WHITE PAPER

PKI Automation for the Future

KEYFACTOR

Table of Contents

INTRODUCTION

In 1950, Albert Einstein wrote that “Perfection of means and confusion of goals seem, in my opinion, to characterize our age.” At the time, he was referring to the safety and welfare of mankind. Today, he might be referring to many technology solutions we adopt without fully calculating what they’ll deliver—or fail to deliver. Public Key Infrastructure (PKI) can be one such technology. Nobody deploys PKI solely for PKI’s sake. Trusted roots, keys, and certificates are a proven method to achieving meaningful authentication, encryption, and digital signing across key application and networking workloads within IT infrastructures.

Three Goals of PKI

The primary goals of a quality PKI deployment are comprehensive security, operational efficiency, and business continuity. If we do not ultimately achieve greater security, simplified administration, and increased productivity through the use of certificates, our goals have not been met. Either way, we haven’t achieved what PKI is capable of delivering today and in the future.

A key element of all three goals is automation. An automated approach optimizes PKI management throughout the enterprise and across IoT devices. Automation swaps out aging algorithms and ensures updated certificates are applied. For enterprises, it allows certificates to be re-used, saves administrators time, and enables crypto-agility.

Why is automation so important? One of the leading sources of errors like data breaches or financial loss, is not technology but rather, human negligence. Manual processes set us up for a higher than acceptable rate of error, and ultimately increases exposure and risk. As our infrastructures and workloads grow in size and complexity, that rate only increases. PKI automation is a proven way of ensuring these overarching goals are met no matter how sizable or complex the steps are to reach them.

> One of the leading sources of data breaches or financial loss is not technology but, rather, human negligence. Manual processes create a higher-than-acceptable rate of error, and ultimately increases exposure and risk.

01 | COMPREHENSIVE SECURITY

02 | OPERATIONAL EFFICIENCY

03 | BUSINESS CONTINUITY

Automation's Role in Successful PKI

01 | COMPREHENSIVE SECURITY

Simply put, PKI automation reduces the room for errors that result in risk and harm. Not only does it ensure that tasks are performed correctly, it also ensures they're being done comprehensively. A good example is the very common renewal or replacement of certificates and their deployment to servers, IoT devices and network appliances. Automation ensures that the correct certificate is always requested and issued using the correct template with proper parameters. Additionally, automation will ensure that all endpoints requiring new certificates are immediately addressed. PKI automation eliminates the chance of forgetting about an endpoint (because it went temporarily offline, for example) and leaving unsafe certificates, bad keys, and untrusted roots active.

Replacement of certificates can also come as a result of a breach or the discovery of a vulnerability. This includes replacing certificates from Roots of Trust (RoT) that have been compromised or deprecated. In this case, the configuration of trusted roots also needs modification across the infrastructure. In many of these instances, timing is of the utmost importance. Until all endpoints are updated, risk levels are increased. When dealing with numerous endpoints, and administrators who run from one box to another hoping they haven't missed any, PKI automation ensures that delays are minimized in performing these updates across the organization.

Comprehensive security also requires absolute knowledge of your certificate inventory. PKI automation means direct communication and synchronization with issuing certificate authorities, and complete certainty of inventory. Gaining 100% visibility into the existence and presence of a certificate requires direct knowledge of certificates issued, along with understanding of all lifecycle actions taken on those certificates. Automated synchronization with certificate authorities (CA), including your own private CAs as well as public CAs, is essential.

Another security measure that automation enables is the reduction of reliance on network credentials to update key stores and trust stores. When an administrator wants to update multiple servers and network devices, they must reach out to those endpoints over the network or directly one-by-one, using credentials with sufficient rights to perform every update. Especially in cases involving service providers and multiple domains, there is a desire to limit how many such standing credentials are floating around. Temporary credentials may be established for each administrative routine, adding extra steps, time, and room for error. Through automation, leveraging device and appliance integrations configured with sufficient rights, reduces the administrator's need to carry or request such credentials.

As more devices come onto your network and more apps are rolled out, the need for your PKI to scale, enforce encryption, authenticate and manage overall security grows every day. You should not hold back or hand-select certain devices because of budget limitations or per-certificate fees. It's critical to cover every identity across the enterprise.

02 | OPERATIONAL EFFICIENCY

Operational efficiency is a goal in nearly everything we set out to do. In the realm of PKI, our desire may be to save money in the performance of routine tasks, or enable our resources to take on additional, higher-priority workloads. Very often, often it's a combination of both. Automation of key certificate lifecycle management tasks reduces the amount of manual work required, while reducing the time it takes to complete them.

PKI automation also helps us meet service level agreement (SLA) obligations. When commitments are made between service provider and customer (including when both are within the same organization), manual execution of work can play a big role. Due to a high degree of specialization, it's common for organizations to rely on very small teams, or even a single individual or two, to manage their PKI. When work piles up or when resources are out of office or unavailable, execution of these tasks within acceptable SLA timeframes can be a challenge. Automation of those same routines means that the work gets done regardless of your PKI administrator's availability or work queue. Automation allows enterprises to re-use certificates, as well as swap out identities across servers, load balancers, firewalls, containers, cloud workloads, mobile and IoT devices.

