KEYFACTOR

SECURE EVERY DIGITAL IDENTITY

WHITE PAPER

PKI: The New Best Practices

THE GUIDE TO BUILDING A POWERHOUSE PKI TO PROTECT YOUR BUSINESS

Table of Contents

Overview

IT and security leaders no doubt recognize public key infrastructure (PKI) as a proven and time-tested security tool in the enterprise. At the same time the digital landscape has changed, and along with it the need for PKI to adapt. PKI deployments have evolved and expanded to protect more business-critical infrastructure and applications than ever before, emerging as a secure and cost-effective technology to enable new initiatives from the cloud to the IoT.

DEMAND FOR NEW BEST PRACTICES

Today, enterprises face new uncertainties. Explosive growth in network scale and complexity demands a next generation PKI. The number of digital certificates in use across the organization has exploded, coupled with the demand to integrate with a growing number of tools and applications – from cloud platforms to security information and event management (SEIM) solutions. To support this new reality, IT and security leaders must make decisions on how to re-build or re-engineer their disjointed and aging PKI environments, as well the certificates issued from them.

In this white paper, you will learn how the role of PKI in the enterprise has evolved, as well as the new challenges and risks in running it effectively and keeping it secure. You'll discover insights and best practices to identify these challenges, address the risks, and take action to adopt the next generation of PKI that can support your business needs today and into the future.

> "Organizations are expanding the use of PKI within IoT and DevOps pipelines. Technical professionals need to transform the perception – and the deployment – of PKI to establish an automated management regime for PKI."[1]
>
> GARTNER

[1] https://www.gartner.com/en/documents/3891976/the-resurgence-of-pki-in-certificate-management-the-iot-

Legacy PKI vs Digital Transformation

PKI is nothing new. Many PKI implementations are more than a decade old and already support a multitude of applications across the business. However, deploying a PKI 10 years ago meant an entirely different set of use cases, challenges, and standards than enterprises face today. Once viewed as a complex tool used for niche use cases like Wi-Fi authentication, email security, and SSL certificates, PKI has emerged as a core technology to secure applications at the forefront of digital transformation.

CLOUD / MULTI-CLOUD

Adoption of cloud infrastructure and applications allows businesses to take advantage of countless cost and operational efficiencies. At the same time, hybrid and multi-cloud have increased the risk of exposure, making it difficult to secure data between instances, services, and applications. Enterprises now rely on digital certificates to secure connections both in the cloud and behind their firewall, but existing PKI deployments can be challenging to integrate and scale in highly distributed environments.

MOBILE / BYOD

With the widespread use of mobile devices enabling remote workforces, the need to secure access from outside the network is critical. Wi-Fi and public networks are a common entry point for attackers, and applying outdated security measures (i.e. usernames and passwords) to this new mobile environment is ineffective. Digital certificates are supported by mobile operating systems, offering a proven and secure way to ensure that only authorized devices can access the corporate network, email, and applications.

DEVOPS

Enterprises have adopted a DevOps culture to deliver applications faster than ever before, but this fast-paced and agile environment brings new challenges, especially when it comes to security. DevOps teams have become dependent on digital certificates to securely spin up containers, gain access to applications, and digitally sign code before it's pushed to production. Agility and speed are the name of the game – PKI deployments must adapt to seamlessly integrate certificates into the CI/CD pipeline, without tradeoffs between speed and security.

IoT DEVICES

The newest challenges on the horizon come from the emergence of IoT devices. Connected vehicles, smart light bulbs, implanted medical devices, software, and sensitive data all need to be verified as authentic and protected from malicious access or corrupted code. How can disparate IoT components that need to connect to an enterprise network (and sometimes back to the manufacturer) be secured? What level of trust and assurance is needed for each of those components? How can security be built into devices with limited compute power? PKI and certificate-based authentication, encryption, and firmware signing offer an effective and scalable way to overcome a host of IoT challenges.

