digicert®

PKI Modernization Whitepaper

WHITE PAPER

Modernize your PKI for security, efficiency and agility

PKI technology came to the enterprise in a haphazard way, creating a situation of inflexibility, inefficiency, and – ironically – insecurity. A modern PKI can bring the entire ecosystem under control to address these problems without the need to rip and replace existing tech.

IT environments dependent on legacy PKI systems can experience frequent outages, require high levels of effort to maintain, and do not meet current and evolving security standards. Even if brought as up-to-date as possible, they lack the agility to support new use cases and deploy protections quickly and without disruption to business. Many existing PKI systems are simply incapable of being modernized sufficiently to support the technology initiatives that enterprises have embraced in the last decade or the changing industry regulations and standards.

In this paper, we describe the problem and solutions. We give examples of companies that have modernized their PKI systems, putting them in the best position to support the business and block next-generation attacks.

The state of PKI today

The purpose of a PKI is to establish trust everywhere in our networks and even within individual systems. Our reliance on PKI systems constantly grows, but our ability to manage these systems has not kept up.

This problem shows up most commonly in the development of "PKI silos," which are separate PKI implementations within the same company. The silos may have been acquired in a merger or acquisition, or they may have been created for a specific project, either not considering or despite the option of centralizing PKI management. The result, in the best case, is overhead: the silos must be managed separately, probably with different tools and perhaps by different teams. If the management is not coordinated, the policy, governance, and implementations may conflict.

We use cryptographic operations throughout the enterprise and in many kinds of software. At many steps in a software stack, PKI may be used to authenticate parties or to exchange keys and other resources for application communication and privacy purposes.

The role of PKI in the enterprise

Public/private key cryptography is the mechanism by which parties on the Internet or inside an enterprise establish trust. We use it to prove that a user is who they claim to be, that a server or other device is what it purports to be and to exchange encryption keys to secure data. PKI, or Public Key Infrastructure, is a set of trusted protocols, libraries, and standards that allow users and devices to exchange information with privacy, safety and efficiency. Learn more about the role of PKI.

These transactions happen constantly within our systems and across networks, and the enterprise's security depends on their correct execution.

Enterprise-wide PKI management is a relatively recent phenomenon. Before its adoption, applications that implemented PKI would tend to include their own tools and security policies, leading to PKI silos in enterprises.

There are many common examples:

- VPN systems, by their nature, implement separate networks and issue certificates to support their identity and encryption functions.
- Microservices environments generally create their own PKI for identifying containers and performing encryption.
- Many UEM (unified endpoint management) systems issue certificates for authentication.
- IoT device management platforms are often set up with a special PKI with which the management software identifies and controls devices.

Also, as with other software, mergers and acquisitions often introduce different PKI systems into an enterprise.

The haphazard PKI

In a modern enterprise, technology adoption and growth are often haphazard. Technologies may be acquired not as part of a formal plan but through a corporate acquisition or an initiative from the ranks. Significant infrastructure features that rely on PKI, such as mobile devices, cloud computing, and DevOps, were often presented to IT, already in operation, as a fait accompli.

In these and other examples, PKI functionality may have been provided for that purpose only and not integrated into a managed infrastructure. As a result, PKI management tasks must be performed by multiple personnel using many different tools, often at the same time. Even so, many systems in the typical large enterprise are not yet implementing strong encryption and authentication using PKI.

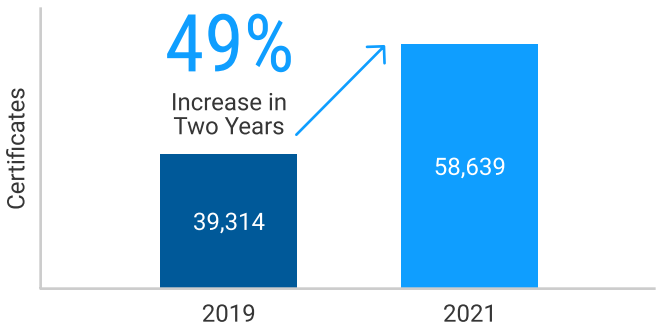
Digital certificates and PKI

The main resource used in PKI authentication is the digital certificate. It identifies the thing to be authenticated, which could be a user, a program, a phone, or anything else running software. Consequently, the number of certificates under management has grown tremendously and will only continue to grow. A 2021 study Ponemon Institute showed that the typical enterprise manages more than 50,000 certificates. The number is undoubtedly much larger now.

