

# AKTUELLER STAND DER PKI-AUTOMATISIERUNG

Bericht 2021



# BERICHT ZUM AKTUELLEN STAND DER PKI-AUTOMATISIERUNG

Beinahe allem, was Technologie betrifft, liegt eine PKI zugrunde. Sie ermöglicht die Authentifizierung und Signierung für Benutzer, Server, IoT- und sonstige Geräte sowie DevOps-Anwendungen und -Dienste. Neben vielen weiteren Einsatzmöglichkeiten unterstützt sie auch die digitale Dokumentsignierung.

Doch die manuelle Verwaltung einer PKI übersteigt schnell die verfügbaren Ressourcen. Laut einer aktuellen Ponemon-Untersuchung<sup>1</sup> mussten Unternehmen 2020 im Vergleich zum Vorjahr 43 Prozent mehr PKI-Zertifikate verwalten. Hinzu kommen immer kürzere Zertifikatslaufzeiten und so dauert es wohl nicht mehr lange, bis die PKI-Zertifikatsverwaltung Unternehmen in die Knie zwingt.

Um besser zu verstehen, wie Unternehmen mit dieser Herausforderung umgehen, beauftragte DigiCert das Marktforschungsunternehmen ReRez Research aus Dallas mit einer Umfrage unter IT-Führungskräften mit PKI-Verantwortung in weltweit 400 Unternehmen. Das Ergebnis zeigt eine PKI-Zertifikatslandschaft in Aufruhr, gibt aber auch Aufschluss darüber, wie erfolgreiche Unternehmen ihre PKI managen.

## WAS IST PKI-AUTOMATISIERUNG?

Wir haben für die Umfrageteilnehmer definiert, welche Aspekte die PKI-Automatisierung umfasst:

- Ermittlung vorhandener digitaler Zertifikate
- Ausstellung neuer digitaler Zertifikate
- Erneuerung digitaler Zertifikate, deren Ablaufdatum kurz bevorsteht
- Widerruf digitaler Zertifikate bei Bedarf
- Automatisierung des Code Signing
- Registrierungsprozess für Client-Zertifikate
- Identitätsprüfung (z. B. zum Signieren von Dokumenten)
- Automatisierung erweiterter Bereitstellungsaktivitäten wie dem Eintrag bei LDAP und Exchange
- Sonstige organisatorische Aufgaben der PKI-Verwaltung

Die Anzahl der PKI-Zertifikate, die Unternehmen verwalten müssen, stieg um

**43 %**

<sup>1</sup> „2020 Global PKI and IoT Trends Study“, Ponemon

## RASCHE VERBREITUNG VON PKI SORGT FÜR VERWIRRUNG

Laut unserer Untersuchung verwaltet ein modernes Unternehmen im Schnitt mittlerweile mehr als 50.000 Zertifikate. Am häufigsten kommen Benutzer- und Serverzertifikate vor, gefolgt von Zertifikaten für Webserver, Mobilgeräte und E-Mail. Unternehmen verwalten ein Drittel mehr öffentliche Zertifikate (ausgestellt von öffentlichen Zertifizierungsstellen) als private (ausgestellt von einer internen, privaten Zertifizierungsstelle).

Ein Unternehmen verwaltet im Schnitt heute  
mittlerweile mehr als **50.000** Zertifikate.

Im Vergleich zu den Vorjahren ist das ein starker Anstieg und es gibt zahlreiche Hinweise darauf, dass die Unternehmen dieser Aufgabe kaum Herr werden. So haben zwei Drittel von ihnen bereits einen Ausfall erlebt, weil ein Zertifikat unerwartet ablief. Ein Viertel trafen solche Ausfälle fünf bis sechs Mal – allein in den letzten sechs Monaten.