> "The most significant challenge organizations will continue to face, with respect to enabling applications to use PKI, is the inability of an existing PKI to support new applications."[2]
>
> NCIPHER-PONEMON

[2] https://www.ncipher.com/2019/pki-iot-trends-study

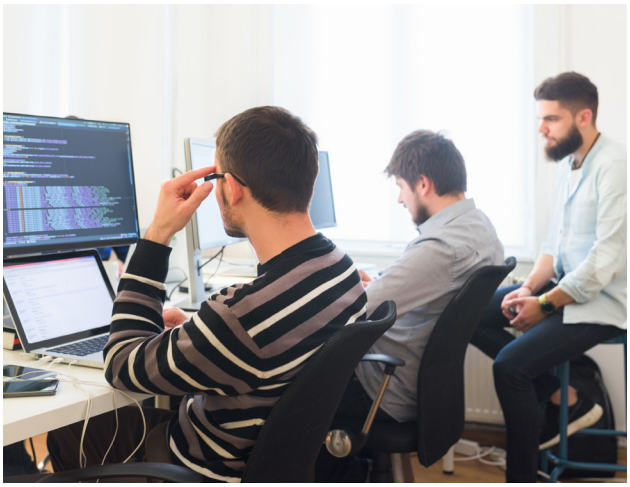
NEW TECH, NEW THREATS

No other technology has impacted PKI deployments, and the security landscape as a whole more than the IoT. Even an office printer connected to the Internet has security implications. Still these connected devices – whether within or on the edge of the network – are often overlooked. Moving forward, organizations will need to understand the required security controls, what data is transmitted, and which network resources the device needs to access to determine privacy implications, potential vulnerabilities, and new risks that could result from enabling connectivity.

BUILDING ON WHAT'S ALREADY BROKEN

While the PKI that may have been built for a Wi-Fi and SSL years ago hasn't changed much, the PKI required for the uber-connected IT environments of today must address vastly different needs and vulnerabilities. PKI implementations of the past were not designed to support the scale and complexity of systems that now rely on digital certificates to run securely, and many organizations are building on what's already broken in an attempt to keep pace.

Far too often, existing PKI deployments lack the flexibility to adapt to changing standards or support new use cases. Teams responsible for PKI operations are now challenged to retrofit or re-engineer existing infrastructure to enable new use cases, but the reality is that once your PKI is deployed, it is more or less set in stone. PKI is one of those technologies where you have exactly one chance to get it right: at installation. After that, re-deployment becomes the only way to fix a mistake.



IF IT ISN'T PROTECTED, IT SHOULDN'T BE CONNECTED

From the Mirai botnet to hacked medical devices, the threat of IoT compromise is now a reality that is both business- and life-critical. Everything is connected – even toilets and office printers. Default passwords and security settings have proven to fail. Enterprises must ensure that these devices are properly inventoried, secured, and easily updatable before allowing them to join the network.

PKI Then and Now

PUBLIC VS PRIVATE PKI

When building out a PKI program, enterprises are confronted with the choice between public and private Certificate Authorities (CAs). Depending on organizational needs, it may make sense to just purchase certificates from a public CA such as DigiCert or Entrust. If you're running a public-facing website for example, you need a certificate issued from a public CA. However, this approach can become expensive at scale, particularly when certificates don't need to be trusted outside the enterprise. That's where private PKI – also known as in-house PKI – comes into play.

Standing up a PKI in-house allows organizations to support large-scale certificate deployments used for internal operations – things like network access, email encryption (S/MIME), cloud-based applications, IoT and mobile devices. Rather than purchase certificates from a third-party public CA, deploying a private PKI makes more economic sense. But as enterprises become increasingly reliant on their private PKI to support business growth, they often overlook the cost and complexity of maintaining the policies, security controls, hardware and software required to run it effectively.

Today, most organizations take a hybrid approach, using a mix of digital certificates from both public and private CAs. Knowing how many certificates you have, where they live, and whether they are compliant becomes incredibly difficult. Following best practices is next to impossible when you're too busy chasing down application owners to renew certificates, or recovering from the latest outage.

TWO-TIER VS THREE-TIER DESIGN

In the past, IT teams had to discuss the architecture of their PKI and determine whether to implement a two- or three-tier design. Today that discussion is no longer necessary, as years of successful PKI operations have established reasons for either method, depending on your requirements. The vast majority of PKI deployments are two-tier, with three-tier designs being implemented only when specific technical or industry-imposed requirements must be met.

