SECTIGO®

Moving beyond Microsoft AD CS

Why it's time to adopt an enterprise-wide certificate management solution

Table of contents

Chapter 1

The changing enterprise landscape

- The way we work has transformed dramatically over the past decade. Cloud computing, mobile devices, the Internet of Things (IoT), and trends like bring-your-own-device (BYOD) have changed how enterprises operate. This shift has enabled greater flexibility and productivity through technology. However, it has also brought new challenges in managing and securing an increasingly heterogeneous IT environment.

- Gone are the days when companies could rely on a homogeneous Microsoft technology stack. While Active Directory and Windows clients still play a central role, other operating systems, devices, and applications have become commonplace. Smartphones and tablets are now ubiquitous, with many organizations embracing iOS and Android to boost employee productivity. The average enterprise uses over 1000 cloud services from multiple providers according to the Netskope 2019 Cloud Report. Linux and open-source software now run many back-end systems and web servers.

- This diversification strains companies that depend on Microsoft's Active Directory Certificate Services (AD CS) as their sole certificate authority (CA). While AD CS works seamlessly within the Microsoft ecosystem, it lacks integrations with third-party technologies. Manual workarounds may suffice temporarily, but eventually take their toll on IT teams. The costs and risks of relying exclusively on AD CS only increase as environments become more sophisticated.

- At the same time, digital certificates have become more vital than ever before to secure today's enterprises. From Wi-Fi authentication to VPN access, from DevOps to IoT devices, certificates enable security across an array of devices, operating systems, and applications. They encrypt and decrypt sensitive corporate data, verify identities and ensure trust.

To keep pace with these major changes, today’s organizations need to rethink their certificate management strategies.

Chapter 2

The challenges of Microsoft AD CS

Microsoft Active Directory Certificate Services (AD CS) provides a free, built-in option for enterprises to issue and manage PKI certificates. At first glance, it seems like an easy choice. But relying solely on AD CS comes with some significant downsides that quickly emerge.

Manual management overhead

With AD CS, all certificate lifecycle processes - issuing, renewing, revoking - must be handled manually. Microsoft provides auto-enrollment for some functions, but it is limited to Group Policy-joined Windows devices. Renewing and managing certificates on other platforms still requires manual work.

This administrative overhead only increases in diverse environments with many device types and operating systems. IT staff spend valuable time tracking expiration dates, coordinating renewals, and ensuring policies are kept up to date across servers, clients, mobile devices, and more.

Limited integrations

A key weakness of AD CS is its lack of integration beyond Microsoft's ecosystem. AD CS relies on Group Policy Objects (GPOs) to deploy certificates to Windows devices. But GPOs do not work for non-Windows clients. This creates headaches managing and securing certificates on other platforms.

While workarounds like AD CS connectors for mobile device management (MDM) exist, they add complexity. At best, these stopgaps only partially automate certificate management. Extensive manual efforts are still needed for the many use cases AD CS cannot handle natively.

Chapter 2

The challenges of Microsoft AD CS

On-premises restrictions

AD CS is an on-premises solution that cannot be deployed to the cloud. This limits organizational agility, as IT teams cannot take advantage of cloud elasticity and benefits. Regular maintenance like backups and restores remains a largely manual task. The on premises factor also hampers efforts to support remote workers. During the pandemic, lack of AD CS access outside corporate networks created availability issues that disrupted operations.

Security and compliance risks

While not intrinsically insecure, AD CS is prone to misconfiguration given its complexity. Enterprises using it must follow strict security practices to minimize risk. If not, compromised, or forged certificates could be issued, enabling serious attacks. Limited visibility into the full certificate inventory also poses compliance problems. Without full lifecycle tracking, expired or non-compliant certificates may go undetected. This visibility gap makes demonstrating compliance far more difficult.

Transitioning away from AD CS is daunting, given dependencies built up over time. But augmenting it with a dedicated certificate lifecycle management solution can offset these weaknesses while leveraging existing PKI investments.

Chapter 3

The risks of partial visibility

In many organizations, public-facing and internal certificate management are divided between separate teams. Public certificates secure the company's external domains and sites, while private certificates manage internal security and authentication.

