

Untergeordnete öffentliche CA

Auf Ihr Unternehmen gebrandete öffentliche SSL-, Code-Signing- und S/MIME-Zertifikate

Einführung

Für Partner sind öffentliche Zertifikate ein vertrauenswürdiges Angebot mit wiederkehrenden Umsätzen. Der Aufbau und Betrieb einer konformen Zertifizierungsstelle (Certificate Authority, CA) ist jedoch kostspielig und komplex. Das Subordinate-CA-Programm von Sectigo ermöglicht es Ihnen, dieses Geschäft unter Ihrer eigenen Marke zu betreiben – ohne jeglichen operationalen Aufwand. Partner stellen digitale Zertifikate über ein individuell gebrandetes untergeordnetes CA-Zertifikat aus, das an die weltweit vertrauenswürdige Root-CA von Sectigo angebunden ist. Ihre dedizierte untergeordnete CA zeigt Ihre Marke auf jedem Kundenzertifikat, während die Endbenutzer-Zertifikate (End-Leaf) dieselbe globale Vertrauenswürdigkeit genießen wie kommerzielle Sectigo-Zertifikate.

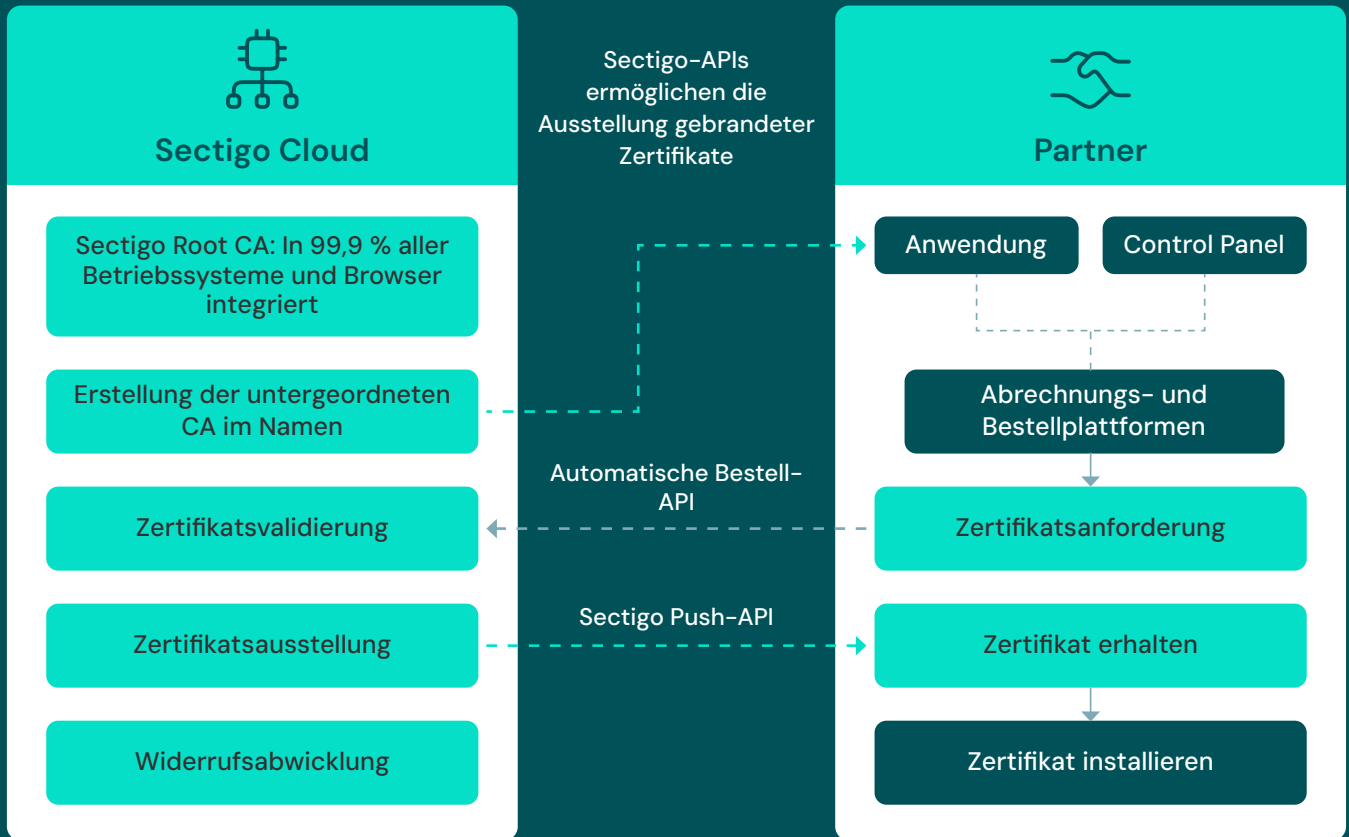
Sectigo hostet und verwaltet alle erforderlichen Dienste und Infrastrukturen und stellt die Einhaltung relevanter Branchenstandards wie der Baseline Requirements und EV-Richtlinien des CA/Browser Forums sicher.



