KEYFACTOR

EBOOK

Migrating to Microsoft Azure with a Modern PKI

Microsoft Azure + EJBCA

Table of contents

Advantages of hybrid and multi-cloud

Hybrid and multi-cloud strategies aren't just inevitable, they're already a reality for most organizations.

It's no secret that organizations are embracing cloud services to drive more efficiency, enable automation, and scale their digital footprint to meet new business needs. Like the mainframes before them, data centers are gradually becoming obsolete, replaced by increasingly reliable and scalable cloud-based solutions.

PKI is everywhere, with different teams leveraging different tools to issue certificates — from internal CAs and self-signed certificates to cloud-based PKI and CAs built into DevOps tooling. On average, respondents estimate they have 9 different CA and PKI solutions in use across the organization.[1]

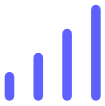
[1] Keyfactor State of Machine Identity Management Report 2023

Challenges of cloud migration

The transition from traditional datacenters to cloud infrastructure is complex and introduces several new challenges for identity and security teams.

Today, applications need to run anywhere and scale quickly. Whether your organization already has a cloud-first strategy or you're migrating legacy applications to Microsoft Azure, public key infrastructure (PKI) is an essential building block to establish digital trust and securely connect workloads and applications at scale.

Everyone from security architects, network engineers, and application and operations teams now rely on PKI and digital certificates to secure machine-to-machine connections across hybrid cloud environments. However, the shift to dynamic workloads and infrastructure as code introduces new challenges for PKI deployments.



More identities

The number of machines and workloads is growing exponentially, bringing many more machine identities into the mix.

Dynamic workloads

The dynamic nature of cloud infrastructure increases the velocity of certificate issuance, deployment, and revocation.

IT complexity

Different teams often deploy multiple CA and PKI technologies to support specialized use cases, increasing complexity, and cost.

PKI and machine identities in Microsoft Azure

As organizations shift to modern cloud infrastructure with Azure, identity takes a central role in protecting machines and applications.

Migrating or building new applications in Microsoft Azure helps teams drive efficiency and value for the business. As a result, the number of workloads, such as virtual machines, containers, and microservices, grows exponentially. In this new environment, security is predicated on ensuring that every connection is authenticated, encrypted, and authorized using unique and trusted identities.

Machine identities, such as X.509 certificates, are everywhere in the cloud. Developers and engineers running in Azure rely on certificates every day to securely develop and run their applications. A holistic approach to cloud migration, including your PKI and certificate services, is therefore critical to ensure your teams can unlock the full advantages of Azure while staying secure.

Azure AD

Humans and machines authenticate to a directory to gain access to resources in Azure via certificate-based authentication (CBA).

Azure DevOps

Container management services and microservices use certificates to implement strong authentication within the Azure ecosystem.

Azure IoT

IoT and edge devices require certificates as critical security components for authentication and code signing.

Microsoft Endpoint Manager

Microsoft Intune-connected machines such as mobile devices and laptops are authenticated and authorized using certificates.

Outdated PKI: A roadblock to cloud success

While migrating applications to the cloud, the reality often sets in that tools and processes once used to secure traditional on-premise environments become much less effective. These legacy tools can even become operational roadblocks to successful cloud migration in many cases. PKI and certificate management are no exception.

Microsoft Active Directory Certificate Services (ADCS), often referred to as Microsoft CA, has long been the de facto choice for PKI in traditional IT environments. It makes sense, it's built into Active Directory (AD), and it works well with Microsoft infrastructure. However, the legacy CA solution is no longer able to live up to the common requirements of today.

In fact, ADCS has become an operational roadblock for many organizations embracing the cloud. For starters, it's not natively supported on Azure. More importantly, though, ADCS cannot integrate with modern tools and platforms, and since only one CA can be installed per server, it quickly becomes an overly complex and costly piece of infrastructure as you scale.

Bottom line: Whether you're just beginning your migration to Azure, or your organization already has a mature, multi-cloud strategy, the demands on PKI infrastructure are increasing. Legacy PKI deployments cannot provide sufficient support.

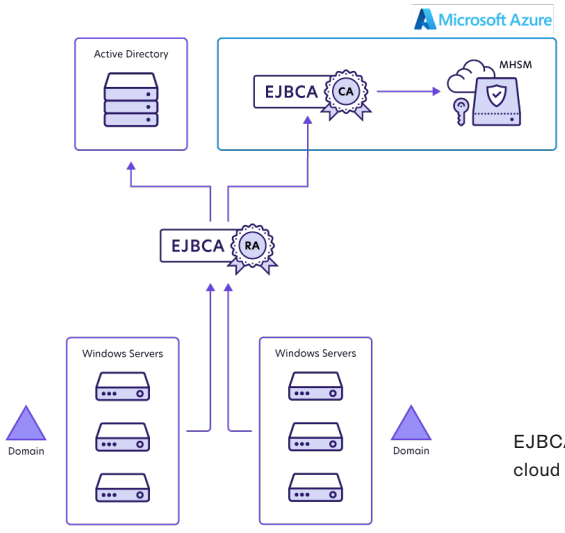
Modernizing PKI with EJBCA for Azure

A complete PKI platform built to support the scale, availability, and agility of hybrid and multi-cloud environments.

