Comparing Public CAs:
DigiCert, Sectigo, GlobalSign, and More

Choosing among public Certificate Authorities involves more than comparing sticker prices, since each major CA differentiates itself through validation options, automation support, support quality, and specific enterprise features. This article compares several of the major players in the space to help frame that decision, without treating any single vendor as universally the right answer.

DigiCert: Enterprise Depth and Broad Product Range

DigiCert has built a reputation for strong enterprise account management, a broad range of certificate types spanning Domain, Organization, and Extended Validation, and robust support for large-scale certificate management through its CertCentral platform. Organizations with complex, multi-CA, multi-cloud environments and a need for dedicated enterprise support often gravitate toward DigiCert specifically for the depth of its account management and platform tooling, which can justify a premium price point for organizations that value that level of hands-on support.

Sectigo: Value-Oriented With Strong Automation Support

Sectigo, one of the largest CAs by issuance volume, has positioned itself with competitive pricing relative to some of the more premium enterprise-focused CAs, while still offering solid ACME automation support and a full range of validation levels. Organizations prioritizing cost efficiency across a large certificate volume, without necessarily needing the deepest enterprise account management relationship, often find Sectigo a strong fit, particularly for organizations already comfortable managing certificate operations largely through automation rather than relying heavily on vendor support.

GlobalSign: Strong IoT and Managed PKI Focus

GlobalSign has built particular strength in managed PKI services and IoT-specific certificate issuance at scale, aligning well with the IoT certificate provisioning challenges discussed elsewhere in this series. Organizations with significant device fleet certificate needs, beyond standard web server certificates, often find GlobalSign's specific tooling and experience in this area a meaningful differentiator compared to CAs more narrowly focused on traditional web and enterprise certificates.

Let's Encrypt: The Free, Fully Automated Baseline

Covered in depth elsewhere in this series, Let's Encrypt remains the standard choice for free, fully ACME-automated Domain Validated certificates, without Organization or Extended Validation options and without the dedicated commercial support tier the CAs above provide. Most large organizations use Let's Encrypt alongside, rather than instead of, a commercial CA, reserving it for the bulk of lower-risk internal and public endpoints while using a commercial CA for the smaller set of certificates genuinely requiring deeper validation or dedicated support.

Comparing Automation and API Support Across CAs

Nearly every major CA now supports ACME to some degree, but the depth and reliability of that support varies, along with the quality of each CA's broader API for programmatic issuance, certificate management, and reporting beyond basic ACME functionality. Organizations building serious automation around a chosen CA should evaluate this API depth directly, through testing rather than marketing claims, since the practical experience of integrating a CA into an automated pipeline varies meaningfully even among CAs that all technically claim strong automation support.

Considering Root Program Trust and Incident History

Beyond features and pricing, a CA's track record with browser and operating system root programs matters, since CA incidents, including validation failures or policy violations serious enough to trigger mass certificate distrust events, have real operational consequences for anyone relying on that CA. Reviewing a CA's public incident history and its responsiveness to past issues offers a useful, concrete signal about operational maturity that goes beyond whatever a sales conversation alone would reveal.

Choosing CAs for AI Infrastructure Specifically

Organizations issuing large volumes of certificates for AI-driven infrastructure should weigh API robustness and issuance rate limits particularly heavily in their CA evaluation, since AI infrastructure can generate certificate demand that scales considerably faster than traditional web server certificate growth, and a CA whose automation and rate limit structure was not designed with this kind of rapid scaling in mind can become an unexpected bottleneck as AI initiatives grow.

The Countdown Is Already Running: 200 Days, 100 Days, 47 Days

Every certificate conversation in 2026 eventually arrives at the same clock, and it is worth closing on it here. The CA/Browser Forum's Ballot SC-081v3 is not a proposal under discussion; it is an approved, already-in-motion schedule. Maximum public TLS certificate lifetimes fall from 398 days to 200 days on March 15, 2026. They fall again to 100 days on March 15, 2027. By March 15, 2029, they drop to just 47 days, with domain validation itself needing to be re-proven roughly every 10 days.

01

Translate that into operational terms and the picture gets stark quickly. An organization currently renewing certificates a few times a year will be handling renewal events on the order of every couple of weeks by the end of this countdown, across every endpoint it operates. Manual tracking, calendar reminders, and a spreadsheet somebody checks once a month will not survive contact with that cadence. What has always been an occasional chore is becoming a continuous, automated operation, whether an organization plans for it or not.

02

Whichever CA an organization chooses, its ability to support fully automated issuance at the pace required by the shrinking lifetime schedule below should be a primary evaluation criterion, since a CA that cannot keep up with renewals every 47 days will need to be reconsidered well before that deadline actually arrives.

03

The 200-day, 100-day, and 47-day milestones are not distant hypotheticals; the first has already arrived. Organizations that build the automation loop now, generating keys, vaulting them securely, brokering issuance across Certificate Authorities through APIs, and rebinding certificates to live endpoints without manual intervention, will meet each deadline without disruption. Organizations that wait will be rebuilding their certificate operations under deadline pressure, with far less room for error and far less time to get it right. The countdown is the call to action. The only real decision left is whether to automate on your own schedule, or on the CA/Browser Forum's.