Warum? Teilweise ist der erhöhte Arbeitsaufwand das Problem. Beinahe zwei Drittel der Befragten äußerten sich einigermaßen bis äußerst besorgt über den zeitlichen Aufwand für die Zertifikatsverwaltung. Aber auch mangelnde Transparenz wurde als Problem genannt. In 37 Prozent der Unternehmen sind mehr als drei Abteilungen an der Zertifikatsverwaltung beteiligt, was ein einheitliches Vorgehen erschwert. Die an der Umfrage beteiligten Unternehmen geben an, dass im Schnitt bis zu 1.200 Zertifikate eigentlich gar nicht verwaltet werden, und beinahe die Hälfte der Befragten (47 Prozent) entdeckt regelmäßig nicht genehmigte Zertifikate, also Zertifikate, die ohne das Wissen oder die Hilfe der IT-Abteilung implementiert wurden. PKI-Automatisierung bietet hier offensichtlich Abhilfe, weshalb wir uns für den PKI-Automatisierungsgrad in den befragten Unternehmen interessierten.

**61 %** BESCHWEREN SICH ÜBER  
DEN ZEITAUFWAND FÜR DIE  
ZERTIFIKATSVERWALTUNG

**47 %** FINDEN REGELMÄSSIG  
NICHT GENEHMIGTE  
ZERTIFIKATE

**37 %** BETEILIGEN  
MINDESTENS DREI  
ABTEILUNGEN AN DER  
ZERTIFIKATSVERWALTUNG

**1 VON 4**    

UNTERNEHMEN VERZEICHNETE 5–6 DURCH PKIS VERURSACHTE  
AUSFÄLLE IN DEN LETZTEN SECHS MONATEN

# 91 % DER UNTERNEHMEN WÜNSCHEN SICH PKI-AUTOMATISIERUNG

Aus unserer Umfrage ging hervor, dass die PKI-Automatisierung in den meisten Unternehmen (91 Prozent) zumindest diskutiert wird. Nur neun Prozent gaben an, PKI-Automatisierung nicht in Erwägung zu ziehen und dies auch nicht ändern zu wollen. Ein Großteil der Unternehmen (70 Prozent) geht davon aus, innerhalb von 12 Monaten eine Lösung zu implementieren. Ein Viertel der Befragten befindet sich derzeit in der Implementierungsphase oder hat diese sogar schon abgeschlossen. Doch leicht ist es nicht. Als gängige Hürden nennen Unternehmen hohe Automatisierungskosten, Komplexität, Compliance-Probleme sowie Widerstand bei Mitarbeitern und Managern.



## TRENDS

Häufige Gründe für die Einführung von PKI-Automatisierung:

1. Zertifikatwildwuchs
2. Bereitschaft für das Quantenzeitalter
3. Rapide schrumpfende Zertifikatslaufzeiten, die Unmengen an Mehrarbeit verursachen
4. Sehr schnell ansteigende Anzahl der verwalteten Zertifikate
5. Trend zur Arbeit im Homeoffice



## PROBLEME

Sicherheitsprobleme, die Unternehmen zur Automatisierung bewegen:

1. Langsame Bereitstellung neuer Zertifikate
2. Tendenz zur Fehlkonfiguration von Zertifikaten
3. Überlastetes Personal
4. Zu viele nicht konforme Zertifikate
5. Verpasste Ablauffristen von Zertifikaten
6. Langsames oder gar ausbleibendes Widerrufen von Zertifikaten, wenn dies nötig ist



## NEGATIVE KONSEQUENZEN

Die Nachteile ohne PKI-Automatisierung:

1. Compliance-Probleme
2. Sicherheitsprobleme
3. Hohe Kosten
4. Ausfälle
5. Verärgerte Kunden oder Mitarbeiter



## ZIELE

Vorteile der PKI-Automatisierung in Unternehmen:

1. Mehr Sicherheit
2. Bessere Compliance
3. Mehr Flexibilität
4. Mehr Produktivität
5. Weniger Ausfälle und Kosten

# SPITZENREITER UND SCHLUSSLICHTER

Mit einer Reihe von Fragen überprüften wir, wie die Befragten in einem breiten Spektrum an PKI-Kennzahlen abschnitten:

