die asymmetrische Kryptografie darstellen. Mit exponentiellem Vorteil gegenüber klassischen Computern können mit diesem Algorithmus auf Quantencomputern die mathematischen Probleme gelöst werden, auf denen aktuell die Sicherheit der meisten asymmetrischen Kryptografie gründet. 1994 war man allerdings noch weit von einer praktischen Bedrohung entfernt. Die Entwicklung von hinreichend großen, stabilen und fehlertoleranten Quantencomputern, die diese Algorithmen auch ausführen können, steckte damals noch in den Kinderschuhen. An ihrer Entwicklung wird seither mit Hochdruck gearbeitet. Im Jahr 2023 schätzen selbst vorsichtige Expertinnen und Experten für Quantencomputer die Wahrscheinlichkeit auf über 50 Prozent, dass Quantencomputer in 20 Jahren in der Lage sein werden, heute verwendete Kryptografie in weniger als 24 Stunden zu brechen.⁹

Ebenfalls mit Hochdruck wird an der Entwicklung von quanten-resistenter Kryptografie gearbeitet. Es lässt sich inzwischen von einem „Zoo“¹⁰ von Verfahren der Post-

Quanten-Kryptografie (PQC) sprechen. Jedes einzelne hat Vor- und Nachteile. Die Zeit der „one size fits all“-Verfahren, wie es beispielsweise RSA und ECC im Bereich der asymmetrischen Kryptografie waren, scheint vorbei.

Forschungsfragen und dringender Handlungsbedarf

Für digitale Kommunikation und digitale Systeme gibt es vielfältige Bedrohungen, denen mit immer besseren und bedarfsangepassten kryptografischen Verfahren begegnet werden muss. In vielen Fällen existieren diese besseren Verfahren bereits oder werden entwickelt, wie im Bereich der möglichen Bedrohung durch Quantencomputer. Doch oft dauert es lange, bis sie genutzt werden, und in der Praxis werden geschwächte oder sogar gebrochene Kryptoverfahren oft viele Jahre weiterverwendet – und deren Nutzung manchmal sogar ausgeweitet.¹¹

Wie lassen sich die Lösungen von der Theorie in die Praxis übertragen? Wie lässt sich Kryptografie dauerhaft sicher halten? Wie lassen sich Aktualisierungen und Verbesserungen schnell und praxistauglich einsetzen? Das sind Forschungsfragen und Haupthandlungsfelder der Kryptoagilität.

Inkompatible Standards

Eine weitere Herausforderung in der Nutzung von Kryptografie sind inkompatible Standards. Ein Beispiel hierfür sind PQC-Verfahren. Für deren Standardisierung startete das *National Institute for Standards and Technology (NIST)* in den USA bereits 2016 einen offenen Prozess unter breiter Beteiligung der einschlägigen Community.¹² Faktisch handelt es sich um einen Wettbewerb. In der ersten Runde wurden Dutzende Verfahren eingereicht. Nach mehreren Runden von Evaluierungen, Nachbesserungen und teilweise auch durch Kombinationen zweier Verfahren zu einem, stehen die vorläufigen Gewinner fest: Die PQC-Verfahren CRYSTALS-KYBER, CRYSTALS-DILITHIUM¹³, FALCON¹⁴ und SPHINCS+¹⁵ befinden sich in der Standardisierung. Erste Standardisierungsentwürfe wurden 2023 veröffentlicht.¹⁶ Weitere PQC-Verfahren befinden sich in der vierten Runde, um weiter untersucht zu werden. Ebenfalls 2023 startete ein weiterer Prozess, der quanten-resistente Signatur-Verfahren zur Standardisierung bringen soll.

Parallel dazu existieren Empfehlungen für Post-Quanten-Kryptografie in vielen Staaten. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlicht seit 2020 Handlungsempfehlungen für die Migration zu PQC und aktualisiert diese nach Bedarf. Darin empfiehlt das BSI unter anderem die Nutzung der PQC-Verfahren FrodoKEM und Classic McEliece.

