STATE OF PKI AUTOMATION

2021 Report

STATE OF PKI AUTOMATION REPORT

PKI lies at the heart of nearly every aspect of technology. It is crucial to authenticating and signing for users, servers, devices, IoT, DevOps applications and services, digital document signing and so much more.

But managing PKI is quickly becoming impossible to do manually. The number of PKI certificates enterprises need to manage grew by 43 percent year-over-year in a recent Ponemon study[1]. Add that to shrinking certificate validity periods, and the stage is set for enterprises to become overwhelmed by PKI certificate management.

In order to better understand how enterprises are handling this challenge, DigiCert commissioned ReRez Research of Dallas, Texas, to survey IT managers responsible for PKI management at 400 enterprises worldwide. Overall, the results paint a picture of PKI certificate turmoil and also show how the very best organizations are staying on top of PKI management.

The number of PKI certificates enterprises need to manage grew by **43%**

WHAT IS PKI AUTOMATION?

We defined PKI automation for survey respondents as including the following aspects:

- Discovering existing digital certificates
- Issuing new digital certificates
- Renewing digital certificates when they are about to expire
- Revoking digital certificates when necessary
- Automating code signing
- Enrollment process for client certificates
- Identity verification (e.g., for document signing)
- Automating extended provisioning activities, such as entry into LDAP and Exchange
- Other housekeeping activities related to PKI management

1 2020 Global PKI and IoT Trends Study (Ponemon)

RAPID GROWTH OF PKI IS DRIVING CONFUSION

The typical enterprise in our study now manages more than 50,000 certificates. The most common types of certificates are user and server certificates, followed by web servers, mobile devices and email. Enterprises manage a third more public certificates, or those issued by public Certificate Authorities (CAs), than private certificates which are issued by an internal, private CA.

Enterprises today typically manage more than **50,000** certificates.

This is a sharp increase from prior years, and there is ample evidence that enterprises are having trouble managing the workload. In fact, two-thirds have experienced outages caused by certificates expiring unexpectedly. One in four experienced five to six such outages in the past six months alone.

Why? Part of the reason is the increased workload. Nearly two-thirds are somewhat to extremely concerned about how much time is spent managing certificates. But there is also a lack of visibility problem. Thirty-seven percent of enterprises use more than three departments to manage certificates, leading to confusion. The typical enterprise says as many as 1,200 of the certificates are actually unmanaged, and nearly half, or 47 percent, say they frequently discover so-called "rogue" certificates—certificates that were implemented without IT's knowledge or management. An obvious solution to these problems is PKI automation, so we explored how involved enterprises are with PKI automation.

61% ARE CONCERNED ABOUT TIME REQUIRED TO MANAGE CERTIFICATES

47% ENCOUNTER ROGUE CERTIFICATES FREQUENTLY

37% HAVE 3 OR MORE DEPARTMENTS MANAGING CERTIFICATES

1 IN 4 EXPERIENCED 5-6 PKI-RELATED OUTAGES IN THE PAST SIX MONTHS

91% OF ENTERPRISES WANT PKI AUTOMATION

Our survey results showed most companies—or 91 percent—are at the very least, discussing PKI automation. Only nine percent say they are not discussing PKI automation and have no plans to do so. The majority of enterprises, or 70 percent, expect to implement a solution within 12 months. A quarter are actually at the stage where they're already implementing or maybe even finished implementing a solution. But it's not easy. The challenges enterprises cite included high costs to automate, complexity, issues with compliance, and staff and management resistance to change.

TRENDS

Common reasons enterprises are adopting PKI automation:

1. Rogue certificates
2. Post-quantum computing readiness
3. Rapidly shrinking certificate validity periods causing workloads to explode
4. Rapid increases in the number of certificates managed
5. Remote work trends

PAIN POINTS

Security issues driving enterprises to automate:

1. Slowness in provisioning new certificates
2. Propensity to misconfigure certificates
3. Overburdened staff
4. Too many rogue certificates
5. Missing the expiration of certificates
6. A slowness, or even a failure, to revoke certificates when necessary

PENALTIES

The negative costs of not automating PKI:

1. Compliance issues
2. Security issues
3. Cost
4. Downtime
5. Angry customers or employees

GOALS

Enterprises implementing PKI automation want to:

1. Improve security
2. Improve compliance
3. Become more agile
4. Improve productivity
5. Reduce downtime and costs.

TOP-TIER VS. BOTTOM-TIER

We asked a series of questions to determine how well, or poorly, each respondent was doing across a wide range of PKI metrics:

- Avoiding downtime due to certificates expiring unexpectedly
- Revoking certificates quickly when necessary
- Efficiency of managing digital certificates
- Minimizing security risks due to improper certificate management
- Compliance issues due to improper certificate management
- Keeping rogue certificates to a minimum
- Meeting PKI-related SLAs
- Speed of PKI issuance and revocation

We assigned a value to each question based on whether they were doing well or poorly—positive to negative. We then totaled their scores.

To tease out differences in how the respondents were doing, we split the respondents into three groups:

1 **LEADERS**

These are the organizations that had the best scores across the range of metrics listed above.

2 **MIDRANGE**

These are the organizations that scored in the center across the range of metrics listed above.

3 **LAGGARDS**

These are the organizations that had the worst scores across the range of metrics listed above.

We then compared the leaders and laggards to explore those differences and explore what the leaders were doing differently.

LEADING VS. LAGGING

Respondents were open about the PKI management challenges they face. They are seeing rogue certificates, outages from unexpected certificate expiration and a host of other problems. But not all enterprises are seeing the same level of issues. We divided the responses into three tiers, and compared the top versus the bottom tier. The differences were striking.

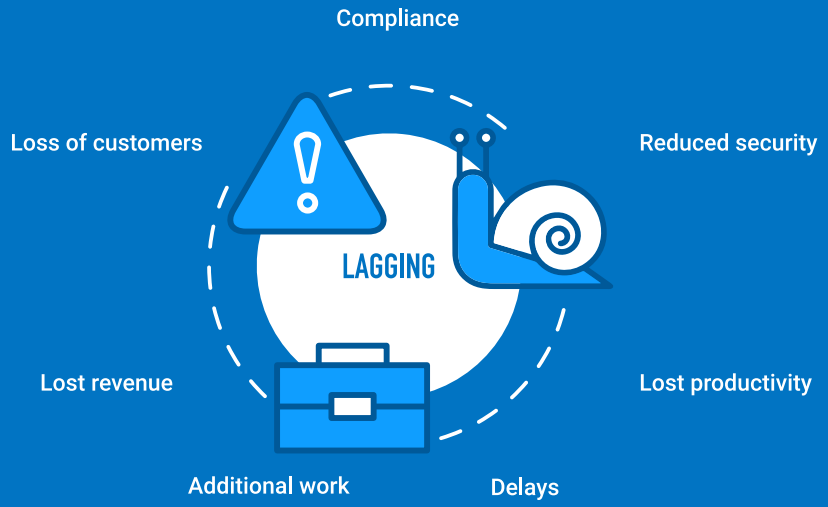
The leaders right off the top are doing better. Notably, a third or 33 percent, are more likely to say they think PKI automation is important in the first place. The leaders are two or three times better at:

- Minimizing PKI security risks
- Avoiding PKI downtime
- Minimizing rogue certificates
- Meeting PKI SLAs
- Managing digital certificates
- Issuing and revoking certs
- Compliance

On the other hand, the laggards experience severe penalties for their lack of skill at managing PKI certificates. These included:

- Compliance issues
- Security issues
- Lost productivity
- Delays
- They are overworked
- They are losing customers
- They are losing revenue.

So, what makes a leader a leader? Are there lessons we can learn from these PKI leaders?



PKI AUTOMATION LEADERSHIP TRAITS

PKI leaders are twice as concerned about the time it takes to manage PKI certificates. This keeps them focused on PKI management. Second, they are more concerned about rogue certificates. Third, leaders believe PKI automation is important to their organization's future. Perhaps this is why they are six times as likely to have already implemented PKI automation. So, what are the lessons and what should you do differently?

THE WILD WEST EFFECT

When we drilled into the data, we noticed an interesting wrinkle. We found that cohorts who on paper seemed like they should have been having an easier time with PKI certificate management often were having a worse time managing certificates.

