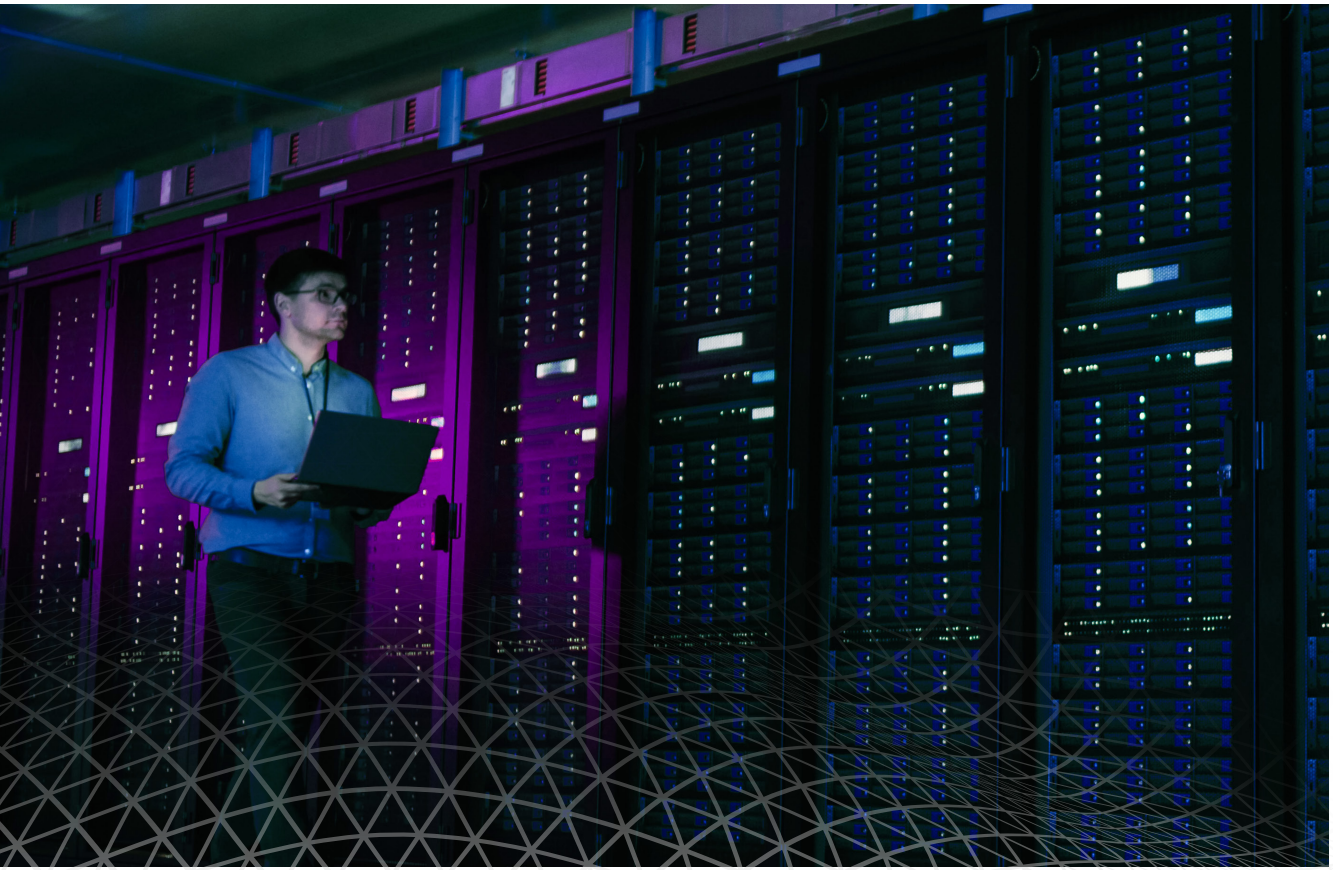
KEYFACTOR
SECURE EVERY DIGITAL IDENTITY

EBOOK

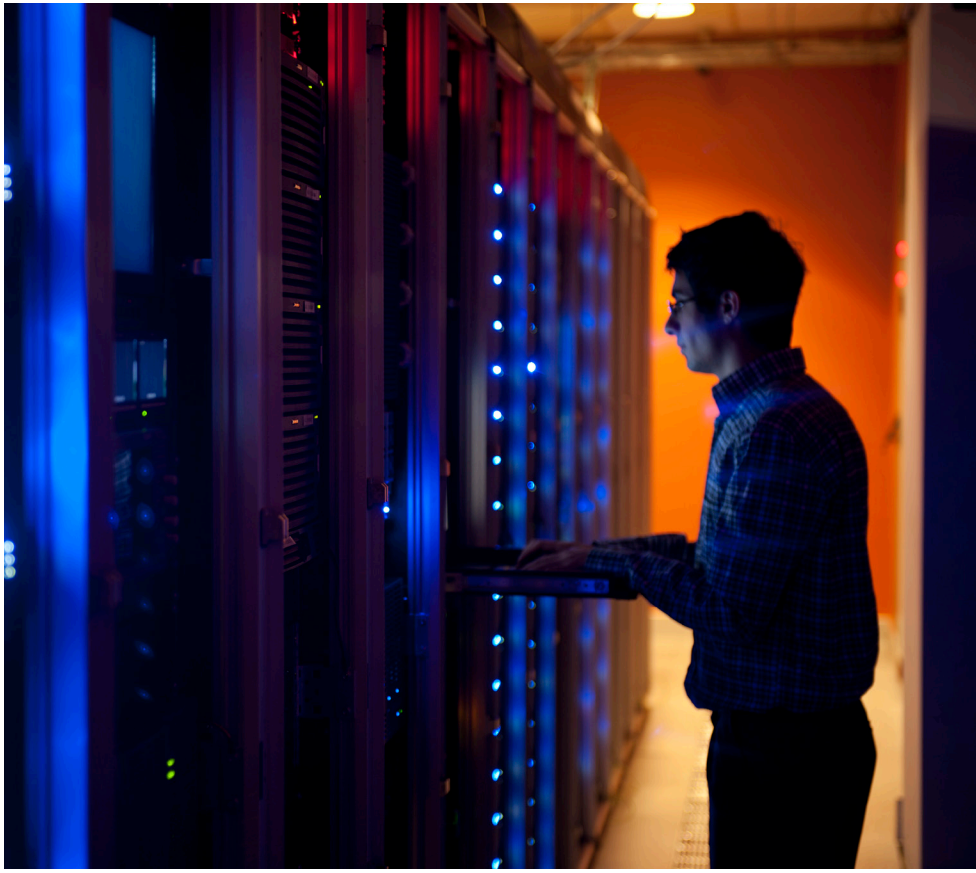
IS YOUR PKI SECURE?

5 Common PKI Pitfalls to Avoid



Introduction

Public key infrastructure (PKI) is a core building block of IT in your enterprise, providing secure digital identities for people, devices, and applications. Many organizations build and deploy their own PKI to support things like data protection and network authentication. Furthermore, PKI today is expected to support new use cases like the Internet of Things (IoT), DevOps and Cloud initiatives. But if PKI is so critical to the business, then why do so many PKI deployments fail?



Running your own private PKI — what we call "DIY" PKI — comes with a number of advantages, but most organizations underestimate the scope of work that goes into building it right, not to mention the continuous "care and feeding" it requires once its production-ready. If mistakes are made from design through operations, it can create problems, headaches, and sometimes even more serious issues like an network outage or a security breach down the line.

While it's often quite easy to deploy, PKI is a technology where you have exactly one chance to get it right — at installation. After that, parameters are more or less set in stone, and re-deployment becomes the only way to fix a mistake.

Here are five of the most common mistakes we see with "DIY" PKI and why you re-evaluate your PKI deployment.

Pitfall 01

POOR PKI PLANNING & DESIGN

Most organizations deploy a PKI quickly to meet a specific project requirement, without consideration for proper planning and security controls. After all, Microsoft makes it easy to build a server with a Certificate Authority (CA) role. Just a couple of clicks on the “Next” button later and your new CA is ready to issue certificates to your devices. Mission accomplished, right? Unfortunately, not. Lack of upfront investment in PKI planning and design can lead to serious risks and headaches down the line.