This divide between external and internal PKI breeds visibility and communication issues. Public certificate management often falls under NetOps or Security teams.
Private certificate management with AD CS is handled by Windows Server admins.
With limited insight into each other's processes, critical information falls through the cracks. Certificates may be renewed inconsistently or allowed to expire without notification.
Knowledge transfer is hampered when team members leave.

Manual tracking methods

To track certificates manually, IT admins use makeshift methods like spreadsheets or SharePoint lists. While better than nothing, these approaches have significant limitations:

- **No central repository** - information siloed in fragmented tracking documents.
- **Labor-intensive** to compile and update.
- Easy to introduce errors that undermine **trustworthiness**.
- Difficult to surface important details like **expiration alerts.**

Without automation, the admin must manually review hundreds or thousands of certificates regularly. Important dates and renewals are easy to miss. Outages occur if actively used certificates unexpectedly expire.

Renewal risks

Microsoft AD CS lacks built-in monitoring and expiration notifications. The admin must set up their own manual monitoring to watch for certificates nearing expiration. Renewals must also be triggered and approved manually.
For particularly overworked admins, renewals inevitably fall through the cracks.
Short-lived certificates like those used in browsers are especially prone to expiring prematurely.
Auditors and regulators require strong reporting and logs to demonstrate certificate program compliance. But AD CS provides minimal built-in reporting.
Piecing together audit trails from fragmented manual records becomes tedious.
This makes compliance far more difficult and riskier.

The solution is centralized visibility and lifecycle automation for both public and private certificate management.

Chapter 3

The risks of partial visibility

The solution: centralized visibility and lifecycle automation

To address all these risks, enterprises need a unified view into all their certificates - public and private, Microsoft-issued and from other CAs.
A centralized certificate management platform provides total visibility by discovering certificates across the entire network. This gives administrators a single pane of glass to track and manage every certificate from one system.
Automating the certificate lifecycle is equally important. With automation, mundane tasks like issuance, renewal, and expiration alerts happen in the background without admin intervention. This lifts the manual burden while ensuring certificates remain valid and compliant.

Key aspects of automation include:

- Auto-discovery to detect all certificates from any source.
- Bulk renewals and provisions based on policies.
- Notifications when certificates near expiration.
- Consolidated logs and reports for auditing.

With complete visibility and automation, organizations can:

- Eliminate blind spots and communication gaps.
- Proactively renew certificates to avoid outages.
- Maintain compliance with strong audit trails.
- Reduce manual labor so admins focus on higher value work.

This prevents certificates from becoming a ticking time bomb and removes the background worry of unexpected expirations. Just as importantly, it restores confidence that the organization meets security and compliance requirements.
By filling the gaps in certificate visibility and lifecycle management, companies can securely embrace heterogeneous environments without added risk or costly overhead.

Chapter 4

Automated certificate lifecycle management

Manual certificate management quickly becomes unscalable as organizations grow. At some point, the overhead of tracking renewals, monitoring expiration dates, and fixing slip-ups becomes unsustainable.

Automating certificate lifecycle management solves this problem. Often abbreviated as CLM, certificate lifecycle management streamlines the end-to-end processes of:

- Provisioning new certificates.
- Keeping certificates renewed and valid.
- Revoking certificates when required.
- Providing visibility into certificate inventories.
- Logging activity for audits.

With CLM software, these tasks happen automatically according to predefined policies. IT security teams can ensure the certificate program meets business needs, while the software handles the day-to-day workload.

Key benefits of CLM

Centralized visibility

A CLM system acts as a hub for all certificate activity, providing total visibility into inventories. Certificate repositories are consolidated instead of siloed in different tracking documents or tools.
This unified view enables administrators to easily monitor and manage all certificates from one dashboard. They gain insights needed to optimize renewals, identify risks, and demonstrate compliance.

Automated workflows

Mundane management tasks like bulk certificate renewal happen automatically in the background. IT staff simply define desired policies and criteria like validity periods. The CLM software does the heavy lifting.
Notifications and alerts also create proactive awareness of issues like expiring certificates. Problems can be prevented instead of requiring reactive fire drills.

