SECTIGO®

Choosing a reputable
Certificate Authority

Table of Contents

Introduction

Recent events have shaken the digital trust ecosystem. 2024 saw a major public Certificate Authority (CA) distrusted by browsers serving many large enterprises around the globe. This came after a rash of avoidable compliance incidents among public CAs and widespread outcry about the responsible CA's poor handling of many of these incidents.

When a CA takes shortcuts, the consequences ripple across the entire internet, putting encryption, authentication, and compliance in jeopardy. But the industry can't afford to falter, especially not with the impending launch of quantum computers.

Quantum computers, by their nature, will render today's RSA and ECC encryption obsolete, exposing previously unreadable data. Today, threat actors are already harvesting this encrypted data for later decryption once sufficient quantum computing power becomes available.

Between evolving cyber threats, new emerging technologies, and tightening regulatory frameworks, the CA's role has never been more critical. Organizations rely on CAs to ensure data integrity, maintain privacy, and establish credibility in a world where trust is currency. The reality is that not all CAs operate with the same level of rigor, transparency, and ethical responsibility.

This eBook is your guide to understanding what sets a reputable CA apart from the rest. It's about more than just digital certificates. It's about trust, reputation, and the critical decisions that impact your security posture now and in the future. We'll explore why choosing the right CA isn't just a compliance checkbox but also a strategic necessity for businesses and industries worldwide. Preparedness is key, and choosing a reputable CA is paramount. You cannot afford to gamble with your security.

1. Understanding Certificate Authorities

What is a Certificate Authority (CA)?

Digital certificates serve as the identity credentials for websites and IT systems. If these credentials are compromised, access is denied, trust is lost, and operations are halted. Certificates authenticate domains and enable encrypted communication, protecting sensitive data from passwords to financial information, personal records and more.

A Certificate Authority (CA) is the trusted third party responsible for issuing and managing these certificates. The security and reliability of the digital ecosystem depend on reputable CAs – without them, organizations face significant risks including phishing attacks, domain spoofing, data breaches, and loss of user trust.

As with any service, not all CAs are the same. While all must follow compliance standards, not every CA will offer an enhanced level of technical knowledge. As the industry has seen in the past, this trust is not equally reliable. When digital integrity is on the line, reputation matters more than marketing

The choice of CA directly impacts:

Your organization's uptime: Encryption mitigates risks like data breaches and identity theft, resulting in less risk of costly downtime.

Customer trust: Browsers provide padlocks or "Secure" indicators in the web address bar to improve user confidence.

Regulatory compliance: Certificates from accredited CAs help businesses meet industry regulations and avoid penalties.

The role of a CA in operational reliability

Modern CAs deliver concrete business benefits that directly impact your organization's security, operations, and bottom line. A trustworthy CA will:

- Prevent costly outages and downtime through reliable certificate management that ensures critical systems stay online 24/7
- Reduce security risks by maintaining encryption standards that protect sensitive data from breaches and unauthorized access
- Simplify compliance with automated systems that ensure you meet regulatory requirements across jurisdictions
- Cut operational costs by eliminating the need for extensive in–house certificate expertise and management
- Enable digital transformation by providing the trust infrastructure needed for cloud migration, remote work, and digital customer experiences
- Future–proof your business through early preparation for emerging threats posed by quantum computing

> "Digital certificates are the backbone of a secure internet," says Tim Callan, Chief Compliance Officer at Sectigo. "Every protected transaction, authenticated identity, and secure connection relies on the trust established by digital certificates."

The impact of a CA on uptime and customer trust

Choosing the wrong CA can have lasting consequences, exposing businesses to potential downtime and eroding customer confidence. A single misissued certificate or lapse in renewal can cause business interruptions, compromise sensitive data, damage brand reputation, and lead to financial losses.

“In today’s digital economy, trust is the currency that matters most. Once lost, it’s extraordinarily difficult to rebuild,” says Kevin Weiss, CEO at Sectigo. Customers expect secure, encrypted connections – anything less puts your business at risk.

For enterprises undergoing digital transformation, selecting a reputable CA is more than an IT decision, it’s a strategic investment in customer experience, revenue protection, and brand integrity. The right CA ensures compliance, enhances cybersecurity, and reinforces public trust, making it a cornerstone of long–term success in an increasingly interconnected world.

2. Factors to consider when selecting a CA

Reputation and industry recognition

Imagine relying on a car for your daily commute that's never been road–tested, has no service history, and comes from an unknown manufacturer. You wouldn't count on it to get you where you need to go, so why entrust your organization's digital infrastructure to a Certificate Authority with no proven track record?