Certificates have a defined lifespan. For example, the maximum lifespan for publicly trusted TLS certificates is 398 days, or about 13 months, while certificates used for internal uses like cloud workloads have dramatically shorter lifespans. The need to automate certificate renewal is plain enough, especially as the number of certificates increases and lifespans shorten.

One of the difficult parts of certificate lifecycle management is managing revocation. There have been two methods, CRLs (Certificate Revocation Lists) and OCSP (Online Certificate Status Protocol), both of which are difficult to implement efficiently and at scale.

The idea with short-lived certificates is that we won't bother with revocation; instead, we will just let the certificate expire. Certificate revocation and renewal are two examples of certificate operations that often need to be orchestrated across multiple systems and processes,



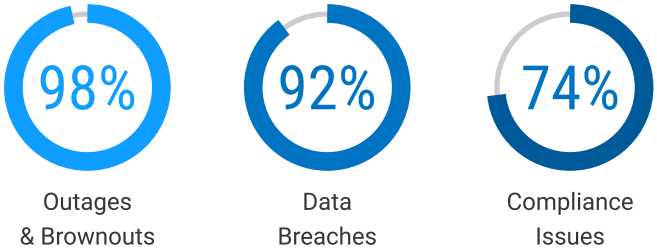
Ponemon IoT and PKI Trends 2021

Continued outages

Expired certificates are just one cause of outages and Government Risk & Compliance (GRC) failures that result from inadequate PKI management, but they are the most common. As with the overall volume of certificates, their number will likely grow.

Even with these developments, the number of certificates that are renewed manually is large. Outages occur not just because certificates must be manually renewed. In a large and complex enterprise, those in charge may not even know what certificates they have. With disorganization like this, making technology or budget plans becomes impossible.

Even if you manage the system well, outages are possible, so the modern PKI must be able to function and quickly recover in the event of one.



DigiCert 2024 Digital Trust Report

The monetary costs of legacy systems

By their nature, every PKI system you add will also add maintenance and administrative costs. Every system needs to be administered by a person with sufficient expertise (that is increasingly difficult to find), and the software itself may have ongoing license and maintenance costs. This can lead to significant operational overhead, especially when dealing with multiple systems. Disparate systems and isolated operations can also create challenges in visibility and management, increasing the risk of outages and security breaches.

Defining the Modern PKI Platform

Discovery, inventory, and ownership

Bringing order to a haphazard enterprise PKI begins with a discovery process. The modern PKI scans all reachable parts of the network and ingests data from other systems about existing certificates, and creates an inventory, preferably as part of your asset-tracking system, with which IT can plan. A good discovery process should identify many types of certificates, both public and private – regardless of the issuing certificate authority – and will likely find multiple PKI silos.

These are isolated systems for issuing digital certificates from internal or public CAs. Where did they all come from? They were likely set up to support specific applications or were added as part of a merger or internal consolidation. There are many reasons for them, and they all may have made sense at the time.

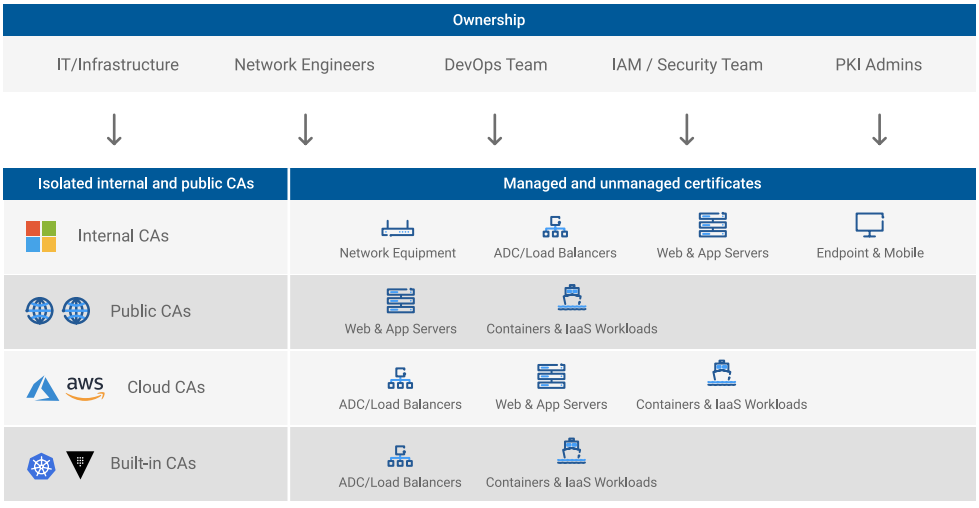
In the discovery process, you will establish ownership of the certificates and assign lifecycle management and budget reporting duties for them to the right people. At the same time, you can establish an inventory and ownership of applications that use PKI.