Reduced workload

By automating tedious, repetitive tasks, CLM significantly reduces the manual workload associated with certificate management. Time once spent tracking spreadsheets can be redirected to core projects that move the business forward.

Standardized policies

CLM allows organizations to define consistent global policies around their certificate lifecycles. This improves security posture while reducing reliance on individual administrators' tribal knowledge.

Lower costs

For most enterprises, the accumulated labor costs and risks of manual certificate tracking exceed the cost of CLM software. Automation pays for itself by enabling staff to focus on higher value initiatives.

Chapter 4

Automated certificate lifecycle management

How CLM augments AD CS

For organizations relying on Active Directory Certificate Services, CLM can fill critical gaps in visibility and lifecycle automation. A unified platform manages certificates across the entire environment, not just the Microsoft ecosystem.
While AD CS works smoothly within the Microsoft ecosystem, it lacks key capabilities needed for diverse platforms and certificate sources. CLM complements AD CS by tackling these limitations:

Achieve Unified Visibility: Automated discovery of all certificates from any CA, including AD CS, provides a unified view of your organization's entire certificate inventory. This eliminates blind spots and gives admins the visibility needed to manage certificates beyond the Microsoft ecosystem.

Reduce Manual Workload: With policy-based automation for provisioning, renewal and revocation, CLM handles the ongoing workload across diverse platforms. This reduces the manual burden on IT teams while ensuring certificates remain valid and compliant.

Enable Scalable Automation: Support for protocols like ACME, SCEP and EST enables scalable, automated issuance and renewal for certificates from third-party CAs. Admins can offload repetitive tasks to reduce labor.

Streamline Heterogeneous Environments: CLM's out-of-the-box integrations with commonly used apps like F5, AWS and more streamlines certificate management across heterogeneous environments. Workarounds are avoided.

Simplify Compliance Reporting: Centralized reporting and dashboards provide operational insights and audit readiness that AD CS lacks. This simplifies compliance and audits for internal and external requirements.

Improve User Experience: Secure and convenient access to CLM console via AD credentials improves user experience and reduces credential sprawl.

Support Appropriate Delegation: Precise access controls through organizational units and admin roles enables appropriate delegation aligned to team responsibilities.

Extend Automation: CLM's REST APIs allow building custom integrations and workflows to extend automation capabilities. Certificate management can enhance complementary systems.

With CLM augmenting AD CS in these key areas, organizations finally get complete visibility, automation and control to simplify certificate management in today's modern diverse environments.

Chapter 5

Introducing Sectigo Certificate Manager

Sectigo Certificate Manager provides full-lifecycle automation for digital certificate management. It acts as a universal hub to streamline certificate operations, boost compliance, and reduce security risks.

As an enterprise-grade certificate management platform, Certificate Manager offers:

- Discovery of all certificates from any CA or device.
- Centralized visibility across public and private certificates.
- Policy-based certificate lifecycle automation.
- Near real-time monitoring and notifications.
- Consolidated reporting and logs.

This enables overburdened IT teams to offload the manual minutiae of tracking expirations, renewals, and inventory to an automated system.

Comprehensive features:

Intuitive dashboard
The centralized dashboard offers one-click access to inventory visibility, lifecycle status, alerts, reports, and more. Admins gain instant insights into their entire certificate ecosystem.

Discovery and inventory
Discover all certificates across public and private CAs through automated network scans. Inventory and track every certificate from one unified console.

Lifecycle automation
Create policy-driven rules to automatically issue, renew, and revoke certificates. Bulk actions scale to handle large volumes with ease.

Monitoring and notifications
Ongoing monitoring proactively alerts teams to expiring and misconfigured certificates before problems occur.

Consolidated audit trails
Detailed visibility into certificate histories provides air-tight audit trails for internal and external reporting.

REST APIs
Integration with complementary systems through REST APIs, ACME, SCEP, and EST enhances automation capabilities.

