sectigo

DATASHEET

Sectigo as your public Certificate Authority (CA)

Role of public Certificate Authority (CA)

Certificate Authorities (CAs) are vital for digital security, providing SSL/TLS certificates that authenticate and secure online communications. They ensure data integrity and privacy, protecting against security threats. A reputable CA adheres to industry standards, undergoes rigorous audits, and complies with CA/Browser Forum regulations.

Choose a CA that works for you

Given the critical role CAs play in internet security and user trust, selecting the right CA that meets your specific needs requires careful consideration. Evaluate your options closely, keeping the following important factors in mind:

Reputation

Look for a CA with a strong reputation within the industry and among diverse customers.

Domain Flexibility

Evaluate their options provided to securing multiple domains or subdomains.

Customer Support

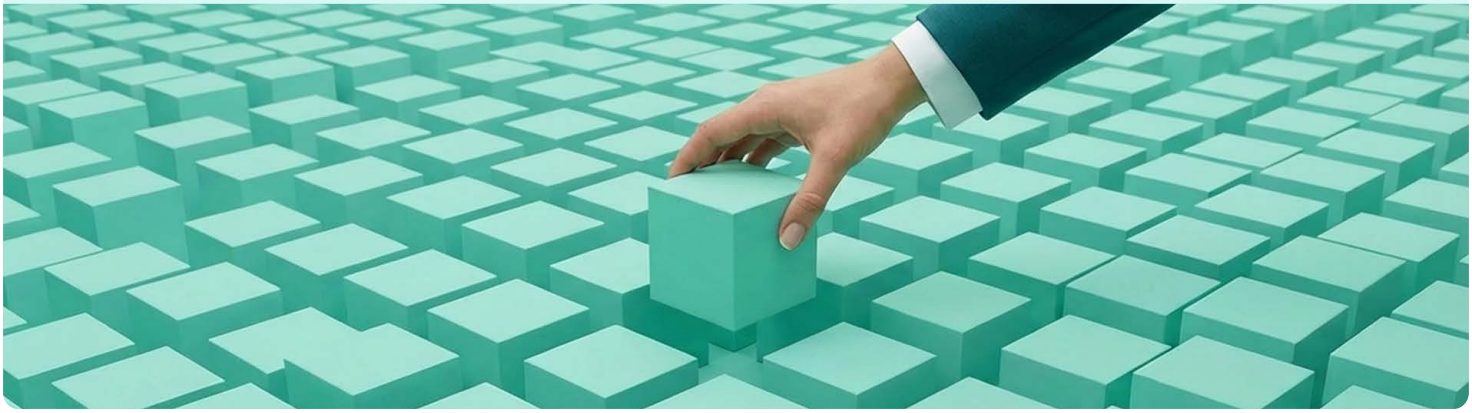
Choose a CA known for excellent customer support throughout the validation process and beyond.

Validation Levels

Ideally the CA would offer a range of certificates (DV, OV, EV) to match your security needs and compliance requirements.

Automated Lifecycle Management

Check for solutions supporting automated certificate lifecycle management, especially with the upcoming shift to 90-day SSL certificates.



Sectigo as a public CA

Sectigo stands as one of the most established leading Certificate Authorities in the industry for over two decades. We take digital trust extremely seriously and maintain rigorous compliance with Webtrust audits and CA/B Forum policies, guaranteeing reliability and trust in certificate validation, issuance, and revocation processes.

We submit to regular independent audits, follow industry guidelines, and maintain best practices to secure our infrastructure. Additionally, Sectigo is heavily involved in industry groups and plays a pivotal role in the development of industry standards to meet the evolving needs of the digital landscape:

- Holds 4 offices in CABF and 1 office in ESTI, more than any other organizations.
- Built and maintain crt.sh, the de facto standard for tracking and reporting SSL leaf certificates.
- Actively operates a Certificate Transparency (CT) log.

Main drivers of public CA distrust events

Browser distrust events of public CAs occur approximately every 1.23 years on average. A significant 68% of these distrust events are due to poor compliance handling, with 21% specifically resulting from inadequate incident response management*.

Sectigo's proven trust by the numbers

- Over **95%** of Sectigo incidents are self-reported.
- Responds to all questions and comments within **7 days or less**.
- Resolves most incidents within **2 weeks or less**.

Types of certificates issued by Sectigo

- SSL certificates:
  - Domain Validation (DV) Certificates.
  - Organization Validation (OV) Certificates.
  - Extended Validation (EV) Certificates.
- Code Signing Certificates
- Email Security (S/MIME) Certificates
- Document Signing Certificates
- eIDAS Certificates

Validation and support

- Comprehensive validation processes for each type of certificate.
- Detailed guides and resources for certificate installation and management.
- Award-winning 24/7 customer support is available across the globe.

Did you know?

Sectigo strictly adheres to industry audits and standards such as Webtrust, eIDAS, CA/B Forum, ISO27001, SOC 2/3, ETSI, and PCI-DSS.

