Case study

Streamlining CLM and enabling secure PKI operations for a German multinational corporation

A global sporting goods leader operating within a complex infrastructure environment required a trusted certificate authority to support the migration of its certificate ecosystem while maintaining operational continuity. Following developments affecting its previous certificate authority relationship, the organization began evaluating providers capable of delivering transparent collaboration, reliable support, and a scalable platform for managing digital certificates.

By partnering with Sectigo, the organization successfully migrated its certificate infrastructure while minimizing disruption to internal teams. The transition streamlined certificate lifecycle management, reduced operational overhead, and enabled the organization to explore additional cryptographic use cases such as S/MIME email signing and code signing.

The challenge

The organization operates a mature Public Key Infrastructure (PKI) environment managed by a dedicated PKI and Key Management Services team responsible for maintaining trust across internal systems, applications, and communications.

When developments affecting its existing certificate provider required the company to reassess its certificate strategy, the team began evaluating alternative certificate authorities capable of supporting its operational and security requirements.

Migrating certificates across a large, distributed infrastructure presented several technical and operational challenges. Certificates were deployed across numerous applications and systems, often managed by different service owners responsible for installation, renewal, and lifecycle management. Coordinating the migration therefore required careful planning to avoid service disruption, prevent duplicate renewal work, and maintain operational continuity throughout the transition.

During the transition to a new certificate authority, the PKI team needed to:

- Migrate certificates across multiple systems and environments.
- Coordinate renewal and deployment activities with numerous certificate owners.
- Prevent duplicate work during the migration process.
- Maintain operational continuity throughout the transition.
- Establish trust with a new certificate authority partner.

Why Sectigo

During the transition process, Sectigo emerged as a trusted partner capable of supporting both the technical and operational aspects of the migration. A key differentiator was Sectigo's collaborative approach and willingness to provide direct support throughout the process.

Rather than waiting for the previous certificate contract to expire before initiating migration activities, Sectigo enabled early access to its platform. This allowed the PKI team to begin preparing systems in advance and migrate certificates in a controlled and coordinated manner. This proactive approach helped reduce operational pressure on internal teams and ensured that certificate renewal processes could be completed without unnecessary duplication of work.

Transparency also played an important role in establishing trust between the teams. The business emphasized the importance of working with vendors who provide clear communication and realistic expectations about product capabilities and implementation timelines. Sectigo's willingness to provide honest guidance, both when solutions were available and when certain capabilities were not yet implemented, reinforced confidence in the partnership.

Implementation experience

The migration process was supported by close collaboration between the organization's PKI team and Sectigo's customer and technical teams. Smooth onboarding and consistently responsive support have been key factors in both the organization's initial satisfaction and its continued confidence today.

From the beginning, Sectigo worked directly with the organization to understand its environment and operational requirements. This hands-on engagement helped ensure that migration activities could be planned carefully while minimizing disruption to production systems.

Providing access to the Sectigo platform ahead of contract transition proved particularly valuable. By allowing the organization to begin configuring its certificate environment early, the PKI team was able to stage migration activities and prepare internal systems before certificate renewals were required. This approach helped avoid scenarios in which system owners would need to renew and reinstall certificates multiple times during the migration period.

While Sectigo's product capabilities and technical knowledge in PKI and certificate lifecycle management were central to the decision, the organization also placed significant value on the people behind the platform. The team highlighted responsive support, clear communication, and the strong, trust-based relationship established with Sectigo.

Rather than simply delivering certificates as a commodity service, Sectigo's technical team contributed expertise that helped the organization explore new capabilities and optimize its certificate strategy in a relationship built on trust.

Results and impact

Since completing the migration to Sectigo, the organization has experienced several operational improvements across its certificate management processes.

Reduced operational burden on internal teams

By enabling earlier migration preparation and reducing the need for duplicate certificate renewal tasks, Sectigo helped streamline operational workflows for the PKI team and system owners.

Previously, system owners might have needed to perform certificate installation or renewal operations multiple times as part of the migration process. With Sectigo's platform and migration support, these redundant tasks were largely avoided.

This approach reduced manual effort across the organization while minimizing disruptions to application owners responsible for maintaining services.

Strong technical partnership and support

Throughout onboarding and implementation, the organization consistently experienced responsive and knowledgeable support from the Sectigo team.

This support extended beyond routine service interactions, with Sectigo engineers actively collaborating with the organization to evaluate potential solutions and explore new cryptographic capabilities.

For the PKI team, working with a vendor capable of adding technical insight and value to ongoing projects was a key factor in the success of the relationship.

Enabling new security initiatives

Following the migration, the organization also began exploring additional use cases for digital certificates within its environment.

One example is the evaluation of S/MIME certificates, which enable secure email signing and help verify the authenticity and integrity of internal communications. To support this initiative, Sectigo provided trial certificates that allowed the organization to test and evaluate S/MIME deployment before implementing the solution more broadly.

The organization is also evaluating the future adoption of code signing certificates, which can help ensure the integrity and authenticity of internally developed software and applications.

These initiatives demonstrate how a strong certificate management foundation can support broader cryptographic security strategies across the enterprise.

Support experience

Throughout the engagement, the organization highlighted the consistency and reliability of Sectigo's support teams.

Whether assisting with implementation questions, evaluating potential use cases, or helping troubleshoot technical issues, Sectigo's teams maintained a collaborative approach that emphasized responsiveness and clear communication.

For the organization, working with a vendor that could provide both technical expertise and transparent guidance was essential to maintaining confidence throughout the transition.

As the PKI lead noted:

> "The support has been so great. We felt that Sectigo was always by our side whenever we wanted to implement something new or explore a solution."

Looking ahead

With the migration completed and certificate operations stabilized, the organization is continuing to expand its use of digital certificates to support additional security initiatives. Future projects include the broader deployment of S/MIME for secure email communication and potential adoption of code signing certificates to strengthen software integrity across development environments.

As certificate lifecycles continue to shorten and cryptographic requirements evolve, the organization sees certificate lifecycle management as an increasingly critical capability for maintaining security and operational resilience. By partnering with Sectigo, the company has established a foundation for managing digital trust more efficiently while enabling its security teams to focus on strategic initiatives.

Customer perspective

> Transparency and good work are mandatory whenever we engage with a vendor. Sectigo provides those values. The migration saved us time and avoided a lot of pain for our teams, and the support has always been there whenever we wanted to explore something new.”
>
> **~ PKI and Key Management Lead, Global Enterprise**

About Sectigo

Sectigo is the most innovative provider of certificate lifecycle management (CLM), delivering comprehensive solutions that secure human and machine identities for the world’s largest brands. Sectigo’s automated, cloud-native CLM platform issues and manages digital certificates across all certificate authorities (CAs) to simplify and improve security protocols within the enterprise. Sectigo is one of the largest, longest-standing, and most reputable CAs with more than 700,000 customers and two decades of delivering unparalleled digital trust.