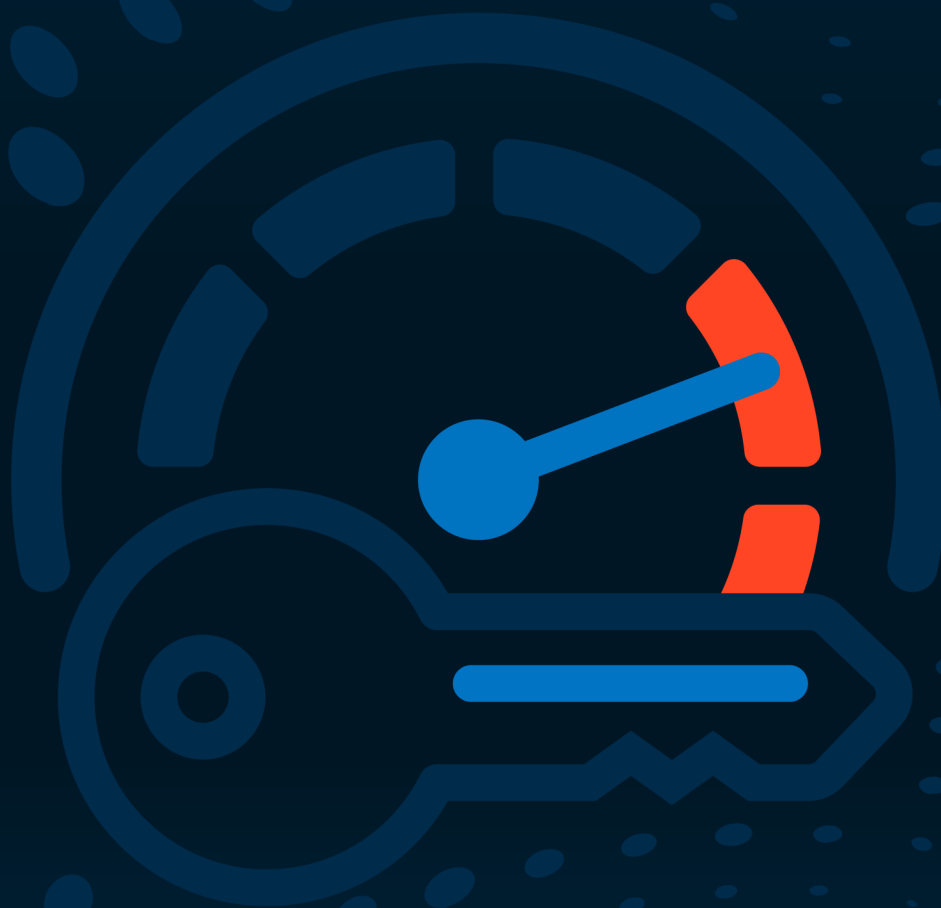


Globaler Forschungsbericht zu PKI 2026

PKI unter Druck: Der Wendepunkt für die Modernisierung



Inhaltsverzeichnis



Vorwort von Lakshmi Hanspal, Chief Trust Officer, DigiCert	3
Zusammenfassung	4
Die Herausforderung – PKI unter Druck	5
Transparenz und Risiko	7
Komplexität und Reife	9
KI und Quanten	14
Die Lösung – Modernisierung der PKI	16
Methodik	17
Autoren und Mitwirkende	18

Vorwort



Lakshmi Hanspal

Chief Trust Officer | DigiCert

Die Modernisierung der PKI und die Vorbereitung auf die Post-Quantum-Ära sind keine Zukunftsthemen mehr. Sie gehören bereits heute zur betrieblichen Realität.

Verantwortliche für Sicherheit und Infrastruktur stehen vor dem Zusammenspiel mehrerer Herausforderungen. Organisationen sehen sich mit immer mehr Maschinenidentitäten, immer stärker vernetzten Systemen, zunehmender KI-bedingter Unsicherheit und immer kleineren Handlungsfenstern konfrontiert, bevor kryptografische Schwachstellen zu Geschäftsrisiken werden. All dies führt zu zusätzlichen Herausforderungen durch die zunehmende Komplexität – zu einer Zeit, in der zertifikatsbedingte Ausfälle und Trust-Probleme immer häufiger Betriebsstörungen verursachen. Kryptografische Agilität ist längst kein Nice-to-have mehr. Sie entwickelt sich auf allen Ebenen schnell zu einem unverzichtbaren Bestandteil des täglichen Betriebs.

Um zu verstehen, wo die Organisationen stehen, haben wir mehr als 400 hochrangige IT- und Sicherheitsentscheider befragt, darunter CISOs, CIOs und Führungskräfte aus den Bereichen Cybersicherheit, IT-Betrieb, GRC und Produktentwicklung weltweit. Was sie uns erzählten, war gleichermaßen aufschlussreich wie ernüchternd.

Den meisten Organisationen ist bewusst, was auf dem Spiel steht. Weitaus weniger haben aus dieser Erkenntnis Konsequenzen gezogen.

Bei DigiCert haben wir dieses Problem nicht nur untersucht, wir haben es erlebt. Mit dem Wachstum unserer eigenen Umfelder, sahen wir uns mit denselben harten Wahrheiten konfrontiert. Unsere Teams hatten nur begrenzten Einblick in kryptografische Assets und mussten sich gleichzeitig mit fragmentierten Zertifikatsbesitzverhältnissen und dem sehr realen Druck auseinandersetzen, die Infrastruktur zu modernisieren, ohne den darauf aufbauenden Geschäftsbetrieb zu stören. Die Vorbereitung auf die Post-Quanten-Ära verlieh der Situation eine zusätzliche Dringlichkeit, die wir nicht ignorieren konnten.

Wir wurden also unser eigener Kunde Null. Wir haben unsere kryptografischen Assets inventarisiert, nicht verwaltete Zertifikate aufgedeckt, das Lebenszyklusmanagement automatisiert und mit der Härtung kritischer Systeme für quantenfähige Kryptographie begonnen. Es war notwendig und hat uns einen unmittelbaren, realen Einblick in die Herausforderungen gegeben, denen sich Organisationen in jeder Phase dieser Reise stellen müssen.

Eines weiß ich mit Sicherheit: Man braucht kein perfektes Budget, keinen makellosen Fahrplan und keine radikale Umgestaltung, um wirkliche Fortschritte zu erzielen. Was Sie brauchen, ist ein klarer Ausgangspunkt, die richtige Transparenz und die Bereitschaft, den nächsten Schritt zu gehen.

Dieser Bericht liefert Ihnen die Daten, die Benchmarks sowie ein realistisches Bild davon, wo die Branche heute steht. Ich lade Sie ein, diese Erkenntnisse zu nutzen, um den Dialog anzustoßen, überzeugende Argumente zu entwickeln und die nächsten Schritte einzuleiten.

Die Organisationen, die jetzt handeln, sind am besten aufgestellt, um die heutigen Herausforderungen zu bewältigen und zugleich den kontinuierlichen Veränderungen der kryptografischen Landschaft von morgen gewachsen zu sein.

*Lakshmi
Hanspal*

Zusammenfassung

Diese Studie zeigt einen zunehmenden Wandel in Unternehmen auf, weg von der bloßen Anerkennung von PKI-Herausforderungen hin zu deren aktiver Bewältigung mit dem Ziel einer verbesserten betrieblichen Resilienz. PKI gewinnt genau dann an Bedeutung, wenn ihre Verwaltung gleichzeitig schwieriger wird. Die Diskrepanz zwischen der Bedeutung, die PKI beigemessen wird, und der tatsächlichen operativen Einsatzbereitschaft ist inzwischen so groß, dass das Thema auch auf Führungsebene Aufmerksamkeit erfordert. Führungskräfte verstehen das Risiko. Vielen Organisationen fehlt es jedoch noch an der nötigen Transparenz, Governance und Automatisierung, um PKI als unternehmensweites System statt als Ansammlung einzelner Insellösungen zu verwalten.