In der neuesten Veröffentlichung des BSI¹⁷ wird CRYSTALS-KYBER bereits erwähnt und die Technische Richtlinie stellt die Empfehlung nach der abgeschlossenen Standardisierung in Aussicht. Für die Nutzung von PQC-Verfahren unterscheiden sich im Übrigen die Empfehlungen von NIST und BSI. Auf der einen Seite wären allgemeingültige Standards wünschenswert; die Wirtschaftlichkeitserwägungen hierfür liegen auf der Hand. Auf der anderen Seite kann es gute Gründe für abweichende nationale Standards geben. Die NIST-Standards zielen eher auf Effizienz von Verfahren, mit dem Ergebnis, dass die Favoriten teilweise recht neu sind. Die BSI-Standards fokussieren sich auf die Sicherheit, mit dem Ergebnis, dass das Amt langjährig bewährte PQC-Verfahren ausgewählt hat.

Wenn Hersteller sowohl für deutsche Sicherheitsbehörden als auch für den Weltmarkt produzieren, dann müssen sie ggf. alle Standards unterstützen. Wie dies auf einer einheitlichen (Software-)Entwicklungsplattform und über den gesamten Lebenszyklus im Betrieb gelingen kann, ist ebenfalls ein Thema der Kryptoagilität.

Sichtweisen auf Kryptoagilität

Kryptoagilität bezeichnet die Fähigkeit, kryptografische Verfahren schnell und einfach auszutauschen. Hierüber herrscht weitgehend Einigkeit.¹⁸ Doch, um ein kryptoagiles System zu entwerfen oder um beantworten zu können, wie bestehende Systeme in einen höheren Reifegrad von Kryptoagilität gebracht werden können, ist diese Aussage wenig hilfreich. Es drängt sich die Frage auf: Einfach für wen? Aus unterschiedlichen Blickwinkeln betrachtet, ergeben sich unterschiedliche Schwierigkeiten und somit andere Schwerpunkte.

Zudem taucht das Thema Kryptoagilität in Richtlinien und Empfehlungen bisher oft nur als Forderung auf. Empfehlungen zur Umsetzung gibt es kaum. Selbst über eine detaillierte und praxisorientierte Begriffsdefinition gibt es noch keinen Konsens. Darüber hinaus wird Kryptoagilität meist nur durch die Bedrohung durch Quantencomputer motiviert oder findet Erwähnung nur als Unterthema der Migration zu quanten-resistenter Kryptografie.

Die Kryptoagilität muss aus dem Schatten der Post-Quanten-Kryptografie herausgeholt und als eigenständiges Ziel verfolgt werden. Es geht um ein weitreichenderes und umfassenderes Konzept, mit dem wir uns auf zukünftige Bedrohungen besser vorbereiten können. Dies könnte selbst für solche Bedrohungen gelingen, die wir heute noch gar nicht vorhersehen können.

Um Kryptoagilität konkreter zu fassen, unterscheiden wir fünf Sichtweisen, die auch als Handlungsfelder aufgefasst werden können:¹⁹

1. Wissen über Kryptoagilität – Es wird Wissen erworben und verfügbar gemacht zu verschiedenen heute verwendeten kryptografischen Verfahren und Alternativen, auch der Post-Quanten-Kryptografie, genauso wie theoretisches und praktisches Wissen zu Kryptoagilität und wie sie umgesetzt werden kann.

Ziel: Es können fundierte Entscheidungen im Bereich der Kryptografie getroffen werden.

2. Systemwissen – Es wird zusammengetragen und dokumentiert, wer verantwortlich ist für welche Teile eines Systems, wie Updates durchgeführt werden können und welche Zugänge nötig sind. Ebenfalls wird untersucht, wo Kryptografie eingesetzt und wie diese aufgerufen wird, und welche kryptografischen Algorithmen verwendet werden.