Chapter 5

Introducing Sectigo Certificate Manager

Using Sectigo to augment AD CS

Sectigo Certificate Manager complements Active Directory Certificate Services in two key ways:

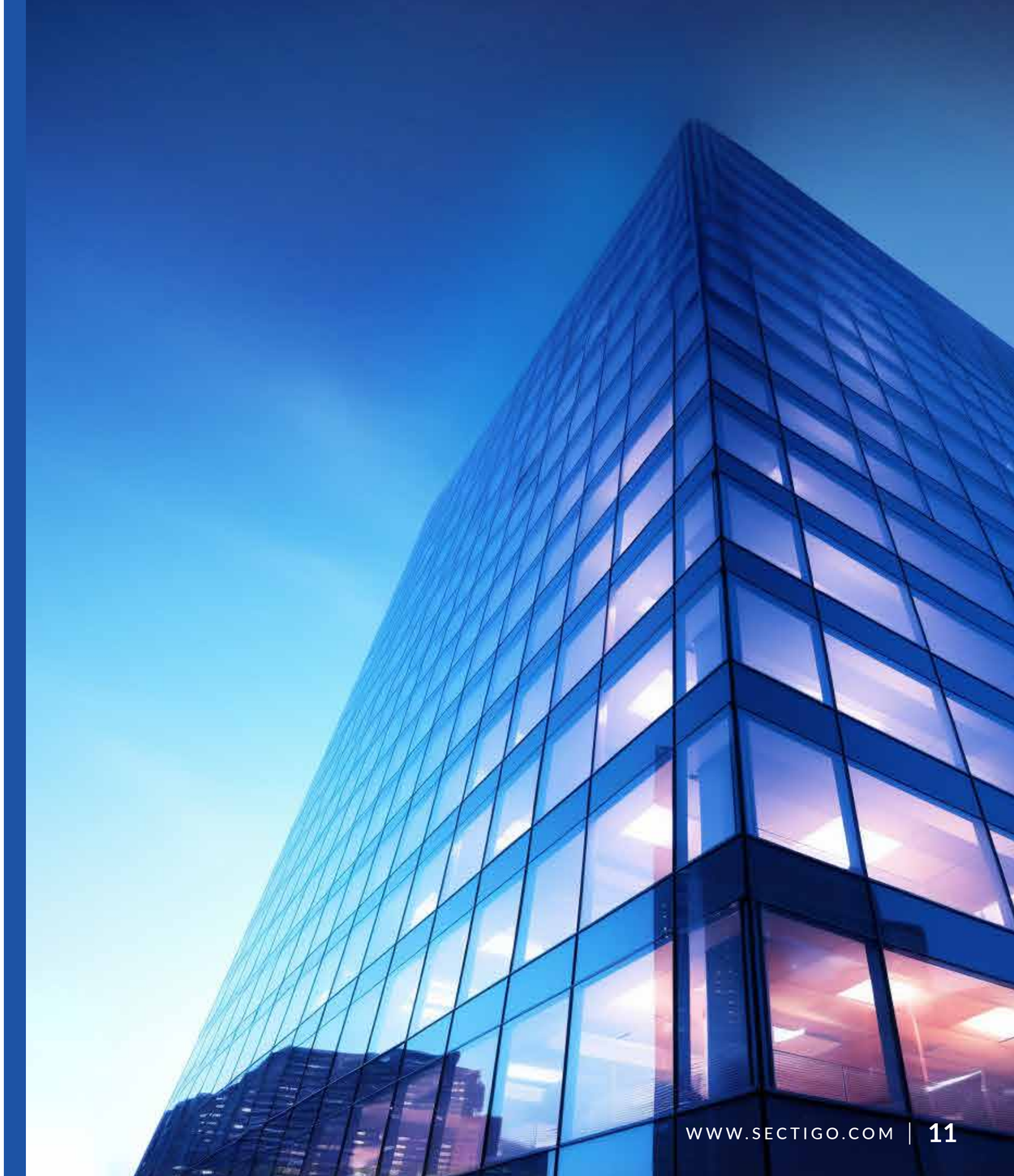
1. Enhance AD CS with Sectigo to manage non-Microsoft certificates
2. Gradually shift to a cloud-based Sectigo CA for full lifecycle automation.

The first path retains AD CS for Microsoft ecosystem needs while using Certificate Manager to fill gaps like mobile devices.
The second path sees enterprises migrate fully over time to Certificate Manager for all certificate management. This enables a scalable, cloud-based CA with 100% visibility and automation.

