STELLWERK DER ZUKUNFT

Kryptoagilität als Schlüssel zur digitalen Souveränität

Wie Organisationen ihre Kryptolandschaften steuern, Risiken beherrschen und den Weg in eine post-quantenresiliente Zukunft souverän gestalten.

Die neue Realität kryptografischer Risiken

Wie gut ist Ihre Organisation tatsächlich darauf vorbereitet, dass kryptografische Verfahren von heute in wenigen Jahren nicht mehr tragfähig sein könnten?

Der technologische Fortschritt im Quantencomputing stellt bewährte Sicherheitsmechanismen vor tiefgreifende Herausforderungen: Asymmetrische Verfahren werden langfristig strukturell angreifbar, elektronische Signaturen verlieren ihre Prüfbarkeit und Informationen mit langer Vertraulichkeitsdauer sind bereits heute gefährdet.

Doch die eigentliche Dringlichkeit entsteht nicht erst, wenn ein leistungsfähiger Quantencomputer verfügbar ist. Sie entsteht schon viel früher, nämlich heute: **die enorme Komplexität und Dauer kryptografischer Migrationen**, die sich über Jahre erstrecken und zahlreiche Systeme, Prozesse und Partnerketten betreffen.

In diesem Whitepaper zeigen wir, warum **Kryptoagilität** – also die Fähigkeit, kryptografische Verfahren und Protokolle kontrolliert, transparent und effizient auszutauschen – zum zentralen strategischen **Erfolgsfaktor** wird. Sie erhalten ein vollständiges, praxiserprobtes Vorgehensmodell inklusive Checkliste, das alle relevanten Ebenen integriert: Governance, Architektur, Prozesse und Organisation. So schaffen Sie die Grundlage, Ihr Unternehmen Schritt für Schritt in eine postquantenfähige Zukunft zu führen.

Kryptografische Resilienz im Zeitalter des Quantencomputings

Mit dem absehbaren Fortschritt leistungsfähiger Quantencomputer geraten heute weit verbreitete kryptografische Verfahren unter erheblichen Druck.

Insbesondere asymmetrische Algorithmen wie RSA oder Elliptic Curve Cryptography (ECC) gelten langfristig als nicht mehr sicher. Unternehmen stehen daher vor der strategischen Herausforderung, ihre IT und Sicherheitsarchitekturen frühzeitig auf diese Bedrohung vorzubereiten.

Kryptoagilität, die Fähigkeit, kryptografische Verfahren und Protokolle effizient, systematisch und risikominimiert auszutauschen, bildet zusammen mit Post-Quanten-Kryptografie (PQC) den entscheidenden **Lösungsansatz**, um auch in einer postquantenfähigen Welt **Vertraulichkeit**, **Integrität** und **Authentizität** zu demonstrieren und Sicherheitsarchitekturen frühzeitig auf diese Bedrohung vorzubereiten.

Warum Quantenrisiken Ihre Kryptografie bereits heute betreffen

Relevanz und Auswirkungen auf bestehende Verschlüsselung

Quantencomputer entwickeln sich nicht zu einem Ersatz klassischer IT-Systeme. Ihre Bedeutung entsteht vielmehr aus ihrer Fähigkeit, bestimmte mathematische Probleme erheblich schneller zu lösen als heutige Computer. Genau diese Eigenschaft macht viele heute genutzte Verschlüsselungsverfahren verwundbar, da ihre Sicherheitsannahmen auf der Schwierigkeit eben solcher Probleme beruhen.

Damit wird klar: Die Frage lautet nicht, ob Quantencomputer Auswirkungen auf bestehende Kryptografie haben werden, sondern wann ihre Leistungsfähigkeit groß genug ist, um diese Verfahren tatsächlich zu brechen und wie früh Organisationen darauf vorbereitet sein müssen.

Erwartete technologische Entwicklung

Hersteller wie IBM[1] sowie internationale Forschungs-einrichtungen gehen davon aus, dass Quantencomputer in den kommenden Jahren schrittweise stabiler und zuverlässiger werden. Zwar sind aktuelle Systeme noch durch hohe Fehlerraten und limitierte Anwendungsfälle geprägt, doch der technische Fortschritt konzentriert sich zunehmend auf die Verbesserung der Stabilität, nicht allein auf die Anzahl von Qubits.

