Case study | Darling Ingredients

Streamlining certificate management and reducing outages with Sectigo

Darling Ingredients, a global leader in sustainable food and feed ingredients, relies heavily on digital infrastructure to support its supply chain, manufacturing, and customer-facing systems.

With a lean but globally distributed identity team managing all identity platforms and services across the company, the team inherited ownership of the private Certificate Authority (CA) via Microsoft Active Directory Certificate Services (MS AD CS) to provision certificates for its over 17,000 employees. Meanwhile, public certificates were managed separately by a different team using GoDaddy. After experiencing recurring outages due to expired internal certificates with no native alerting or reporting, the team needed a more reliable, scalable, and centralized solution. Sectigo Certificate Manager (SCM) provided the automation, visibility, and control Darling needed to unify public and private certificate management under one roof.

"SCM saved the day and made life easy by bringing public and private CAs under one console."

Why Sectigo

Darling Ingredients chose SCM as a future-ready alternative with end-to-end automation and centralized control, helping the team reduce risk and streamline operations. After evaluating several vendors, including DigiCert, Sectigo was selected for its unified, flexible and comprehensive approach to solving its challenges. A few standout features helped Darling pull the trigger on Sectigo:

Discovery & visibility

SCM provides Darling with deep certificate discovery across environments and delivers real-time visibility into certificate status, ownership, and expiration, empowering the team to proactively manage risk and prevent outages before they occur.

Single pane of glass

By consolidating public and private certificate management into a single platform, SCM enables Darling to have a unified view across environments. This "single pane of glass" approach improves visibility, reduces operational silos, and enables faster, more coordinated response to certificate-related issues.

Enterprise integrations

Darling's infrastructure spans many technologies including Oracle, MS AD CS, Okta, Microsoft 365 and more. SCM's 50+ integrations with leading technology providers allow Darling to incorporate certificate management into current IT workflows, to streamline operations, enhance security, and ensure regulatory compliance.

Challenges

Reoccuring outages from expired certificates

Darling's internal ERP system relied heavily on private certificates, but MS AD CS' limitations quickly became a source of disruption. When those certificates expired without warning or notification to the team, systems went offline, denying access to applications and triggering urgent remediation efforts.

"We had outage after outage. No notifications, no visibility. Our ERP system would go down, and our team had to scramble to get things back online," said Chris Snell, Darling's identity & access management architect.

With limited visibility and manual processes, outages became a recurring issue. As Darling modernized its infrastructure, the limitations of MS AD CS became increasingly apparent: it lacked the automation, scalability, and visibility needed to support a global, cloud-first environment, which made outages more likely and certificate management more reactive than strategic.

Fragmented certificate management across teams

Darling had a separate team managing public certificates using GoDaddy while the identity team managed private certificates via MS AD CS. This siloed approach created inefficiencies, increased the risk of mismanaged certificates, and made it difficult to scale securely and confidently.

Automation

On the public side, Darling's sister team continues to use Ansible scripts to automate certificate deployment tasks—such as handling CSRs, placing certificates on endpoints, and restarting services. While effective for configuration management, this approach still requires centralized governance, visibility, and lifecycle controls. SCM enables a hybrid approach which allows Darling to maintain operational consistency while benefiting from policy-driven automation, centralized inventory, and compliance-ready controls.

For the private CA, SCM's automated renewal and redeployment of private certificates to servers has been a major win for Darling. Previously, expired certificates caused outages due to lack of reporting in MS AD CS. With SCM, certificates are automatically renewed and pushed to endpoints, eliminating manual intervention and reducing downtime. Where required, keys are rotated per policy to maintain strong cryptographic hygiene.

Optimization

With SCM, Darling gained visibility into certificate usage and cost, prompting a more strategic approach to provisioning. The team now consolidates use cases, assigning a single certificate to multiple services where appropriate, resulting in better resource utilization, reduced spend, and streamlined management.

Implementation and results

Since adopting Sectigo, Darling Ingredients has significantly improved its ability to provision certificates at scale, reduce outages, and respond to internal requests more efficiently.

"It's been a game-changer," said Snell. "Our internal customers get certificates faster, and we avoid the outages that used to disrupt operations. SCM saved the day by bringing private and public CA under one console."

About Sectigo

Sectigo is a leader in certificate lifecycle management (CLM), providing innovative and comprehensive solutions to secure both human and machine identities for some of the world's most prominent brands. Its cloud-native, automated, and universal CLM platform simplifies and enhances enterprise security by issuing and managing digital certificates from all trusted certificate authorities (CAs). With over two decades of experience, Sectigo stands as one of the largest and most established CAs, serving more than 700,000 customers worldwide.

By delivering unparalleled digital trust, Sectigo continues to empower organizations to implement robust securityprotocols with efficiency and confidence.