Either way, Certificate Manager cost-effectively augments AD CS as organizations embracing heterogeneous environments.

Conclusion:

With Sectigo Certificate Manager, resource-strapped IT teams finally get relief from the endless manual tasks associated with tracking and renewing digital certificates. They gain an automated, efficient solution purpose-built to enhance and ultimately replace AD CS.



Chapter 6

Leveraging Sectigo Certificate Manager

Once implemented, Sectigo Certificate Manager delivers value across the certificate lifecycle through comprehensive capabilities:

Automated discovery and inventory

The first step is gaining full visibility through automated certificate discovery. Certificate Manager scans the network to create a centralized inventory of all certificates from any CA or device.
This repository eliminates blind spots by consolidating disparate tracking documents. With all certificates cataloged in one system, organizations gain a single source of truth for reporting and management.

Streamlined cloud-based deployment

Certificate Manager seamlessly integrates with your existing infrastructure through an exclusive cloud-based deployment, ensuring easy scalability and efficient management. The core functionality remains unchanged - all certificates are discovered and visible through the centralized management console. This cloud-native solution is perfectly designed to elevate certificate management and augment Microsoft AD CS with:

- Elimination of on-premise server costs and maintenance
- Faster feature enablement aligned to customer needs
- High scalability to handle growth in certificates
- Robust security provided by a certificate authority

Lifecycle automation

Once certificates are discovered, lifecycle automation kicks in to streamline ongoing management. The platform provisions new certificates and renews existing ones based on policy-defined rules.
Administrators simply set the validity period, crypto algorithms, etc. and automation handles the rest. Misconfigured or expiring certificates are revoked before problems emerge.

Chapter 6

Leveraging Sectigo Certificate Manager

Ongoing monitoring and notifications

Since certificates have a defined lifespan, tracking expiration dates is critical. Certificate Manager provides near real-time monitoring to identify certificates approaching expiration.
Email, SMS or platform alerts notify administrators to take action. Unexpected outages due to missed renewals become a thing of the past.

Consolidated reporting and audit trails

The platform's consolidated dashboard delivers reports needed for both operational and compliance requirements. Detailed certificate histories provide comprehensive audit trails.

REST APIs and integrations

APIs enable integration with existing infrastructure like identity management and ITSM solutions. By providing out-of-the-box integrations with leading technologies across key categories such as cloud platforms, web servers, DevOps tools, load balancers and other networking gear, Sectigo Certificate Manager enriches certificate management across your existing infrastructure.

A future-ready solution

With Sectigo Certificate Manager, enterprises finally get a truly holistic and automated approach to certificate lifecycle management. It fulfills the promise that overburdened AD CS could never deliver across today's heterogeneous environments.

Chapter 7

Replacing expiring Microsoft infrastructure

As AD CS infrastructure ages, it reaches end-of-life and requires upgrades to continue being supported.
These obligatory upgrades come with substantial costs and effort. Significant planning goes into upgrading AD CS to a compatible version. Downtime is inevitable during a cutover.

And Microsoft's consulting services to facilitate the complex transition don't come cheap.
Rather than sink more resources into perpetuating old systems, forward-thinking enterprises are choosing to migrate instead. They are adopting flexible, cloud-based PKI solutions that leave legacy limitations behind.

Why migrate to the cloud?

For companies with expiring AD CS systems, migrating to a modern cloud PKI delivers multiple advantages:

- Avoid large upgrade costs by retiring legacy infrastructure.
- Improve business agility through cloud scalability.
- Enable remote management without on-prem dependencies.
- Reduce overheads with automated management.
- Eliminate reliance on scarce PKI expertise.

With the right solution like Sectigo Certificate Manager, replacing AD CS can happen gradually without disrupting existing services. Cloud migration eliminates the looming expense of upgrading antiquated systems just to maintain the status quo.

Modernizing PKI in the cloud

As part of a cloud-first strategy, Sectigo Certificate Manager provides:

- Cloud-based issuance, lifecycle automation, and management.
- Discovery of all existing AD CS certificates.
- Options to re-issue or renew legacy certificates.
- Consistent workflows before and after migration.
- Familiar CA hierarchy and PKI structure.