Ziel: Eine Organisation ist im eigenen System handlungsfähig mit Blick auf Kryptografie.

3. Agilität im Prozess – Entscheidungsprozesse und Strukturen werden angepasst, um schnell und zentral Entscheidungen zur Kryptografie treffen zu können. Diese werden anhand von Guidelines getroffen, die wiederum an Empfehlungen von übergeordneten Behörden oder Gremien ausgerichtet sind, die festlegen, welche kryptografischen Verfahren genutzt werden. Es werden Prozesse entwickelt für Updates, die umfangreiches Testen beinhalten.

Ziel: Entscheidungsprozesse sind so aufgebaut, dass sie agiles Handeln in der Kryptografie unterstützen.

4. Agilität im System – Die Hardware wird modular aufgebaut. Einzelne Komponenten können ohne großen Aufwand ausgetauscht werden. Insbesondere werden Hard- und Software unabhängig voneinander austauschbar. Rechenleistung, Speicher, Schnittstellen – alle Bestandteile eines Systems sollen genügend Puffer bereithalten für komplexere Berechnungen und größere Schlüssel, verschlüsselte Nachrichten und Signaturen.

Ziel: Im System sind genügend Kapazitäten für die Nutzung anderer kryptografischer Verfahren vorhanden – auch quanten-resistenter Verfahren.

5. Agilität der Algorithmen – Auch die Software wird modular aufgebaut. Einzelne Komponenten sollen ohne großen Aufwand ausgetauscht werden können. Kryptografie wird über abstrakte Schnittstellen genutzt. Es wird softwareseitig ermöglicht, schnell und unkompliziert kryptografische Algorithmen hinzuzufügen und zu entfernen.

Ziel: Es stehen verschiedene kryptografische Algorithmen zur Verfügung, die flexibel genutzt werden können.

Grundsätzlich kann Kryptoagilität auf verschiedenen Ebenen umgesetzt werden. Die Bandbreite reicht von dem Austausch einzelner Primitive, wie Hashfunktionen oder Zufallsgeneratoren, bis zum Austausch ganzer Cipher Suites, bei der eine ganze Bandbreite von aufeinander abgestimmten kryptografischen Algorithmen definiert wird. Der Internetstandard TLS beispielsweise setzt auf die Umsetzung von Kryptoagilität auf Ebene der Cipher Suites. Für weniger umfangreiche Protokollstacks könnte auch die Umsetzung auf anderer Ebene interessant sein. Wir brauchen anwendungsorientierte Forschung, die auch diese Frage der passenden Ebene(n) für die Implementierung von Kryptoagilität beantwortet.

Die Umsetzung von Kryptoagilität in jeweils höheren Reifegraden ist eine langwierige Aufgabe mit vielen kleinen Schritten. Wenn sich ein Unternehmen, eine Kommune, Schule oder sonstige Organisation ohne Unterstützung auf diesen Weg machen müsste, wären die Hürden ungleich höher. Aber niemand muss das Rad neu erfinden. Die Herausforderungen werden an vielen Stellen ähnlich gelagert sein. Detailliertere, praxisorientierte Definitionen und vor allen Dingen Standards und Empfehlungen zur Umsetzung von Kryptoagilität können einen wesentlichen Beitrag zu Beginn des Prozesses sein. Mit Guidelines und Publikationen von untersuchten Good-Practice-Beispielen können Behörden, Verbände und Forschungseinrichtungen die Hürden senken – gerade zum schwierigen Beginn des Weges. Unternehmen und andere Organisationen können sich wiederum an diesen Empfehlungen orientieren und beispielsweise als Anforderung bei der Beauftragung oder Vergabe von IT-Dienstleistungen aufnehmen.