Der von Sectigo bereitgestellte Subordinate-CA-Service umfasst:

- Schlüsselsignierung und Erstellung einzigartiger, untergeordneter Zwischen-CAs
- Sichere Verwahrung aller Root-Schlüssel
- Öffentliche Root-Zertifikate, denen über 99,9 % aller Browser vertrauen
- Angebot von SSL-, S/MIME- und Code-Signing-Zertifikaten
- Wahlmöglichkeit zwischen RSA- und ECC-Algorithmen
- Zugriff auf die Bereitstellungssoftware von Sectigo
- Volle Nutzung der umfangreichen Sectigo-API-Bibliothek
- Hosting in hochsicheren Rechenzentren mit Hochverfügbarkeit und Disaster Recovery
- OCSP- und CRL-Sperrdienste
- Dedizierter Account Manager und Prioritäts-Support

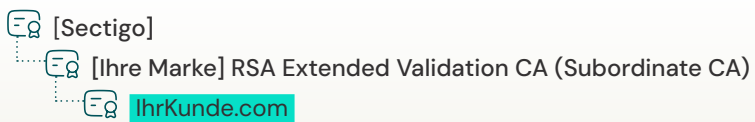




Auf Ihr Unternehmen gebrandete Zertifikate

Ihre untergeordnete Sectigo-CA trägt Ihr Branding sowohl in der Zertifikatskette als auch auf dem Endzertifikat.

Zertifizierungspfad



Ihre Marke in der Zertifizierungskette



Vertrauen, das Ihre Kunden überprüfen können

Zertifikate, die unter Ihrer untergeordneten CA ausgestellt werden, sind direkt an die globale Root-CA von Sectigo gekoppelt. Dadurch werden sie von Browsern, Betriebssystemen und Endgeräten automatisch erkannt – ohne dass Ihre Kunden Konfigurationen vornehmen müssen. Ihre Marke ist fest in der Vertrauenskette verankert.

Jedes Zertifikat wird zudem in öffentlichen Certificate Transparency (CT)-Registern protokolliert. Dies bietet Ihren Kunden einen auditierbaren Nachweis über alle unter Ihrer Marke ausgestellten Zertifikate. Zusammen mit einer domänenbeschränkten Ausstellung gewährleistet dies verifizierbares Markenvertrauen, das bei Erneuerungen automatisch erhalten bleibt.

Einhaltung von Branchenstandards für öffentliche Zertifikate

Alle CAs, die öffentliche Zertifikate ausstellen, müssen strenge Auflagen erfüllen. Sectigo stellt die Compliance wie folgt sicher:

- 1** Sectigo richtet die CA ein, betreibt sie und führt jährliche WebTrust-Audits durch. Sectigo verwaltet die Einhaltung aller CA/Browser Forum-Regeln.
- 2** Die untergeordnete CA kann nur Zertifikate für Domänen ausstellen, die von Sectigo geprüft und konfiguriert wurden. Dies schließt Fehlerausstellungen aus.
- 3** Die untergeordnete CA prüft automatisch, ob der Antragsteller die Kontrolle über die angeforderte Domäne besitzt.

Häufig gestellte Fragen (FAQ)

F Welche Zertifikatstypen kann ich anbieten?

Sie können SSL/TLS-, Code-Signing- und S/MIME-Zertifikate anbieten. SSL-Zertifikate sind in den Validierungsstufen Domain Validation (DV), Organization Validation (OV) und Extended Validation (EV) als Einzeldomänen-, Wildcard- oder Multidomänen-Zertifikate verfügbar.

F Muss ich Dienste in meiner eigenen Infrastruktur betreiben?

Nein. Sectigo hostet und verwaltet alle CA-Dienste in sicheren Rechenzentren. Sicherheits- und Compliance-Vorgaben untersagen das Hosting untergeordneter CAs außerhalb der Sectigo-Infrastruktur.

F Kann ich die Zertifikatsprodukte umbenennen?

Ja, Sie können die Produkte an Ihre eigenen Namenskonventionen anpassen.

F Kann ich neben RSA auch ECC-Zertifikate anbieten?

Ja, beide Schlüsseltypen stehen zur Verfügung.

F Muss ich die Validierung der Zertifikate selbst durchführen?

Nein. Um Qualität und Compliance zu gewährleisten, führt Sectigo alle Validierungen mit eigenen Prozessen und Fachpersonal durch.

F Kann ich eigene gebrandete Zertifikate zusammen mit Sectigo-Produkten anbieten?

Ja, Sie können über denselben Account sowohl gebrandete als auch Sectigo-Zertifikate über einfache API-Parameter steuern.

Über Sectigo

Sectigo ist ein führender Anbieter von Certificate Lifecycle Management (CLM), der Unternehmen dabei unterstützt, menschliche und maschinelle Identitäten zu sichern und digitale Risiken zu minimieren. Sectigo nutzt orchestrierte Automatisierung, um Einfachheit und Skalierbarkeit über seine cloud-native CLM-Plattform zu bieten.

Mit über 700.000 Kunden und mehr als 20 Jahren Erfahrung schützt Sectigo 65 % der Fortune-500-Unternehmen.

Weitere Informationen finden Sie unter www.sectigo.com oder folgen Sie uns auf [LinkedIn](#).