This enables a cloud transition focused on business continuity, not disruption. Organizations can retire AD CS securely and adopt agile, automated PKI built for the future.

Conclusion:
For enterprises with expiring Microsoft PKI infrastructure, migrating to a cloud-based solution cost-effectively replaces legacy limitations with modern scalability and automation. Sectigo Certificate Manager precisely delivers this, enabling the secure retirement of AD CS.

Chapter 8

Integrating beyond Microsoft

A persistent pain point with Microsoft Active Directory Certificate Services (AD CS) is its limited ability to integrate with non-Microsoft systems.

AD CS relies heavily on Group Policy Objects (GPOs) to manage certificates within its ecosystem. But GPOs only work for Microsoft clients joined to Active Directory.
This closed architecture creates headaches as organizations embrace diverse technologies. Integrating AD CS with third-party mobile devices, operating systems, and infrastructure becomes a manual, ad-hoc process.

The need for openness

In today's heterogeneous environments, certificate management solutions must interoperate flexibly across platforms:

- Mobile devices like iOS and Android.
- Directory services beyond Active Directory.
- Multi-cloud configurations spanning AWS, Azure, GCP.
- IoT systems not joined to AD.
- Linux, Apache, Nginx and other DevOps tools.

Organizations need "out-of-the-box" integrations that don't require costly custom development and maintenance. Certificate management should unite disparate systems, not create new silos.

Take an agnostic approach

Sectigo Certificate Manager was designed for multi-technology organizations. It provides turnkey integrations with:

- Major mobile device management (MDM) solutions.
- Leading identity access management (IAM) providers.
- Top cloud computing platforms.
- CI/CD pipelines and DevOps tools.
- And more...

This open architecture offers frictionless certificate management across heterogeneous environments. Enterprises no longer struggle integrating AD CS with other business-critical technologies.
With Sectigo, PKI becomes a unifying layer of trust across diverse systems. Organizations can securely scale without being locked into Microsoft's walled garden.

Conclusion:
For enterprises with expiring Microsoft PKI infrastructure, migrating to a cloud-based solution cost-effectively replaces legacy limitations with modern scalability and automation. Sectigo Certificate Manager precisely delivers this, enabling the secure retirement of AD CS.

Chapter 9

Eliminating manual tracking burdens

One of the toughest aspects of relying on Microsoft Active Directory Certificate Services (AD CS) is the extensive manual effort required. AD CS provides no user dashboard, notifications, or consolidated reporting.

Administrators are left to track everything related to certificates in fragmented spreadsheets and tribal knowledge. This clumsy manual tracking comes with major productivity, compliance, and security drawbacks.

Spreadsheet scramble

Without lifecycle automation, administrators manually track certificate expirations in spreadsheets. This constant log updating is tedious and error-prone:

- No central data source means piecing together limited insights from different documents.
- Information gaps are inevitable as certificates are issued, renewed, and revoked.
- Important dates and renewals are easily missed, leading to outages.
- Version control failures erase institutional knowledge as admins turnover.

Chaotic renewal process

Spreadsheet-based tracking forces chaotic manual processes around renewals:

- Each certificate must be individually identified and renewed.
- Different validation steps apply based on certificate type.
- Approvals are done through email, chat, or ticketing workflows.
- Procurement and billing are managed separately.

These manual efforts don't scale as certificate volumes grow across diverse platforms. Days are wasted annually on repetitive administrative work.

Chapter 9

Eliminating manual tracking burdens

Weak compliance posture

Auditors demand strong evidence like centralized reports and activity logs. Manual records are insufficient for modern standards.

- Tedious certificate lookups fail to provide rapid audit response.
- Certificate histories are scattered across multiple documents.
- It's nearly impossible to demonstrate comprehensive compliance.

Solving the tracking problem

Purpose-built certificate lifecycle automation eliminates these manual burdens. Certificate Manager provides:

- A unified dashboard with insights into the full inventory
- Policy-based workflows that issue and renew certificates at scale
- Proactive alerts to prevent expiration surprises
- Consolidated audit trails for instant compliance reporting

By automating cumbersome tracking tasks, Sectigo Certificate Manager restores productivity while reducing business risk.