Für die Sicherheit bedeutet das: Es geht nicht darum, wann Quantencomputer erstmals kryptografische Berechnungen ausführen können, das können sie bereits heute. Die eigentliche Zäsur entsteht, sobald ihre Leistungsfähigkeit ausreicht, um bestehende Verschlüsselungsverfahren zu brechen. Dieser Übergang ist ein Prozess, der frühzeitig in Risiko- und Sicherheitsstrategien einfließen muss. Institutionen wie NIST und ENISA betonen daher, dass dieser Entwicklungspfad trotz Unsicherheiten verbindlich in Sicherheits- und Risikoplanungen einbezogen werden muss.

[1] IBM lays out clear path to fault-tolerant quantum computing | IBM Quantum Computing Blog

Das veränderte Bedrohungsbild: Kryptografie unter Druck

Quantencomputer wirken sich nicht einheitlich auf alle Verschlüsselungsverfahren aus. Entscheidend ist, welche mathematischen Grundlagen einem Verfahren zugrunde liegen.

Asymmetrische Kryptografie im Übergang zu modernen PQC-Verfahren

Asymmetrische Verfahren bilden das Fundament digitaler Identitäten, sicherer Kommunikation und Vertrauensanker. Experten sind sich einig, dass sie durch zukünftige Quantencomputer langfristig strukturell angreifbar werden, unabhängig von der Schlüssellänge.

Für Führungskräfte bedeutet das: Es handelt sich nicht um eine allmähliche Schwächung, sondern um einen grundlegenden Paradigmenwechsel. Diese Verfahren müssen perspektivisch ersetzt oder durch quantensichere Alternativen ergänzt werden.

Symmetrische Kryptografie: Weiter nutzbar, aber mit Anpassungsbedarf

Symmetrische Verfahren sind weniger stark betroffen. Ihre Sicherheitsreserve sinkt zwar, doch mit ausreichend großen Schlüsseln und korrekt gewählten Parametern bleiben sie weiterhin zuverlässig einsetzbar. NIST und ENISA gehen daher davon aus, dass symmetrische Kryptografie auch in einer post-quantenfähigen Welt eine zentrale Rolle spielt, vorausgesetzt, sie wird bewusst und konsequent konfiguriert.

„Harvest now, decrypt later“: Das unterschätzte Zeitproblem

Die zentrale Herausforderung liegt nicht im genauen Zeitpunkt eines Quanten-Durchbruchs, sondern in der Dauer der erforderlichen Migration. Kryptografische Umstellungen betreffen häufig viele Systeme, Anwendungen, Partner und Prozesse. Entsprechend langwierig sind Planung, Tests und organisatorische Verankerung.

Zusätzlich verschärft das „Harvest now, decrypt later“-Risiko die Situation: Informationen, die heute verschlüsselt abgefangen werden, könnten künftig entschlüsselt werden. Damit wird das Thema besonders für Daten mit langer Schutzdauer bereits heute relevant.

Elektronische Signaturen: Eine stille Zeitbombe

Auch elektronische Signaturen sind betroffen, da sie ausschließlich auf asymmetrischer Kryptografie basieren und über viele Jahre gültig bleiben müssen. Mit zunehmender Alterung der zugrunde liegenden Algorithmen verlieren selbst korrekt archivierte Signaturen schrittweise ihre kryptografische Sicherheit.

Bereits heute eingesetzte Long-Term-Validation Konzepte verlängern zwar die Prüfbarkeit einer Signatur, können aber die kryptografische Schwächung der zugrunde liegenden Algorithmen nicht verhindern. Damit entsteht das eigentliche Risiko: Eine LTV-Signatur bleibt formal verifizierbar, verliert jedoch an kryptografischer Vertrauenswürdigkeit, sobald das Basissystem angreifbar wird, etwa durch Algorithmusalterung oder künftige Quantenrechner. Eine rechtzeitige Neusignierung gewinnt daher strategische Bedeutung, um Signaturen mit aktuellen oder künftig quantensicheren Verfahren abzusichern.

Kryptoagilität: Die Fähigkeit, Kryptografie strategisch zu steuern

Kryptoagilität ist die strukturelle Fähigkeit einer Organisation, kryptografische Verfahren kontrolliert und risikobasiert auszutauschen – ohne Betriebsunterbrechungen oder kostspielige Systemneubauten. Sie schafft die Grundlage, auf technologische Entwicklungen wie PQC reagieren zu können.

