WHITE PAPER

HOW TO SCALE PKI AND CERTIFICATE MANAGEMENT IN

Hybrid & Multi-Cloud Operations

The guide to managing decentralized PKI in a zero-trust world

KEYFACTOR

Table of Contents

ESTABLISHING TRUST IN THE CLOUD 3

DECENTRALIZED PKI: THE NEW REALITY 4

DIFFERENT CAs, DIFFERENT CHALLENGES 5

ROADBLOCKS TO SUCCESS 8

KEY CONSIDERATIONS 9

PKI THE WAY YOU WANT IT 10

CONCLUSION 12

Establishing trust in the cloud

Hybrid and multi-cloud environments are the new norm. Of course, where your organization is on that journey is another story, but the reality is that it's the direction we're all headed. In this imminent shift, security teams are re-thinking how to protect their applications and infrastructure across increasingly complex and untrusted environments.

Cloud and Zero-Trust are the top factors driving the deployment of more PKI and machine identities.

2021 State of Machine Identity Management

Zero trust security

As we move to the cloud, the security focus shifts from boundaries to identities. In this perimeterless model, nothing is inherently trusted until authenticated and authorized — an idea known as zero trust security.

Public key infrastructure (PKI) and machine identities, such as X.509 certificates, are key ingredients to zero trust security. Everything from virtual machines, containers, applications, container orchestration and service mesh platforms all rely on keys and certificates to authenticate and securely communicate with one another.

Knowing what can be trusted, in which environments, and when, depends on machine identities and the PKI infrastructure that sits behind them.

Traditional PKI

Behind every certificate is a certificate authority (CA). Microsoft Active Directory Certificate Services (ADCS), often referred to as Microsoft CA, has long been the de facto choice for many organizations, since it's well-integrated with Microsoft infrastructure and it supports standard use cases like user and device authentication.

However, the path to the cloud introduces new challenges. For starters, most on-premise PKI deployments just weren't built to handle the volume and velocity of certificate usage today. Not to mention a lack of out-of-the-box integrations and easily overlooked misconfigurations.

Organizations now face a dilemma — they've outgrown their traditional PKI. As a result, many need to re-build or redesign to support this new reality. It starts with looking at the wide array of CAs that serve as the backbone of PKI today.

Decentralized PKI: the new reality

The reality is that PKI no longer consists of just one or two CAs behind the four walls of your datacenter. Today's hybrid and multi-cloud operations involve various public, private, and cloud-based CAs, each implemented by different teams to meet specific use cases and requirements.

In other words, PKI is everywhere, certificates are everywhere, your machines are everywhere, and it's all being driven by:

> "Trust requirements, migration, specialized use cases, hybrid environments, and the lack of out-of-the-box integrations are all drivers for the usage of multiple PKIs and CAs.[1]"

Hybrid trust

Every enterprise relies on a mix of public CAs and internal private CAs to meet trust models within and outside the organization.

Hybrid / multi-cloud

Most companies leverage multiple cloud services, each with their own built-in capabilities for PKI and certificate issuance.

Specialized use cases

CI/CD toolchains and containers require shorter-lived certificates when compared to traditional web servers and devices.

Dispersed teams

Different teams and departments across the organization prefer different CAs due to cost, requirements, assurance levels, etc.

Lack of integrations

ADCS is well-suited for Microsoft infrastructure, but it does not offer native support for other applications, creating a heavy burden on teams.

Business growth

Mergers and acquisitions in high-growth companies result in mixed CA environments, often with conflicting rules and security policies.