- Vermeiden von Ausfällen aufgrund unerwartet abgelaufener Zertifikate
- Schnelles Widerrufen von Zertifikaten, wenn dies nötig ist
- Effizienz der Verwaltung digitaler Zertifikate
- Minimieren von Sicherheitsrisiken aufgrund unsachgemäßer Zertifikatsverwaltung
- Vermeiden von Compliance-Problemen aufgrund unsachgemäßer Zertifikatsverwaltung
- Minimieren des Zertifikatwildwuchses
- Einhaltung PKI-spezifischer SLAs
- Schnelligkeit beim Ausstellen und Widerrufen von PKI-Zertifikaten

Je nach Erfolg bewerteten wir jede Antwort von positiv bis negativ und rechneten dann alles zusammen.

Um ein genaueres Bild vom Stand der Dinge bei den Befragten zu erhalten, teilten wir sie in drei Gruppen ein:

1

## SPITZENREITER

Über alle oben aufgeführten Bereiche hinweg erzielten diese Unternehmen die besten Ergebnisse.

2

## MITTELFELD

Über alle oben aufgeführten Bereiche hinweg erzielten diese Unternehmen mittlere Ergebnisse.

3

## SCHLUSSLICHTER

Über alle oben aufgeführten Bereiche hinweg erzielten diese Unternehmen die schlechtesten Ergebnisse.

Anschließend verglichen wir die Spitzenreiter mit den Schlusslichtern, um die Unterschiede zu ermitteln und herauszufinden, was die Spitzenreiter anders machen.

# VORNEWEG STATT HINTERHER

Die befragten Unternehmen äußerten sich freimütig zu den Herausforderungen, vor die die PKI-Verwaltung sie stellt, z. B. Zertifikatwildwuchs, Ausfälle durch unerwartet abgelaufene Zertifikate und vieles mehr. Doch nicht alle Unternehmen haben gleichermaßen zu kämpfen. Wir teilten also die Befragten in drei Stufen ein und verglichen die oberste mit der untersten. Dabei traten markante Unterschiede zutage.

Die Spitzenreiter sind rundum erfolgreicher. Auffallend ist, dass ein Drittel (33 Prozent) mit größerer Wahrscheinlichkeit angibt, PKI-Automatisierung sei überhaupt wichtig. In den folgenden Punkten sind die Spitzenreiter zwei- bis dreimal besser:

- Minimieren PKI-bezogener Sicherheitsrisiken
- Vermeiden von Ausfällen der PKI
- Reduzieren nicht konformer Zertifikate
- Einhalten PKI-relevanter SLAs
- Verwalten digitaler Zertifikate
- Ausstellen und Widerrufen von Zertifikaten
- Compliance

Die Schlusslichter hingegen erleben schwerwiegende negative Konsequenzen aus der unzureichenden PKI-Zertifikatsverwaltung. Zum Beispiel:

- Compliance-Probleme
- Sicherheitsprobleme
- Produktivitätsverluste
- Verzögerungen
- Überarbeitung
- Kundenabwanderung
- Umsatzverlust

Wie wird man aber zum Spitzenreiter? Was könnte man sich von diesen PKI-Profis abschauen?



# DAS MACHEN SPITZENREITER DER PKI-AUTOMATISIERUNG ANDERS

Der Zeitaufwand für das PKI-Management bereitet Spitzenreitern doppelt so viele Sorgen. Dadurch bleibt das PKI-Management bei ihnen immer im Fokus. Außerdem machen sie sich mehr Gedanken über Zertifikatwildwuchs. Und sie sind der Meinung, PKI-Automatisierung sei wichtig für die Zukunft ihrer Unternehmen. Möglicherweise ist die PKI deshalb bei ihnen mit sechs Mal größerer Wahrscheinlichkeit bereits automatisiert. Was können Sie daraus ableiten und in Zukunft anders machen?