Chapter 10

The true cost of Microsoft AD CS

At first glance, Microsoft Active Directory Certificate Services (AD CS) appears "free" since it's included with Windows Server. But this perception masks the substantial hidden costs of relying on AD CS.

Manual management overhead

The sheer amount of manual workload required to track certificates on spreadsheets comes with a real cost.

- Administrators spend countless hours on repetitive tasks like inventory tracking, expiration monitoring, and manual renewals.
- Highly paid IT staff waste time on administrative minutiae instead of strategic initiatives.
- Additional headcount may be needed to handle the manual burden.

Business disruption

According to researchers, 50% or more of outages are caused by expired certificates. The business costs quickly compound when critical systems go down unexpectedly.

- Loss of customer transactions and access during downtime.
- IT teams scrambling to fix certificate crises in reactionary mode.
- Delayed or canceled projects as resources get diverted to outages.

Compliance risks

Without proper automation and audit trails, compliance gaps inevitably occur.

- Audits and regulations require strong reporting and lifecycle visibility. Manual records are insufficient.
- Penalties, fines and remediation for non-compliance are expensive.
- Certificate authority compromise can severely damage an organization's reputation.

A better approach

When all factors are considered, the true cost of perpetuating manual tracking with AD CS far outweighs investing in automation.
Sectigo Certificate Manager purpose-built certificate lifecycle management solution delivers an attractive ROI by:

- Reducing manual workload to improve productivity
- Preventing outages that threaten business continuity
- Enabling compliant operations that avoid penalties

Conclusion:

Relying solely on Microsoft AD CS for certificate management may seem "free" but brings substantial hidden costs from compliance risks, manual inefficiencies, and too many outages.

Chapter 11

Augmenting Microsoft with Sectigo

For most enterprises, a "rip and replace" approach to replacing Microsoft AD CS would be too disruptive. A better path forward is augmenting AD CS with solutions that fill functional gaps.

Sectigo Certificate Manager integrates seamlessly with AD CS in two key ways:

1. Manage ADCS-issued certificates

2. Fill automation, visibility and integration gaps

Manage ADCS-issued certificates

For organizations that want to retain their investment in ADCS-issued certificates, Certificate Manager can manage and monitor these alongside certificates from other sources.

Certificate Manager discovers and imports ADCS certificates into its consolidated inventory. Ongoing lifecycle automation, monitoring, reporting and more can then be applied to these certificates.

This allows you to keep issuing from ADCS when needed while leveraging Certificate Manager's capabilities for centralized visibility, compliance and reduced manual workload.

Fill critical gaps

For broader heterogeneous environments, Certificate Manager fills gaps in AD CS's capabilities:

- Automates lifecycles for diverse systems beyond Microsoft.
- Enables integrations with third-party solutions.
- Provides proactive monitoring and alerts.
- Generates consolidated reports for improved compliance.

Gradual deployment

Certificate Manager can be deployed incrementally to avoid disrupting existing services:

1. Implement Certificate Manager in audit mode to discover existing certificates.
2. Microsoft use cases first.
3. Shift workloads over time until AD CS is no longer needed.

This gradual path prevents "landmine" certificates during the transition.

Get the best of both

The combined capabilities deliver the best of both worlds:

- AD CS handles core Windows PKI needs
- Certificate Manager strengthens everything else

With critical gaps addressed, organizations can confidently expand across diverse platforms knowing certificates won't hold them back.

Conclusion

Transitioning fully from AD CS overnight is risky, but augmenting it with Certificate Manager fills key gaps - no rip and replace required. This empowers organizations to complement AD CS investments while mastering certificate management for heterogeneous environments.

Chapter 12

The path forward

This eBook has explored the mounting challenges enterprises face relying solely on Microsoft Active Directory Certificate Services (AD CS) in today's hybrid environments.

While AD CS works smoothly within the Microsoft ecosystem, it was never designed for the heterogeneous infrastructure realities most organizations now operate within.

As we've seen across the various chapters, core weaknesses in lifecycle automation, visibility, compliance, and integration inevitably manifest as environments diversify. The total cost of ownership is higher than many realize when factoring in the manual inefficiencies, non-compliance risks, and too many certificate-related outages.