> “Certificate hierarchy planning is one of the most important aspects of PKI design”[1]
>
> MICROSOFT

[1] source: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn786436(v=ws.11)

Pitfall 01 (Cont'd)

OVER-ARCHITECTING THE CA HIERARCHY

With many IT systems, a picture truly is worth a thousand words. An architectural diagram with "boxes and lines" makes up the majority of the design. This is the case for networks diagrams, database architectures, directory structures, and many other IT components. Following this mindset, many first-time PKI architects focus almost exclusively on the hierarchy of certificate authorities (CAs).

01
02
03
04
05

An overly-high level of focus on the PKI hierarchy can lead to a tendency to include more "boxes and lines," resulting in designs that involve more CAs than necessary. Additional CAs not only come at a cost, they also make it much more difficult to keep certificate issuance processes secure and under control.

While the CA hierarchy is important to the overall design, it is not the whole story. The "boxes and lines" get all the attention, but there are many other design decisions that are of equal, and often greater, importance. Policies, certificate revocation lists (CRLs) and planning, algorithms and key sizes, and validity periods are just some examples that can have a much more significant and lasting impact on the integrity of your PKI than the hierarchy of CAs.

UNDER-ARCHITECTING EVERYTHING ELSE

Sometimes, it's just too easy to click "Next." Unfortunately, with PKI, there are a large number of design aspects that, once configured, cannot be changed without a complete re-deployment. As mentioned above, many of these can have a significant impact on the long-term success of your PKI, including:

- **Certificate validity, key sizes, and signing algorithms**: Every certificate issued from your CA carries these attributes, and they cannot easily be changed. Since PKI components last for many years, the ramifications of these choices can be significant.
- **CRL Distribution Points (CDP)**: CRL locations are included in issued certificates, so changing the location of your CRL means you'll need to re-issue every certificate.
- **Availability Planning**: If a CA is down, you'll be unable to issue new certificates, but if your CRL or OCSP servers are not available, all of your certificates become immediately unusable.
- **Operational Policies**: The moment you issue your first certificate – whether you planned to or not – you just set the issuance policy for your CA. Once you've set the bar, you can only lower it

Pitfall 02

OVERLOOKING THE "INFRASTRUCTURE" IN PKI

In the interest of saving time or avoiding operational effort, far too many PKIs get deployed with lower-than-desired security controls. But most IT and security teams don't realize the impact if they lose control of their PKI, if it's compromised, or if it's mishandled internally. Because PKI supports business-critical applications, security must come first.

The key word in PKI is infrastructure. When it comes to security, most organizations will focus heavily on who has access to the CAs. While access controls are critical, many fail to consider the security around all of the infrastructure involved in PKI.

Pitfall 02 (Cont'd)

SERVER/OS SECURITY

Who has permission to login to the CA for administrative tasks? If you have multiple infrastructure support teams with rights to login to the server – whether locally or through remote desktop – this could potentially expose the device to an internal threat or compromised user account. If a sensitive file, such as a private key (PFX), is mistakenly left within the file system, this can be the nail in the coffin.

TRACKING AND MONITORING

PKI logs should be captured and continuously monitored to detect any potentially malicious activity in your environment. Your PKI doesn't keep office hours, so you'll need a dedicated resource that can ensure your PKI is secure and available around the clock.

BACKUP SECURITY

When backing up your CA environment, consider who has access to the data within those backups, and who has the ability to restore it. Data-at-rest and in-transit should always be encrypted, and only a specific subset of individuals should have the ability to restore operations of that data.

HARDWARE SECURITY

Because the majority of attacks today occur over the network, not much attention is given to physical security of hardware, in fact, it's often assumed to be in place. However, when designing a PKI, additional consideration must be given to protect the underlying infrastructure. Without highly-specialized controls, unauthorized physical access or mishandled hardware can quickly undermine the integrity of your PKI, and subsequently the critical applications that rely on it.