What are "PKI?" and "the PKI?" What is the "web PKI?" And what does the "P" stand for?

Public key cryptography involves public and private keys, and PKI is the term for the systems and services that make these operations possible. Even though you might say it's "public/private key infrastructure," there's only one "P," and the first word used is "public." Perhaps this is because the private keys are private, and the infrastructure is public.

It is also common to find private PKIs within enterprises. These may have been set up specifically to service a particular application, like a large Enterprise Java Beans system or a Kubernetes cluster. They may also be part of a rogue "shadow IT" operation. You'll probably only learn about them through discovery.

You will also hear the terms "the PKI" and "the web PKI" thrown about. The "web PKI" refers to the public – as in Internet-facing – PKI, the one of which public CAs like DigiCert are a part. "The PKI" might refer to it as well, but it also might refer to a private PKI in a discussion specifically about it.



Discovery and ownership

Centralized governance, distributed use

A modern PKI platform provides centralized governance and oversight with distributed certificate use and lifecycle management. This means that the teams throughout the enterprise can manage their own acquisition and use of certificates, subject to company policy. As with most cloud software, a modern PKI works best when it provides some level of self-service.

What is self-service in this context? The PKI system, part of which is a Certificate Lifecycle Management system, has central control of many features, including policies for the system's use and infrastructure management. But teams and individuals within the organization should be able to perform many common CLM operations according to policy.

For this, the CLM should provide an accessible web portal or dedicated app through which users can request and obtain certificates and assistance with more complicated operations that require the central PKI team's assistance. It is also critical that the modern PKI system support automated delivery and installation to systems and devices via standard protocols, APIs, and integrations.

Centralized administration, where possible, allows you to put PKI systems in the hands of administrators who have the most expertise and free up personnel and budget that had been dedicated to legacy PKI systems.

Public and internal (private) use cases

To consolidate disparate PKIs requires support for any certificate authority and a wide variety of cloud, on-premises, and hybrid enterprise architectures. Some will be public certificate authorities like DigiCert, but an in-house private CA is appropriate for some applications. They should be managed the same way. While industry standards provide interoperability of certificates among public certificate authorities, there are no such standards for private certificate authorities. A modern PKI should accommodate both but with intelligence to prevent risky private certificate authority practices.

Why would you want to run a private CA? Certain applications, such as high-volume container-based applications, use large numbers of certificates for short-lived tasks. The authentication and encryption provided by the private PKI is valuable for securing these workloads and environments. The highest-performance solution will be a local, private CA that can respond quickly to certificate requests and log all operations.

Even in these circumstances, where the application is logically isolated, it is best practice for the private CA to be governed using the global PKI policy. A managed PKI offering that provides this style of governance is ideal for most organizations.

Out of the box support for diverse workloads

The modern PKI system is adaptable to any workload, including those on end-user devices, servers, services, applications, containers, VMs, and others. Because of a long history of open standards, any PKI system can generally be made to interoperate with any other. A modern system works – out of the box – with any other system or application you are likely to have through standard interfaces and vendor alliances. As described later in this paper, the ability to seamlessly interoperate and integrate with enterprise architectures is a must.