[1] Gartner, Solution Comparison for PKI and Certificate Management

Different CAs, different challenges

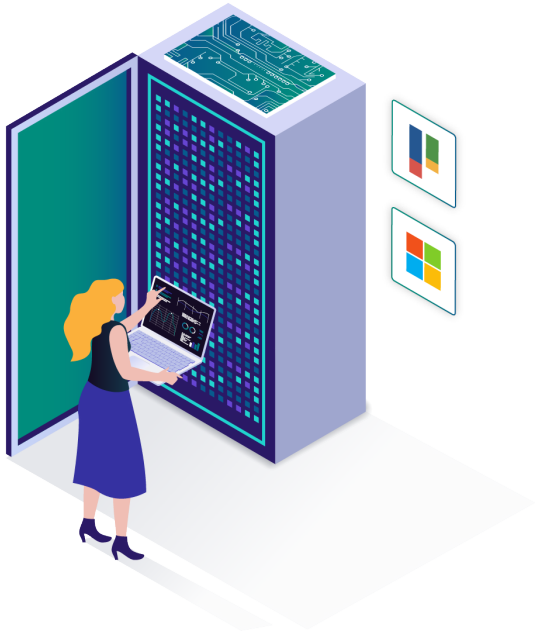
Whether you have multiple CAs already in production, or you're starting from scratch, there is a lot to consider. Let's take a look at the various types of CAs, when and where they are used, and key considerations for implementation.

Public CAs (third party)

Publicly trusted certificates issued from third-party CA providers are deployed to public-facing assets (e.g., web servers, load balancers, services, and applications) to avoid browser warnings and ensure trust.

Recommendations:

- Do not use public certificates where private certificates are better suited
- Avoid CA-provided certificate management tools that lack discovery, automation, and multi-CA support
- Ensure that you can add or switch CA vendors easily in the event of disruptions or changes



Private PKI (internal)

Most organizations deploy and run their own internally trusted PKI to support user and device authentication, machine-to-machine connections, and to provide trust for employees, partners, and internal assets.

Recommendations:

- Ensure you have the bandwidth, expertise, and infrastructure to setup and run PKI in-house
- Watch out for ADCS "configuration drift" which creates vulnerabilities that are difficult to remediate
- Consider a more flexible, scalable, and supported alternative to ADCS (e.g., PrimeKey EJBCA)

PKI as a Service

Fully managed, cloud-hosted PKI services offer the benefits of private PKI, without the effort and expense of running it in house. Modern PKI as a Service (PKIaaS) solutions combine dedicated private PKI and certificate lifecycle automation into a single cloud solution.

Recommendations:

- → Consider PKIaaS to get the benefits of private PKI without the risk and cost of running it in house
- → Evaluate root key storage, assurance levels, support and services, and vendor experience
- → Avoid look-alike "PKI as a Service" solutions

Built-in issuers

DevOps tools such as HashiCorp Vault, Istio, and Kubernetes offer built-in certificate issuance capabilities. These are typically used for high-volume issuance of short-lived certificates in containers and CI/CD pipelines.

Recommendations:

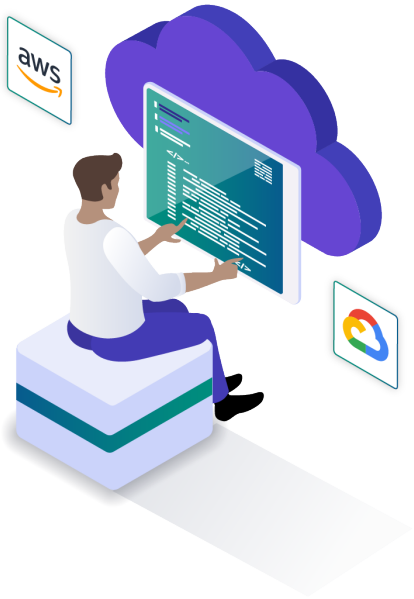
- → Beware of self-signed CAs that do not provide assurance and lack proper policy and safeguards
- → Integrate secrets managers and DevOps tools with policy-compliant issuers (private or public CAs)
- → Do not use these tools without certificate monitoring

Free SSL/TLS providers

Some use cases can be supported by free SSL/TLS certificate providers such as Let's Encrypt and ZeroSSL. These CAs issue domain-vallidated 90-day and one-year certificates and support integration via APIs or the popular ACME protocol.