SECURING YOUR ROOT CA

The root CA is the foundation of trust for every certificate issued in your environment. If it is breached, either physically or over the network, your entire PKI is compromised. Because the root CA is only accessed a few times each year, it should be kept offline and air-gapped from your network. There is no five-second rule here. Even if the CA is powered on for a short time-span, once you connect, you are online, and there is no walking back. Time to re-build if that occurs.

Pitfall 03

LEAVING PRIVATE KEYS UNPROTECTED

A critical consideration in any PKI deployment is how private keys are stored and managed, particularly for certificate authorities (CAs). A robust key protection strategy, including physical and logical security controls, is a must to protect private keys from external hackers or insider threats that seek to compromise the integrity of your business-critical systems and sensitive data.

61% of IT and security professionals say they are concerned about their ability to keep keys and certificates secure throughout their lifecycle.[2]

[2] source: https://info.keyfactor.com/the-impact-of-unsecured-digital-identities-ponemon-report

Pitfall 03 (Cont'd)

STORAGE OF CA PRIVATE KEYS

When building your CAs, the private keys should never exist outside of the systems they are installed on. Extreme caution must be taken when considering how these keys are stored and accessed. For instance, in a default Active Directory Certificate Services (ADCS) deployment, the CA private key can be accessed by any user that authenticates as a local administrator. Organizations should avoid software-based keys for CAs and enforce strong hardware-level protection with multi-person authentication.

IT specialists are often reluctant to deploy Hardware Security Modules (HSMs) to store their private keys due to the upfront cost. HSMs are either viewed as unnecessary overhead or an additional component that can be added later on. However, the integrity of your PKI and every certificate issued from it relies entirely on the security of your private keys. Protecting these keys is mission-critical and HSMs make it nearly impossible for any malicious actor to export or compromise them. This level of protection can be the difference between a secure environment and a major breach.

DISTRIBUTION OF PRIVATE KEYS

Private keys are critical, because they enable decryption and are blindly trusted by your network, as well as browsers and operating systems in the case of publicly-issued SSL/TLS certificates. If a malicious insider or hacker finds a private key, they can hide in your encrypted traffic, access systems, and decrypt sensitive data. Ensuring that these keys are not compromised or mishandled is critical.

We have seen many organizations where the standard practice is for the PKI administrator to generate the certificate, then email it to the end-user or share it on a file system with the associated private key. By this simple step, your private keys are exposed to multiple points across the organization, including: in the administrators outbox, in the end-users inbox, on synced mobile devices, in email archive and backup systems, and in any systems that scan email attachments for viruses or malicious code. All it takes is a well-crafted phishing attack to gain access to an inbox and compromise the private key.

Pitfall 04

LACK OF CERTIFICATE LIFECYCLE PLANNING

Without the right tools and processes in place to effectively manage PKI operations, there are a number of consequences that can be hard to remediate. IT specialists may overemphasize focus on the infrastructure and how to get certificates out initially and underestimate the effort of dealing with certificate expirations and outage prevention.

74% of organizations say that digital certificates still cause unplanned outages and downtime.[3]

[3] source: https://info.keyfactor.com/the-impact-of-unsecured-digital-identities-ponemon-report

Pitfall 04 (Cont'd)

Developing a certificate lifecycle plan, which is also secure, can take a significant amount of time and effort to get it right. If your PKI is being used for embedded systems, network-enabled products and devices, developing a secure, high-volume issuance process is also critical.

A common mistake when deploying certificate-enabled applications is to focus short-term on the rollout, and the tasks involved with initial deployment. All certificates expire, and if planning doesn't include the entire certificate lifecycle, major problems can result. The unexpected and unhandled expiration of certificates can cause significant outages and downtime.

This concern isn't exclusively tied to certificate expiration either. Depending on the application involved, planning for other certificate lifecycle events such as revocation or key archival and recovery processes can be even more important than certificate renewal planning.

01
02
03
04
05

DEATH BY SCRIPTS AND SPREADSHEETS

Many organizations today still use a manual spreadsheet-based approach to inventory and manage their certificates. Not only is this approach prone to error, it simply doesn't scale to the thousands or hundreds of thousands of certificates in use across your organization. A single miss can cause a serious outage that quickly turns your IT issue into a business problem.

