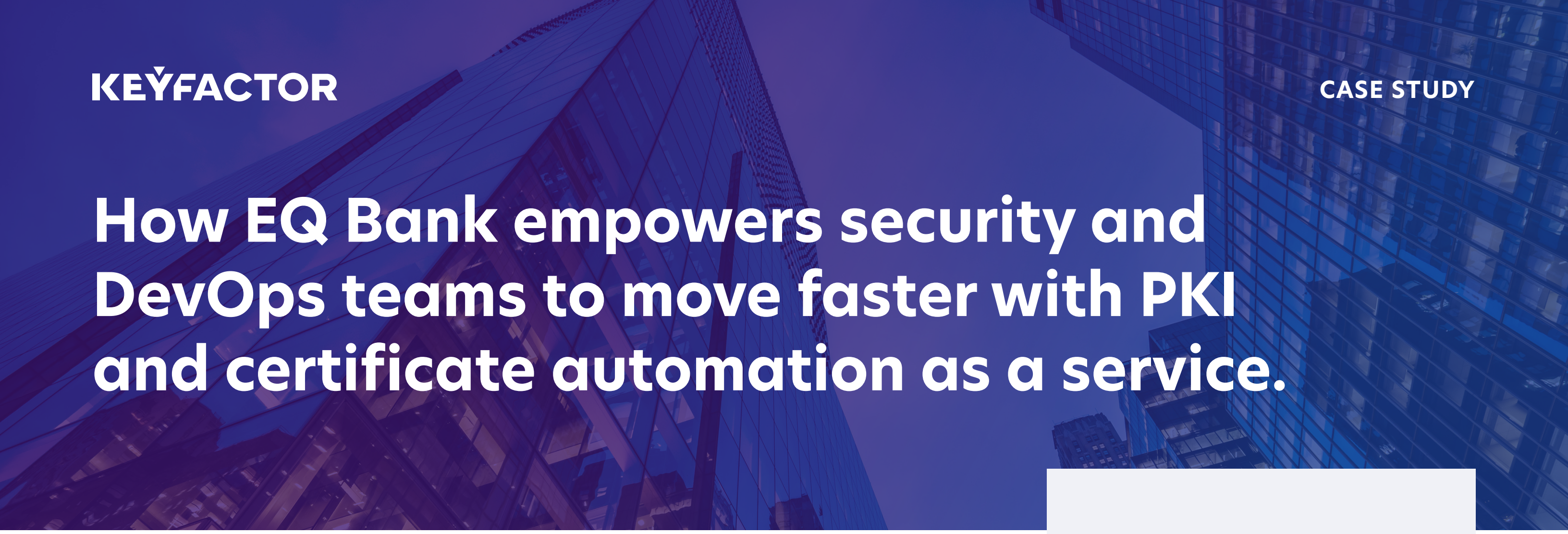
KEYFACTOR

CASE STUDY



How EQ Bank empowers security and DevOps teams to move faster with PKI and certificate automation as a service.

Company Overview

EQ Bank is the digital platform of Equitable Bank, based in Toronto. Founded over 50 years ago, Equitable manages more than $40B in assets and has grown to serve more than a quarter-million Canadians. Launched in 2016 as Canada's first-born digital bank, EQ Bank has fueled rapid growth by challenging traditional banks with a completely branchless experience and smarter banking solutions.

Challenges

As a leader in digital banking and the first bank in Canada to fully host a core banking system in the cloud, security and availability mean everything to EQ. But what if an expired certificate brings down underlying infrastructure or halts productivity for IT teams? That's exactly the challenge David Yu, VP of Security Architecture, needed to solve in the face of rapid digital transformation and business growth.

"Two years ago, we noticed that we were using a lot more certificates for the applications we run within the business and the applications we develop internally," says David Yu. "We had DigiCert for publicly trusted certificates, but we didn't have an internal certificate authority (CA), and there were only ad hoc processes for application owners to request and provision certificates. IT and infrastructure teams would just issue their own certs in development environments and move on."

Ad hoc certificate issuance made it difficult for them to maintain comprehensive visibility and provide reports to internal auditors. Without defined processes, they could not track how other teams across the company were provisioning certificates. As a result, unknown and untracked certificates would expire without their knowledge, causing applications to stop working, and pulling key resources away from their day-to-day tasks to remediate outages.

Historically, the security team was able to manually manage a few certificates in spreadsheets; they also dabbled in Active Directory Certificate Services (ADCS), sometimes referred to as Microsoft CA, to issue certificates for limited internal use cases. However, the IT team has since expanded from 20 to more than 150, a rate of growth that was impossible to support with their limited Microsoft CA deployment and manual certificate management processes.

Equitable Bank

INDUSTRY

Financial Services

LOCATION

Toronto, Canada

PAIN POINTS

- Legacy Active Directory Certificate Services (ADCS) could not support DevOps and Cloud use cases
- Poor visibility led to unexpected outages caused by expired and misconfigured certificates
- Use of self-signed certificates that did not meet security standards

SOLUTION

EQ Bank leverages Keyfactor Command PKI as a Service (PKIaaS) and certificate lifecycle automation to eliminate outages and enable DevOps teams to move faster — without the cost and complexity of running PKI on-premise.