Flexible deployment models

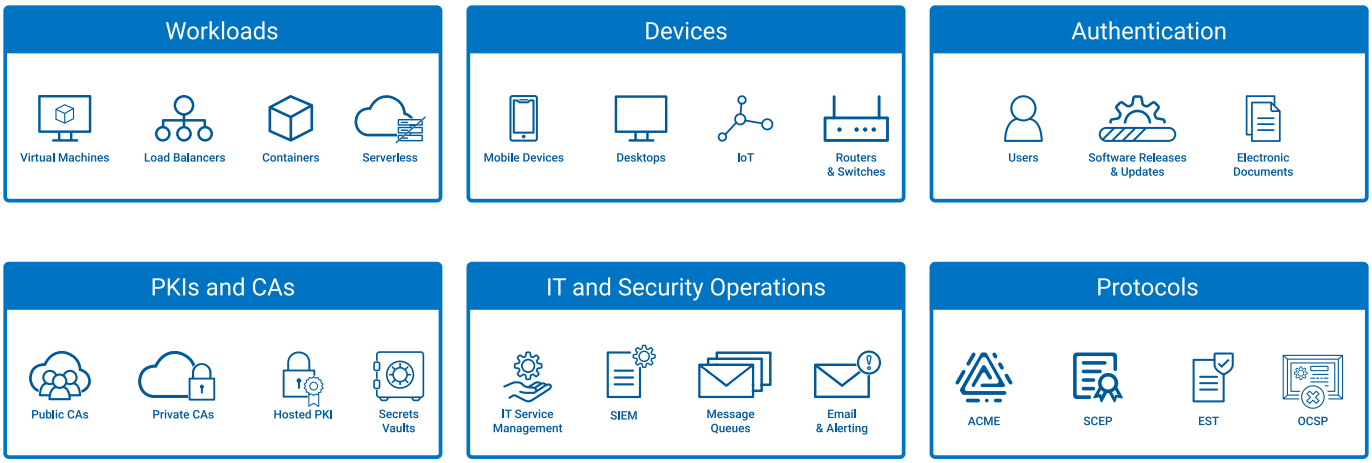
Hybrid enterprises are especially tricky and important. A single logical application could have components on on-premises systems and in multiple clouds. It could also manage client and vendor certificates embedded in proprietary appliances. Complex enterprises may have units that operate independently in different jurisdictions with different legal requirements and require the flexibility to manage appropriately.

The modern PKI system should make managing certificates in such circumstances logical, if not easy. This includes integration with on-premises directory services for traditional IT infrastructures, compatibility with cloud provider certificate services for cloud-native applications, and the ability to manage certificates across hybrid setups. By providing consistent management tools and automation capabilities across these environments, organizations can streamline certificate lifecycle processes and avoid security risks.

Workflows and automation

A modern PKI system formalizes key procedures and workflows, such as approvals necessary for events like certificate revocation and record-keeping of all events (or at least all the customer wishes to keep).

It should automate routine and extraordinary use cases to improve user experience, lower administrative overhead, and reduce opportunities for misconfigurations that cause outages and security incidents.



The PKI Ecosystem

Reporting, analytics, and notifications

It also should provide many default reports and the ability to customize them. Examples include

- Inventory report
- Report of expired certificates and those nearing expiration
- Report on certificates that have been revoked
- Reports on how the certificates comply with the enterprise's security policies, industry standards, and relevant government regulations.

A modern PKI system should provide analytics to show important problems, such as which certificates still use weak encryption algorithms or key lengths. It could also do cost analysis and recommend opportunities for cost optimization. It could even do risk assessment relative to certificate mismanagement or regulatory compliance.