42% of organizations today use HSMs to secure their PKI.[3]

HSM VS SOFTWARE

Another topic of debate has been whether or not to implement a Hardware Security Module (HSM) to protect CAs and private keys that could otherwise be compromised. Now HSMs are becoming standard practice to protect the long-term integrity of PKI implementations. "It won't happen to us" is no longer a valid argument, as attackers have realized the value of using private keys to breach enterprise networks.

DEDICATED PKI EXPERTS VS IT / SECURITY TEAMS

Large enterprises used to have a dedicated team responsible for all things PKI, but over time that task has typically been transitioned to the responsibility of the security team. While security professionals are knowledgeable, they have dozens of tools and applications to run outside of PKI. This tends to place conflicting pressure on multiple teams with responsibilities for PKI, from infrastructure to application engineering. A lack of internal skills and resources matched with a waning number of PKI experts in the industry leaves most organizations with no alternative.

[3] https://www.ncipher.com/2019/pki-iot-trends-study

Evolving Risks and Challenges

Organizations turn to PKI to remediate risks as they adopt new technology, but insecure keys and digital certificates issued from disjointed and poorly managed PKI have become a prime target for attackers seeking to breach the network. Without knowing the potential vulnerabilities, establishing policies and procedures to prevent them, and having a way to identify impacted certificates, your PKI and IT assets are at risk. A simple misconfiguration can compromise the trust of an entire PKI and all certificates issued from it. Failure to respond to incidents and adapt to changing crypto-standards can leave the organization exposed to serious risks.

CRYPTO-LIBRARY BUGS

Discovery of a bug in crypto-libraries can compromise the security of devices on your network, resulting in the need to not only install firmware or software updates, but also generate new keys and re-issue certificates according to the technology used in patching or replacing it.

ROOT COMPROMISE

Another challenge comes from attacks on root certificate key stores relied upon by applications, browsers, and devices. When a Root of Trust (RoT) is compromised, all trust is lost. In the case of a compromised CA, the chain of trust and all public and private keypairs are rendered moot, or even dangerous, as they can be issued and used maliciously.

WEAK CRYPTO AND HASHING

Cryptography deployed today will not be secure in the future. In fact, it's hard to find any cryptographic algorithm or hashing mechanism that hasn't failed us in recent years, only to be replaced by a stronger, less breakable alternative. Think MD5, SHA-1, and 1024-bit RSA keys, to name a few.

CERTIFICATE EXPIRATION

It's common to see organizations extend the validity period of a certificate, sometimes to 25, 50, or even 99 years to avoid any chance of it expiring while in service. Certificate expiration is an important check and balance system to verify legitimacy and authorization, and ensure certificates are regularly re-issued. However, experts recommend validity periods of no more than two-to-three years. Maintaining a regular cadence for certificates will enable the management of certificates running like a well-oiled machine.

POST-QUANTUM THREATS

Most experts predict that quantum computing will become viable sometime between 2024 and 2030. The scale of the potential impact to cryptography is immense. Most public-key algorithms in use today will be susceptible to attack by quantum computing processors.

ARE YOU QUANTUM READY?

Google's recent breakthrough in "quantum supremacy" has sparked a debate about the impact quantum computing will have on cryptography. The introduction of a quantum computer capable of solving a calculation in under 4 minutes that would otherwise take even a supercomputer 10,000+ years to solve has put PKI in the spotlight. Failure to prepare for these advances will leave many organizations with no choice but to re-deploy their PKI entirely.[4]

[4] https://www.nytimes.com/2019/10/23/technology/quantum-computing-google.html

INCREASED PKI SCRUTINY

As enterprises rely more heavily on keys and digital certificates, PKI is coming under increased scrutiny from internal compliance teams, external auditors, and regulatory entities. Most organizations recognize PKI as a core component of enterprise security, yet far too often, it's left under-supported.

Many PKI deployments are outdated, unable to meet the requirements of emerging technologies. Others don't receive the dedicated expertise they once had, with PKI operations being folded into other security and IT functions. Others are simply forgotten, yet continue to issue certificates with little or no oversight. In any case, lack of investment and attention to PKI often manifests itself through widespread network and application outages, or worse yet, a serious security breach.