In an industry where trust is the ultimate product, reputation speaks for itself. The most reputable CAs lead across multiple domains: technical innovation, standards development, industry collaboration, and customer service. Their influence shapes the future of digital identity, ensuring organizations stay ahead of evolving threats.

Industry recognition serves as external validation of a CA's reputation. The difference between industry leaders and followers becomes clear when you assess their contributions: publication of cutting–edge research, development of new cryptographic standards, active participation in security communities like the CA/Browser Forum, and speaking engagements at major security conferences. Additionally, top–tier CAs often collaborate with governments, enterprises, and security vendors to drive best practices in encryption, certificate management, and postquantum cryptography.

"When evaluating Certificate Authorities, look beyond the feature checklist," advises Jason Soroko, Senior Fellow at Sectigo. "The best indicator of future performance is a proven track record of anticipating industry changes, influencing standards development, and helping customers navigate complex security challenges."

Compliance and security standards

Being a CA entails maintaining guardianship over digital trust. And as guardians of internet security, CAs are responsible for adhering to any and all compliance and security standards set by browsers, industries, or governments.

The most universally recognized framework for CA trustworthiness is WebTrust for CAs, developed by the Canadian Institute of Chartered Accountants (CICA) and the American Institute of Certified Public Accountants (AICPA). CAs undergo annual third–party audits to prove compliance with these standards, which assess everything from policy documentation and identity validation to secure key management practices. Major root programs operated by Microsoft, Mozilla, Apple, and Google require CAs to pass these audits—compliance isn't optional; it's foundational. In parallel, many top–tier CAs also align with broader security frameworks such as ISO/IEC 27001, SOC 2 Type II, and FIPS 140–2 for cryptographic hardware.

These standards demand robust controls around data protection, access management, physical security, change management, and incident response. Additionally, CAs must comply with Baseline Requirements and other technical mandates issued by the CA/Browser Forum, a consortium of CAs and browser vendors that sets rules for certificate issuance and management. Non–compliance with these requirements can result in browser distrust, effectively removing the CA's ability to function on the public internet.

The CA/Browser Forum: Safeguarding trust

The CA/Browser Forum (CA/B Forum) is the industry's governing body responsible for establishing certificate standards that protect the global digital ecosystem. Formed in 2005, the CA/B Forum unites CAs and major browser vendors to define best practices for certificate issuance, management, and security. Its guidelines – including the Baseline Requirements and Extended Validation (EV) standards – ensure that digital certificates maintain the highest levels of trust and integrity.

The CA/Browser Forum has set Baseline Requirements that all publicly trusted CAs must follow, covering everything from certificate issuance, validation processes, and security practices. In order to uphold their reputation and maintain their trusted status, CAs are required to maintain secure and compliant certificates and services.

Customer support and scalability

In a digital environment where businesses deploy certificates at scale across websites, APIs, IoT devices, DevOps pipelines, and more, CAs must be able to meet demand instantly, reliably, and without compromise.

Responsive, knowledgeable, and accessible customer support is vital for a reputable CA. Whether due to a misissued certificate, a looming expiration, or a compliance question, when trust is on the line, customers need direct access to experts who can resolve issues quickly and decisively. The best CAs treat customer relationships as strategic partnerships, offering everything from 24/7 technical support to dedicated account management and proactive onboarding. Trust is personal, and CAs that invest in meaningful, human support build long–term loyalty in an increasingly commoditized market.

Equally vital is the ability to scale as needed for customers. Scalability isn’t just about handling volume; it’s about delivering speed, resilience, and automation at global level. Whether it's issuing millions of certificates for a cloud–native enterprise or supporting the dynamic needs of a growing startup, a reputable CA must offer robust APIs, seamless integrations, and infrastructure that can handle spikes in issuance, revocation, and validation with zero downtime. Modern organizations expect Certificate Lifecycle Management to be embedded into their workflows, and CAs must rise to that challenge with platforms built for performance and elasticity.

The critical relationship between a CA and Certificate Lifecycle Management (CLM)

At the heart of digital trust lies not just the issuance of certificates, but the management of their entire lifecycle, from creation to renewal to revocation. This is where the relationship between a CA and Certificate Lifecycle Management (CLM) becomes critical. CLM ensures that certificates are properly deployed, continuously monitored, renewed before expiration, and revoked if compromised. Without strong lifecycle oversight, even the most securely issued certificates can become liabilities, exposing organizations to outages, compliance failures, or breaches.