Wir sehen in unseren Kooperationen, dass viele große Unternehmen das Thema Kryptoagilität aktiv angehen. Die Implementierung von Kryptoagilität können kleinere Unternehmen oder Organisationen jedoch in vielen Fällen kaum allein stemmen.

Herausforderungen bei der Umsetzung von Kryptoagilität

Es gibt (noch) keinen Standardweg für die Umsetzung von Kryptoagilität. Gerade deswegen lohnt sich eine Betrachtung von Systemen, die schon kryptoagil oder zumindest auf dem Weg dorthin sind. In diesem Abschnitt greifen wir zwei Beispiele gesondert heraus. Das erste Beispiel zeigt, dass es zahlreiche Herausforderungen bei der Umsetzung von Kryptoagilität gibt. Das zweite Beispiel verdeutlicht, dass der Versuch sich mit Kryptoagilität gegen Bedrohungen in der Zukunft zu schützen, wiederum sogar neue Schwachstellen

schaffen kann: Wird Kryptoagilität schlecht umgesetzt, können Verfahren und Protokolle geschwächt werden. Es können neue Angriffsstellen entstehen und letztlich wird das Gegenteil des Erwünschten erzielt: Das Gesamtsystem wird unsicher(er).

E-Ladesäulen mit *Plug&Charge* bieten eine Möglichkeit, Elektroautos zu laden, bei der es nach dem Einstecken des Kabels keine weitere Interaktion oder Autorisierung braucht. Authentisierung und Bezahlung laufen automatisch ab, gesichert über kryptografische Verfahren, die in der ISO-Norm 15118²⁰ festgelegt sind. Genutzt wird das TLS-Protokoll und kryptografische Verfahren mit elliptischen Kurven ECDSA und EdDSA zur gegenseitigen Authentisierung. Prozessoren und Speicher sind auf diese Algorithmen mit kurzen Schlüsseln und vielen Rechenoperationen auf elliptischen Kurven ausgelegt. Ladesäulen sollen eine Lebensdauer von mindestens zehn Jahren haben²¹, die zu ladenden Elektroautos hingegen bis zu 35 Jahre. Wenn also morgen Quantencomputer praktisch einsatzfähig würden, um Shors Algorithmus auszuführen, könnten damit die hier verwendeten kryptografischen Verfahren gebrochen und Signaturen gefälscht werden. Elektroautos könnten Jahrzehnte im Namen von anderen und vor allem zulasten anderer Bankkonten geladen werden.

In diesem Szenario wird klar, wie dringend Kryptoagilität gebraucht wird. 2023 veröffentlichten Wissenschaftlerinnen und Wissenschaftler von der Hochschule Darmstadt / ATHENE, der University of Southern Denmark und der Academia Sinica in Taipei ihren Entwurf für eine kryptoagile PQC-Erweiterung für diese ISO-Norm. In Quantum-Charge wurden Hash- und Gitterbasierte Verfahren für den Plug&Charge-Vorgang implementiert. Herausforderungen waren insbesondere die deutlich längeren Schlüssel und Signaturen bei den quantenresistenten Verfahren. Außerdem sind die kleinen Prozessoren der eingebetteten Systeme optimiert auf die Anforderungen von Kryptografie mit elliptischen Kurven, wohingegen bei Gitter-basierten Verfahren viele Matrix-Operationen durchgeführt werden müssen.

Das zweite Beispiel findet sich in DNSSEC, einer Sicherheits-erweiterung des *Domain Name Systems*, mit der Domains im Internetverkehr IP-Adressen zugeordnet werden. In DNSSEC sind Ansätze von Kryptoagilität implementiert, da dynamisch neue kryptografische Algorithmen hinzugefügt werden können. Allerdings fanden Wissenschaftlerinnen und Wissenschaftler von ATHENE (hier der Goethe-Universität Frankfurt, der TU Darmstadt und des Fraunhofer SIT) heraus, dass dieser Agilitätsmechanismus dazu missbraucht werden kann, die Sicherheit von DNSSEC zu umgehen.²² Solche Downgrading-Angriffe bleiben eine Herausforderung

für Kryptoagilität. Wichtig ist dabei außerdem die Abwägung zwischen Interoperabilität auch in Übergangszeiträumen und der Sicherheit des Gesamtsystems.