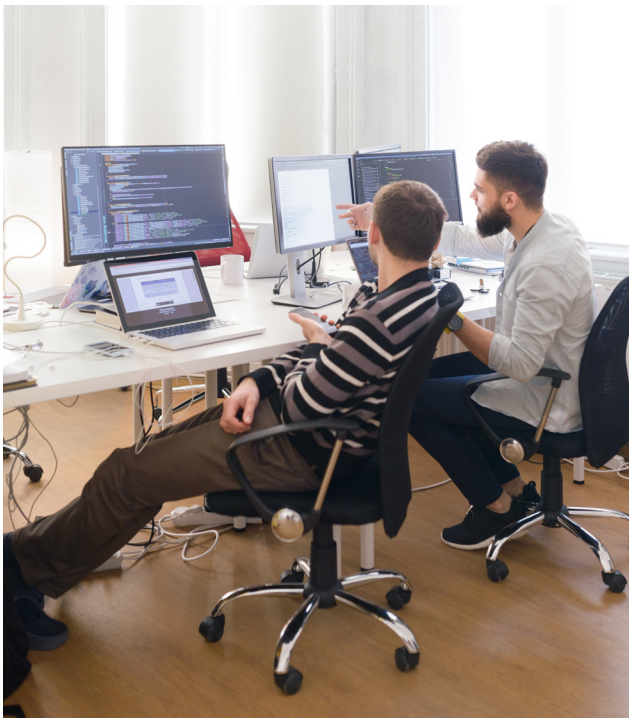
Organizations successfully taking advantage of PKI are active in conducting their own internal audits. They are also implementing tools to enable real-time PKI health and compliance reporting in an effort to reduce risk and prove the intended PKI assurance level needed to meet and exceed standards from NIST and SANS Institute, as well as other industry and regulatory requirements.

INTERNAL AUDIT

A strong framework for assessing and auditing security can be found in the 20 SANS CIS Critical Security Controls. A number of the SANS CIS controls can be useful for PKI auditing to identify and assess the devices and applications authorized to connect to a network and those that are not. Part of the assessment for these controls should include identifying the location of certificates on every device and application, as well as how those certificates are issued and managed over time. Most organizations are unaware of where their certificates live or even how many they have. Regular and thorough audits can provide a clear understanding of your certificate landscape and how it evolves over time.

INCIDENT REPORTING

Incident monitoring and alerts help organizations minimize the potential for holes in their security infrastructure. One example highlighting the importance of actively monitoring your PKI operations lies in how an organization suspends network access for a severed employee. Most organizations will shut off the Active Directory (AD) access. That may be fine if all authentication occurs through AD, but if the employee had a device that authenticated to the network solely through a certificate, more steps must be taken. If the organization does not know to revoke the certificate, the employee can still access the network and the organization may not know. An auditor may ask how an organization can be sure that a terminated employee isn't still connecting their iPad or other device to the network. Being able to answer questions like these go a long way in complying with audit requirements.



EXTERNAL AUDIT

The last piece of the puzzle is to be able to quickly respond to external auditors that want to know that an organization's applications and systems are secure. Auditors will often want to ensure that certificates are valid and aligned with defined security policies, and that key and encryption strength are up to par with industry standards. Preparing for these audits is especially critical in highly regulated industries like finance and healthcare.

WHY YOUR PKI MAY BE AT RISK

Good Intentions Gone Bad

PKI vulnerabilities are likely not intentional. Vulnerabilities are more often the result of highly skilled IT professionals with good intentions that do not work in PKI 100% of the time. The task of standing up and running a PKI is often delegated to an individual with no previous experience or specialized knowledge in PKI. The expectation is that PKI is simple – requiring only a quick read through the install manual and a few hours to spin it up. Let's explore what can happen when this approach is taken.

In one Keyfactor client example, an IT team member cleaning out some old server racks decided to dispose of an old, non-supported server that hadn't been powered up for months – that "old server" was the root CA. As there were no compensating controls to require verification with another team member before retiring a server, the root CA needed to be recovered. While there was a backup, it was a hosted in the cloud, so the root had to be published online in order to be recovered, thereby putting the entire infrastructure and certificates at risk.

An enterprise may choose to build their own PKI or buy certificates from a public CA that meet a certain assurance level. In either case, the assumption is that those certificates offer an expected level of trust. However, due to inconsistent enforcement or adherence to policies and procedures, lack of knowledge or limited resources, enterprises often unknowingly downgrade the overall security of their PKI over time. It's like a sliding scale where, without proper maintenance, your PKI grows less secure with age.