When a CA also provides an integrated CLM platform, it signals a holistic, modern approach to trust management. It means the CA isn't just handing off certificates and leaving customers to figure out the rest—they're actively helping organizations avoid downtime, reduce risk, and streamline operations. Automated discovery, renewal, and alerting are no longer nice–to–haves; they're mission–critical features for enterprises managing thousands of digital identities across hybrid or multi–cloud environments.

A CA that doubles as a CLM provider demonstrates deep understanding of real–world customer needs. It combines root–level trust with operational agility, giving organizations a single pane of glass to manage cryptographic assets at scale. This tight integration reduces the complexity and risk of managing disparate tools, simplifies audits and reporting, and improves security posture by ensuring that no certificate is forgotten or mismanaged.

By partnering with a CA that also provides built–in CLM, organizations can automate policy enforcement, generate real–time compliance reports, and drastically reduce the manual burden of audits.

3. The blueprint:
What makes the most compliant and secure CA in the industry

A CA must respond swiftly to security incidents, certificate misissuance, and shifting compliance requirements – any delay or oversight can expose vulnerabilities and erode confidence in digital certificates.

At Sectigo, we believe adherence to industry standards, and a culture of compliance are essential. We are committed to setting the standard for compliance and security in the CA industry and sharing our blueprint for success. Our commitment to rigorous security practices and strict adherence to global standards ensure the highest level of trust and reliability. And our executive leadership team plays a key role in shaping industry policies to maintain a safe and secure future for all.

Unrivaled compliance and industry certifications

Serving as the backbone of online trust, a CA must demonstrate unrivaled compliance and hold the necessary certifications to ensure the integrity, reliability, and security of its operations. These standards not only validate the CA's adherence to strict security protocols but also reinforce customer confidence, safeguard against breaches, and maintain compliance with global regulations and best practices across industries.

The responsibilities of a trustworthy CA extend beyond issuing certificates. Ongoing security practices such as continuous monitoring, transparent incident response, and active participation in policy development contribute to raising industry standards. By upholding these practices, a CA plays a key role in protecting sensitive data and supporting long-term digital identity trust across diverse sectors.

Sectigo holds crucial security certifications and compliance validations, ensuring the highest level of trust:

- **WebTrust Seal of Assurance** – Demonstrates Sectigo's operational integrity and regulatory compliance.
- **ISO 27001 Certification** – Sectigo upholds global information security and risk management best practices.
- **CA/Browser Forum Leadership** – Sectigo actively shapes industry standards with more CA/B Forum seats than any other CA.
- **ETSI EN 319 411–1 Certification** – Sectigo meets European trust service provider requirements.
- **Regular Third–Party Security Audits** – Sectigo conducts independent validations of our security posture.

Proactive security and incident management

Given their role in safeguarding the digital identities and communications of countless organizations, CAs must anticipate threats before they occur and respond swiftly to any potential incidents. By maintaining a robust, proactive approach, a CA can minimize vulnerabilities, reduce downtime, and protect the trust placed in its infrastructure, ensuring the security and continuity that clients and partners expect in today's evolving threat landscape.

Sectigo goes beyond compliance with a commitment to transparency, rapid incident resolution, and continuous security improvements:

Industry–leading incident response

Most incidents are self–reported, thoroughly documented, and resolved within two weeks.

Zero delayed revocations in recent years

We take immediate action to maintain trust and security.

100% responsiveness

Every Certificate Problem Report has been handled on time since 2020.

Contributions to WebPKI infrastructure

The WebPKI is a global framework of CAs, browser vendors, and cryptographic standards that enables secure, authenticated, and encrypted communication across the internet using digital certificates. It ensures that websites, applications, and digital identities remain verifiable, protected, and resilient against cyber threats. A strong WebPKI is essential for safeguarding businesses and users from fraud, data breaches, and privacy compromises.

Maintaining and advancing the WebPKI requires constant innovation, infrastructure support, and adherence to evolving security standards. Sectigo leads these efforts with technical excellence, contributing critical tools, open–source projects, and policy advancements that strengthen the entire ecosystem.

Sectigo isn’t just compliant – we define the future of digital trust by driving technological innovation, strengthening the WebPKI, and ensuring the highest security standards.