PKI-Risiken sind bekannt, werden jedoch nicht ausreichend kontrolliert.

Adam Strange, leitender Analyst für Datensicherheit bei Omdia.

Die drei zentralen PKI-Herausforderungen von heute

1

Je weniger Transparenz, desto höher das Risiko.

Die größte Herausforderung für Unternehmen besteht darin, dass es an Transparenz hinsichtlich der gesamten Zertifikatslandschaft mangelt. Lediglich 34 % der Organisationen geben an, über ein vollständiges und aktuelles Verzeichnis aller digitalen Zertifikate zu verfügen. Zwischen Sichtbarkeit und Risiko besteht ein klarer Zusammenhang. 73 % der Organisationen sehen in Ausfällen durch abgelaufene Zertifikate ein großes oder sehr großes Risiko.

2

Komplexität und PKI-Reife erschweren es, wachsenden Geschäftsanforderungen gerecht zu werden.

74 % der Unternehmen sind besorgt über die unkontrollierte Zunahme von Zertifikaten, und 52 % erwarten, dass die PKI-Investitionen in den nächsten drei Jahren steigen werden. Doch selbst wenn IT- und Sicherheitsexperten die Bedrohungen und die Notwendigkeit einer PKI-Modernisierung erkennen, fällt es vielen schwer, Gespräche über Ressourcen und PKI-Risiken auf die Ebene der Entscheidungsträger zu heben.

3

Die Anpassung an den rasanten Wandel im Bereich der KI und die zunehmende Bedrohung durch Quantencomputer erfordert Agilität und Planung.

Mehr als 73 % der Organisationen geben an, dass PKI eine entscheidende Rolle beim Aufbau von Vertrauen in KI-Anwendungsfälle spielen wird. Bei der Vorbereitung auf die Bedrohungen durch Quantencomputing besteht noch Nachholbedarf: Nur 22 % der Unternehmen prüfen ihre kryptografischen Systeme vollständig auf künftige quantenbezogene Schwachstellen.

Die PKI-Modernisierung bietet Lösungen für diese Herausforderungen

Die operative Notwendigkeit der Modernisierung der PKI ist zunehmend selbstverständlich, doch viele Organisationen befinden sich noch in der Anfangsphase der Umsetzung. Da Modernisierungen komplex sein können, verfolgen die meisten Unternehmen einen stufenweisen Ansatz. Dabei zeigt sich, dass eine erfolgreiche Modernisierung voraussetzt, manuelle Prozesse zu reduzieren, die Transparenz zu verbessern und die erforderliche Expertise und operative Unterstützung einzubeziehen.



Auswirkungen der PKI-Modernisierung

Organisationen, die ihre PKI modernisiert haben, berichten von 60% weniger Ausfällen.

Einleitung

PKI unter Druck

PKI steht unter Druck, weil das operative Umfeld, weil die Rahmenbedingungen, auf denen bisherige Betriebsmodelle beruhen, nicht mehr gegeben sind. Die Anzahl der Zertifikate steigt, nicht-menschliche Identitäten nehmen zu, die Lebensdauer von Zertifikaten verkürzt sich und die Anzahl der Systeme, die auf kryptografischem Vertrauen basieren, wächst stetig. Gleichzeitig rücken regulatorische und branchenspezifische Compliance-Vorgaben die PKI in den Fokus und machen Führungskräfte für Ergebnisse wie Verfügbarkeit, Ausfallsicherheit und KI-Governance verantwortlich. Damit entwickelt sich PKI von einer Infrastruktur im Hintergrund zu einem strategischen Faktor, für dessen Implementierung, Überwachung und Management die IT- und Sicherheitsleitung verantwortlich ist.

So nutzen Sie diesen Bericht

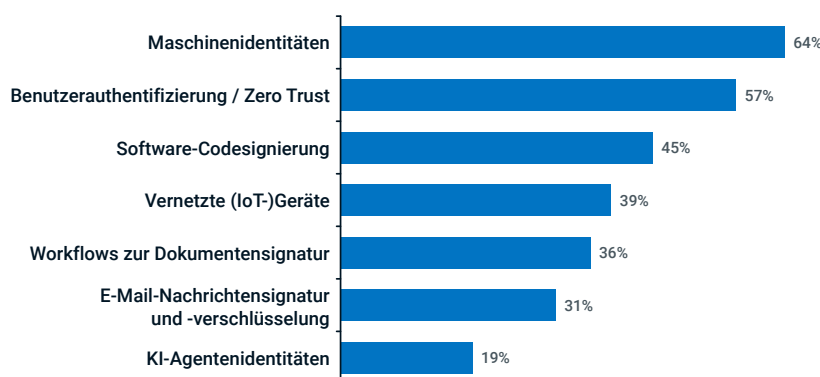
Dieser Bericht beleuchtet den täglichen PKI-Betrieb aus der Perspektive der verantwortlichen Führungskräfte. Ihre Antworten geben Aufschluss darüber, wo PKI heute steht und wie sie sich weiterentwickeln muss, um auch künftig zuverlässig zu funktionieren. Die folgenden Ergebnisse vermitteln Ihnen einen Überblick über den aktuellen Stand des PKI-Betriebs und ermöglichen es Ihnen, die eigene Organisation mit dem Durchschnitt zu vergleichen. Gleichzeitig liefern sie Daten und Anhaltspunkte für Ihre weitere Planung – sowohl intern als auch im Austausch mit Entscheidungsträgern im gesamten Unternehmen.

Die heutige Enterprise-PKI verstehen

Bevor wir PKI anhand der drei wichtigsten Herausforderungen betrachten, sehen wir uns zunächst an, wie PKI in heutigen Organisationen existiert. Die Daten zeigen, dass PKI weit über öffentliche Webzertifikate hinausgewachsen ist. Maschinenidentitäten, Benutzerauthentifizierung und Zero-Trust-Initiativen sind bei über der Hälfte der Befragten wichtige Bestandteile der PKI, wobei auch andere Anwendungsfälle außerhalb des Webs wie Software-Codesignierung, IoT und Inhalte eine bedeutende Rolle spielen.

Diese Ergebnisse zeigen, warum Unternehmen das Risiko von Ausfällen große Sorgen bereiten, denn PKI bietet Verschlüsselung, Identitätsprüfung, Authentifizierung und vieles mehr für eine breite Palette kritischer Unternehmensinfrastrukturen, weit über öffentlich zugängliche Webserver hinaus.

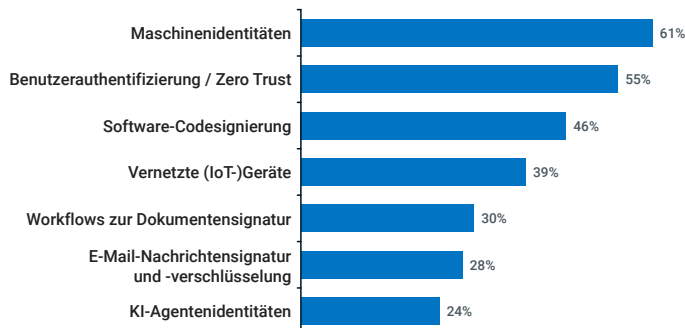
Welche der folgenden Bereiche deckt Ihre aktuelle PKI-Infrastruktur ab?



Prioritäten für die PKI-Modernisierung

Es überrascht daher nicht, dass wir eine Korrelation zwischen der Nutzung der Infrastruktur und den Prioritäten der PKI-Modernisierung feststellen. Fast drei Viertel der Befragten befürchten Ausfälle, die durch abgelaufene Zertifikate und die unkontrollierte Ausbreitung von Zertifikaten verursacht werden. Fachleute verstehen die Folgen eines Scheiterns und richten die einzelnen Modernisierungsphasen auf die Bereiche mit dem größten Bedarf und dem höchsten Risiko aus.

