Subordinate Public CA

SSL, Code Signing, and S/MIME Public Certificates Branded for Your Organization

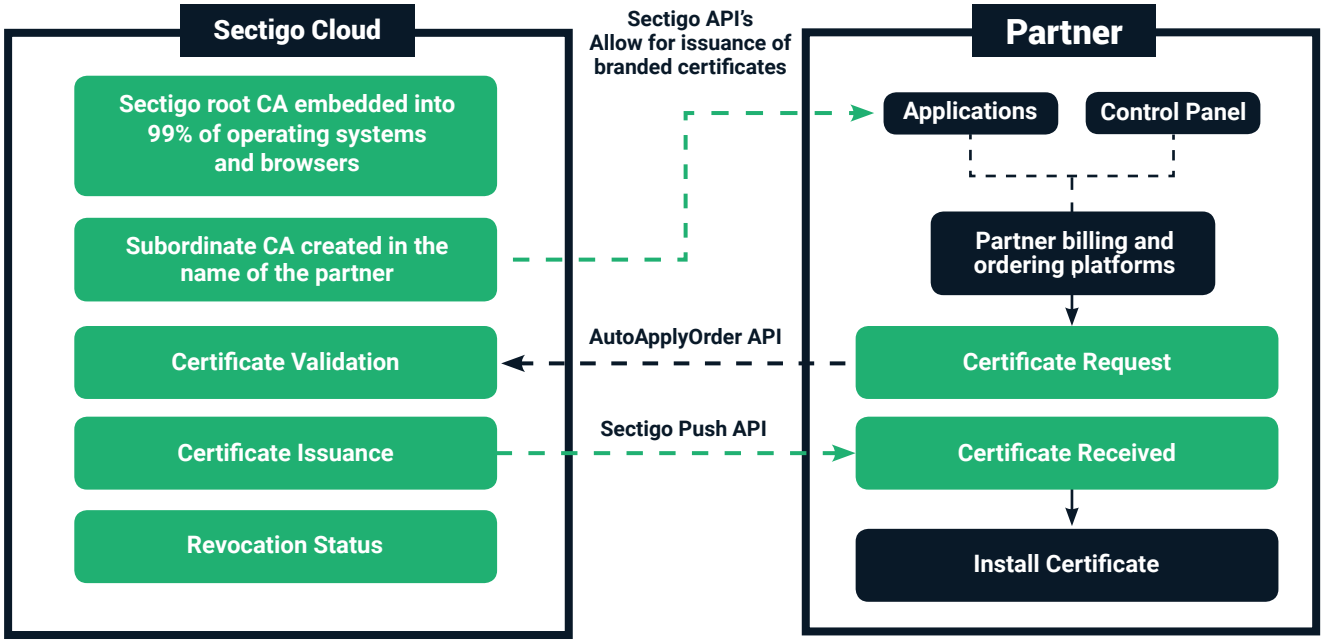
Introduction

The Sectigo subordinate CA program allows partners to issue digital certificates using a custom-branded subordinate CA certificate from Sectigo's globally-trusted root CA. The dedicated subordinate CA displays your brand for all customer certificates. End-leaf certificates issued on your subordinate CA enjoy the exact same ubiquitous global trust as do 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 service features high speed FIPS 140-1 Level 4 signing devices within our WebTrust-compliant environment.

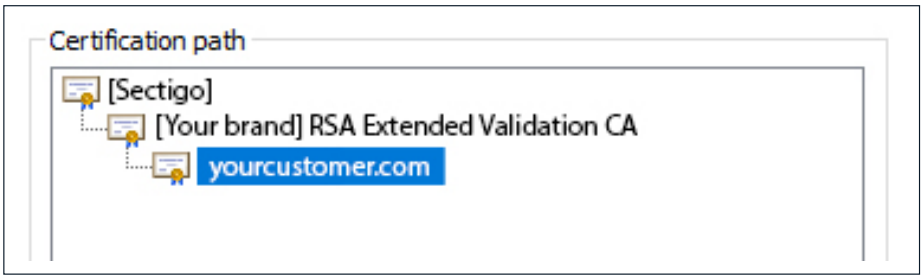
The hosted subordinate CA service provided by Sectigo includes:

- 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

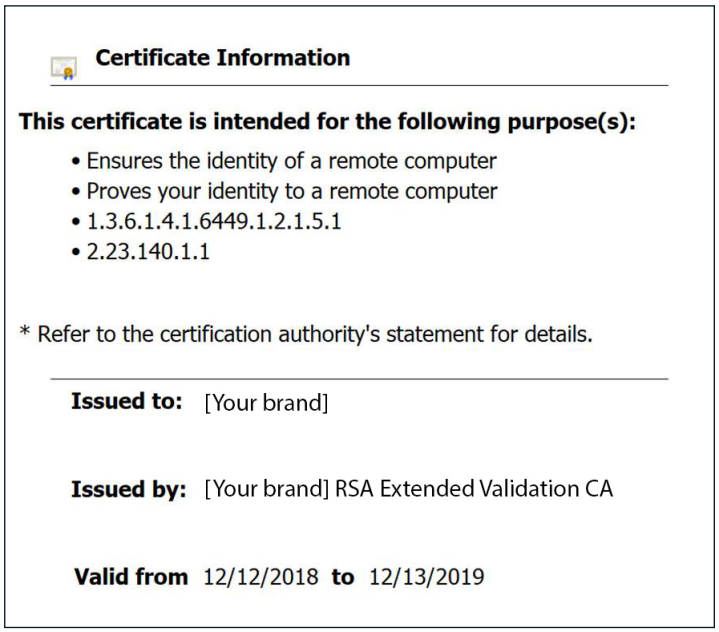
Your Sectigo subordinate CA carries your branding in the certificate chain and end certificate.



Your brand in the certificate chain

Control which certificates your applications and browsers trust

The browsers used by your community are configurable to trust only certificates issued by your subordinate CA, instead of the hundreds of Root CAs included in commercial browsers and operating systems. This technique is called Certificate Pinning. During the establishment of an SSL/TLS connection the client can authenticate the server it is talking to by validating that the SSL certificate was issued by your company's subordinate CA.



Your brand in the end user certificate

Note that while Google Chrome removed support for certificate pinning in 2018, it is still available for other browsers and applications. A popular approach for Android mobile applications is the Network Security Configuration (NSC) feature.

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.

SECTIGO

FAQ

Q: Which types of certificate can I offer?

A: 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?

A: 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?

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

Q: Can I offer ECC certificates as well as RSA?

A: Yes, both key types are available.

Q: Do I need to perform validation for my certificates?

A: 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?

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

About Sectigo

Trusted by enterprises globally for more than 20 years, Sectigo (formerly Comodo CA) provides web security products that help customers protect, monitor, recover, and manage their web presence and connected devices. As the largest commercial Certificate Authority, with more than 100 million SSL certificates issued across 150 countries, Sectigo has the proven performance and experience to meet the growing needs of securing today's digital landscape.

For more information about Sectigo, please contact us at **+1-703-581-6361** or **sales@sectigo.com**