From maintaining industry–standard Certificate Transparency tools to developing cutting–edge security solutions, Sectigo plays a pivotal role in ensuring accountability, compliance, and innovation within the WebPKI landscape, contributing more essential infrastructure and services to the public CA industry and WebPKI than any other organization:

- **Open MPIC:** Sectigo plays a pivotal role in the Open MPIC (Multi–Perspective Issuance Corroboration) project, developing an open–source tool that helps all CAs comply with new CA/Browser Forum requirements aimed at enhancing the security of digital certificate issuance against Border Gateway Protocol (BGP) attacks.

- **Certbot contributions:** Sectigo enhances certificate automation by contributing to Certbot, the most widely used open–source tool for ACME–based certificate deployment.

- **crt.sh:** Sectigo operates crt.sh, the industry–standard tool for searching Certificate Transparency (CT) logs, officially recognized by both CCADB and Mozilla policy.

- **Trillium PostgreSQL integration:** In response to CT infrastructure challenges, Sectigo added PostgreSQL support to Trillium, bolstering the resilience and scalability of CT log operations.

- **PKIMetal:** A high–performance PKI meta–linter developed by Sectigo that streamlines pre–issuance linting for public CAs, helping ensure compliance and interoperability.

Leadership contributions continued...

- **Weak key detection:** Sectigo developed open–source tools to detect and mitigate weak Debian keys, helping the industry prevent key misuse and protect end–users.

- **Certificate Transparency leadership:** Sectigo operates and maintains public CT logs, reinforcing accountability and trust across the certificate ecosystem.

- **CA cross–signing services:** Sectigo provides critical cross–signing capabilities, enabling greater trust and interoperability for other certificate authorities.

- **Open–source linting tools:** As a major contributor to zlint and certlint, Sectigo strengthens certificate validation processes that are widely relied upon by CAs and browsers alike.

- **CA/Browser Forum infrastructure support:** Sectigo personnel help maintain core CA/Browser Forum infrastructure, including mailing lists, wikis, and the organization's official website, supporting industry coordination and policy development.

Intellectual leadership

True intellectual leadership means challenging the status quo, raising industry standards, and inspiring best practices. At Sectigo, we take this responsibility seriously – educating the community through whitepapers, podcasts, and advocacy while actively shaping the future of digital security. Our experts are regularly invited to speak at industry events hosted by such organizations as ENISA, ETSI, and the PKI Consortium, where they share critical insights that influence global cybersecurity policies.

Additionally, our Root Causes podcast – now with over 500 episodes – has become the world's most popular podcast dedicated to digital certificates and PKI, delivering essential security updates to a global audience with over 500,000 listens.

ROOT CAUSES

A PKI & Security Podcast

Tune in on your favourite streaming platform:

Listen on Apple Podcasts

Listen on Spotify

Listen on SOUNDCLOUD

Discover Root Causes

4. Sectigo's commitment to innovation and security

Sectigo's leadership extends beyond education; we hold more chairs in the CA/Browser Forum than any other CA in history and maintain a key leadership seat in ETSI, reinforcing our deep commitment to industry standards.

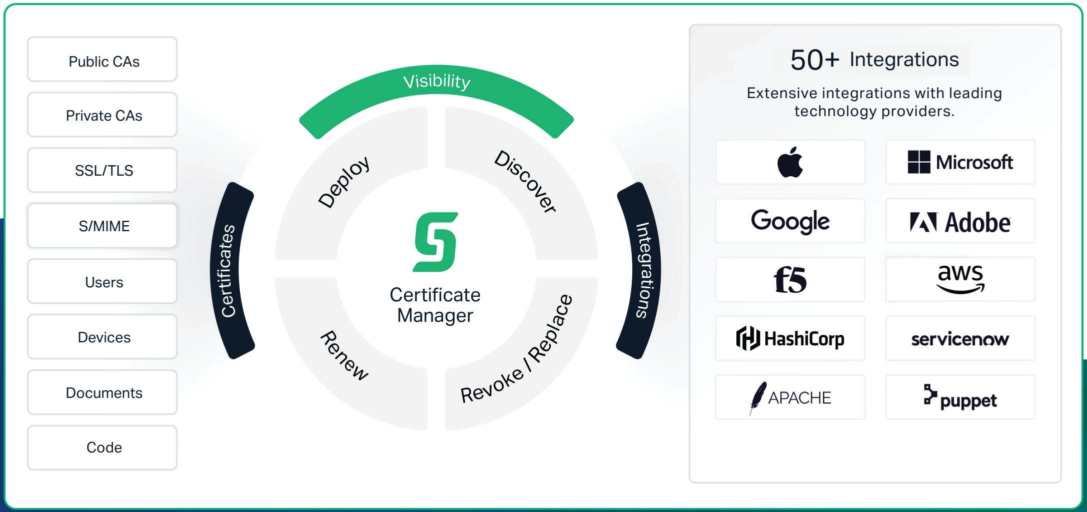
We have led the charge in enterprise education on postquantum cryptography (PQC) and were the first public CA to develop a CA–agnostic Certificate Lifecycle Management (CLM) platform, ensuring businesses can seamlessly manage digital certificates regardless of their CA provider.