It's clear that PKI and machine identities serve as the backbone of digital trust in the cloud, securing mission-critical services and enabling connectivity at massive scale. To realize the benefits of digital transformation and cloud migration, organizations must simplify and modernize their PKI infrastructure.

Keyfactor's EJBCA is a powerful and flexible certificate authority (CA) and PKI management platform to issue and provision certificates at cloud scale. It integrates seamlessly with your Microsoft and Azure infrastructure, making it easy to issue certificates for any use case, whether on-premise or in the cloud. Even better, teams can deploy EJBCA directly from the Azure or AWS cloud marketplace.

Built on open standards and an open source platform, EJBCA brings the maturity and transparency expected from modern security infrastructure. It's designed for the scalability and availability of the cloud, while ensuring robustness and compliance with industry best practices and standards such as Common Crtieria.



EJBCA runs in Azure and integrates into your Azure cloud application environment.

Benefits of EJBCA for Microsoft Azure

Azure integration

EJBCA integrates with Microsoft and Azure-native platforms via auto-enrollment, SCEP, and support for Intune. Authentication and authorization to manage EJBCA is done via certificate authentication or Azure OAuth, and the visibility and monitoring of your PKI can be handled via Azure Insight.

Flexible deployment

To meet the unique business challenges of your organization, you can deploy EJBCA however you need it. It is available on Azure Cloud as a hosted and managed service or as infrastructure as a service (IaaS), as well as hardware or software appliances for specific compliance or other requirements.

Built-in HSM support

Using an HSM brings enterprise-grade security, compliance, and keeps all cryptographic keys secure. EJBCA integrates with all HSMs, including Azure Key Vault and Azure Key Vault Managed HSM, as well as Thales DPoD and most FIPS and CC-certified HSMs on the market.

Infinite scalability

Unlike MS ADCS, EJBCA can host multiple CA and PKI infrastructures in a single installation. Multi-domain and multi-forest deployment is supported, enabling you to consolidate PKI use cases into one platform — and you only pay for what you use.

Multiple use cases

EJBCA supports all certificate use cases and certificate formats in one platform. Thanks to extensive integration and automation support, via standard protocols and APIs, such as EST, SCEP, CMP, ACME, REST and web services, EJBCA is easily extensible.

Certificate lifecycle automation

By adding Keyfactor Command, you can combine highly scalable PKI with full certificate lifecycle automation. Keyfactor Command provides visibility and control of all certificates across your environment, whether issued from EJBCA or any other public, private, or cloud-based CA service.

Choose the migration strategy that works best for you

Find the most secure and efficient way for your organization to modernize PKI in Azure.

The stakes are high when migrating or consolidating enterprise PKI infrastructure. It is imperative that current solutions enabled by existing certificate services continue to work with limited interruption, that the migration project manages existing interfaces and integrations to external systems, and that the robustness of the infrastructure is maintained — or improved — with the migration.

With EJBCA, you can choose the migration strategy that works best for your current situation. Here are three common migration options:

Start fresh

Start a fresh EJBCA deployment for new use cases and migrate existing certificate services down the line.

Migrate

Simplify and consolidate your PKI infrastructure with a full cut-cover to EJBCA and migrating all existing use cases now.

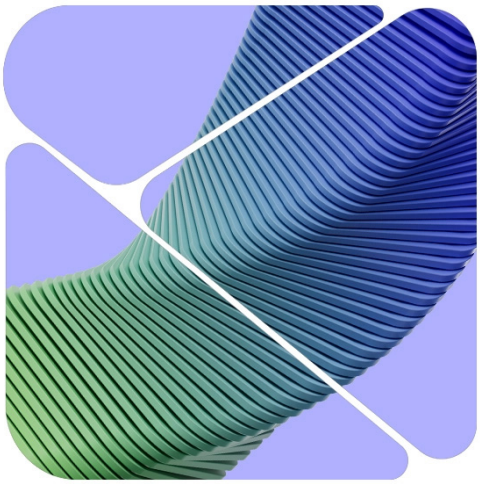
Extend

Keep your Microsoft CA, but implement EJBCA for modern use cases that require more flexibility and scale.

Get started with EJBCA SaaS

If you're ready to modernize your PKI, you can start trying EJBCA SaaS today — and for free.

Try EJBCA on Azure ↗



Explore use cases:

- Achieving End-to-End Certificate Management with Keyfactor and EJBCA
- Migrating from ADCS to EJBCA
- Securing your Microsoft environment with EJBCA
- Integrating EJBCA with Microsoft Intune

KEYFACTOR

Keyfactor brings digital trust to the hyper-connected world with identity-first security for every machine and human. By simplifying PKI, automating certificate lifecycle management, and securing every device, workload, and thing, Keyfactor helps organizations move fast to establish digital trust at scale — and then maintain it. In a zero-trust world, every machine needs an identity and every identity must be managed. For more, visit keyfactor.com or follow @keyfactor.

Contact us

- www.keyfactor.com
- +1 216 785 2990