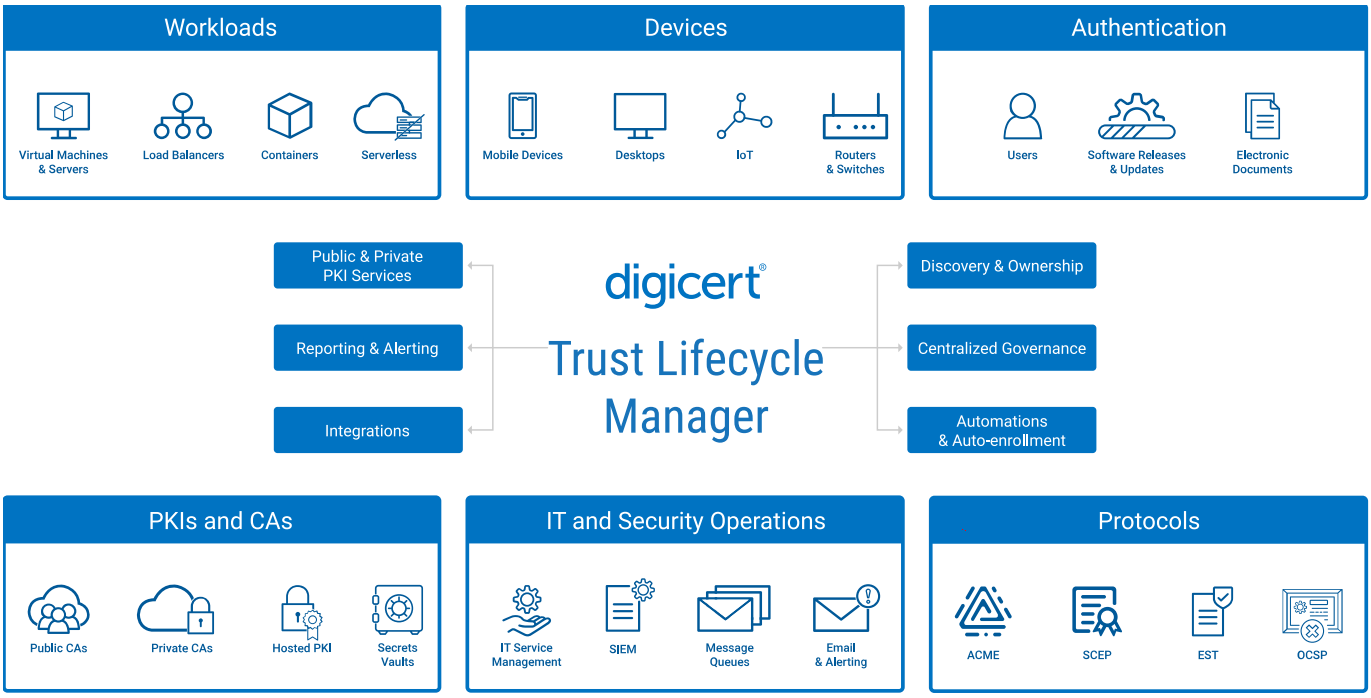
On the proactive side, a modern PKI should alert users to many events and allow event escalation and configuration. The obvious one is a warning of certificates that are approaching expiration. In most cases, it is best to set the certificate to renew automatically and for the alert to say when the renewal will occur. The right users must be notified of a certificate revocation, a policy violation, the discovery of certificates outside the system, and many other events, both normal and otherwise. Of course, the alerts should flow according to the organization's existing practices for service management and security operations.

The importance of ecosystem support

Finally, it should integrate with relevant software in the enterprise ecosystem, using both standard and proprietary interfaces. The PKI ecosystem is extensive, complex, and interoperability is not completely standardized. A good, modern PKI will integrate directly with major cloud services and DevOps infrastructure providers, such as Amazon Web Services and HashiCorp, to ease the discovery process and to establish central governance.

Because of the expanding reach of PKI in the enterprise, many large companies have products that rely on it. Microsoft Windows and other operating systems rely on PKI for networking and authentication. Microsoft applications platforms like Office and Exchange Server use PKI extensively for networking, authentication, and encryption. Apple and Google products rely on PKI for the same reasons. Adobe Acrobat and other PDF tools can use digital certificates to digitally sign PDF files to prove the identity of their creator. Custom applications written by consultants may rely on PKI, for instance, to ensure that digital transactions and communications are secure and verifiable to meet regulatory compliance requirements. All of them work better and are more secure with a modern PKI.

The major special case in this space is Microsoft Active Directory on Windows and Azure. AD may have been modern and sophisticated when designed in the 1990s, but today, it is a technological island. Microsoft is moving towards modern standards with Azure Active Directory (now Microsoft Entra Domain Services), which uses protocols such as SAML, OAuth, and OpenID Connect rather than NTLM and Kerberos. Azure AD makes multi-factor authentication, conditional access, and single-sign-on core features.



DigiCert Trust Lifecycle Manager

Enterprises are likely to be highly dependent on Active Directory for user, server, and domain management but also need to manage mobile devices, Internet services, and other resources through other means. They have many other applications with PKI needs, and the modern PKI should integrate with as many of them as possible, as seamlessly as possible. Developers use DevOps tools that are most secure when they have robust PKI support. Web servers, load balancers, and other application platforms have core PKI needs. Network devices like firewalls and routers use PKI for secure communications. Mobile Device Management uses PKI extensively. The list goes on and on.

A modern PKI combines all these elements in one system, allowing the enterprise to manage them logically and in concert with other PKI systems.