Pitfall 05

INSUFFICIENT TRAINING & EXPERTISE

When deploying PKI, many times the task is delegated to an administrator (or a team) with no previous PKI knowledge or experience. This is often done with the expectation that PKI is simple – requiring only a quick read through the install manual and a few hours to spin it up. Evidently, this is not the case.

Deploying PKI in-house can be complicated from a technology perspective, and even more difficult from a process standpoint. Ultimately, though, it is people and processes that drive the success of your PKI from deployment through operation. It's critical then, that your people understand all of the components, as well as certificate policy and certificate practice statements (CP/CPS), that make up a robust PKI, and how to deploy and operate it effectively. That means investment in proper PKI training and full-time operations management. Without it, organizations will unavoidably run into one or more of the PKI pitfalls mentioned above.

Pitfall 05 (Cont'd)

Here are a few real examples where we've seen well-intentioned administrators make costly mistakes:

Certificate Oversight

An administrator was assigned permissions to generate certificates for web servers. For every certificate issued, they would also be emailed to the team's distribution list and placed on a Microsoft SharePoint site. Over 1,200 certificates were shared and stored without the knowledge of the security team.

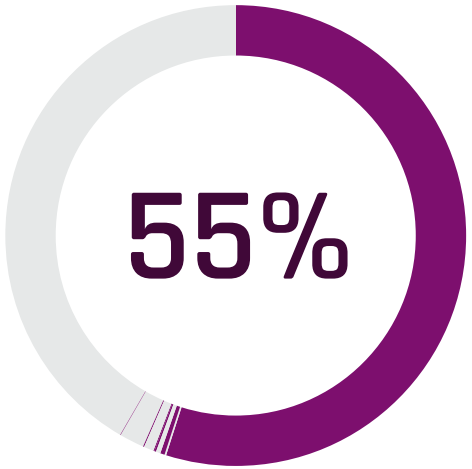
Template Mishap

A developer requested a code signing certificate to sign developed software. The administrator decided the easiest way to accomplish this was to add code signing capabilities to the user certificate template and re-deploy throughout the environment. Every user in the company was now able to sign code.

Root Un-Racked

A new root CA was deployed within the data center, and for security reasons, was powered off and unplugged from the network. However, because the server was not physically secured, the data center team un-racked the server and disposed of it during routine maintenance, since it appeared not in use.

These scenarios can be avoided with the right expertise, but the reality is that most organizations don't have sufficient IT and security resources to dedicate to their PKI. Even if resources are available, in today's workforce, personnel can quickly shift, leaving PKI in unfamiliar hands. Due to the intricacies of PKI, problems are likely to arise unless you happen to have that knowledge within your organization, and equally important, the depth in personnel to be able to execute it properly.



More IT and security professionals have or plan to outsource their PKI deployment to reduce complexity and improve security.[4]

Build it Right – Move Your PKI to the Cloud

Deploying and running a PKI in-house can be a complex undertaking for even the most experienced IT and security professionals. Unlike other tools in your IT stack, it's not just about technology. PKI is a set of moving parts including hardware, software, policies and procedures. And there is no room for error. Mistakes made during PKI design and deployment not only create headaches for administrators and certificate users, they also significantly increase the risk of a widespread outage or security breach.

We frequently run into scenarios where complex PKI deployments are inherited by a new IT specialist unfamiliar with PKI; sometimes it's a "temporary" deployment that went wrong. Other times, it's simply a matter of maintenance and operational overhead taking critical IT and security resources away from their core competencies.

In any case, moving your PKI to the cloud can help.

[4] source: https://info.keyfactor.com/the-impact-of-unsecured-digital-identities-ponemon-report

Rethink Your PKI

Find out why more IT and security teams are offloading their PKI to the cloud with PKI as-a-Service. Read our guide to re-thinking your PKI. It's easier than you think.

Learn More ▶

ABOUT KEYFACTOR

Keyfactor is a leading provider of secure digital identity management solutions that enables organizations to confirm authenticity, and ensure the right things are interacting in the right ways in our connected world.

CONTACT US

▶ www.keyfactor.com ▶ 216.785.2990