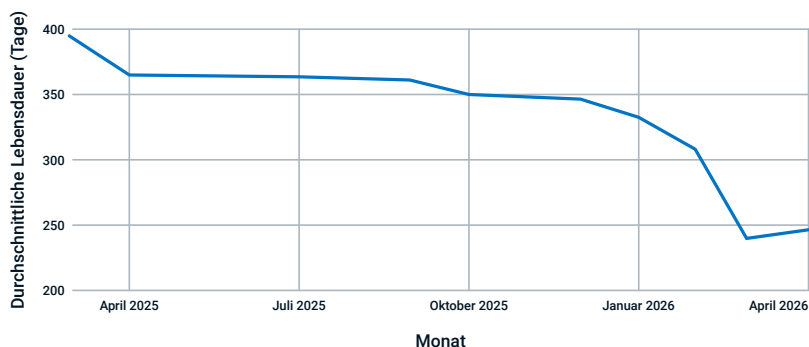
Welche Bereiche hat Ihre Organisation bei der PKI-Modernisierung priorisiert?



Kürzere Zertifikatslaufzeiten erhöhen den Druck

Trotz zunehmender Komplexität und einer wachsender Anzahl von Verbindungen, Identitäten und Anwendungsfällen verkürzt sich die Laufzeit öffentlicher Zertifikate. Die Branche steuert auf eine maximale Gültigkeitsdauer von 47 Tagen für öffentliche TLS-Zertifikate ab März 2029 zu. Dies lässt noch weniger Spielraum für Teams, die weiterhin auf manuelle Installation, unklare Eigentumsverhältnisse oder Tabellenkalkulationen als Aufzeichnungssystem angewiesen sind. In vielen Organisationen hat sich PKI zu einem Ökosystem entwickelt, das schneller fragmentiert, als die Teams es integrieren und steuern können.

Monatliche mediane Zertifikatslaufzeit (2025–2026)



KI und Quantentechnologie verkomplizieren ein ohnehin schon komplexes System zusätzlich.

Durch KI steigen die Anforderungen an die Absicherung von Identität und Integrität, die Nachvollziehbarkeit der Herkunft sowie die Durchsetzung von Richtlinien für Inhalte, Modelle und Agenten. Der Übergang zu quantensicherer Kryptographie erhöht die Anforderungen an Transparenz und Agilität in der gesamten Umgebung. Zusammen sprechen sie dafür, dass die Modernisierung der PKI eine logische Antwort auf die wachsenden Herausforderungen im Bereich Digital Trust darstellt.

Die zentrale Erkenntnis

Der Druck auf PKI hat nicht nur eine Ursache. Er entsteht durch das Zusammenspiel mehrerer Entwicklungen: die wachsende Zahl von Maschinenidentitäten, kürzere Zertifikatslaufzeiten, den Bedarf an KI-Governance und die notwendige Vorbereitung auf das Quantenzeitalter. Besonders relevant ist dies vor dem Hintergrund, dass Gartner's Prognose für den Q-Day¹ mit dem Beginn der 47-tägigen Zertifikatslebenszyklus-Vorschrift im Jahr 2029 zusammenfällt.

¹ Gartner Insights Abstract: Wie die kryptografischen Risiken des Quantencomputings reduziert werden

Sichtbarkeit & Risiko

Wenn Unternehmen ihre Transparenz erhöhen, sinkt das Risiko.

Nur eine vollständige Bestandsaufnahme über Einsatz und Status jedes einzelnen Zertifikats im Unternehmen liefert die nötigen Erkenntnisse, um Lücken, Versäumnisse und Ausfälle zu vermeiden.

Transparenz verhindert Ausfälle und Angriffe

Die Studie verdeutlicht eines: Ohne Transparenz können Organisationen das Zertifikatsrisiko nicht effektiv managen. Die Ergebnisse zeigen, dass nur 34% der Organisationen angeben, über ein vollständiges und aktuelles Verzeichnis aller digitalen Zertifikate zu verfügen. Zwei Drittel haben demnach nur einen Teil ihrer Zertifikate erfasst, führen gar kein Verzeichnis oder haben keinen verlässlichen Überblick über ihre Zertifikatslandschaft. Die meisten Unternehmen verwalten Tausende von Zertifikaten. Die Tatsache, dass bereits ein einziges abgelaufenes Zertifikat eine ganze Geschäftsanwendung lahmlegen kann, erklärt, warum das Risiko so hoch ist, wenn die Verzeichnisse unvollständig sind.

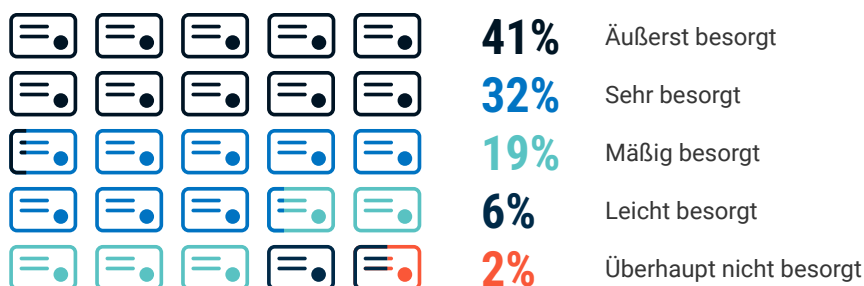
Wie lässt sich das Verständnis/die Nachverfolgung digitaler Zertifikate in Ihrer Organisation am besten beschreiben?



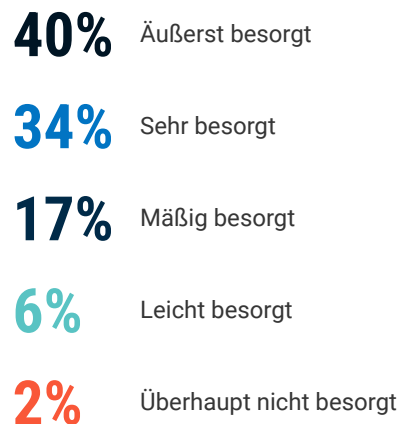
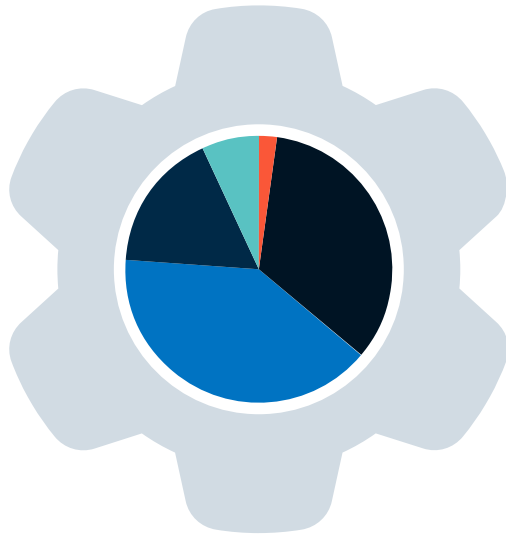
Diese Bedenken sind der Führungsebene durchaus bewusst. Fast drei Viertel der Befragten sind sehr oder extrem besorgt über Ausfälle aufgrund abgelaufener Zertifikate, und fast der gleiche Anteil ist sehr oder extrem besorgt über die zunehmende Verbreitung von Zertifikaten. Zusammengefasst beschreiben diese Ergebnisse eine bekannte Spannung in Unternehmen: Organisationen verstehen die Konsequenzen eines Zertifikatsausfalls, aber vielen fehlt es immer noch an der nötigen Transparenz, um dies konsequent zu verhindern.