Recommendations:

- → Know where and when to use domain-validated versus higher assurance certificates
- → Understand limitations - no custom certificate content (e.g. SAN), more frequent configuration changes, etc.
- → Use a certificate lifecycle automation solution w/ ACME support to monitor, revoke, and renew certificates



Cloud CA services

Cloud service providers like AWS and Google Cloud offer their own cloud-native CAs. In addition, there are turnkey PKI solutions, such as PrimeKey EJBCA SaaS, which can be deployed directly from the cloud marketplace.

Recommendations:

- → Remember, you're still responsible for configuring and managing issuing and root CAs
- → Ensure that you have the expertise and bandwidth to properly configure and maintain CAs
- → Avoid siloes – use a certificate management solution that integrates with multiple cloud-based CAs

Roadblocks to success

As companies adopt a decentralized PKI model, the task of governing multiple CAs and managing thousands of certificates becomes extremely complex. Without proper management, PKI and machine identities created to establish trust wind up becoming your biggest security risk.

Without standardized PKI and machine identity management processes, organizations run into several roadblocks to establishing trust. Every CA introduced into an environment brings a new interface, configuration settings, protocols, and enrollment processes that create more and more siloes in visibility and control.

Unfortunately, the resulting situation isn't unlike the "wild west," where application owners ignore policies and issue certificates outside of corporate security (e.g., self-signed certificates, wildcard certificates). Even worse, poorly configured CAs and configuration drift create unknown vulnerabilities that go overlooked until they cause an outage or audit failure.

The problem is that there is no consistent source of control and governance across your PKI and certificate infrastructure. These challenges only multiply with the adoption of hybrid and multi-cloud environments where high-volume issuance and short-lived certificates are the norm.

Band-aid solutions such as homegrown scripts and pouring more resources into the problem only go so far in filling the gaps. Teams end up spending far too much time on certificate issuance and installation — distracting them from important projects and delaying timelines.

To enable cloud security, teams need the flexibility to deploy PKI where and when they want, without running into these roadblocks.

Key Considerations

So, what now? Do you spin up a new cloud CA? Do you extend your existing PKI to the cloud? Do you allow teams to use a built-in issuer? How do you manage decentralized PKI? There are plenty of important questions and discussions ahead of you, but it starts with these five key considerations.

Trust requirements

Determine where public and private certificates are best suited on a case-by-case basis to avoid blurring trust boundaries. Then consider the PKI infrastructure you'll need to support this trust model and how you'll delegate and manage trust across different siloes.

Use cases

Identify use cases across infrastructure, security, network, and application teams. Determine the certificate types, templates, issuance volume, protocols, integrations, self-service and automation capabilities these teams will need to support their specific use cases.

Assurance levels

Consider the physical and digital safeguards around your root and issuing CAs. For testing purposes, it may be acceptable to issue certs from a low-assurance PKI, whereas production certs require higher levels of assurance.

Business continuity

Mergers, acquisitions, divestitures, and overall business growth will change your PKI over time. Ensure that you have the ability to take these different business environments and propagate trust across all of them appropriately.

Required expertise

Determine if you have the right expertise, bandwidth, hardware and security controls in place to implement a secure internal PKI, including an offline air-gapped root CA, and maintain it over a 10-20 year lifespan.

Crypto-agility

Prepare for the eventual migration to new key sizes and algorithms, or in the short term, for a potential CA failure or vulnerability. The ability to revoke and re-issue certificates at massive scale is critical to your success.

