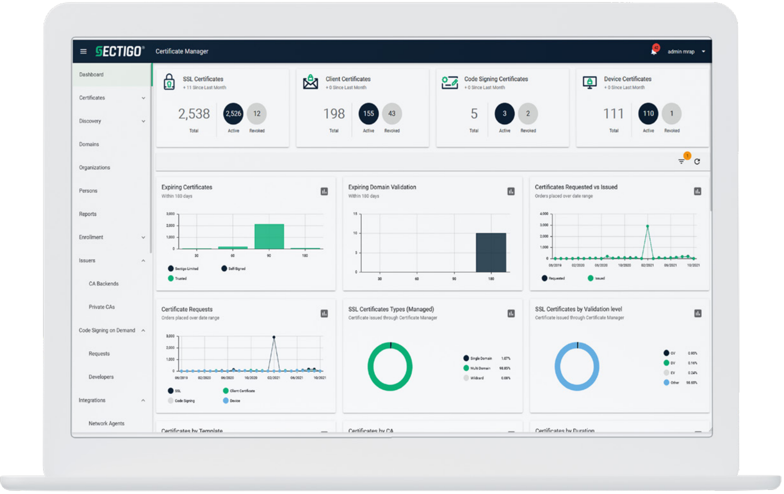
SECTIGO PRODUCT BRIEF

Sectigo Certificate Manager

CA Agnostic Certificate Lifecycle Management for the Modern Enterprise

Manage Public and Private Certificates Issued by Sectigo and Other CAs From a Single Platform.

Sectigo Certificate Manager (SCM) is an industry-leading, CA agnostic platform, purpose-built to issue and manage the lifecycles of all public and private digital certificates through a single pane of glass. SCM authenticates and secures every human and machine identity across the enterprise. Customers can automate the issuance and management of Sectigo digital certificates, alongside digital certificates originating from other public Certificate Authorities (CAs) as well as private CAs such as Microsoft Active Directory Certificate Services (ADCS), AWS Cloud Services and Google Cloud Platform (GCP).



SCM HIGHLIGHTS:

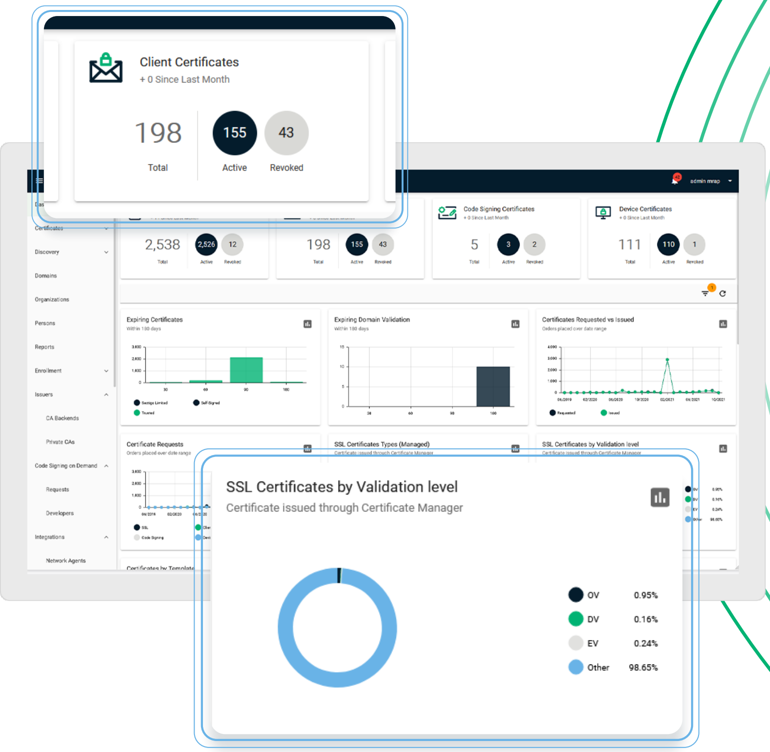
- Crypto Agility - Single pane of glass for private and public digital certificate management
- CA agnostic - Manage the full lifecycle of all digital certificates, regardless of origin
- Vendor Consolidation - Open, interoperable, and easy-to-deploy, avoiding vendor lock-in
- Automatically secure human and machine identities with a single click
- CLM in the Cloud - Lower cost of deployment, faster threat discovery, and advanced automation
- Integrations - Connect with leading technology providers for enhanced flexibility with customized environments
- Dedicated support - Industry-leading customer support with white glove service from onboarding to continued account services

PRODUCT BRIEF | Sectigo Certificate Manager

Certificate Lifecycle Management

SCM leverages Sectigo's extensive portfolio of public and private digital certificates which can be deployed to address a wide range of use cases, including:

- TLS/SSL certificates
- User certificates
- Device or machine certificates
- Document signing certificates
- Code signing certificates
- S/MIME certificates
- eIDAS certificates



SCM offers a variety of functions, enabling IT teams to manage the entire lifecycle of the diverse set of digital certificates and keys used in the enteprise.