Zentrale Bausteine kryptoagiler Architekturen

- **Vollständige Transparenz** über alle eingesetzten kryptografischen Verfahren
- Klare **Governance** und Verantwortlichkeiten
- **Entkoppelte Architekturprinzipien**, die Algorithmuswechsel ermöglichen
- Standardisierte **Lifecycle-Prozesse** für Schlüssel, Zertifikate, Algorithmen und Protokolle

In der Realität verhindern jedoch komplexe, historisch gewachsene Kryptolandschaften häufig genau diese Flexibilität. Kryptografie steckt tief in Code, Embedded-Systemen oder Legacy-Integrationen und ist oft schlecht dokumentiert. Kryptoagilität adressiert diese strukturelle Komplexität und macht kryptografische Steuerung überhaupt erst möglich.

Strategische Einordnung für CIOs, CISOs und Entscheider

Aus Management- und Risikoperspektive ergeben sich mehrere wesentliche Schlussfolgerungen:

- Klassische asymmetrische Verfahren sind langfristig nicht tragfähig.
- Symmetrische Verfahren bleiben relevant, benötigen aber klare Parameter- und Schlüsselvorgaben.
- Der kritische Erfolgsfaktor ist nicht der Algorithmus, sondern die Fähigkeit, Verfahren flexibel zu wechseln.
- Die nächsten fünf bis zehn Jahre sind ein strategisches Gestaltungsfenster, um Strukturen, Prozesse und Verantwortlichkeiten aufzubauen.
- Elektronische Signaturen müssen neu gedacht werden: PQC betrifft nicht nur neue Dokumente, sondern vor allem Archive, Verträge und Beweisdaten mit langer Lebensdauer.

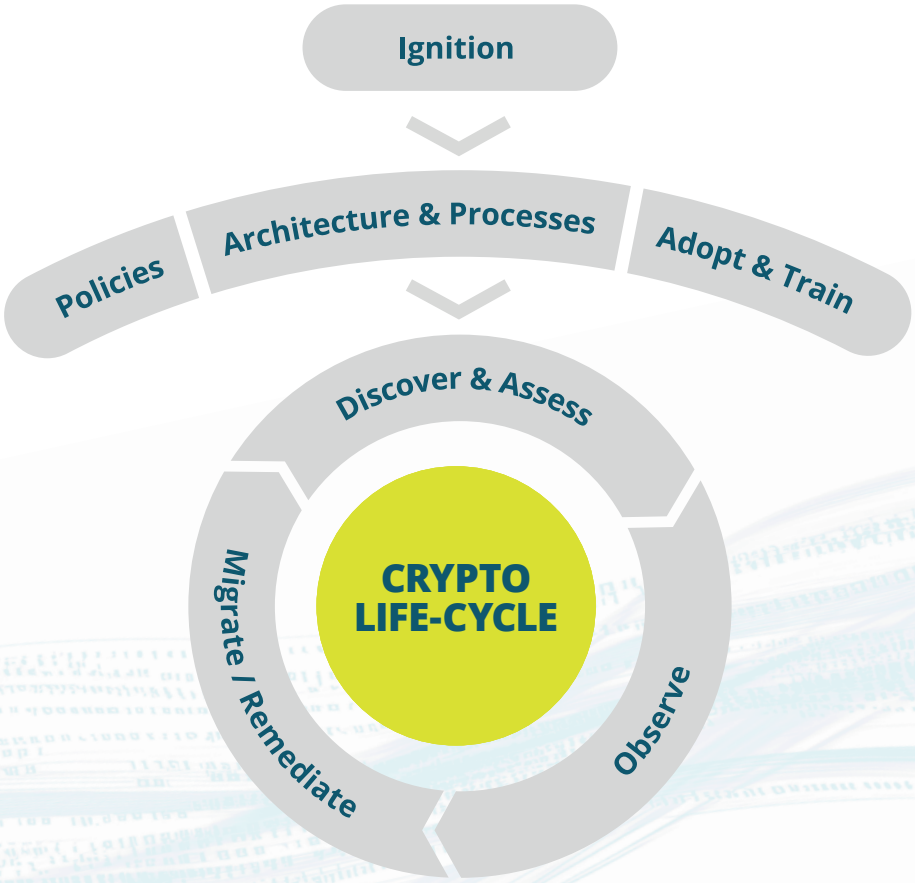
Vor diesem Hintergrund verschiebt sich der Fokus weg von einzelnen Technologien hin zu Kryptoagilität und planbarer Migration. Organisationen, die frühzeitig Transparenz herstellen und Migrationspfade definieren, sichern ihre Handlungsfähigkeit und können souverän auf die Entwicklungen im Quantencomputing reagieren.