Modern PKI in Action

A modern PKI solution is not an abstract thought. It exists today but is commonly associated with a modernization project or journey.
Below are three customer stories to highlight the modernization journey and the associated benefits.

Discovering savings and security

This large financial services group relied on numerous siloed Public Key Infrastructure (PKI) systems that were difficult to manage. The outdated PKI environment caused frequent outages due to expired certificates. The situation was exacerbated by limited visibility of the certificates and sometimes the lack of PKI expertise among IT administrators of the systems consuming them; in one instance, they had to contact a former employee to help restore operations.

The company initiated a PKI modernization journey with DigiCert Trust Lifecycle Manager beginning with a comprehensive discovery of all certificates and assigning ownership. This revealed a surprising number of unused certificates linked to inactive systems still being managed in silos.

The discovery, inventory, and ownership process facilitated by DigiCert Trust Lifecycle Manager allowed them to:

- **Reduce Costs and Improve Efficiency:** DigiCert facilitated the decommissioning of unnecessary certificates and systems, saving budget and streamlining IT operations.
- **Enhance Security Posture:** Improved understanding of the PKI environment helped identify vulnerabilities and reduce the attack surface by decommissioning unused systems.
- **Streamline Management:** DigiCert consolidated certificate management under the direct purview of the IT team, enabling proactive management and reducing outages.

Simplification through automation

A technology company, operating a complex IT infrastructure with thousands of virtual machines across multiple data centers was struggling to manage certificates because of the increasing number of certificates and the manual processes involved in provisioning and installation.

The site reliability team struggled with time-consuming and error-prone manual certificate management processes. Provisioning and installing a single certificate could take hours. The lack of visibility into certificate inventory and lifecycles increased the risk of outages due to expired or misconfigured certificates.

DigiCert Trust Lifecycle Manager automated and streamlined certificate lifecycle management, significantly improving efficiency and reducing the risk of outages.

Key benefits included:

- **Simplified autoenrollment:** Configuration templates and automation reduced certificate provisioning time from hours to minutes.
- **Enhanced visibility:** Automated discovery and inventory of certificates provided better oversight.
- **Improved security:** Automated workflows for revoking and replacing compromised certificates enhanced security posture.
- **Increased efficiency:** Seamless integration with diverse workloads and automation of routine tasks reduced IT burden.

Overcoming PKI blind spots in mergers and acquisitions

This large enterprise was often surprised by certificate management challenges associated with IT operations assumed by mergers or acquisitions. This complex environment includes on-premises and cloud-based infrastructures with certificates issued by multiple CAs, managed with varying policies and processes.

Certificate blind spots due to multiple CAs, inconsistent policies, and lack of centralized management hindered efficient certificate management. Mergers and acquisitions exacerbated these challenges by introducing new certificate inventories, policies, and systems. This resulted in increased risk of outages, breaches, and business disruptions caused by expired or compromised certificates.

The organization partnered with DigiCert for PKI modernization. Using Trust Lifecycle Manager they addressed these challenges by providing:

- **Comprehensive discovery:** Identifying and inventorying certificates across multiple CAs and environments.
- **Centralized management:** Consolidating certificate policies and processes for efficient management.
- **Automation:** Streamlining certificate issuance, renewal, and revocation processes.
- **Integration:** Seamlessly integrating with existing certificate management systems.

Crypto-agility and the PKI landscape

PKI is a rich area for offensive and defensive security research because it is central to security in all domains. Over the years, many changes have been adopted to the standards implemented in PKI to address weaknesses in those standards.

Implementing these changes in a haphazard PKI is difficult at best and unlikely to succeed in an acceptable timeframe and with minimal disruption to business.

There are many examples, one of which is key lengths. As computing power increases over the years, attackers can increasingly compromise shorter, weaker keys.
A modern PKI system can tell you if you have weak keys and then facilitate swapping them out for stronger ones.

Over time, researchers have found weaknesses in some cryptographic algorithms. This has happened more than once to hash algorithms, with the demonstrated weakness of the popular MD5 and SHA1 hash algorithms. Enterprises with modern PKI systems are better positioned to ensure they are not using weak algorithms.

But the biggest problem has yet to come. Quantum computing can potentially allow successful attacks against many widespread cryptographic algorithms. NIST has been working on the problem for many years and has published their first set of post-quantum standards. Some algorithms are “quantum-safe” using larger keys, but others must be replaced entirely.