A modern enterprise will have a wide variety of certificates addressing various use cases. These may include SSL certificates for websites and load balancers on both sides of the firewall, user certificates to authenticate employees and device certificates to authenticate their laptop or mobile device.

Development teams may have sourced their own certificates to facilitate the authentication of applications. In some cases, these certificates will have been acquired from other certificate providers by different teams and with limited oversight by IT. Enterprises now recognise the risk inherent in such an approach and see the increasing need for gaining greater visibility and control of the certificates regardless of the CA using a single CLM platform.

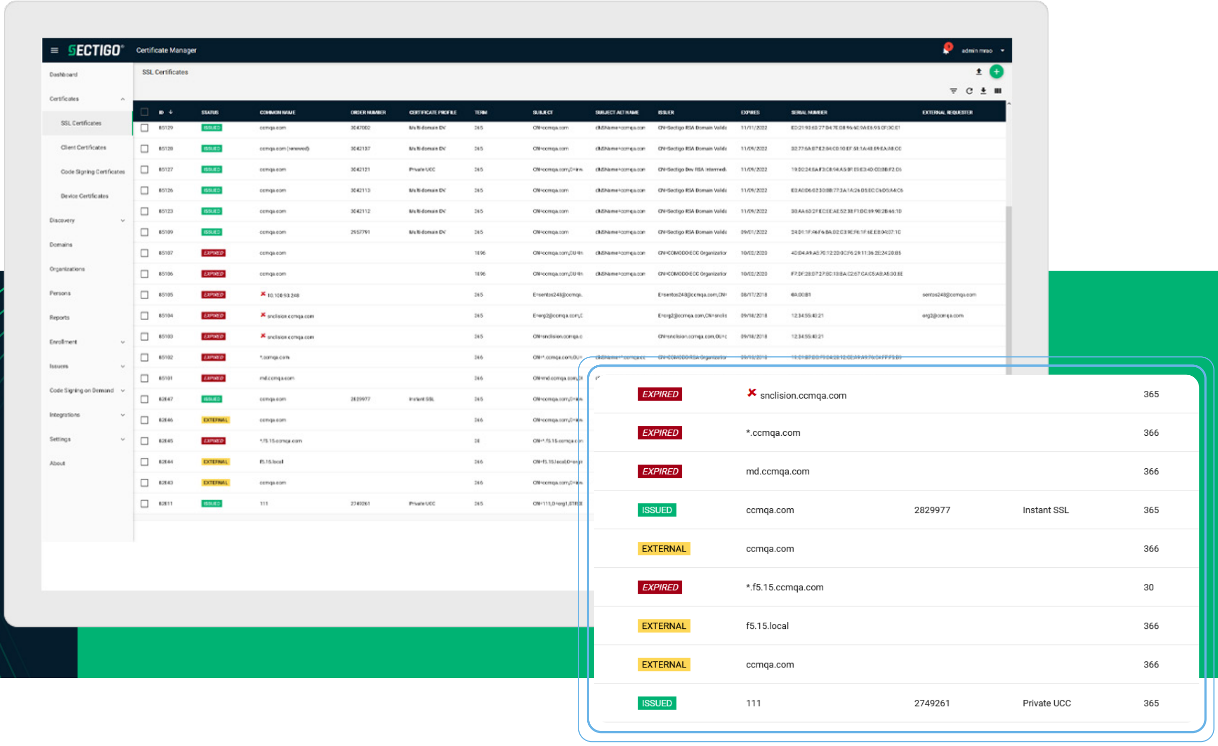
The first step in enabling crypto-agility, to establish a strong foundation of digital trust in the enterprise is to discover what certificates are already deployed.

Continuous Certificate Discovery

SCM enables the discovery of all digital certificates issued across the enterprise, enabling greater visibility into all digital certificates deployed across the network. Sectigo discovers SSL/TLS certificates originating from any CA using a port scan of the enterprise network. The discovery of digital certificates can also be achieved by directly querying other CA management platforms such as Microsoft ADCS.

SCM populates the dashboard with a list of all discovered digital certificates, providing valuable information about the status and owner of each.