Darüber hinaus bemängelt etwa die Hälfte der Befragten isolierte, schwer zu verwaltende Lösungen, und 47 % weisen auf fehleranfällige Tabellenkalkulationen hin. Mit anderen Worten: Der mangelnde Überblick ist nicht allein darauf zurückzuführen, dass nicht alle Zertifikate erfasst werden. Sie ist auch das Ergebnis fragmentierter Tools, fragmentierter Zuständigkeiten und fragmentierter Prozesse.

Wie besorgt sind Sie über das Risiko von Ausfällen/ Dienstunterbrechungen aufgrund abgelaufener Zertifikate?



Wie besorgt sind Sie über die zunehmende Verbreitung von Zertifikaten in Ihrem Unternehmen angesichts der wachsenden Anzahl von Systemen/Identitäten?



4.1 Milliarden

öffentliche Zertifikate, die im Jahr 2025 ausgestellt werden

Dies entspricht einem Anstieg von 55 % gegenüber dem Vorjahr, als laut öffentlichen Transparenzprotokollen im Jahr 2024 weltweit 2,6 Milliarden Zertifikate ausgegeben wurden. Interne Zertifikate werden in weitaus größerem Umfang ausgestellt.



Die richtigen Tools und Prozesse erhöhen die Transparenz und senken gleichzeitig das Risiko.

Trotz unterschiedlicher Umsetzungsmethoden bei der Modernisierung waren sich die Befragten einig darüber, was eine bessere PKI ausmacht. Verbesserte Überwachung und stärkere Kontrolle über Zertifikate, zentrale Transparenz, Zeitersparnis und weniger Ausfälle führen zu einem einfacheren und effizienteren Management bei geringerem Risiko. Wir gehen davon aus, dass die zentrale Transparenz und ein Single-Pane-of-Glass-Ansatz weiterhin höchste Priorität für Organisationen haben werden, die die Komplexität ihrer PKI bewältigen müssen.

Deshalb sollte die Erfassung der Zertifikate als erster Schritt der Modernisierung betrachtet werden. Ein verlässliches Inventar schafft Gewissheit statt bloßer Annahmen. Es ermöglicht Teams, Verantwortlichkeiten zuzuweisen, Abhängigkeiten bei der Erneuerung zu identifizieren, die Automatisierung zu priorisieren und zu verstehen, wo kryptografische Agilität am schwierigsten zu erreichen ist. Ohne diese Transparenz basieren alle weiteren Modernisierungsmaßnahmen auf unvollständigen Informationen.

Die zentrale Erkenntnis

Transparenz hilft, die Risiken von Zertifikatsausfällen zu minimieren und bildet die Grundlage für die Modernisierung der PKI.

Komplexität und Reife

Komplexität und geringe Reife sind wesentliche Ursachen für mangelnde Transparenz und hohe Risiken.

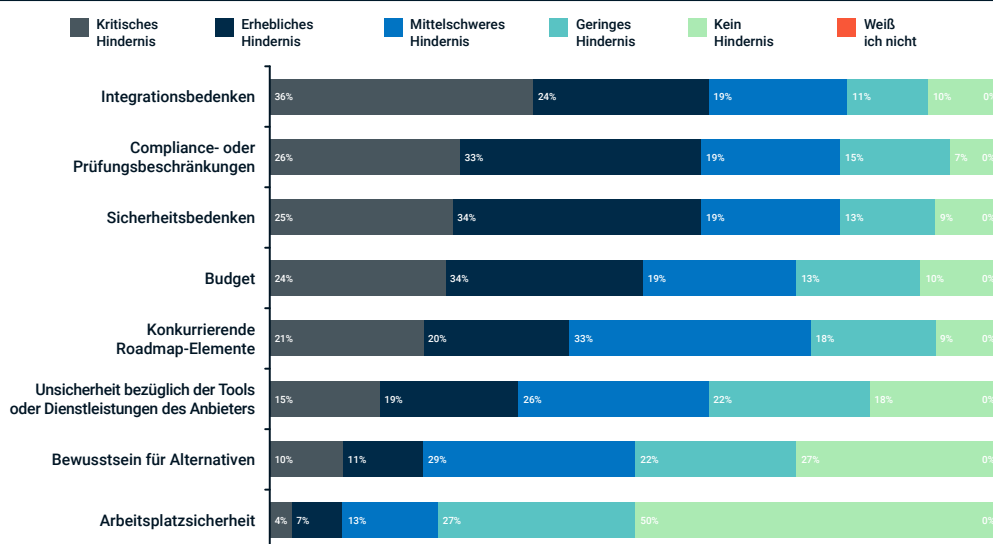
Fragmentierte PKI und fragmentiertes PKI-Management erschweren es zunehmend, die unkontrollierte Zunahme von Zertifikaten in den Griff zu bekommen.

Komplexität stellt sowohl eine strukturelle als auch eine technische Herausforderung dar.

Komplexität ist eine wesentliche Ursache für die anhaltenden Transparenzprobleme. PKI ist nicht nur technisch, sondern auch strukturell komplex geworden. Das Problem besteht nicht einfach nur darin, dass eine Integration schwierig oder ein Arbeitsablauf umständlich ist. Das Problem liegt darin, dass sich das digitale Vertrauen über öffentliche und private PKI, Cloud-Dienste, Legacy-Zertifizierungsstellen, Maschinenidentitäten, Codesignierung, vernetzte Geräte und spezialisierte Plattformen schneller ausgebreitet hat, als die meisten Organisationen in der Lage waren, es zu integrieren und zu steuern.

Die Befragten berichten von Bedenken hinsichtlich einer Vielzahl von Themen, die alle Formen der Komplexität umfassen. Herausforderungen bei der Integration zählen zu den größten Hindernissen für Fortschritte im operativen Betrieb. Fachleute nannten jedoch auch Sicherheits- und Compliance-Probleme sowie Herausforderungen bei Budget und Planung. Hier zeigt sich, dass Organisationen nicht mit einem einzigen Hindernis zu kämpfen haben. Die Implementierung und der Betrieb einer leistungsfähigeren PKI werden durch ein Geflecht architektonischer, prozessbezogener und organisatorischer Abhängigkeiten erschwert.

Inwieweit stellen die folgenden Punkte ein Hindernis für die Einführung der automatisierten Zertifikatsverwaltung in Ihrem Unternehmen dar?



Welche Herausforderungen haben Sie bei der Implementierung der PKI-Modernisierung erlebt bzw. erwarten Sie in der Zukunft?

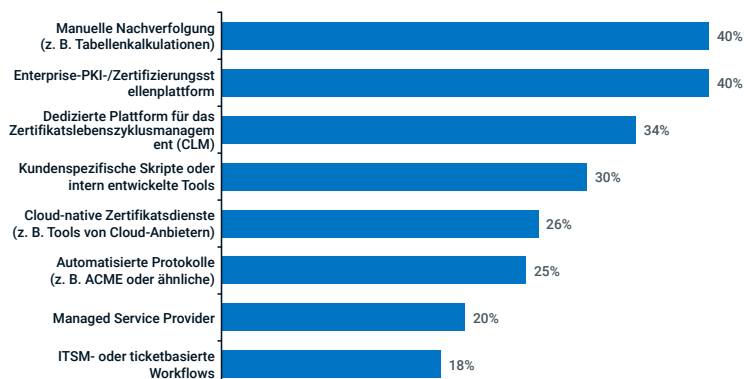


Mehrere Zertifikatsverwaltungsprozesse genügen den Anforderungen von Unternehmen nicht.

Viele Unternehmen arbeiten nicht mit einem einheitlichen Zertifikatsverwaltungsmodell. Sie verwenden mehrere Methoden gleichzeitig, wobei die manuelle Nachverfolgung oft neben Enterprise-PKI-Lösungen (Private CA), Zertifikatslebenszyklus-Management-Plattformen, benutzerdefinierten Skripten und IT-Workflow-Software (ITSM) existiert.