As with the hash algorithms, managing this process without a modern PKI is unlikely to succeed. Modern PKI systems have already begun supporting the new NIST post-quantum algorithms. And these aren't the only problems likely to occur in the algorithm space; it's not a stretch of the imagination to assume it will take multiple tries to get quantum-safe cryptography right.

Recommendations

Adopting a modern PKI is not a "rip and replace" proposition. It allows you to use your existing cryptographic assets more securely and efficiently. The path to a modern PKI will likely be complex and take some time, but fortunately it always begins the same:

1. **Discovery and Assessment:** Begin by evaluating your current PKI systems. Even if you go no further, you will be better off after running a discovery process. This will give you an accounting of what certificates you have and an idea of how widespread PKI is in your enterprise. If you're like most enterprises, you will see many surprises in the discovery report and conclude that you need to bring some order to the chaos. Identify strengths, weaknesses, and areas for improvement of your PKI systems. Assess the alignment of your PKI with business objectives and regulatory requirements. This assessment will provide a solid foundation for your modernization journey.

2. **Prioritize Use Cases:** Determine the critical use cases that drive your business operations. Focus on modernizing PKI for these high-priority areas first. This approach will deliver the most significant benefits and return on investment.

3. **Centralize Policy and Governance:** Centralizing your PKI into a single system or hierarchy may work in some organizations, but for more complex organizations or deployments, a focus on centralizing policy and governance in combination with visibility via discovery allows the modern PKI to be agile and fine-tuned to specific use cases throughout the enterprise.

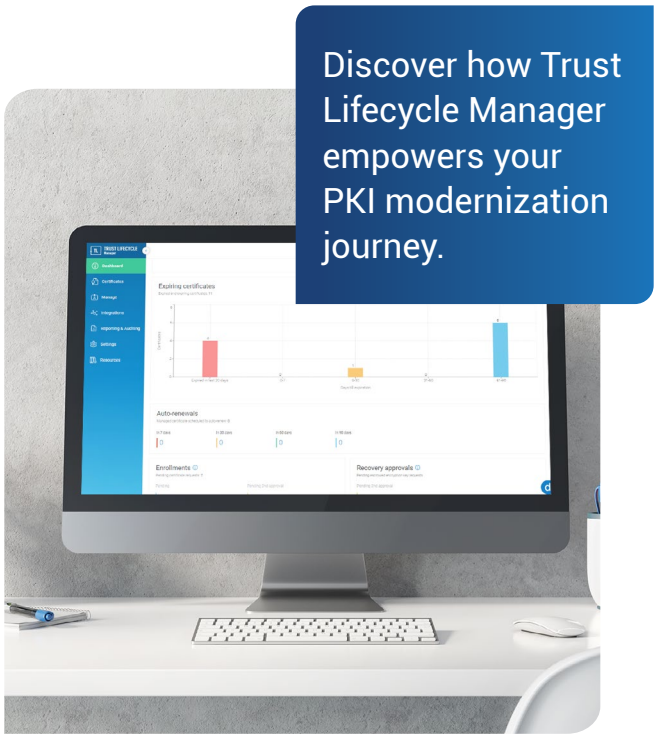
4. **Consolidate Public and Private:** Consolidating your public and private PKI use cases onto a unified platform is a common initiative related to PKI modernization. Doing so simplifies management, reduces costs, and improves security. Evaluate the potential benefits and challenges associated with consolidation and select a platform that meets your specific requirements.

Enterprises that lack a modern PKI are prone to outages that would be prevented by automating processes enabled by modern PKIs. They also waste large amounts of money by requiring extra management resources for a disorganized cryptographic infrastructure and on unnecessary certificates.

The best solution for you is one that helps you eliminate such waste, interoperates with your existing ecosystem, and makes changes and upgrades possible without business disruption.

About DigiCert

At DigiCert, finding a better way to secure the internet goes all the way back to our roots. That's why our PQC, TLS, PKI, and IoT solutions are trusted everywhere, millions of times a day, by people and companies around the globe. It's why our customers consistently award us the most five-star service and support reviews in the industry. And it's why we'll continue to lead the way toward a quantum-safe future powered by digital trust for the real world.



© 2024 DigiCert, Inc. All rights reserved. DigiCert is a registered trademark of DigiCert, Inc. in the USA and elsewhere. All other trademarks and registered trademarks are the property of their respective owners.