Ebenfalls gilt es zwischen den Kosten und der Sicherheit abzuwägen. Diese Abwägung kann nicht im Allgemeinen getroffen werden. Gerade für kleine Geräte des Internets der Dinge (IoT Devices) mit kurzer Lebensdauer, wie zum Beispiel Sensoren, scheint Kryptoagilität eine Abwägungsfrage zu sein. Je nachdem, wo und wie das Gerät verbaut ist, und wo es sich befindet, könnte es leichter sein, das Gerät auszutauschen, statt intern das kryptografische Verfahren zu tauschen.

Empfehlungen an Stakeholder

Kryptoagilität betrifft alle. Mehrere Aktivitäten wurden bereits begonnen. Diese gilt es fortzuführen und zu intensivieren.

Forschung und Lehre: Kryptoagilität als eigenen Forschungsgegenstand betrachten

Die Erforschung von Kryptoagilität wird in Deutschland bereits vorangetrieben. Alle Projekte des Bundesministeriums für Bildung und Forschung (BMBF) im Themenfeld Post-Quantum-Kryptografie haben Arbeitspakete, die sich mit Fragestellungen der Kryptoagilität beschäftigen. Darüber hinaus wird das Thema in vielen Verbundvorhaben bei der Erforschung von Zukunftstechnologien aufgegriffen, wie beispielsweise in den 6G-Forschungs-Hubs, die 6G als souveräne und neue Mobilfunkgeneration in Deutschland und Europa mitgestalteten.

Empfehlung: Forschungseinrichtungen und die Forschungsförderung sollten Kryptoagilität als eigenen Forschungsgegenstand betrachten und auf ihre Agenda setzen. Hochschulen sollten Kryptoagilität in Lehrveranstaltungen vermitteln.

Staat und Behörden: Kryptoagilität pro digitale Souveränität

Fortschritte pro Kryptoagilität tragen zu Zielen der digitalen Souveränität, speziell der technologischen Souveränität bei. Bei disruptiven Ereignissen, wie dem Bekanntwerden von akuten kryptografischen Implementierungsfehlern ohne sofortige Reparaturmöglichkeit, können Ausweichmechanismen essenziell für die Aufrechterhaltung der Kontrolle über Systeme und ganzer Infrastrukturen werden.

Empfehlung: Der Staat und seine Behörden sollten Kryptoagilität in ihre Agenda pro digitale Souveränität aufnehmen. Wenn sie einen höheren Reifegrad von Kryptoagilität als aktuell erreichen, wird die Abhängigkeit von einzelnen Anbietern, Produkten, Primitiven und Verfahren reduziert und dies wirkt sich dementsprechend positiv auf die Handlungsfähigkeit aus und erweitert die Handlungsoptionen. Eine

Vorreiterrolle kann insbesondere in den Handlungsfeldern Ausschreibungen, Vergaben und Einkauf erreicht werden.

Wirtschaft: Kryptoagilität als Chance für Innovation

Die Schwächung oder der Wegfall von kryptografischen Verfahren und/oder deren Implementierungen ist eine anerkannte Bedrohung. Viele Unternehmen haben bereits die damit verbundenen Herausforderungen erkannt und Maßnahmen entwickelt, um sich möglichst kryptoagil aufzustellen. Für die Wirtschaftsunternehmen der Informations- und Kommunikationstechnologien enthält das Thema vielfältige Chancen für Innovationen.