An independent audit and gap analysis from a long-time IT partner confirmed that a certificate management solution was critical to improve their security posture and prevent further outages — a risk amplified by the widespread use of machine identities in their sprawling Azure and DevOps infrastructure. That's where security architecture became involved in the project.

Solution

First and foremost, the infrastructure team needed a solution that would provide the certificate issuance capabilities of a robust internal CA, but without the burden to build and maintain it internally. Yu explained they knew from the start that the effort and expense of setting up a PKI implementation would be far too much of a drain on their teams. To run a CA that meets their information security standards would have been very difficult to achieve in-house.

The solution would also need to provide centralized visibility of public and private certificates for the security team to effectively oversee and manage their IT estate. At the same time, system admins and developers needed an easy way to consume certificates and integrate with automated tools in their DevOps environment, including Azure Key Vault, Kubernetes, and Istio service mesh.

After evaluating several vendors in a proof of concept, the team chose Keyfactor. The key reason for their decision is that Keyfactor was the only vendor that could provide a fully managed and hosted CA alongside the capabilities of a complete certificate lifecycle automation solution in one cloud platform. Keyfactor also offered the most robust set of APIs and integrations that their DevOps team could start using right away.

> "Certificates would expire, but we wouldn't know until systems went down. Since deploying Keyfactor, we've eliminated these incidents entirely."
>
> **David Yu**
>
> VP, Security Architecture
> EQ Bank

RESULTS

- Delivered a robust cloud PKI infrastructure to replace their outdated ADCS deployment
- Reduced certificate-related task workload by 2 full-time equivalents (FTE)
- Ensured that DevOps tools and infrastructure are protected as the business continues to innovate

PRODUCTS

- Keyfactor Command
- Keyfactor PKI as a Service

Business Impact

Shifted PKI to the Cloud

One of EQ's first goals was to get a new internal CA up and running. Within two months, the bank migrated from their on-premise Microsoft CA to the new cloud-hosted PKI. SOC 2 Type II compliance and a comprehensive root signing ceremony made it easy for them to get the compliance and security approvals they needed for the project.

"With Keyfactor now handling key aspects of our PKI infrastructure, we're able to focus on being proactive across our security, software delivery, and infrastructure domains," says Yu.

Keyfactor also helped the EQ team to set up certificate templates, approval workflows, and policies to help standardize issuance and provisioning processes.

Now developers and engineers can avoid self-signed certificates and instead obtain certificates from DigiCert or their Keyfactor-hosted PKI as a Service (PKIaaS)using the self-service capabilities in Keyfactor Command. As a result, the time spent requesting and provisioning security-approved certificates was cut from hours to just minutes.

Gained complete visibility to remediate risks

Keyfactor also provided complete visibility of certificates by first scanning CA databases in DigiCert CertCentral and their existing on-prem ADCS implementation. Then, they worked with the EQ team to enable network discovery of all internal and external certificates. This discovery process provided actionable insights to immediately identify and remediate vulnerabilities, including self-signed certificates.

With a complete inventory, security engineers no longer have to be concerned about unknown, expired, or weak certificates that could threaten the availability and security of applications. They can also respond much faster to requests from internal auditors using scheduled reports on the status and expiration of certificates.

Eliminated outages with automation

Since running with Keyfactor Command, EQ Bank has not experienced a single certificate-related outage. Using a combination of expiration alerting and automated renewal workflows, the team has effectively eliminated outages and significantly reduced the rate of human error.

Yu explained that their IT organization has saved two full-time equivalents (FTE) that would have previously been wasted on manual certificate-related tasks, including troubleshooting issues and remediating frequent outages.

One of the team's first goals was to automate provisioning and renewal workflows for Azure Key Vault using certificates provisioned from their new cloud-hosted PKI. In just a few days, Keyfactor worked with the EQ team to install a Keyfactor Orchestrator and configure the out-of-the-box integration to work with their Azure Key Vault environment. Now whenever a certificate is due to expire, Keyfactor automates the renewal process, and automatically replaces the expiring certificate with a certificate from their new PKI.

Integrated certificate provisioning with DevOps workflows

For cloud-first entities like EQ Bank, trust is everything. Every machine must be authenticated and verified with certificate-based identities to ensure connections are trusted and secure. To achieve this, the DevOps team leverages the comprehensive Keyfactor API and reference tools to integrate with their toolsets and infrastructure.

Already the DevOps team has used Keyfactor to automate issuance and rotation of certificates for HTTPS encryption and ingress points across their Docker containers, Azure Kubernetes Service (AKS), and Istio service mesh deployments.

"We see this as a transformational move. Our DevOps team doesn't need to jump through hoops anymore to get things done. Now they can move faster and rotate certificates more frequently with zero downtime," says Yu.

And this is just the beginning. EQ Bank is working to expand automation and further integrate the Keyfactor Command platform into its DevOps processes. Yu concluded that "Keyfactor worked with us every step of the way from kick-off to production, and they were extremely proactive. Their expertise and support made an immeasurable difference in the success of our teams."

> " We see this as a transformational move. Our DevOps team doesn't need to jump through hoops anymore to get things done. Now they can move much faster and rotate certificates more frequently with zero downtime. "
>
> **David Yu**
>
> VP, Security Architecture
> EQ Bank

ABOUT 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.

CONTACT US

- ▶ www.keyfactor.com
- ▶ +1.216.785.2990