sectigo

DATASHEET

Subordinate Public CA

SSL, code signing, and S/MIME public certificates branded for your organization

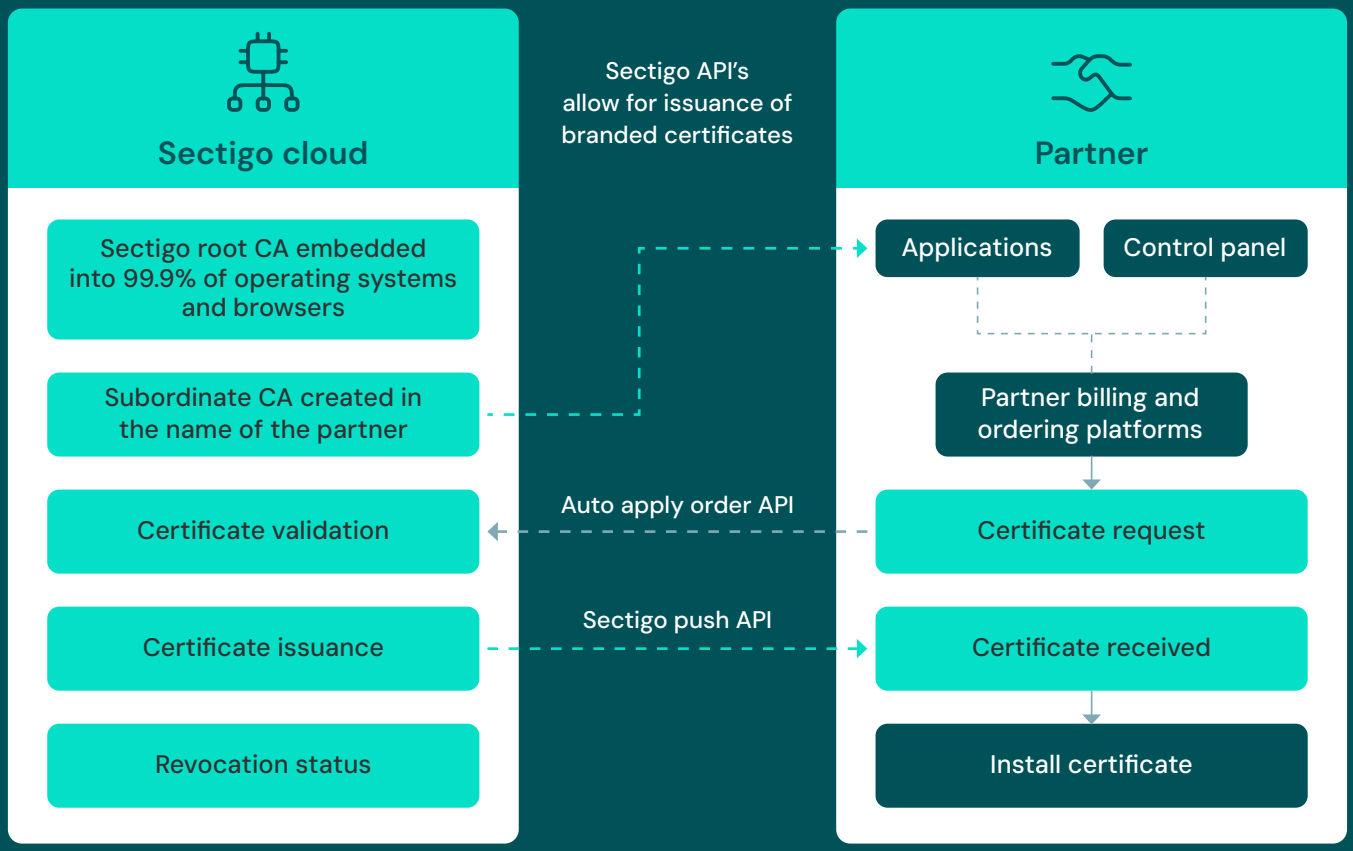
Introduction

For partners, public certificates are a high-trust, recurring-revenue offering, but building and operating a compliant Certificate Authority is costly and complex. The Sectigo subordinate CA program gives you that business under your own brand, with none of the operational burden. Partners issue digital certificates using a custom-branded subordinate CA certificate from Sectigo's globally trusted root. Your dedicated subordinate CA displays your brand on every customer certificate, and end-leaf certificates carry the same global trust as commercial certificates from Sectigo.