KEYFACTOR COMMAND

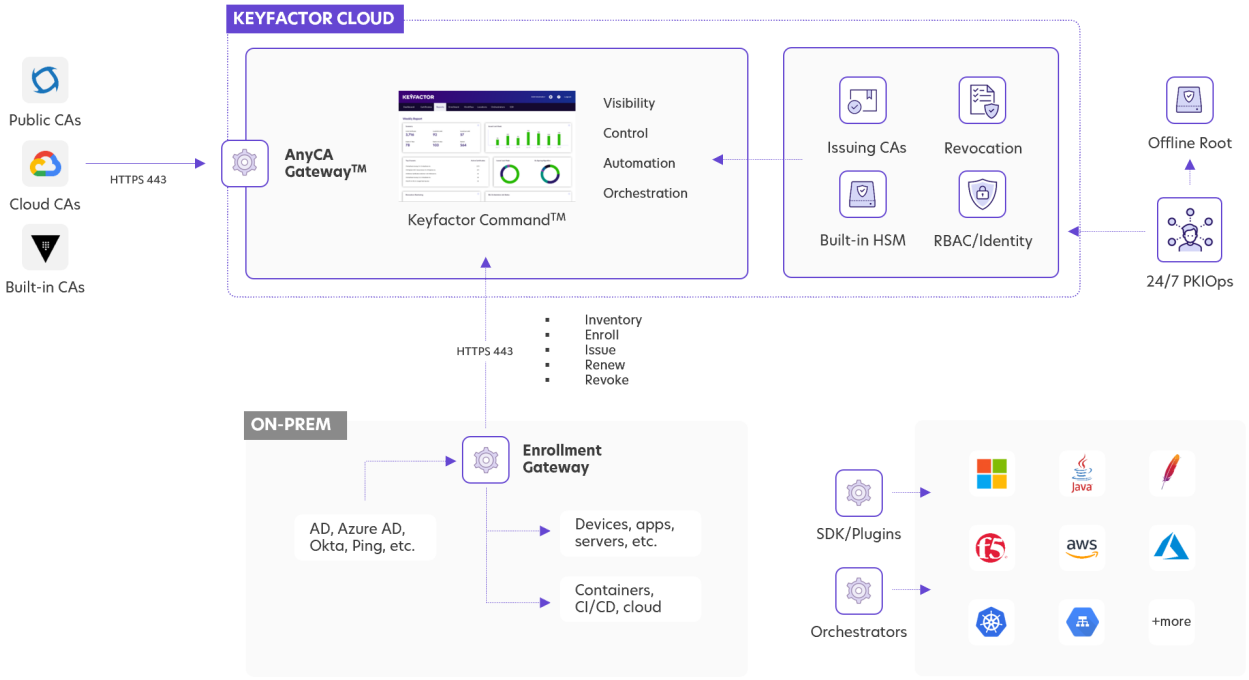
PKI the way you want it

Keyfactor delivers multiple, flexible solutions to help your teams simplify PKI and take control of every machine identity in today's complex hybrid and multi-cloud deployments.

In this section, we'll briefly explore the different Keyfactor Command models that enable you to deploy PKI where and when you need it — with a single platform to manage it all.

Option 1 | PKI as a Service

Organizations with a cloud-first strategy look for solutions that deliver high performance and scalability, without the heavy lifting. By combining an enterprise-grade private PKI, 24/7 managed services, and end-to-end certificate lifecycle automation in a single-tenant cloud solution, Keyfactor Command PKIaaS is the ideal fit for cloud-first teams.