## WIE IM WILDEN WESTEN

Bei genauerer Betrachtung verriet uns die Daten ein interessantes Detail. Gruppen, denen die PKI-Zertifikatsverwaltung theoretisch leichter fallen sollte, hatten im Umgang mit Zertifikaten jedoch oft mehr Schwierigkeiten.

So waren zum Beispiel Unternehmen mit der geringsten Anzahl an Zertifikaten viel eher von Ausfällen durch unerwartet abgelaufene Zertifikate betroffen. Zudem war ihre Leistung bei unterschiedlichen Kennzahlen der PKI-Verwaltung durch die Bank schlechter.

Deshalb zeigten sich diese Unternehmen mit wenigen PKI-Zertifikaten erheblich besorgter in Bezug auf die PKI-Verwaltung, obwohl sie damit in einem viel geringeren Ausmaß beschäftigt sind als Unternehmen mit Unmengen an Zertifikaten. Geringbelastete Unternehmen beispielsweise gaben fast 50 Prozent häufiger an, dass ihnen der Zeitaufwand für die PKI-Zertifikatsverwaltung Sorgen bereite. Darüber hinaus wird bei ihnen ein beinahe doppelt so großer Anteil an PKI-Zertifikaten automatisch verwaltet.

Auf den ersten Blick ein Widerspruch. Die Realität jedoch sieht so aus: Unternehmen mit wenigen Zertifikaten sind bei der PKI-Verwaltung einfach noch nicht so weit wie Unternehmen mit sehr vielen Zertifikaten. Oft verwalten diese 100.000 Zertifikate und mehr, weshalb sie in dieser Hinsicht weit fortgeschritten sind. Unternehmen mit wenigen Zertifikaten befinden sich in einer Art Wildem Westen: keine Regeln, jeder verwaltet Zertifikate auf seine eigene Weise.



**UNTERNEHMEN MIT  
WENIGEN ZERTIFIKATEN  
BEFINDEN SICH IN EINER  
ART WILDEM WESTEN:  
KEINE REGELN, JEDER  
VERWALTET ZERTIFIKATE  
AUF SEINE EIGENE WEISE.**

# DAS MACHEN SPITZENREITER DER PKI-AUTOMATISIERUNG ANDERS

Bei der PKI-Verwaltung erfolgreiche Unternehmen hatten auch einen weitaus besseren Überblick über ihre Zertifikatsbestände, bewerteten sich gleichzeitig aber schlechter als ihre unbesorgteren Mitstreiter. Allerdings verzeichneten dieselben Unternehmen seltener zertifikatsspezifische Ausfälle oder Zertifikatwildwuchs und bewiesen damit, dass sie viel besser zurechtkamen, als sie selbst vermuteten.


## PARADOXE SELBSTEINSCHÄTZUNG

Ebenfalls interessant ist die Selbsteinschätzung der Unternehmen, denen die PKI-Zertifikatsverwaltung die größten Sorgen macht. Besorgte Unternehmen hatten laut unserer Untersuchung objektiv gesehen weniger Probleme, stuften sich selbst aber als weniger erfolgreich ein.

Beispielsweise äußerten sich Unternehmen, die am ehesten antworteten, PKI-Verwaltung sei eine Herausforderung, drei bis fünf Mal eher einigermaßen bis äußerst besorgt über Zertifikatsprobleme wie die Geschwindigkeit, mit der neue Zertifikate ausgestellt werden, das versehentliche Fehlkonfigurieren von Zertifikaten und Zertifikatwildwuchs.

Dennoch berichteten sie von einer weit geringeren Anzahl an nicht konformen Zertifikaten (nur zwei Drittel so viele wie bei vielen der unbesorgten Unternehmen). Zudem erlebten sie viel seltener Ausfälle in Verbindung mit versehentlich abgelaufenen Zertifikaten (nur ein Ausfall in den vergangenen sechs Monaten verglichen mit drei bis fünf Ausfällen bei unbesorgten Unternehmen).