For example, enterprises that manage the fewest number of certificates were much more likely to have experienced outages related to unexpected certificate expiration. They also performed uniformly worse under a broad set of PKI management metrics.

This drove these "low-volume PKI certificate" enterprises to be significantly more concerned about PKI management, even though they manage several orders of magnitude fewer certificates than high-volume enterprises. For example, the low-volume enterprises were nearly 50 percent more likely to say they are concerned about the amount of time it takes to manage PKI certificates. They also have nearly twice the share of the certificates under a PKI automation program.

At first, this seems paradoxical. The reality, however, is that these low-volume enterprises are simply less mature in terms of PKI management. While high-volume enterprises who often manage more than 100,000 certificates, are extremely mature in how they manage PKI certificates, the situation for low volume enterprises is like the Wild West—no rules, everyone managing certificates in their own way.

> FOR LOW VOLUME ENTERPRISES, IT'S LIKE THE WILD WEST—NO RULES, EVERYONE MANAGING CERTIFICATES IN THEIR OWN WAY.

PKI AUTOMATION LEADERSHIP TRAITS

PKI management leaders also showed that they were far more accountable of their certificate inventories, conversely rating themselves worse-off than their less-concerned counterparts. However, these same organizations reported less certificate-related outages or rogue certificates, proving that they were in fact, doing much better than they presumed.

THE SELF-ASSESSMENT PARADOX

Another interesting finding is the difference between enterprises who are most concerned about PKI certificate management. We found concerned enterprises objectively had fewer issues, but subjectively rated themselves worse off.

Take, for example, enterprises who were most likely to say they see PKI management as challenging. These enterprises were three to five times as likely to say they were somewhat to extremely concerned in areas such as speed of issuing new certificates, accidently misconfiguring certificates and seeing rogue certificates, and other certificate issues.

Yet, they also reported far fewer actual rogue certificates (just two-thirds as many of unconcerned enterprises). They also experienced far fewer outages related to accidental certificate expirations (just a single outage during the past six months versus three to five outages for unconcerned enterprises.)

We often see this phenomenon in security-related surveys. What is happening is that those enterprises who pay the closest attention are most aware of their shortcomings and missteps, and therefore tend to rate themselves more harshly than those who are not paying close attention. However, by paying such close attention, they actually do much better than their generally unaware peers.

> ENTERPRISES CONCERNED ABOUT PKI CERTIFICATE MANAGEMENT OBJECTIVELY HAD FEWER ISSUES, BUT SUBJECTIVELY RATED THEMSELVES WORSE OFF.

OUR RECOMMENDATIONS

Use of automation throughout your PKI certificate catalog yields significant benefits in a landscape marked by shorter validation periods, evolving cryptography standards, and broader adoption of digital certificates in business processes throughout the organization. But what should companies consider when embarking on automation initiatives? Here is a checklist of steps where automation may support certificate management objectives.

CERTIFICATE MANAGEMENT

IDENTIFY
Identify and create inventory of certificate landscape.

REMEDIATE
Remediate keys and certificates that are not compliant with corporate policy

PROTECT
Protect with best practices for issuance and revocation. Standardize and automate enrollment, issuance, and renewal.

MONITOR
Monitor for new changes.

CERTIFICATE WORKFLOW AUTOMATION

IDENTIFY
Identify unmanaged or manual certificate workflows.

ADOPT
Adopt automation with software that centralizes and manages certificate workflows.

MONITOR
Monitor with centralized visibility and control.

COMMON CERTIFICATE WORKFLOWS

- Web Servers
- Device Identity & Management
- Code Signing
- Digital Signatures
- Identity & Access

METHODOLOGY

ReRez Research of Dallas, Texas surveyed IT professionals from 400 enterprises of 1,000 or more employees in North America, EMEA, Asia Pacific and Latin America. Respondents were split between IT directors, IT security managers and IT generalists. We focused on IT specialists managing digital certificates for users, servers and mobile devices and we surveyed small, medium and large enterprises.

Talk to a DigiCert PKI automation expert to assess your organization's needs and discuss tailored solutions. Learn more about how to start automating your PKI deployments here.