> "The best practice is to never publish the root online. Exposing the root to your network, even for the briefest of moments, makes it vulnerable to potential access of the CA keys, ultimately putting the entire PKI at risk."

– CHRIS HICKMAN, CSO, KEYFACTOR

Getting it Right Starts at Design

Unfortunately, there are a large number of PKI design aspects that, once configured, cannot be changed without a complete redeployment. Many of these aspects can also have a significant impact on the long-term usefulness of your PKI. And since PKI components are around for many years, the ramifications of decisions made during the design phase can be significant.

WHAT CAN AND CAN'T BE REMEDIATED

What can be done if a component of the PKI is compromised? Or if a change is needed to the CA? What is the net effect of that change? Is it something that can be mitigated or not?

If your PKI has been compromised, the most conservative approach is to consider that even a minor compromise puts the entire environment at risk, and because of that, the intended level of assurance is lost and a new PKI must be implemented. Certificates must be immediately replaced and issued from a new, uncompromised PKI. For some less critical use cases, an enterprise may opt to continue as is, tighten up some of the controls and monitor the PKI environment more closely to ensure the compromise doesn't happen again, but this decision should be made on a case-by-case basis.

HOW REMEDIATION AFFECTS CERTIFICATES

Some things can't be changed, such as CA names — most products forbid it. Signing algorithm and key length are two other certificate features that can't be changed without revoking and re-issuing every certificate. While some minor changes can be made along the way, some changes will have broad-reaching effects. For example, consider the location of your Certificate Revocation Lists (CRL). While you may decide to publish the CRL to a new location, existing certificates that have already been issued will not reflect that new location. If an application performs revocation checking and cannot find the CRL, or if the CRL is expired, revocation checking will fail, which can have significant consequences.

A best practice for many CAs is to issue certificates with a limited life span, say one or two years, depending on the use case. However, through bad practices, necessity, or lack of appropriate tools to manage the certificate lifecycle, organizations sometimes issue certificates with longer life spans. The challenge occurs when a widespread change to certificates is needed. Certificates with longer life spans cannot be updated until the current certificate expires. This is especially true with auto-enrollment certificates, where default settings may control certificate issuance to an old root that should no longer be trusted.

PLANNING FOR THE NEXT AUDIT

Preparing for a security audit is always challenging, often more so when trying to provide an audit trail for security tools like PKI that may have never been audited before, or that do not typically have dedicated monitoring and management. If an enterprise doesn't have access to its complete inventory of certificates, it's impossible to say with any level of certainty that every certificate is under the protection of the established PKI controls and is being employed for the intended use.

THE ROLE OF POLICIES AND PRACTICES

The Certificate Policy (CP) and Certification Practice Statement (CPS) are the guiding documents that outline how certificates and the PKI are managed, providing proof of the intended level of assurance to a relying party during a digital certificate handshake. Even privately rooted CAs, at a minimum, should have corresponding CP and CPS documents that correctly identify how an organization will use, consume, and manage certificates in the infrastructure around them.

BUILD A SECURITY LEVEL AND STICK TO IT

Depending on the use case, an organization may plan for a PKI with low, medium or high assurance. The key is to maintain the original assurance level over time. Not maintaining this original level degrades the integrity of PKI and all application that rely on it. Not only do you risk having to explain why the original level wasn't maintained after a breach, but an auditor may perceive the downgrade as a failure to adhere to a specific standard.

PKI – The New Best Practices

PKI has evolved – demanding a new set of best practices. As more stringent industry and data security regulations come to fruition, businesses are becoming more reliant than ever on their PKI to guarantee trust. Getting it right requires significant investments in infrastructure, personnel, and ongoing operational support, but the payoff for building a robust and reliable PKI is invaluable.

01 UNDERSTAND YOUR USE CASES

A common mistake made before a PKI project leaves the ground is not fully understanding what goes into the design. It may look simple on paper, but the process of architecting a PKI that fits your unique environment and business needs must be verified before getting started.

Begin by understanding and documenting the intended use cases for your PKI thoroughly. Each following step throughout the project will depend on establishing this baseline knowledge. An incomplete inventory could, at the least, create more arduous work to remediate shortcomings, and at worst, result in a PKI that is unable to support growth without a complete re-build. Again, remember that certain settings while building a PKI are more or less "burned" into its fabric, so understanding your needs upfront and designing your PKI to align with them will prevent irreparable post-production issues.