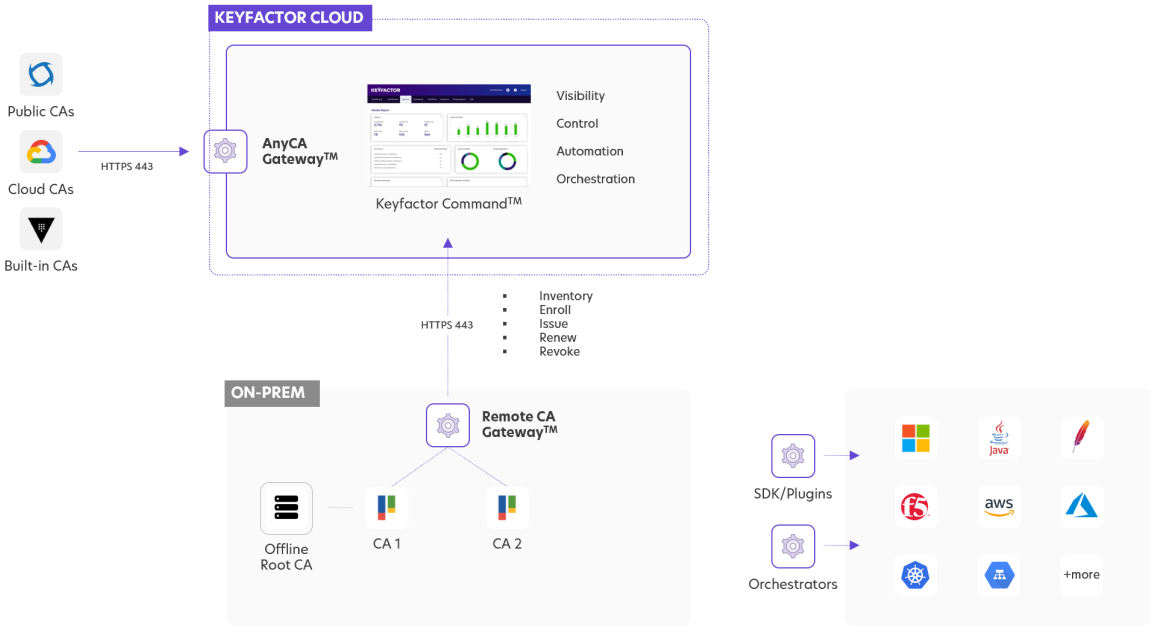


Key benefits:

- Highly secure, highly available PKI infrastructure w/ offline air-gapped root
- 24/7 managed services — freeing up your teams to focus on core competencies
- Full certificate discovery and lifecycle automation to stay ahead of outages
- Integrations with CAs, servers, cloud services, load balancers, DevOps tools, etc.

Option 2 | CLA as a Service

Cloud-first isn't right for every organization. Some teams have strict regulatory or policy mandates that require them to keep their root of trust within their datacenter. Keyfactor Command Certificate Lifecycle Automation as a Service (CLAaaS) enables a hybrid model, where the platform is hosted in the cloud and integrated with private PKI behind the firewall via Remote CA Gateway™.



Key benefits:

- Keep your PKI on-premise — integrate seamlessly via Remote CA Gateway™
- Full certificate discovery and lifecycle automation to stay ahead of outages
- No need to re-configure firewalls or set up a VPN — just a single outbound connection
- Integrations with CAs, servers, cloud services, load balancers, DevOps tools, etc.

Option 3 | On-Premise

Despite our cloud-native roots, we recognize that some customers need to keep both their private PKI and certificate management software on-premise. Keyfactor Command is built on a modular, loosely coupled architecture that makes it an ideal fit in distributed network segments and cloud environments, even when deployed on-premise.

Learn more about our cloud, hybrid and on-prem models. **Compare Deployment Options →**

Conclusion: Zero Trust to Hero

The disruption caused by hybrid and multi-cloud adoption makes zero trust security more important than ever. As a core component to zero trust, PKI and machine identities have become increasingly complex. Without visibility and control over every identity, the risk of compromise is high.

At Keyfactor, we recognize that decentralized PKI is the new reality in hybrid and multi-cloud environments. To achieve zero-trust security, we must authenticate and authorize everything with a unique identity, rather than rely on our boundaries to protect us.

The concept of "moving from zero trust to hero" is driven by the notion that every team across the business relies on machine identities in a zero-trust world, but the burden to manage them falls heavily on the shoulders of PKI, infrastructure, and security teams.

Becoming a PKI champion for your business means putting a stop to costly and disruptive outages, enabling automation wherever possible, and building a model of trust that keeps the business safe, and keeps teams moving fast and without friction.

Put simply, zero-trust is the path to becoming a hero for your business — enabling visibility, control, and automation across your PKI and machine identities is the way to get there.

KEYFACTOR

Keyfactor is the leader in cloud-first PKI as-a-Service and crypto-agility solutions. Our Crypto-Agility Platform empowers security teams to seamlessly orchestrate every key and certificate across the entire enterprise.

For more information, visit www.keyfactor.com or follow us on LinkedIn, Twitter, and Facebook. Built on a foundation of trust and security, Keyfactor is a proud equal opportunity employer, supporter and advocate of growing a trusted, secure, diverse and inclusive workplace.

CONTACT US

- www.keyfactor.com
- +1.216.785.2990