Best practice: our automation and Certificate Lifecycle Management standards

Beyond research and development, Sectigo actively shapes industry standards through initiatives like shortening certificate lifespans and revocation reform, ensuring a more secure, transparent, and future–ready digital landscape. Our intellectual leadership isn't just about innovation – it's about building the trust and security the internet depends on.

Sectigo's naturally CA–agnostic platform, Sectigo Certificate Manager (SCM), in contrast to other certificate lifecycle management products, lets organizations fulfill multi–vendor requirements they may have with an automation offering that makes switching suppliers simple and rapid. SCM supports robust API integrations to streamline certificate issuance and validation, enabling seamless management of public and private certificates across diverse environments.

Sectigo also understands the importance of integrating into the existing infrastructure within organizations. With over 50+ built-in integrations with cloud providers, other CAs, DevOps tools and platforms, web servers, key vaults, email security platforms, and more, Sectigo users can seamlessly integrated SCM into their existing tech stack, without having to rip-and-replace.

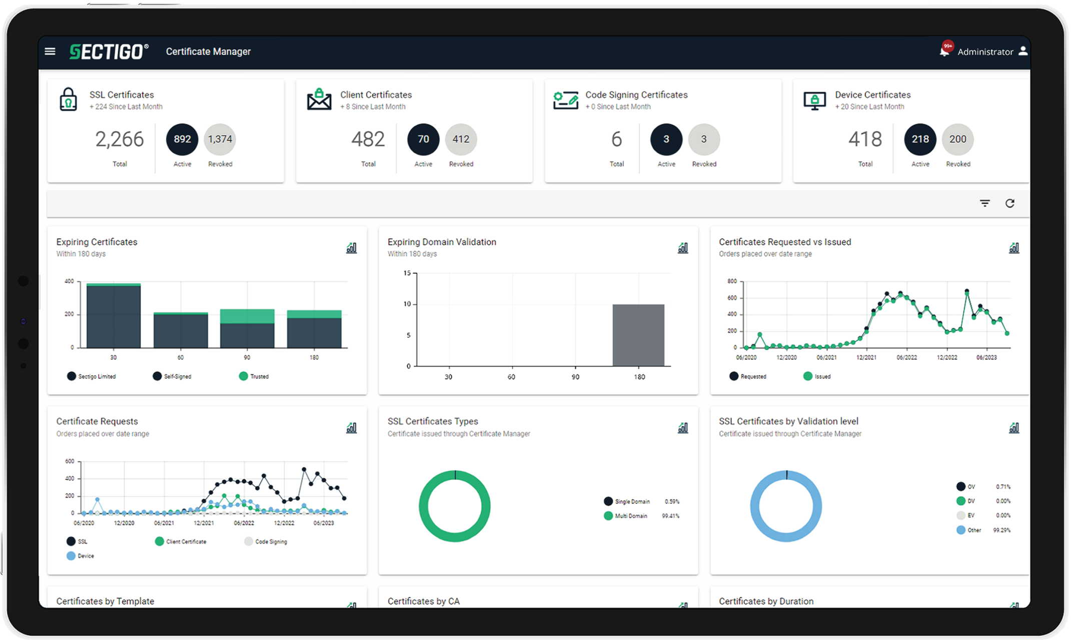


Our best–in–class CLM platform, Sectigo Certificate Manager (SCM)

Automation in certificate management eliminates human error, reduces the risk of outage, and ensures continuous compliance with evolving security standards. By streamlining certificate issuance, renewal, and revocation, organizations can proactively prevent breaches, maintain trust, and focus on advancing their digital initiatives. The unique combination of being both a CA and CLM ensures Sectigo's customers benefit from top–tier security, automation, and efficiency when managing digital certificates at scale.