Empfehlung: Die Möglichkeit der Schwächung bzw. der Wegfall von *kryptografischen Verfahren* und Implementierungen sollte Teil des Risikomanagements aller Einrichtungen werden, die auf die Verfügbarkeit von digitaler Informationstechnologie angewiesen sind. Good-Practices sollten (weiter-)entwickelt und möglichst innerhalb von Branchen und branchenübergreifend zur Verfügung gestellt werden.

Kurzfristige Maßnahmen

Im ersten Schritt steht der Aufbau von Kompetenzen im Mittelpunkt. Wissen über klassische und Post-Quanten-Kryptografie sowie Weiterbildungen zum Thema Kryptoagilität bilden die minimale Grundlage, um Kryptoagilität in der eigenen Organisation umzusetzen. Dafür müssen auch Personalressourcen bereitgestellt werden. Fortbildungen erfordern keine strukturellen Änderungen und können kurzfristig umgesetzt werden:

- ▶ Kompetenzen in Kryptografie aufbauen
- ▶ Kompetenzen in Post-Quanten-Kryptografie aufbauen
- ▶ Kompetenzen in Kryptoagilität aufbauen

Mittelfristige Maßnahmen

Im zweiten Schritt geht es darum, als Organisation mit Blick auf Kryptoagilität handlungsfähig zu werden. Im Zentrum steht deswegen die Analyse des Ist-Zustandes, sowohl der Kryptografie als auch der Zugänge und Updatemechanismen des eigenen Systems. Mit diesem gesammelten Wissen kann eine Organisation nur nachhaltig handlungsfähig werden, wenn dieses Wissen auch langfristig nutzbar bleibt. Dafür sollte ein geeignetes Wissensmanagement etabliert werden:

- ▶ Wissen über das eigene System sammeln
- ▶ Selbst genutzte Kryptografie analysieren
- ▶ Wissensmanagement etablieren/verbessern

Langfristige Maßnahmen

Langfristig sollen auch die internen Entscheidungsprozesse und Strukturen so angepasst werden, dass Kryptoagilität an den relevanten Stellen berücksichtigt werden kann. So könnte insbesondere Einfluss auf Ausschreibungen, Vergaben und Einkauf genommen werden:

- ▶ Migration zu Post-Quanten-Kryptografie angehen (je nach Schutzbedarf sollte die Migration bald eingeleitet werden, beispielsweise für Verschlusssachen)
- ▶ Entscheidungsprozesse und Strukturen an Kryptoagilität anpassen
- ▶ Kryptoagilität bei Ausschreibungen und Vergaben beachten

Zugleich gilt es, das Innovationspotenzial von Kryptoagilität für Wirtschaftsunternehmen der Informations- und Kommunikationstechnologien zu heben: Dadurch, dass das Thema erst am Anfang steht, ergeben sich vielfältige Möglichkeiten für Innovationen – angefangen von teil- bis vollautomatischen Scannern zur Unterstützung der Erstellung von Krypto-Stücklisten (*Crypto Bill of Materials, CBOM*) über Update- und Patchmechanismen von Bestandssystemen, bis hin zu Kryptosystemen, die bereits beim Design und über die gesamte Lebenszeit nach Kriterien der Kryptoagilität gestaltet wurden.

Verbände: Unterstützung bei komplexen Umstellungsprozessen

Für die Umsetzung von Kryptoagilität in kleinen und mittelgroßen Einrichtungen braucht es Vernetzung und weitreichende Unterstützungsangebote. Diese sollten insbesondere kurzfristig und niedrigschwellig umsetzbare Maßnahmen enthalten.

Potenzial Kryptoagilität

Kryptoagilität ist gekommen, um zu bleiben. Die hiesige Forschung ist gut aufgestellt und kann wertvolle Impulse für andere Stakeholder liefern. Diese sollten das Thema ebenfalls systematisch angehen und die Chancen nutzen – insbesondere, um handlungsfähig zu bleiben, selbst bei disruptiven Ereignissen in der Kryptografie.