02 DEFINE POLICIES & PRACTICES

Most organizations deploy a PKI quickly to address a specific project requirement, without consideration for proper policies and procedures. Fortunately, PKI has a well-defined structure for policy and practices defined in the form of Certificate Policy and Certificate Practice Statements (CP/CPS). Drafting a CP/CPS is optional, but your environment will benefit from a high assurance level through the enforcement of these policies. Not every enterprise needs a CP/CPS, but the best secured and managed PKIs usually do.

Once you've documented your use cases, you'll need to define your CP/CPS, which will guide you through the process of implementing controls for your PKI. Creating these documents can be a daunting task, but it's important to note that just copying another set of CP/CPS documents verbatim will not suffice. These tools only have value if they truly represent your organization's specific PKI requirements and operational processes. The NIST 7924 Draft CP/CPS can provide a solid starting point, but you will need to customize it to your organization.

03 PERFORM THE ROOT SIGNING CEREMONY

Building the root CA (i.e., the root signing ceremony) is akin to creating a "master key" to an organization's network and should be treated with the same sensitivity. The building and configuration of the root CA should be well scripted in a controlled environment. Depending on the assurance level desired for the PKI, this ceremony will range from an informal execution of a scripting document (low assurance) to a formal recorded event in a pre-authorized location (high assurance).

From the second the root CA is created, a chain of custody is established, which must remain intact from the minute it's incepted throughout its lifetime. If this chain of custody is broken at any time, the potential for malware infecting the machine, erroneous certificates being created, or the login security of a root CA must be assumed to have happened, and the root should be considered compromised. At that point, your PKI is not trustworthy and all certificates issued are invalid. Do not let this happen. The Root CA is a security measure that you have deliberate control over from start.

CONSIDER AN HSM

It is at this point that you will need to decide if a hardware security model (HSM) is required for your certificate authorities (CAs). This is a critical decision before deploying any of your PKI components. HSMs provide hardware-rooted protection for your PKI, but your budget may or may not allow for them. However, consider that a well-designed PKI is typically in use for decades. While HSMs can be integrated later on, they offer limited protection in comparison to building them in from the start.

04 BUILD & CONFIGURE THE INFRASTRUCTURE

Once the root signing ceremony is complete, it's time to build and configure the subordinate CAs and other ancillary PKI servers. Create a clear set of build documentation and configuration procedures to identify any gaps and ensure that infrastructure aligns with the CP/CPS established earlier. Share and review the plan with other PKI-dependent teams to ensure that you have not missed anything. Before placing the PKI into production, make sure that you're able to properly test all PKI components, as well as certificates across the various platforms and applications you intend to support.

Consider how certificates issued from your PKI will be managed throughout their lifecycle. Using custom scripts and manual spreadsheets may have worked with limited certificate counts, but most enterprises today have thousands, if not tens of thousands of certificates in their environment. Choosing the right solution will allow you to discover, manage, and automate the lifecycle of every key and certificate across your environment, without having to re-engineer your PKI or re-issue certificates.

05 MOVE FROM TEST TO PRODUCTION

While moving into a steady state, make sure that all components of the PKI are then properly operationalized. Like most assets created from a project of this type, when it moves into being part of the corporate infrastructure, there's no longer a project team accountable for the maintenance and upkeep. A PKI requires a significant amount of care and feeding to remain functional – these are dangerous tripping points for security teams who were focused on simply implementing the PKI, but not its ongoing operations. A common tripping point is forgetting about CRL intervals. Many teams forget to publish the CRL, causing all certificates to become immediately unusable.

A critical component to PKI operations involves how to incorporate, explain, and document changes, also known as change control. Compensating controls are another important element. A compensating control is an additional security measure designed to add security to a complex and sensitive environment, such as PKI. Adding an HSM to the root, securing where the HSM is stored, and controlling and monitoring who has access to it are all considered compensating controls. Consistently keeping the HSMs in a separate locked cabinet under 24/7 video surveillance for which only a select few have a key adds additional compensating controls to satisfy audit requirements.