Der Weg zur PQC-Readiness: Ein strukturiertes, risikobasiertes Vorgehensmodell

Eine nachhaltige Einführung von PQC folgt nicht dem Prinzip eines „Big Bang“, sondern erfolgt schrittweise und risikobasiert.

Das folgende Vorgehensmodell beschreibt ein praxiserprobtes, klar strukturiertes Vorgehen, mit dem Organisationen krypto-agile Prozesse nachhaltig verankern und die Migration hin zu quantensicheren Verfahren systematisch vorbereiten können. Es trägt der Tatsache Rechnung, dass kryptografische Migrationen, insbesondere im Kontext von PQC, komplexe, organisationsübergreifende Programme sind, die Planung, Governance und technische Umsetzung über mehrere Jahre erfordern.

Zentraler Bestandteil des Modells ist die Kombination aus übergeordneten Governance- und Enablement-Bausteinen sowie einem operativen „Crypto Life Cycle“, der von der ersten Bestandsaufnahme bis zur technischen Migration reicht. Dieser Aufbau ermöglicht es, Kryptoagilität nicht als isoliertes Technologieprojekt zu behandeln, sondern als festen Bestandteil der Sicherheits- und IT-Governance zu verankern.



Phase 1
Ignition: Strategische Verankerung und Startpunkt

Am Beginn steht die grundlegende Bewertung, ob kryptografische Verfahren im Unternehmen nachhaltig verwaltet werden und inwiefern das Quantenrisiko als relevantes Bedrohungsszenario anerkannt wird.

Diese Phase schafft:

- Management-Awareness
- Eine fundierte Entscheidungsgrundlage
- Ressourcen- und Budgetrahmen
- Die formelle Initiierung eines Kryptoagilitäts-Programms

NIST und ENISA bewerten diese frühe, strategische Verankerung als kritischen Erfolgsfaktor, da kryptografische Migrationen Jahre dauern und hohe organisatorische Reife benötigen.

Phase 2
Policies, Architektur & organisatorische Befähigung

Diese Phase bildet den strukturellen Unterbau für alle weiteren Schritte.

Policies
Vorhandene Richtlinien werden erweitert, um kryptografische Anforderungen, PQC-Roadmaps, Klassifikationen und Lifecycles verbindlich abzubilden. Sie schaffen Auditierbarkeit und Nachvollziehbarkeit.

Architecture & Processes
Hier entsteht die kryptoagile Zielarchitektur:

- Abstraktion kryptografischer Komponenten
- Standardisierte Schnittstellen für Algorithmen, Schlüssel und Zertifikate
- Vorgaben für Resilienz, Redundanz und Interoperabilität
- Automatisierungs- und Orchestrierungsmechanismen

Eine entkoppelte Architektur ermöglicht spätere Algorithmuswechsel ohne tiefgreifende Eingriffe in Applikationen.

Adopt & Train
Damit die Vorgaben wirken, müssen alle beteiligten Rollen, etwa CISO-Office, Architekten, Beschaffung, Entwickler oder Audit, befähigt werden, diese Prozesse anzuwenden. Ohne organisatorische Verankerung bleibt jede technische Vorbereitung wirkungslos.

Phase 3
Discover & Assess: Vollständige Inventarisierung und Risikoanalyse

Diese Phase ist der operative Kern des Modells und gleichzeitig die häufigste Schwachstelle realer Organisationen.

Ziel ist ein vollständiges Krypto-Inventar, das alle relevanten Informationen enthält, darunter:

- Algorithmen
- Schlüssel
- Zertifikate
- Protokolle
- Geräte & Embedded-Systeme
- Schnittstellen und externe Abhängigkeiten

Automatisierte Discovery-Werkzeuge unterstützen die technische Erfassung, doch erst die Kontextualisierung durch Service-Owner liefert belastbare Risikoentscheidungen.