Im Durchschnitt nutzen Unternehmen zwei bis drei verschiedene Methoden gleichzeitig. Dies hat zur Folge, dass sich viele Organisationen in einem Übergangsstadium befinden – von nicht vorhandener Automatisierung über Teilautomatisierung bis hin zur vollständigen Automatisierung. In der Praxis bedeutet Teilautomatisierung die automatische Erneuerung des Zertifikats, nicht aber dessen Installation. Dies ist zwar eine Verbesserung gegenüber vollständig manuellen Prozessen, doch ohne durchgängige Automatisierung bleibt das Ausfallrisiko hoch.

Welche Methoden/Plattformen nutzt Ihre Organisation derzeit für die Zertifikatsverwaltung?



Manuelle Methoden können die unkontrollierte Verbreitung von Zertifikaten nicht bewältigen – insbesondere Tabellenkalkulationen nicht.

Tabellenkalkulationen dienen seit Jahrzehnten als Grundlage für die PKI-Inventar- und Statusverwaltung. Sie sind praktisch, vertraut und oft der schnellste Weg, ein Team in Bewegung zu halten. Das Problem ist, dass sie für eine Aufgabe eingesetzt werden, für die sie nie geschaffen wurden. Mit steigendem Zertifikatsvolumen und sinkenden Verlängerungsfristen verlieren Tabellenkalkulationen ihre Funktion als Managementinstrument und werden stattdessen zu einem Risikomultiplikator.

Bevor es zuverlässige automatisierte Tools gab, waren Tabellenkalkulationen notwendig. Heutzutage können jedoch ausgereifte Plattformen für das Zertifikatslebenszyklusmanagement, Interoperabilitätsstandards, Richtlinienkontrollen und die automatisierte Installation einen erheblichen Teil des Aufwands reduzieren, der mit Tabellenkalkulationen und anderen manuellen Prozessen verbunden ist. Entscheidend ist die richtige Reihenfolge: Rationalisieren, integrieren und automatisieren. Sie zunächst die Zertifikatsanwendungsfälle mit dem größten Nutzen, anstatt zu versuchen, das gesamte PKI-Ökosystem des Unternehmens auf einmal unter einer einzigen Automatisierungsplattform zusammenzuführen.

Die zentrale Erkenntnis

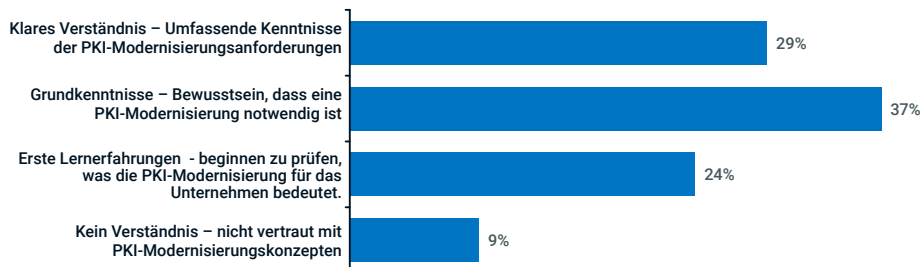
Komplexität ist zwar eine Herausforderung, aber sie ist machbar. Dies ist ein Beweis dafür, dass PKI ein einheitliches Betriebsmodell benötigt, mit schrittweiser Konsolidierung, zuverlässigen Integrationen und Automatisierung, die zunächst dort angewendet wird, wo das Risiko am höchsten ist.

PKI-Reife bedeutet, bewährte Praktiken im Betrieb zu verankern

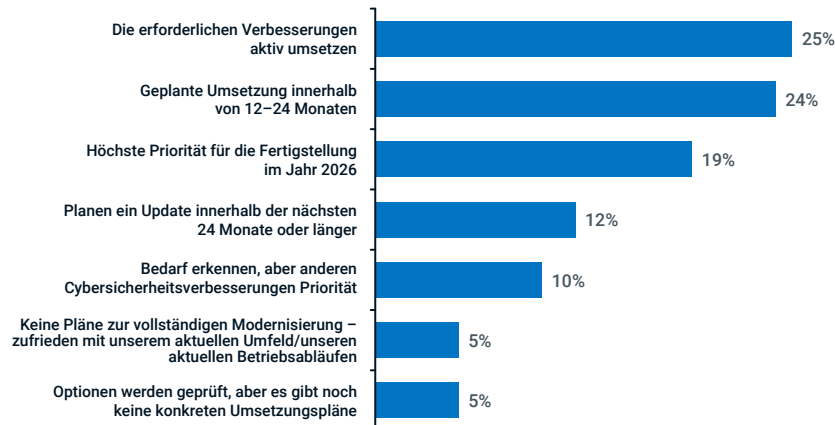
PKI-Reife ist erreicht, wenn aus guten Absichten ein Betriebsmodell wird, das es dem Unternehmen ermöglicht, sicher zu skalieren und schneller zu agieren. Es geht darum, die Transparenz, die Verantwortlichkeit, die Steuerung und die wiederholbaren Prozesse aufzubauen, die erforderlich sind, um PKI als intelligentes System zu betreiben. Gemessen an diesem Maßstab befindet sich die PKI-Modernisierung noch in einem frühen Stadium, aber nicht mehr ganz am Anfang. Das wirkt unausgewogen: Bewusstsein, Dringlichkeit und Umsetzung entwickeln sich nicht im gleichen Tempo.

Diese Diskrepanz wird in der Umfrage deutlich. Fast drei von zehn Befragten geben an, dass ihre Organisation ein klares Verständnis der PKI-Modernisierung hat, und jeder vierte gibt an, dass er die erforderlichen Verbesserungen bereits umsetzt. Gleichzeitig sind etwa 80% entweder bereits aktiv oder planen, in den nächsten ein bis drei Jahren aktiv zu werden. Es gibt zwar eine allgemeine Absicht, aber die Umsetzung bleibt uneinheitlich.

Angesichts der zunehmenden Notwendigkeit, die Lebensdauer von Zertifikaten zu verkürzen, und des bevorstehenden Einflusses von PQC müssen Unternehmen ihre PKI-Infrastrukturen aktualisieren. Wie ist das Verständnis Ihrer Organisation von der PKI-Modernisierung?



Welche Pläne verfolgt Ihre Organisation zur vollständigen Modernisierung der PKI-Infrastruktur?



Es gibt auch Anzeichen dafür, dass sich die Kommunikation innerhalb von Organisationen verbessert. Etwas mehr als die Hälfte der Befragten beschreibt ihr geschäftliches Verständnis von digitaler Identität und kryptografischer Integrität als gründlich oder gut, während weitere 35% angeben, dass das Unternehmen zwar Kryptografie versteht, sie aber dennoch in erster Linie als IT-Thema betrachtet. Mit anderen Worten: PKI gewinnt für die Führungsebene zunehmend an Bedeutung, aber viele Organisationen sind noch dabei, dieses Bewusstsein in Prozessdisziplin und Governance umzusetzen.

Welches allgemeine Verständnis herrscht Ihrer Ansicht nach innerhalb der Branche hinsichtlich der Bedeutung einer effektiven und modernen PKI?

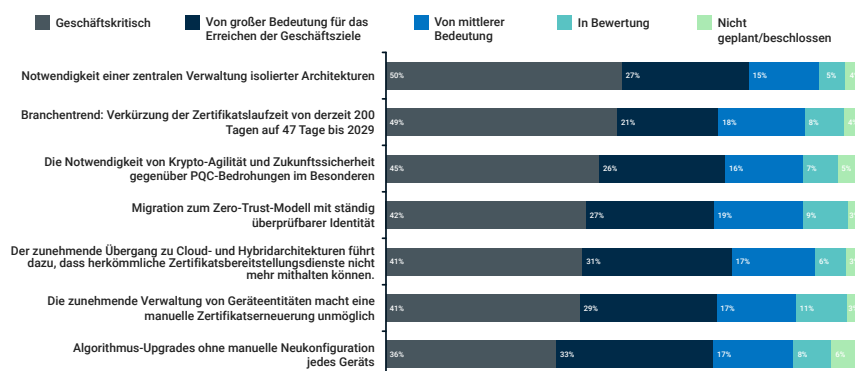


Reife Organisationen setzen auf zentrales PKI-Management.