DON'T FORGET ABOUT DISASTER RECOVERY

Many organizations running their own PKI in-house have never conducted end-to-end disaster recovery (DR) testing. This is different from simply testing a CA or root recovery and re-installing a certificate. An effective DR testing strategy should include:

- Understanding what it would take to rebuild the entire PKI environment, including the root CAs, issuing CAs, validation schemes, and OCSP or CRL
- Ensuring that the certificates are consumable by the relying parties that need them
- Putting together a testing plan and organizing a test environment
- Testing and continual fixes

06 CONTINUOUSLY REVIEW, TEST & AUDIT

Once controls have been documented and operationalized, review and test them on a regular basis. This is often part of an internal audit, and should include review and testing of everything listed in your CP/CPS, business continuity, and DR plans for all PKI components. If there is a legitimate need for a change, kick off a change control to update any of the documents. Think of them as living, breathing documents that evolve with the goal of maintaining the PKI's intended level of assurance.

Organizations that schedule and conduct their own internal audits regularly are able to easily identify issues, answer external auditor questions, and provide proof of the required level of assurance. PKI owners should also monitor and benchmark their enterprise PKI controls against current and emerging standards including the CA/Browser Forum, WebTrust, and industry regulatory agencies. This helps the organization stay ahead of trends that could otherwise lead to PKI shortcomings. Another best practice is to conduct an annual PKI health check to uncover anything the organization may not have considered.

It's Time to Re-Think Your PKI

While PKI has been a backbone of enterprise IT for decades, the role of PKI in the enterprise has changed drastically. No longer viewed as a deep-weeds technology responsible for a limited number of use cases, PKI is now emerging as a core requirement to support digital transformation.

PKI isn't like any other technology in your IT stack – it's a complex ecosystem of roles, policies and procedures, hardware and software. Just keeping it up and running can be challenging enough for organizations, never mind enabling new integrations. Security teams find themselves fighting fires to mitigate the risk of a breach or outage, while the integrity of their PKI continues to degrade.

Executing an in-house PKI successfully is not impractical, but it does require significant investment of time and resources to get it right. Enterprises that limit their PKI deployment to components bundled into their operating system (i.e. Microsoft CA) will quickly realize that this approach is not sustainable.

KNOW YOUR OPTIONS – IN-HOUSE PKI VS CLOUD-HOSTED PKIAAS

When it comes to private PKI, you have two options, either build your own or move it to the cloud. PKI as-a-Service platforms provide all the benefits of a privately-rooted PKI, but without the cost and complexity of running it in-house. With dedicated PKI expertise at their disposal, proactive compliance coverage, and multi-layered security across infrastructure and operations, PKIaaS providers can deliver a much more effective, and ultimately more secure, PKI than most enterprises can achieve on their own.

Whether you deploy internally or work with a reputable provider to build and run it for you, PKI has to be done right. Make the best decision for your business based on the resources available to you. Whichever path you choose, Keyfactor can help you determine your PKI requirements and find the solution that works best for your business.

RUN IT IN-HOUSE

Certificate Lifecycle Automation

- Gain complete visibility of keys and certificates with direct integration into public and private CAs
- Group certificates, monitor status, get alerts and notifications in real-time
- Automate the lifecycle of keys and certificates from issuance to renewal and revocation
- Integrate with existing IT systems as well as Cloud, DevOps, and IoT infrastructure

LET KEYFACTOR RUN IT

Cloud-Hosted PKIaaS

- Get a dedicated, privately-rooted PKI in the cloud without any shared infrastructure
- Leverage our team of experts to manage and monitor your PKI 24 x 7 x 365
- Retain complete control over your PKI root and recovery materials
- Stay confident with proven SLA uptime and guaranteed response commitments

Find out how enterprises are moving their PKI to the cloud to enable digital transformation without compromise to security.

Talk to our experts ▶

ABOUT

KEYFACTOR

Keyfactor empowers enterprises of all sizes to escape the exposure epidemic – when breaches, outages and failed audits from digital certificates and keys impact brand loyalty and the bottom line. Powered by the industry's only PKI as-a-service platform, IT and infosec teams can easily manage digital certificates and keys. And product teams can build IoT devices with crypto-agility and at massive scale.

CONTACT US

▶ www.keyfactor.com

▶ 216.785.2990