Phase 4
Observe: Kontinuierliche Überwachung und Steuerung

Die Observe-Phase überwacht Zielarchitektur, Richtlinien, Risiken und regulatorische Entwicklungen. Sie dient als Steuerungsmechanismus und Reporting-Instanz gegenüber Management und CISO-Office und sorgt dafür, dass Migrationen planbar und transparent bleiben.

Phase 5
Migrate / Remediate: Technische und organisatorische Umsetzung

Hier wird der Wechsel auf neue oder hybride kryptografische Verfahren realisiert. Die Migration erfolgt schrittweise, risikobasiert und unter Anwendung aller zuvor definierten Architektur- und Governance-Elemente.

Abhängig von der Komplexität der betroffenen Systeme und den verfügbaren Ressourcen, kann dieser Schritt einen erheblichen Zeitraum beanspruchen. Auch europäische Leitlinien, etwa von ETSI[2], empfehlen einen geordneten, phasenweisen Übergang von klassischer zu quantensicherer Kryptografie, der auf Inventarisierung, Planung und kontrollierter Umsetzung basiert.

[2] TR 103 619 - V1.1.1 - CYBER; Migration strategies and recommendations to Quantum Safe schemes

Risikobasierter Ansatz

Zur strukturierten Priorisierung dient eine zweidimensionale Risikomatrix, die Protection Relevanz (Schutzbedarfsstärke) und Migrationskomplexität kombiniert. Durch die Kombination beider Achsen entstehen vier grundlegende Handlungscluster:

1 Hohe Protection Relevanz / geringe Migrationskomplexität

Diese Anwendungsfälle haben höchste Priorität für frühe Maßnahmen. Sie eignen sich besonders für Piloteinsätze von Post-Quanten-Kryptografie oder hybriden Verfahren, da der Sicherheitsgewinn hoch und der Umsetzungsaufwand überschaubar ist.

2 Hohe Protection Relevanz / hohe Migrationskomplexität

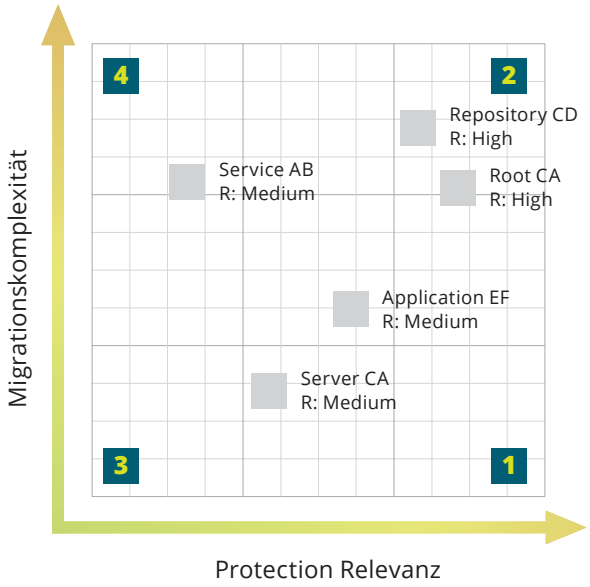
Hier liegt der strategisch kritischste Bereich. Diese Anwendungsfälle erfordern frühzeitige Planung, kryptoagile Architekturmaßnahmen und langfristige Migrations-Roadmaps, um Risiken kontrolliert zu reduzieren.

3 Geringe Protection Relevanz / geringe Migrationskomplexität

Diese Fälle besitzen niedrige Priorität und können im Rahmen regulärer Technologie- oder Lifecycle-Erneuerungen berücksichtigt werden.

4 Geringe Protection Relevanz / hohe Migrationskomplexität

Anwendungsfälle in diesem Bereich werden in der Regel bewusst zurückgestellt, sofern keine regulatorischen oder strategischen Abhängigkeiten bestehen.



Nutzen im Rahmen von Kryptoagilität und PQC-Einführung

Diese Risikomatrix fungiert als verbindendes Element zwischen Technik, Risiko-Management und Management-Entscheidungen. Sie dient als Grundlage für:

- die Priorisierung von Applikationen und Kryptoverfahren
- die Ableitung von Pilot- und Migrationsprojekten
- die Transparenz gegenüber Management, Revision und Aufsicht
- die schrittweise Umsetzung einer kryptoagilen Zielarchitektur

Im Zusammenspiel mit einem vollständigen Krypto-Inventar und klarer Governance ermöglicht die Matrix einen strukturierten, risikobasierten Übergang zur Post-Quanten-Kryptografie.