In isolierten Umgebungen wird es schwieriger, vollständige Transparenz zu gewährleisten, Risiken im Zusammenhang mit der unkontrollierten Ausbreitung von Zertifikaten zu vermeiden und alle Zertifikate zu verwalten. Wir beobachten, dass sich etablierte Unternehmen für ein zentralisiertes PKI-Management entscheiden, wobei 76% es als geschäftskritisch oder äußerst wichtig einstufen.

Neben der einheitlichen Verwaltung zeigen die Verkürzung der Zertifikatslebensdauer und die Vorbereitung auf Post-Quantum-Bedrohungen, wie ein ausgereiftes Betriebsmodell aussehen sollte: kritische PKI-Infrastruktur zentralisieren, wiederkehrende Vorgänge automatisieren und Veränderungen von Anfang an einplanen, anstatt PKI als statisch zu betrachten.

Wie wichtig sind die folgenden Faktoren, die den Bedarf Ihres Unternehmens an einer Modernisierung/Aktualisierung Ihrer PKI-Umgebung beeinflussen/beeinflussen würden?



Verbesserte Ergebnisse durch PKI-Modernisierung

Die Ergebnisse der Umfrage deuten auf deutliche Verbesserungen in den betroffenen Bereichen nach der Einführung einer modernisierten PKI hin. Von den Befragten, die eine modernisierte PKI nutzen, berichten 64% über ein automatisiertes Lebenszyklusmanagement, 60% nennen weniger Ausfallzeiten, 44% weisen auf eine bessere Unterstützung bei der Einhaltung gesetzlicher Vorschriften hin und 43% geben an, mehr Transparenz und Kontrolle gewonnen zu haben. Eine gut durchgeführte Modernisierung reduziert Ausfallzeiten, senkt den Verwaltungsaufwand und vereinfacht die Einhaltung von Vorschriften. Die PKI-Reife definiert sich nicht darüber, wie viele Zertifizierungsstellen eine Organisation besitzt oder wie viele Tools sie erworben hat. Sie wird dadurch definiert, ob die Organisation eine Reihe praktischer operativer Fragen zuverlässig beantworten kann: Was haben wir, wem gehört es, wann wird es erneuert, welcher Dienst ist davon abhängig, welche Richtlinien gelten und können wir Änderungen ohne Unterbrechung vornehmen?

Die zentrale Erkenntnis

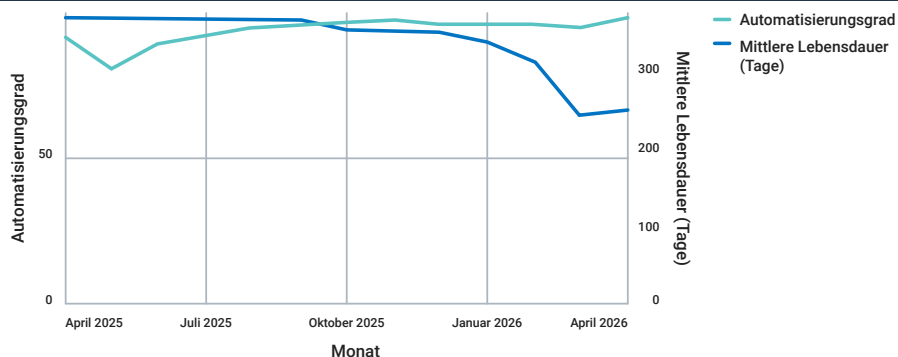
Die Organisationen erkennen das Problem und beginnen zu verstehen, was sie tun müssen. Diejenigen, die bei der Umsetzung am weitesten fortgeschritten sind, sehen bereits die Vorteile.



47-Tage-Vorgabe und Automatisierung

Daten zum Zertifikatsmanagement von DigiCert ONE-Kunden zeigen, dass diese die Laufzeiten öffentlicher TLS-Zertifikate verkürzten, nachdem das CA/B Forum einer schrittweisen Reduzierung der Zertifikatsgültigkeitsdauer auf 47 Tage zugestimmt hatte. Diese schrittweise Reduzierung bedeutet nicht zwangsläufig, dass eine Organisation mehr Zertifikate verwalten muss. Allerdings müssen die Sicherheitsteams die damit verbundenen Aufgaben im Zertifikatslebenszyklus häufiger durchführen.

Automatisierungsgrad vs. mittlere Lebensdauer öffentlicher Zertifikate



KI und Quantencomputing

KI und Quantencomputing beschleunigen den Wandel und markieren zugleich einen Paradigmenwechsel

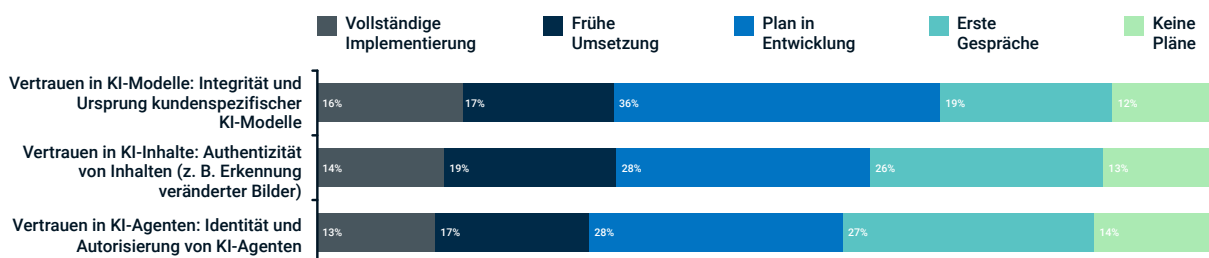
Diese neuen Technologien stellen die größte Herausforderung – und vielleicht die einzige wirklich grundlegende Transformation – für die PKI seit Jahrzehnten dar.

Vertrauen in KI-Inhalte, -Modelle und -Agenten stellt besondere Anforderungen an PKI

Künstliche Intelligenz erhöht die Anforderungen an Digital Trust, da Organisationen, komplexere Fragen zu Identität, Herkunft und Autorisierung in kürzester Zeit zu beantworten. Wenn Unternehmen autonome Agenten einführen, Modelle bereitstellen und Inhalte generieren, benötigen sie verlässlichere Möglichkeiten, um nachzuweisen, was authentisch und vertrauenswürdig ist und was handeln darf. Solche Fragestellungen lassen sich bereits heute mit PKI lösen, doch durch KI treten sie stärker in den Vordergrund.“Die Umfrage zeigt, dass Führungskräfte den starken Zusammenhang zwischen der Herausforderung der künstlichen Intelligenz und PKI bereits erkannt haben. Rund drei Viertel der Befragten geben an, dass PKI eine wichtige Rolle bei der Nutzung von KI spielen wird.

Was noch fehlt, ist die Bereitschaft. Die Befragten gaben an, dass Organisationen zwar zunehmend die Relevanz von PKI für die Sicherheit und Governance im Zusammenhang mit KI erkennen, sich die meisten jedoch noch in der frühen Planungs- und Implementierungsphase befinden. Das vorherrschende Muster ist nicht die breite Übernahme ausgereifter Prozesse, sondern eine Mischung aus ersten Erkundungen, der Entwicklung von Plänen und ersten Projekten.

Wie lässt sich Ihr aktueller Planungsstand hinsichtlich dieser spezifischen Aspekte des Vertrauens in KI am besten beschreiben?