03 | BUSINESS CONTINUITY

One of the most common causes for system outages is certificate expiration. One of the most common causes for expired certificates is the manual process used to renew, reissue, and deploy them. Working from lists that grow and change each day, within networks that spring up new endpoints (many of them from Shadow IT efforts) faster than an administrator can spot them, there is simply no way for an administrator to have full oversight unless PKI automation is in play. There will always be the one “I missed” and someone will most likely find out about it once it’s too late. Through automated discovery of endpoints, automated reporting on impending expirations, and automated handling of renewal and re-issuance, you can be confident with the elements in place designed to ultimately keep servers up, do not paradoxically take them down.

Security teams often don’t know how many certificates they have or when they expire. These unknowns turn into costly outages, such as those seen at Equifax, O2, and LinkedIn. In a more recent example, Microsoft Teams suffered an outage after Microsoft failed to renew a client authentication certificate. The application was down for nearly 3 hours, just as millions of users logged in to start their work week.

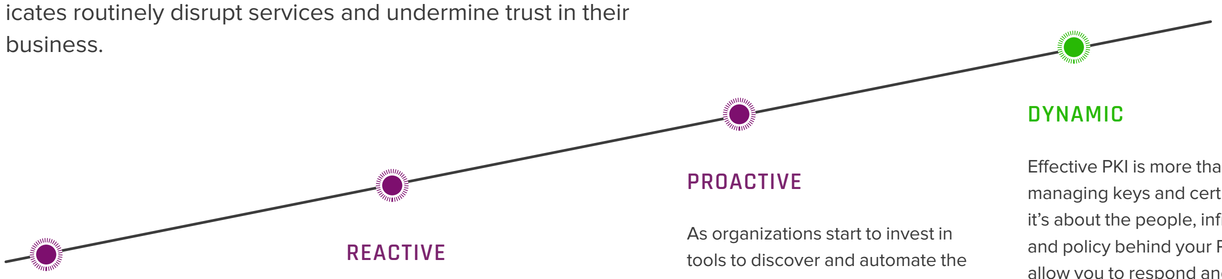
In conjunction with the increased security that automation brings to security response and incident handling, another benefit gained from automation is response readiness. There will always be another fire to put out, whether it’s the result of a breached root or a new vulnerability affecting us overnight. Having automation in place ensures the next such incident requiring the removal or exchange of keys and certificates, can be optimally handled in minimal time. Speed is often of the lifeblood of a response, and PKI automation is a fundamental accelerator.

Close Your Critical Trust Gap™

PKI MATURITY MODEL

More certificates, shorter lifecycles, and changing standards in cryptography have exponentially increased the risk of outages and failed audits. IT and security leaders now face a Critical Trust Gap - where mismanaged keys and digital certificates routinely disrupt services and undermine trust in their business.

Automation is the answer. Industry leading organizations are re-thinking their PKI strategy by adopting a cloud-first and automated approach to close their Critical Trust Gap.



MANUAL

Despite adoption of new technologies like cloud, mobile and IoT devices, most organizations still use manual methods to track and manage certificates.

- Excel Spreadsheets
- Resource-Intensive
- No Discovery
- High-Risk of Outages

REACTIVE

CA-provided tools and PKI interfaces are a level up from spreadsheets, but without centralized discovery and automation, security teams are still locked into a reactive mode.

- Multiple CA Silos
- Limited Visibility & Control
- Limited Automation
- Minimal Reporting

PROACTIVE

As organizations start to invest in tools to discover and automate the lifecycle of certificates, they’re able to focus less on preventing outages and more on enabling new PKI use cases.

- Complete Visibility
- End-to-End Automation
- Reporting & Alerting
- Policy Enforcement

DYNAMIC

Effective PKI is more than just managing keys and certificates, it’s about the people, infrastructure and policy behind your PKI that allow you to respond and adapt to change effectively.

- Cloud-First PKI Strategy
- CA & Technology-Agnostic
- Crypto-Agile
- Highly Scalable & Extensible

One-Step Automation from Keyfactor®

Keyfactor Command is a powerful workforce multiplier, automating real-time discovery, monitoring, provisioning and renewal of millions of keys and certificates issued from inside or outside your organization, while blocking untrusted access.

To learn more, visit:
https://www.keyfactor.com/keyfactor-command-certificate-lifecycle-automation/

KEYFACTOR PROVIDES YOU:

- Automated lifecycle management of certificates issued from public or privately-trusted certificate authorities
- Flexible deployment options - run it on your servers, in the cloud, as-a-service, or combined with dedicated, cloud-hosted PKI as-a-Service
- Complete control over the use of Root CA keys and PKI recovery materials.
- Proven SLAs with clearly stated, guaranteed response times.
- Comprehensive and thorough insight into the operations of digital certificates.
- 24x7x365 service monitoring by a team of trained PKI experts

KEYFACTOR

Keyfactor empowers enterprises of all sizes to escape the impact that breaches, outages and failed audits from mismanaged digital certificates and keys have on brand loyalty and the bottom line. Powered by an award-winning PKI as-a-service platform for certificate lifecycle automation and IoT device security, 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. Exceptional products and a white-glove customer experience for its 500+ global customers have earned Keyfactor a 98.5% retention rate and a 99% support satisfaction rate.

Learn more at **keyfactor.com**

CONTACT US

- www.keyfactor.com
- +1.216.785.2990