Sectigo Certificate Manager (SCM) is Sectigo's universal platform designed to securely manage the lifecycle of digital certificates for both human and machine identities. With a single, centralized interface, SCM simplifies certificate management through automated issuance, renewal, and oversight. Key features include:

- **Automated certificate issuance and renewal:** Reducing the risk of expired certificates
- **Centralized visibility**: Offering a single interface for managing digital certificates
- **Scalability**: Supporting enterprises with large–scale certificate needs



SSL Certificates
+ 224 Since Last Month
2,266 Total | 892 Active | 1,374 Revoked

Client Certificates
+ 8 Since Last Month
482 Total | 70 Active | 412 Revoked

Code Signing Certificates
+ 0 Since Last Month
6 Total | 3 Active | 3 Revoked

Device Certificates
+ 20 Since Last Month
418 Total | 218 Active | 200 Revoked

SSL Certificates Types: Single Domain 0.59%, Multi Domain 99.41%

SSL Certificates by Validation level: OV 0.71%, DV 0.00%, EV 0.00%, Other 99.29%

Quantum readiness

Quantum computing poses a significant threat to traditional encryption methods, as advanced quantum computers could potentially decrypt data protected by current algorithms such as RSA and ECC.

In anticipation of future cryptographic challenges, Sectigo has demonstrated leadership in Postquantum Cryptography (PQC) readiness. Sectigo PQC Labs is the industry's first postquantum cryptographic sandbox, a cutting–edge collaboration with Crypto4A. This platform enables organizations to safely explore, test, validate, and create postquantumcryptographic certificates.

Sectigo PQC Labs is aligned with NIST standards, providing an innovative environment to allow technical professionals to experiment with private–root certificates using NIST–approved postquantumcryptographic algorithms, preparing them for the advent of quantum computing threats, and the transition to a quantum–secure future.

Sectigo's key initiatives include:

- **Transition readiness:** Assisting enterprises in adopting quantum–resistant encryption to safeguard their digital assets in anticipation of quantum advancements.
- **Hybrid certificates:** Developing certificates that combine traditional and quantum–resistant cryptographic methods, facilitating a smooth transition and bridging current and future security needs.

By choosing a CA that leads in quantum readiness, organizations can ensure long–term data protection and stay ahead of evolving security threats.

47–day certificates: shorter is better

The newly approved measure to reduce certificate lifespans to 47 days, initially proposed by Apple and endorsed by Sectigo in January 2025, will gradually step down lifespans between 2025 and 2029. Ballot SC-081v3 formally passed on April 11th, 2025, puts the phased reduction into effect with the following enforcement dates:

- **March 15, 2026:** Maximum certificate lifespan reduced to 200 days
- **March 15, 2027:** Further reduction to 100 days
- **March 15, 2029:** Final enforcement of the 47-day maximum lifespan

This change, supported by Sectigo and major browsers like Apple and Google, marks a turning point for digital certificate management. Organizations will now need to renew certificates nearly every month, which will be unsustainable without an automated solution.

Browsers and Certificate Authorities support this change with good reason. Shortening the lifespan of digital certificates is a crucial step in strengthening internet security. Certificates with longer validity periods increase the risk of compromised keys, outdated encryption standards, and vulnerabilities going undetected for extended periods. And as we rapidly approach the deployment of quantum computing, automation and visibility across an organization's suite of certificates is crucial. By reducing certificate lifespans, organizations benefit from improved security posture, faster adoption of cryptographic advancements, and minimized exposure in the event of key compromise. This proactive approach ensures that businesses can swiftly adapt to evolving security best practices and emerging threats.

Conclusion: A vision for a more secure future

Sectigo isn't just compliant – it defines the future of digital trust by driving technological innovation, strengthening the WebPKI, and ensuring the highest security standards. Through advanced automation, postquantum cryptography readiness, and unmatched contributions to public PKI infrastructure, Sectigo empowers enterprises to navigate the evolving security landscape with confidence.

When choosing a CA, the decision ultimately comes down to trust – not just in technical capabilities, but in strategic vision, industry leadership, and proven performance. In today's rapidly evolving threat landscape, the distinction between leading and following has never been more critical. By staying ahead of emerging threats and pioneering future–proof solutions, Sectigo ensures that businesses can operate securely in an increasingly digital world.

Sectigo's commitment to proactive security, technical excellence, and industry leadership ensures that businesses stay ahead of evolving cyber threats while maintaining the highest level of digital trust. When digital security faces its greatest tests, Sectigo doesn't just participate in the response – it leads it.

Get in Touch