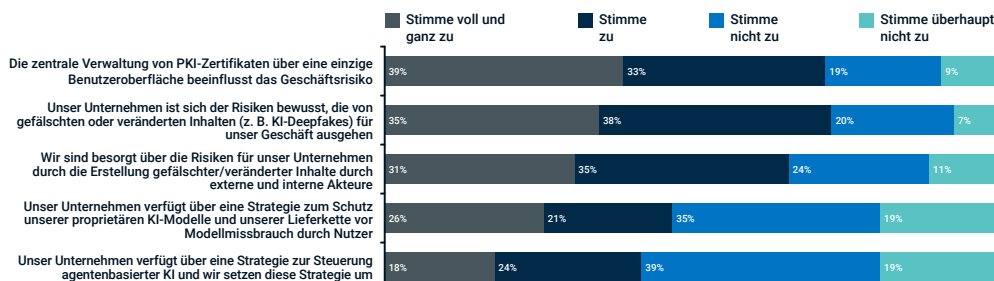


Von der Risikowahrnehmung zu einer operativen Strategie für AI Trust

Im Bereich Governance zeigt sich am deutlichsten, wie groß die Lücke bei der Einsatzbereitschaft noch ist. Die Mehrheit der Befragten ist nicht der Meinung, dass ihr Unternehmen über eine Strategie zur Steuerung und Umsetzung von agentenbasierter KI verfügt. Mehr als die Hälfte gibt zudem an, keine Strategie zu haben, um firmeneigene KI-Modelle zu schützen und die Lieferkette möglicherweise eingesetzter externer Modelle abzusichern. Gleichzeitig geben 73% an, dass ihr Unternehmen die Risiken gefälschter oder veränderter Inhalte versteht, 66% sagen, dass sie trotz der von ihnen ergriffenen Maßnahmen weiterhin besorgt sind, und 72% sagen, dass eine zentrale Transparenz für das PKI-Zertifikatsmanagement im Zeitalter der KI von entscheidender Bedeutung sein wird.

Deshalb sollte KI als Impulsgeber für die Modernisierung der PKI verstanden werden und nicht als eigenständige Digital Trust Initiative. Organisationen, die heute keinen Einblick über den Einsatz ihrer Zertifikate haben und diesen nicht kontrollieren können, werden morgen Schwierigkeiten haben, KI-Agenten, -Modellen und -Inhalten zu vertrauen.

Inwieweit stimmen Sie den folgenden Aussagen zu?



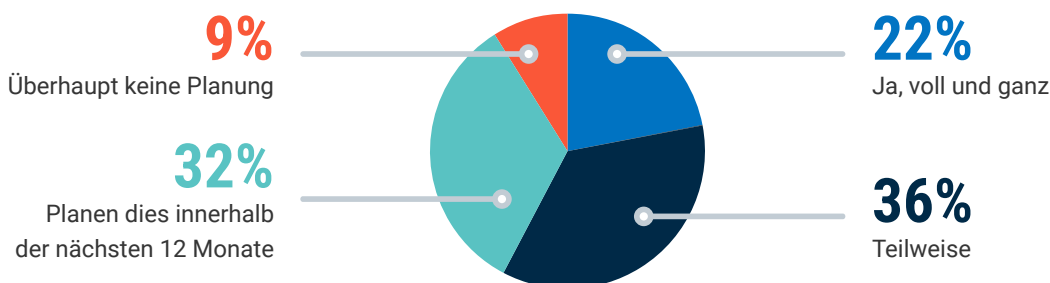
Die zentrale Erkenntnis

KI-Vertrauen ist keine von der PKI-Modernisierung getrennte Disziplin. Das ist einer der deutlichsten Gründe, warum Organisationen jetzt eine stärkere Governance benötigen.

Quantencomputing rückt schnell näher. Planung braucht Zeit.

Während KI derzeit die unmittelbarste Herausforderung für Digital Trust darstellt, rückt auch das Quantencomputing immer näher. Der Übergang zur Post-Quanten-Kryptographie wird keine routinemäßige Aktualisierung oder eine einmalige Aktivität sein. Es wird von den Organisationen ein Verständnis dafür erfordert, wo die Kryptographie angesiedelt ist, welche Systeme von ihr abhängen, wie diese Abhängigkeiten miteinander verbunden sind und wie der Übergang mit möglichst geringen Störungen gestaltet werden kann. Die Umfrageergebnisse zeigen sowohl das Bewusstsein als auch die noch unerledigten Aufgaben auf. Lediglich 22% der Befragten geben an, kryptografische Bibliotheken und Systeme vollständig auf Schwachstellen gegenüber künftigen Angriffen durch Quantencomputer untersucht zu haben. Weitere 36% geben an, sie teilweise bewertet zu haben, und 32% geben an, dies innerhalb der nächsten 12 Monate zu planen. Eine vollständige Einsatzbereitschaft ist noch selten, doch die meisten Organisationen bewegen sich in die richtige Richtung. Dies deckt sich mit den Faktoren, die die Befragten als Treiber der Modernisierung nennen. Mehr als 71% geben an, dass die Notwendigkeit kryptografischer Agilität und Zukunftssicherheit gegenüber Quantenbedrohungen für ihr Geschäft kritisch oder von großer Bedeutung ist. Führungskräfte erkennen die strategische Bedeutung der Vorbereitung auf das Quantenzeitalter, auch wenn die dafür erforderliche Bestandsaufnahme und Migration noch am Anfang stehen.

Hat Ihre Organisation kryptografische Bibliotheken und Systemschwachstellen im Hinblick auf zukünftige Quantencomputerangriffe bewertet?



Der entscheidende Punkt ist, dass die Vorbereitung auf das Quantenzeitalter auf denselben operativen Grundlagen beruht, die in diesem Bericht bereits ausführlich erörtert wurden. Eine Organisation kann nicht kryptografisch agil werden, wenn sie nicht weiß, wo Zertifikate, Schlüssel, Algorithmen und kryptografische Bibliotheken eingesetzt werden. Eine koordinierte Umstellung lässt sich nicht planen, wenn die Zuständigkeiten fragmentiert sind oder die Prozesse im Zertifikatslebenszyklus weiterhin manuell ablaufen. Die Vorbereitung auf das Quantenzeitalter beginnt daher lange bevor eine Organisation einen neuen Algorithmus einführt.

Die zentrale Erkenntnis

Die Vorbereitung auf das Quantenzeitalter ist keine separate Aufgabe. Ein vollständiges Zertifikatsinventar und die Automatisierung des Zertifikatslebenszyklus schaffen zugleich die nötige Agilität für die Migration zur Post-Quanten-Kryptografie.

PKI-Modernisierung

PKI-Modernisierung begegnet den Herausforderungen rund um Transparenz, Komplexität, PKI-Reife, KI und Quantencomputing.

Die zentrale Aussage dieser Studie ist nicht, dass Organisationen bei PKI scheitern. Vielmehr reichen die Ansätze, die viele Organisationen noch immer zur Verwaltung ihrer PKI einsetzen, den heutigen Anforderungen nicht mehr aus. Das Problem ist leichter zu lösen, als es zunächst scheint. Führungskräfte erkennen die Notwendigkeit der Modernisierung und stellen dafür Mittel bereit; die meisten Organisationen planen bereits entsprechende Maßnahmen. Ziel ist es, diese Dynamik in verlässliche operative Kontrolle zu überführen.

Für IT- und Sicherheitsverantwortliche bedeutet dies, die Modernisierung der PKI als zentrale Aufgabe zu verstehen. PKI beeinflusst die Verfügbarkeit, die betriebliche Effizienz, die KI-Governance und die kryptografische Agilität. Organisationen, die ihre Modernisierung effektiv gestalten, werden nicht nur die durch Zertifikatsprobleme bedingten Ausfälle reduzieren oder die betriebliche Effizienz verbessern, sie schaffen darüber hinaus eine intelligente und skalierbare Grundlage für Digital Trust die auch den künftigen Anforderungen durch Maschinenidentitäten, den zunehmenden KI-Einsatz und die Quantensicherheit gerecht wird.