Kryptoagilität spielt eine zentrale Rolle für Innovationen in der Kryptografie und für langfristige Sicherheit. Sie stärkt die technologische Souveränität, und eine kluge Umsetzung kann erhebliche Wettbewerbsvorteile mit sich bringen.

- 1 Williams, R. Stanley. "What's Next? [The end of Moore's law]." *Computing in Science & Engineering* 19.2 (2017): 7-13.
- 2 Smart, Nigel P., and Emmanuel Thomé. "History of Cryptographic Key Sizes." *Computational Cryptography* 469 (2021).
Technische Richtlinie BSI TR-02102-1. Kryptographische Verfahren: Empfehlungen und Schlüssellängen vom 02.02. 2024, abrufbar unter:
<https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.html>
- 3 Beispielsweise „xz-Hintertür“ <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-3094>
- 4 Beispielsweise „Keytrap“ <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-50387>
- 5 Heid, Kris, et al. "Tracing Cryptographic Agility in Android and iOS Apps." *ICISSP*. 2023.
- 6 S. Arzt. »Security code smells in apps: are we getting better?« In: *Proceedings of the 30th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering*. 2022, pp. 245–255
<https://docs.oracle.com/javase/8/docs/technotes/guides/security/crypto/CryptoSpec.html>
- 7 <https://csrc.nist.gov/csrc/media/Projects/post-quantum-cryptography/documents/round-4/submissions/sike-team-note-insecure.pdf>
- 8 <https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/>
- 9 <https://quantumalgorithmzoo.org/>
- 10 Arzt, Steven. "Security code smells in apps: are we getting better?." *Proceedings of the 30th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering*. 2022.
<https://csrc.nist.gov/projects/post-quantum-cryptography>,
- 11 <https://pq-crystals.org/>
- 12 <https://falcon-sign.info/>
- 13 <https://sphincs.org/>
- 14 <https://csrc.nist.gov/news/2023/three-draft-fips-for-post-quantum-cryptography>
- 15 Technische Richtlinie BSI TR-02102-1. Kryptographische Verfahren: Empfehlungen und Schlüssellängen vom 02.02. 2024, abrufbar unter:
<https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.html>
- 16 <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04282021.pdf> ,
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Post-Quanten-Kryptografie.pdf?__blob=publicationFile&v=1
- 17 <https://www.sit.fraunhofer.de/de/kryptoagilitaet/>
- 18 ISO/IEC: Road vehicles – vehicle-to-grid communication interface – part 2: Network and application protocol requirements. ISO 15118-2:2014, ISO (2014)
- 19 Smith, Margaret, and Johnathan Castellano. Costs associated with non-residential electric vehicle supply equipment: Factors to consider in the implementation of electric vehicle charging stations. No. DOE/EE-1289. 2015.
- 20 Heftrig, Elias, Haya Shulman, and Michael Waidner. "Downgrading {DNSSEC}: How to Exploit Crypto Agility for Hijacking Signed Zones." *32nd USENIX Security Symposium (USENIX Security 23)*. 2023.

Wissenschaftliche Arbeitsgruppe Nationaler Cyber-Sicherheitsrat

Die Wissenschaftliche Arbeitsgruppe wurde im Oktober 2018 gegründet und ist Mitglied des Nationalen Cyber-Sicherheitsrats. Sie berät aus Perspektive der Forschung zu Entwicklungen und Herausforderungen im Hinblick auf eine sichere, vertrauenswürdige und nachhaltige Digitalisierung.

Mitglieder der Wissenschaftlichen Arbeitsgruppe sind: Thomas Caspers, Prof. Dr. Gabi Dreo Rodosek, Prof. Dr. Claudia Eckert, Prof. Dr. Jörn Müller-Quade, Prof. Dr.-Ing. Christof Paar, Prof. Dr. Alexander Roßnagel, Prof. Dr. Michael Waidner

Hauptautor des Impulspapiers „Kryptoagilität“: Prof. Dr. Michael Waidner