Rather than perpetuate these limitations through disruptive rip-and-replace, a smarter path forward is augmenting AD CS with solutions purpose-built to fill the gaps

Sectigo Certificate Manager integrates seamlessly with AD CS to provide:

- Unified visibility across public CAs, AD CS, and third-party issuing authorities
- Lifecycle automation for diverse platforms beyond Microsoft's capabilities
- Proactive monitoring and expiration alerts to prevent outages
- Consolidated audit trails for improved compliance
- Support for multi-cloud and on-premises architectures

This allows enterprises to keep AD CS for its strengths in the Microsoft ecosystem while relying on Sectigo for everything else. Organizations can complement rather than replace their Microsoft investments.

For companies with expiring AD CS infrastructure, migrating fully to Sectigo's cloud-based CA provides a cost-effective path to retire legacy systems while retaining PKI continuity. Either path - augmenting or replacing AD CS – delivers the automation, visibility, and integration required to master certificate management across heterogeneous environments.

Chapter 12

The path forward

By augmenting AD CS with an automated, cloud-based certificate lifecycle management solution like Sectigo Certificate Manager, enterprises can securely embrace the future without being handcuffed to the limitations of the past.

The benefits for resource-strapped IT teams are real and substantial:

- Eliminate certificate blind spots with unified visibility
- Reduce manual workload through policy-based automation
- Minimize business disruption from unexpected expirations
- Maintain compliance more confidently with detailed audit trails
- Free staff to focus on more strategic initiatives
- Scale seamlessly as needs grow across heterogeneous infrastructure

As this eBook has shown, Sectigo Certificate Manager integrates cleanly with AD CS to provide comprehensive lifecycle automation. The platform serves as a force multiplier so IT administrators can finally manage certificates efficiently at scale.

Next steps

We encourage you to see Certificate Manager's capabilities live through a personalized demo. Learn how Sectigo can help you achieve your organization's PKI management goals.
Our PKI experts can map out a transition plan tailored to your unique environment and requirements. We enable a phased shift from AD CS that maximizes existing investments while avoiding business disruption.

To learn more or request a demo, visit www.sectigo.com or contact us at sales@sectigo.com. We look forward to showing you how Sectigo Certificate Manager can help your organization modernize certificate management.

Conclusion

A Summary of Key Takeaways

This eBook has covered the mounting challenges companies face relying solely on Microsoft's Active Directory Certificate Services (AD CS) for PKI management.

With hybrid IT environments now the norm, AD CS's lack of visibility and automation beyond the Microsoft ecosystem has become a glaring weakness. Undetected expirations, security risks, and compliance gaps are the price organizations pay for incomplete certificate lifecycle management.

We discussed how certificate management silos frequently exist between NetOps and infrastructure teams. With no centralized visibility, certificates fall through the cracks and outages occur. Laying strong audit trails also becomes far more difficult.

These problems simply compound as companies scale. More certificates get issued. More diverse platforms need support. The manual workload balloons to unsustainable levels.

The solution is unified visibility into all certificates along with policy-based automation across the entire lifecycle. This is exactly what purpose-built certificate lifecycle management (CLM) platforms like Sectigo Certificate Manager deliver.

By seamlessly integrating with AD CS to fill functional gaps, Certificate Manager provides:

- Complete inventory visibility across private and public CAs
- Bulk certificate provisioning and renewals
- Proactive monitoring and expiration alerts
- Consolidated reporting for audits and operations

With these capabilities augmenting Microsoft AD CS, enterprises can confidently embrace hybrid ecosystems. IT teams regain control and confidence in their certificate management programs.

To explore how Certificate Manager can help your organization optimize and automate PKI management, visit www.sectigo.com or contact sales@sectigo.com.

About SECTIGO®

Sectigo is a leading provider of automated Certificate Lifecycle Management (CLM) solutions and digital certificates - trusted by the world's largest brands. Its cloud-based universal CLM platform issues and manages the lifecycles of digital certificates issued by Sectigo and other Certificate Authorities (CAs) to secure every human and machine identity across the enterprise. With over 20 years establishing digital trust, Sectigo is one of the longest-standing and largest CAs with more than 700,000 customers. For more information, visit www.sectigo.com.