Die Kryptoagilitäts-Checkliste: Orientierung für alle Phasen Checkliste

Die Vielzahl beteiligter Systeme, Rollen und Abhängigkeiten macht kryptografische Transformationen anspruchsvoll. Die folgende Checkliste dient als strukturierte Leitlinie, um sicherzustellen, dass alle wesentlichen Bausteine der Kryptoagilität berücksichtigt, priorisiert und geprüft werden. Sie unterstützt Organisationen dabei, Fortschritt zu messen und Transparenz gegenüber Stakeholdern herzustellen.

A Strategische Grundlagen

- [ ] Quantenrisiko formell bewertet
- [ ] Kryptoagilität als Programm verankert
- [ ] Budget, Rollen und Governance definiert

B Richtlinien & Architektur

- [ ] Kryptografie Sicherheitskonzepte und Policies aktualisiert
- [ ] Zielarchitektur für Kryptoagilität definiert
- [ ] Standardisierte Schnittstellen & Prozesse etabliert

C Inventarisierung & Bewertung

- [ ] Vollständiges Krypto Inventar erstellt
- [ ] Klassifikation der Verfahren und Abhängigkeiten
- [ ] Risikomatrix angewendet und priorisiert

D Migration & Umsetzung

- [ ] Laufendes Monitoring implementiert
- [ ] Anpassung an regulatorische Entwicklungen
- [ ] Fortschritts-Reporting etabliert

E Kontinuierliche Steuerung

- [ ] Migrationsstrategien je Anwendungsfall definiert
- [ ] PQC Pilotfälle ausgewählt
- [ ] Hybrid Modi vorbereitet und getestet

Ergebnis

Nach Durchlaufen der Checkliste verfügen Organisationen über eine klare Sicht auf ihre kryptografische Ausgangslage, eine belastbare Priorisierung und eine strukturierte Roadmap, die die Grundlage für eine kontrollierte und nachvollziehbare PQC Migration bildet.

true-Xtender Enterprise PKI Suite – eine zentrale Voraussetzung für Kryptoagilität

PKI bildet in nahezu allen Unternehmen den zentralen Vertrauensanker und ist gleichzeitig einer der komplexesten Bereiche im Kontext von Kryptoagilität und PQC-Migration. Fehlende Transparenz über Zertifikate, Schlüssel oder Abhängigkeiten stellt ein erhebliches Risiko dar.

Die beschriebene true-Xtender Enterprise PKI Suite bietet genau die Fähigkeiten, die eine kryptoagile Organisation benötigt:

Zentrale Kontrolle & Risikoreduktion

Die Suite konsolidiert Zertifikate, Schlüssel und Abhängigkeiten unternehmensweit und schafft damit den Überblick, der für eine priorisierte Migration entscheidend ist.

Enabler für Kryptoagilität und PQC-Readiness

Statt punktueller Algorithmuswechsel ermöglicht die Suite eine kontinuierliche Weiterentwicklung der Kryptografie – abgestimmt auf regulatorische Vorgaben, technologische Entwicklungen und Geschäftsanforderungen.

Integrierte Zertifikats-Discovery

Shadow-IT, Drittsysteme, verstreute Zertifikate: all das wird sichtbar. Erst diese Transparenz ermöglicht belastbare Risikoentscheidungen und sinnvolle Roadmaps.

Kurz: true-Xtender liefert das technische Fundament, auf dem kryptoagile Prozesse überhaupt erst stabil betrieben werden können.

Fazit: Kryptografie wird zum strategischen Steuerungsfeld

Quantencomputing zwingt Organisationen, Kryptografie langfristig als strategisches Thema zu behandeln.

Der Umstieg auf quantensichere Verfahren ist kein Projekt, sondern ein mehrjähriger Organisationswandel. Unternehmen, die heute Transparenz schaffen, Governance stärken und kryptoagile Strukturen etablieren, können den Übergang zur Post-Quanten-Ära souverän, kontrolliert und risikobewusst gestalten.