Bei sicherheitsrelevanten Umfragen erleben wir dieses Phänomen häufig. Tatsächlich ist es so, dass die aufmerksamsten Unternehmen sehr genau über ihre Schwächen und Fehler im Bilde sind und deshalb dazu tendieren, sich selbst kritischer zu bewerten, als dies bei weniger aufmerksamen Unternehmen der Fall ist. Durch ihre Aufmerksamkeit verschaffen sie sich jedoch einen Vorsprung gegenüber ähnlichen Unternehmen, die sich nicht mit der Materie befassen.



**BESORGTE UNTERNEHMEN  
HATTEN OBJEKTIV GESEHEN  
WENIGER PROBLEME,  
STUFTEN SICH SELBST  
ABER ALS WENIGER  
ERFOLGREICH EIN.**



# UNSERE EMPFEHLUNGEN

Die heutige Zertifikatslandschaft ist von kürzeren Gültigkeitszeiträumen, immer neuen Kryptografie-Standards und der zunehmenden unternehmensweiten Einführung digitaler Zertifikate in Geschäftsprozessen geprägt. Vor diesem Hintergrund können Sie sich durch die Automatisierung Ihrer PKI-Zertifikate erhebliche Vorteile sichern. Doch worauf sollten Sie dabei achten? Hier sind einige der Bereiche der Zertifikatsverwaltung, in denen Sie Automatisierung nutzbringend einsetzen können.

## ZERTIFIKATSVERWALTUNG

### INVENTUR

Ermitteln Sie alle Zertifikate und listen Sie den Bestand auf.

### PROBLEMBEHEBUNG

Korrigieren Sie Schlüssel und Zertifikate, die von den Unternehmensrichtlinien abweichen.

### SCHUTZ

Sichern Sie das Ausstellen und Widerrufen von Zertifikaten durch Best Practices ab. Standardisieren und automatisieren Sie die Registrierung, Ausstellung und Erneuerung von Zertifikaten.

### MONITORING

Überprüfen Sie Ihren Bestand auf Änderungen.

## AUTOMATISIERUNG VON ZERTIFIKATS-WORKFLOWS

### INVENTUR

Ermitteln Sie nicht verwaltete oder manuelle Zertifikats-Workflows und listen Sie diese auf.

### EINFÜHRUNG

Nutzen Sie automatisierte Lösungen für die Zentralisierung und Verwaltung von Zertifikats-Workflows.

### MONITORING

Behalten Sie von zentraler Stelle aus den Überblick und die Kontrolle.

## GÄNGIGE ZERTIFIKATS-WORKFLOWS

- Web-Server
- Identitätsmanagement von Geräten
- Code Signing
- Digitale Signaturen
- Authentifizierung der Identität & Zugriffskontrolle

# METHODIK

ReRez Research in Dallas (Texas, USA) befragte IT-Fachleute aus 400 Unternehmen der Regionen EMEA, Nordamerika, Lateinamerika und Asien-Pazifik, die mindestens 1.000 Mitarbeiter beschäftigen. Bei den Befragten handelte es sich um IT-Führungskräfte, IT-Sicherheitsverantwortliche und allgemeine IT-Fachleute. Im Fokus standen IT-Experten für die Verwaltung digitaler Zertifikate für Benutzer, Server und Mobilgeräte. Befragt wurden kleine, mittlere und große Unternehmen.

**Die PKI-Automatisierungsexperten bei DigiCert evaluieren gern den Bedarf Ihres Unternehmens und besprechen mit Ihnen maßgeschneiderte Lösungen. [Hier](#) erfahren Sie mehr über den Einstieg in die Automatisierung Ihrer PKI-Landschaft.**