Ensures reliable/secure digital certificates

International InfoSec standards

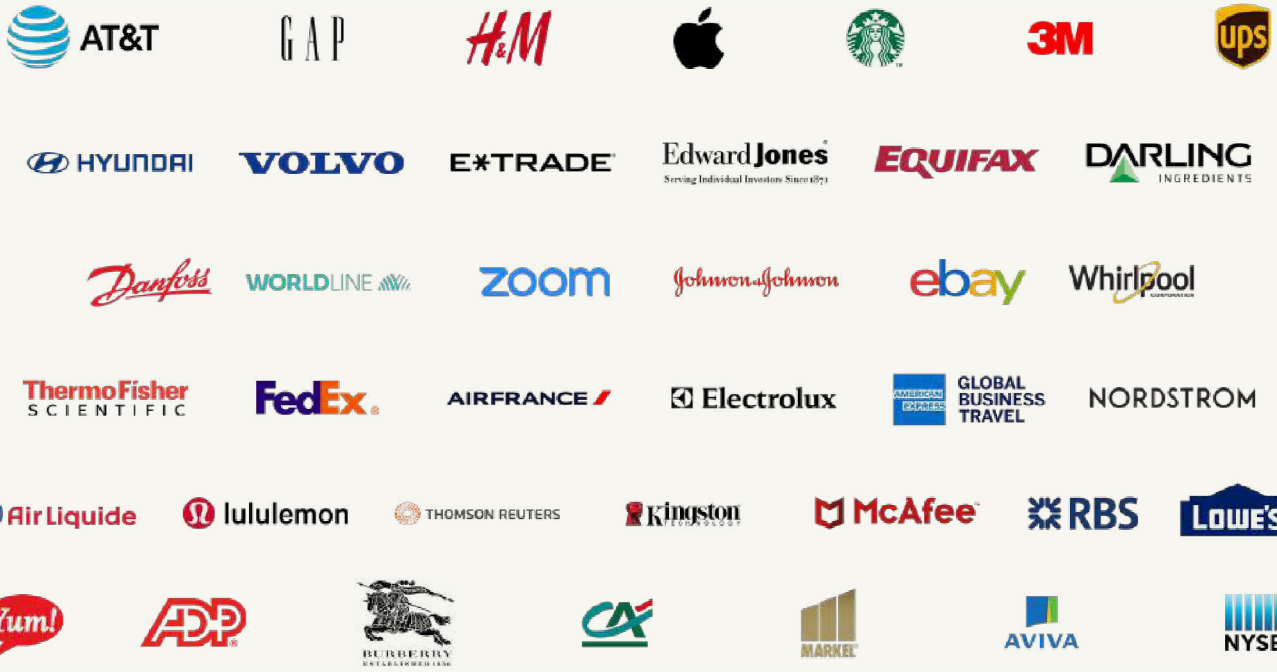
Protects sensitive data from vulnerabilities

Reduces payment card fraud

EU regulation 910/2014

[Source: Exploring Browser Distrust | UNMITIGATED RISK]

Let our customers speak for us



Gartner Peer Insights™ 4.6 ★★★★½

5.0 ★★★★★ Reviewed on Apr 9, 2026

Powerful Certificate Management with a steep but worthwhile learning curve.

"Sectigo has become the backbone of our certificate lifecycle. Once we put in the effort to structure policies and enrollment profiles, the day-to-day certification work went from "firefighting and spreadsheets" to something we barely think about."

5.0 ★★★★★ Reviewed on Nov 19, 2025

Certificate Issuance Streamlined.

"The Sectigo Certificate Manager platform makes the certificate management process simple and straight forward with its ability to allow us to establish certificate profiles, automated renewal, and owner alerting capabilities."

G2 4.5 ★★★★½

5.0 ★★★★★ Reviewed on Jan 29, 2026

Automated Certificate Management with Responsive, Agile Support.

"The biggest advantage of SCM and Sectigo overall is the fully automated certificate management process. Both the customer support team and our assigned TAM are responsive, agile, and easy to work with."

5.0 ★★★★★ Reviewed on Jan 29, 2026

Easy with Helpful Expiration Reminders.

"Sectigo makes the process of generating and managing certificates very easy. I manage the SSL certificates for all three websites under my responsibility, and this setup makes it much easier to stay on top of renewals and keep everything organized."

> "Sectigo Certificate Manager has become a major part of our IT management infrastructure, allowing us to update, add and delete thousands of digital certificates with a streamlined dashboard and email alert system."
>
> - Craig Hurter
> *IT security Manager, University of Colorado at Boulder*

Choose trust

Gaining and maintaining status as a reputable Certificate Authority demands unwavering commitment to stringent standards. A trustworthy CA must proactively address security threats through continuous monitoring and collaboration with industry stakeholders.

For robust and reliable Certificate Authority services to secure your websites, networks, and authenticate users, devices, and applications, Sectigo stands out as an exceptional choice. As one of the largest commercial CAs globally and a leader in innovative certificate lifecycle management (CLM), Sectigo provides a diverse array of solutions tailored to meet your specific needs, backed by our award-winning customer support.

Sectigo Certificate Manager: One-stop shop for all your certificate needs

Lead by automation

Sectigo Certificate Manager (SCM) enhances workflow automation and efficiency as a first-class ACME citizen and supports all major certificate automation standards.

CA-agnostic single pane of glass

Experience streamlined certificate management by consolidating all public and private certificates in one place for effortless administration, regardless of their origins.

Proven Reliability

Benefit from a robust and award-winning certificate management solution known for its proven reliability and performance.

For more information on Sectigo's Pubic CA practices, SSL/TLS certificates or certificate management in general please contact Sectigo Sales at **sales@sectigo.com.**

More related readings

- Understanding the Different Types of Certificate Authorities | Sectigo® Official
- What it takes to be a reputable Certificate Authority | Sectigo® Official
- What Is the CA/Browser Forum? | Sectigo® Official
- Certificate Outages Infographic
- Sectigo as a private CA brief

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.