Sectigo hosts and manages all required services and infrastructure, maintaining compliance with relevant industry regulations such as the CA/B Forum Baseline Requirements and EV Guidelines.

The hosted subordinate CA service provided by Sectigo includes:

- Key signing and creation of unique, intermediary, subordinate CAs
- Secure hosting of all root keys
- Public roots trusted by more than 99.9% of browsers
- Ability to offer SSL, S/MIME, and Code Signing certificates
- Choice of RSA or ECC algorithm
- Access to Sectigo provisioning software
- Full use of the extensive Sectigo API library
- Hosting in a physically secure facility with high availability and disaster recovery
- OCSP and CRL services
- Named account manager and priority support



Certificates branded for your organization

Your Sectigo subordinate CA carries your branding in the certificate chain and end certificate.

Certification path

[Sectigo]
[Your Brand] RSA Extended Validation CA
yourcustomer.com

Your brand in the certificate chain

sectigo.com | Sectigo© 2026. | All rights reserved.

Trust your customers can verify

Certificates you issue under your subordinate CA chain directly to Sectigo's globally trusted root, so they're automatically recognized across browsers, operating systems, and devices with no configuration required on your customers' end. Your brand sits in the trust chain, and the trust itself is universal from day one.

Every certificate is also logged to public Certificate Transparency (CT) records, which gives your customers independently auditable proof of exactly which certificates were issued under your brand, and lets you monitor your own issuance for anything unexpected. Together with controlled, domain-restricted issuance, this gives your customers verifiable brand trust that holds up automatically as certificates renew, with no manual steps and no risk of outages.

Compliance with industry requirements for public certificates

All CAs issuing public certificates must comply with a thorough set of industry standards. Sectigo ensures compliance in these ways:

1. Sectigo sets up and operates the CA and obtains an annual WebTrust audit. Sectigo manages all compliance with CA/Browser Forum rules and other requirements.
2. The Subordinate CA can only issue certificates to domains that are agreed upon and configured by Sectigo. This eliminates the risk of mistakenly issued SSL certs to third party webservers.
3. The subordinate CA will automatically validate that the operator has control of the domain for which the certificate is issued.

FAQ

Q Which types of certificate can I offer?

You can offer your choice of SSL/TLS, Code Signing, and S/MIME certificates. SSL certificates are available at Domain Validation (DV), Organization Validation (OV), and Extended Validation (EV) authentication levels. You can offer single domain, wildcard, and multi-domain SSL certificates.

Q Do I need to host or operate any services within my infrastructure?

No. Sectigo hosts and manages all required CA services in secure, audited data centers using Sectigo's owned infrastructure. Security and compliance requirements prohibit hosting subordinate CAs outside Sectigo's designated infrastructure.

Q Can I rename my certificate products?

Yes, you can rebrand certificate products to your own naming conventions.

Q Can I offer ECC certificates as well as RSA?

Yes, both key types are available.

Q Do I need to perform validation for my certificates?

No. To ensure quality and comply with mandatory requirements, Sectigo will perform all certificate validation using its validation processes and staff.

Q Can I offer my own branded certificates alongside Sectigo products?

Yes, you can offer both branded certificates and Sectigo certificates from the same account, controlled with simple API parameters.

About Sectigo

Sectigo is a leading provider of Certificate Lifecycle Management (CLM), helping organizations secure human and machine identities while reducing the hidden risks of modern digital trust. As certificate volumes grow and lifespans shrink, unmanaged certificates are becoming a source of outages, compliance exposure, and operational disruption. Sectigo uses Orchestrated Automation to deliver Simplicity at Scale through its cloud native CLM platform, bringing visibility, control, and lifecycle management together across complex environments. With more than 700,000 customers, including 65% of the Fortune 500, Sectigo is one of the largest and longest standing certificate authorities, with over 20 years of delivering unparalleled digital trust. For more information, visit www.sectigo.com or follow us on LinkedIn.

sectigo.com | Sectigo© 2026. | All rights reserved.