PKI-Modernisierung kann weit gefasst erscheinen – und das ist sie auch. Unkonkret ist sie deshalb jedoch nicht. Beginnen Sie dort, wo der operative Nutzen unmittelbar ist und der Business Case leicht zu erklären ist.

Zertifikate erfassen und inventarisieren

Risiken aufgrund mangelnder Transparenz beheben

Erstellen Sie ein zuverlässiges Inventar von Zertifikaten und zugehörigen kryptografischen Assets in öffentlichen und privaten Umgebungen. Fügen Sie dann Kontextinformationen wie Zuständigkeiten und Auswirkungen auf das Unternehmen hinzu, um aus den Rohdaten verwertbare Informationen zu gewinnen. Dies ist die Grundlage für alles Folgende. Durch die Bestandsaufnahme wird aus ‚wir glauben‘ ein ‚wir wissen‘.

Automatisierung kritischer Zertifikate

Schließen Sie Prozesslücken und vermeiden Sie Versäumnisse, um die Komplexität zu beherrschen und den PKI-Reifegrad zu erhöhen.

Öffentliches TLS/SSL ist der universellste Anwendungsfall für eine Modernisierung, da jede Organisation mit Internetkontakt von kürzeren Zertifikatslebensdauern betroffen ist. Der Rhythmus verläuft nur in eine Richtung. Die Automatisierung der Ausstellung und Installation öffentlicher TLS-Zertifikate ist daher einer der schnellsten Wege, das Ausfallrisiko zu reduzieren und gleichzeitig eine wiederholbare Lebenszyklusfähigkeit aufzubauen. Sie hilft den Teams außerdem, wiederverwendbare Abläufe zu etablieren, mit denen sich die Automatisierung anschließend auf interne PKI, Codesignierung, Geräteidentitäten und weitere Bereiche von Digital Trust ausweiten lässt.

Standardisierung der internen PKI

Fragmentierung reduzieren und sich auf künftige kryptografische Veränderungen vorbereiten

Interne PKI ist oft der Bereich, in dem sich Komplexität am schnellsten anhäuft und veraltete Praktiken am längsten bestehen bleiben. Mit zunehmendem Zertifikatsvolumen und sich weiterentwickelnden kryptografischen Anforderungen erhöhen uneinheitliche Vorgehensweisen das operationelle Risiko und erschweren die Koordination von Veränderungen.

Organisationen sollten eine zentrale Steuerung etablieren, indem sie Richtlinien für interne PKI-Umgebungen definieren. Richtlinien können Faktoren wie zugelassene Zertifizierungsstellen, Geschäftskritikalität und Zuständigkeiten, Standards für Zertifikate und kryptografische Konfigurationen sowie Compliance-Anforderungen festlegen. Einheitliche Richtlinien verbessern die Transparenz, verringern operative Reibungsverluste, vereinfachen die Einhaltung von Vorschriften und schaffen eine stärkere Grundlage für zukünftige Initiativen wie KI-Governance und Post-Quanten-Kryptographie.

Richtlinien ermöglichen es Organisationen, unnötige oder sich überschneidende Zertifizierungsstellen zu konsolidieren, veraltete Plattformen außer Betrieb zu nehmen und isolierte interne PKI-Umgebungen unter ein einheitlicheres Governance-Modell zu bringen. Zuerst sollten schwerwiegende Verstöße gegen die Richtlinien behoben werden. Ziel ist es nicht, alles auf einmal neu aufzubauen, sondern das Risiko sowohl bei aktuellen als auch bei neuen PKI-Anwendungen systematisch zu reduzieren.

Methodik

Dieser Bericht basiert auf einer von Omdia im April 2026 unabhängig durchgeführten Primärstudie. Die Umfrage befasste sich mit der Entwicklung von PKI, den Treibern der Modernisierung, operative Herausforderungen und künftige Fragestellungen.

An der Studie nahmen 423 Entscheidungsträger auf Führungsebene teil, darunter CISOs, CIOs und leitende IT-/Sicherheitsverantwortliche, die für Cybersicherheit, PKI und digitale Infrastruktur zuständig sind. Die Befragten repräsentierten die Bereiche Produktentwicklung und Forschung & Entwicklung, IT und technische Betriebsabläufe, Cybersicherheit sowie Governance, Risiko und Compliance.

Die Befragten stammten aus Organisationen in Nordamerika, EMEA und dem asiatisch-pazifischen Raum und deckten 11 Branchen ab.



13% Banken,
Finanzdienstleistungen
und Versicherungen



12% Software
oder SaaS



10% Gesundhei-
tswesen



10% Fertigung,
Bauwesen und
Werkstoffe



9% Telekommunikation
und Dienstleistungen



8% Reise und Gastgewerbe



8% Transport und
Logistik



11% Einzelhandel
und
E-Commerce



7% Cloud- oder Managed-
Service-Anbieter



6% Regierung
oder Militär



5% Energie und
Versorgung

Alle teilnehmenden Organisationen hatten mindestens 1.000 Mitarbeiter:

39%

hatten 1.000 bis 4.999
Mitarbeiter

24%

hatten 5.000 bis 9.999
Mitarbeiter

37%

hatten 10.000 oder
mehr Mitarbeiter

Die Fragen zielten darauf ab, die betrieblichen Gegebenheiten und strategischen Prioritäten im Zusammenhang mit der Modernisierung der PKI, Digital Trust und der kryptografischen Zukunftsfähigkeit zu messen. Die Analyse und die Schlussfolgerungen basieren auf den gesammelten Daten, der Forschungsmethodik von Omdia und einem firmeneigenen Datensatz. Bei einigen Fragen waren Mehrfachantworten möglich; daher können die Summen 100 % übersteigen.

Für die ergänzende Analyse wurden Daten aus dem Betrieb der verwalteten PKI und der öffentlichen Zertifizierungsstelle von DigiCert aus dem Zeitraum von Januar 2025 bis März 2026 verwendet. Die Daten umfassten zusammenfassende Statistiken einer Auswahl von 757 Unternehmenskunden. Die Betriebsdaten öffentlicher Zertifizierungsstellen stammten aus den Zertifikattransparenzprotokollen.

Autoren und Mitwirkende

Omdia Consulting

Omdia ist ein marktführendes Daten-, Forschungs- und Beratungsunternehmen, das sich darauf konzentriert, Anbietern digitaler Dienstleistungen, Technologieunternehmen und Unternehmensentscheidern zum Erfolg in der vernetzten digitalen Wirtschaft zu verhelfen. Durch ein globales Netzwerk von Analysten bieten wir Expertenanalysen und strategische Einblicke in die IT-, Telekommunikations- und Medienbranche. Omdias einzigartige Kombination aus verlässlichen Daten, Marktanalysen und branchenspezifischer Expertise dient der Unterstützung von Entscheidungsprozessen. Omdia ist Teil von Informa TechTarget, die Informa-Gruppe ist an der Londoner Börse notiert.

Starten Sie jetzt Ihre
PKI-Modernisierungsreise.



Über DigiCert

DigiCert ist ein weltweit führender Anbieter von intelligenten Vertrauenslösungen. Wir schützen die digitale Welt, indem wir die Sicherheit, den Datenschutz und die Authentizität jeder Interaktion gewährleisten. Unsere KI-gestützte DigiCert ONE Plattform vereint PKI, DNS und Zertifikatslebenszyklusmanagement, um Infrastruktur, Software, Geräte, Nachrichten sowie KI-Inhalte, Agenten und Modelle zu sichern. Erfahren Sie unter www.digicert.com/de, warum mehr als 125.000 Organisationen, darunter 90% der Fortune 500-Unternehmen, DigiCert wählen, um die heutigen Bedrohungen abzuwehren und sich auf eine quantensichere Zukunft vorzubereiten.