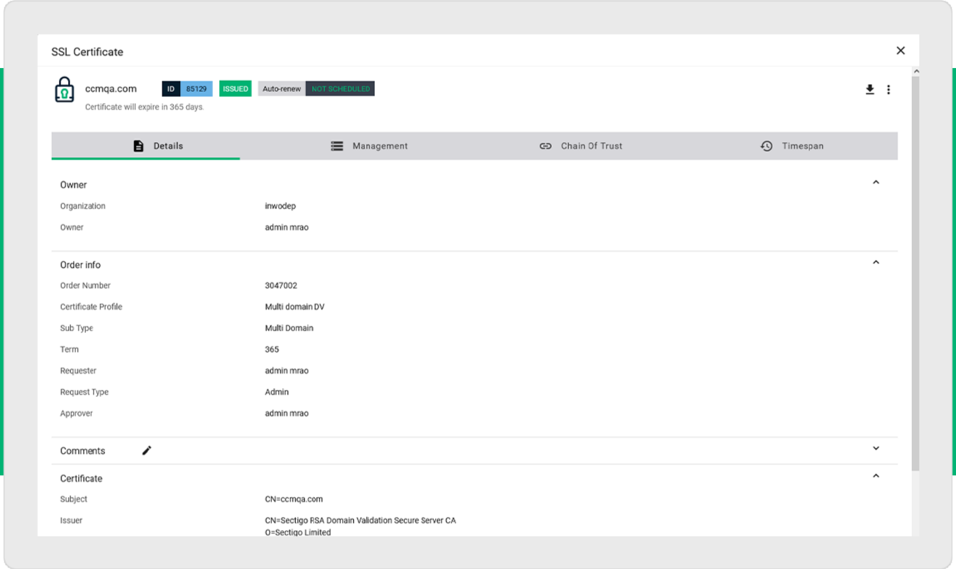
The digital certificates will be verified for compliance to the corporate policy, triggering notifications in the event a certificate is about to expire, and enabling its automatic renewal. It will also detect any humans or machines that have a digital certificate that should not. For example, a web server may be connected to the internet using a digital certificate, but without authorization.



EXPIRED	✕ snclision.ccmqa.com			365
EXPIRED	*.ccmqa.com			366
EXPIRED	md.ccmqa.com			366
ISSUED	ccmqa.com	2829977	Instant SSL	365
EXTERNAL	ccmqa.com			366
EXPIRED	*.f5.15.ccmqa.com			30
EXTERNAL	f5.15.local			366
EXTERNAL	ccmqa.com			366
ISSUED	111	2749261	Private UCC	365

Certificate Issuance

SCM enables the automated delivery and installation of digital certificates from both Public and Private CAs. This authenticates and secures the digital identities for humans and machines, driving secure communication, user authentication and encryption capabilities. In addition to Sectigo's own CA, SCM can also issue and manage digital certificates from Public CAs and from Private CAs such as Microsoft Active Directory Certificate Services (ADCS), AWS Cloud Services and Google Cloud Platform (GCP). SCM addresses all certificate issuance needs, supporting flexibility, redundancy, and compliance.



ccmqa.com ID 85129 ISSUED Auto-renew NOT SCHEDULED

Certificate will expire in 365 days.

Owner

Organization	inwodep
Owner	admin mrao

Order info

Order Number	3047002
Certificate Profile	Multi domain DV
Sub Type	Multi Domain
Term	365
Requester	admin mrao
Request Type	Admin
Approver	admin mrao

Comments

Certificate

Subject	CN=ccmqa.com

Issuer	CN=Sectigo RSA Domain Validation Secure Server CA
	O=Sectigo Limited

With SCM, users can issue and deploy digital certificates to approved users and devices replacing manual operations typically used. SCM also enables automatic renewal of digital certificates.

Technology standards that define certificates such as X.509 provide for a range of fields and values that can be leveraged to support new applications such as identification, policy management and authorisation. Most certificate lifecycle management platforms have limited ability to populate these fields, restricting their only the most basic certificate roles. Only Sectigo provides to populate and manage these fields, applying complex rulesets to control formatting and prevent duplication. It is these capabilities that help SCM enable enterprises to build complex solutions supporting modern IT operations.

Certificate Management

SCM enables the management of any X.509 in the enterprise. This includes issuance, replacement, renewal and revocation. Digital certificates can be managed manually, using the SCM UI or can be automated using built in tools and capabilities.

SCM enables the management of keys, specifically encryption key archiving, installation into authorized machines and ensures all keys are protected in either the machine's Trusted Platfrom Module (TPM) or Hardware Security Module (HSM).

SCM offers a single dashboard to view all digital certificate metrics and status across the entire enterprise. An enterprise can track and control digital certificate creation, expiration and renewal ensuring crypto-agility and creating a strong foundation of digital trust.

> “SCM's certificate lifecycle management capabilities significantly reduce manual effort, prevent human error, avoid service outages and reduce overall cost of operations.”

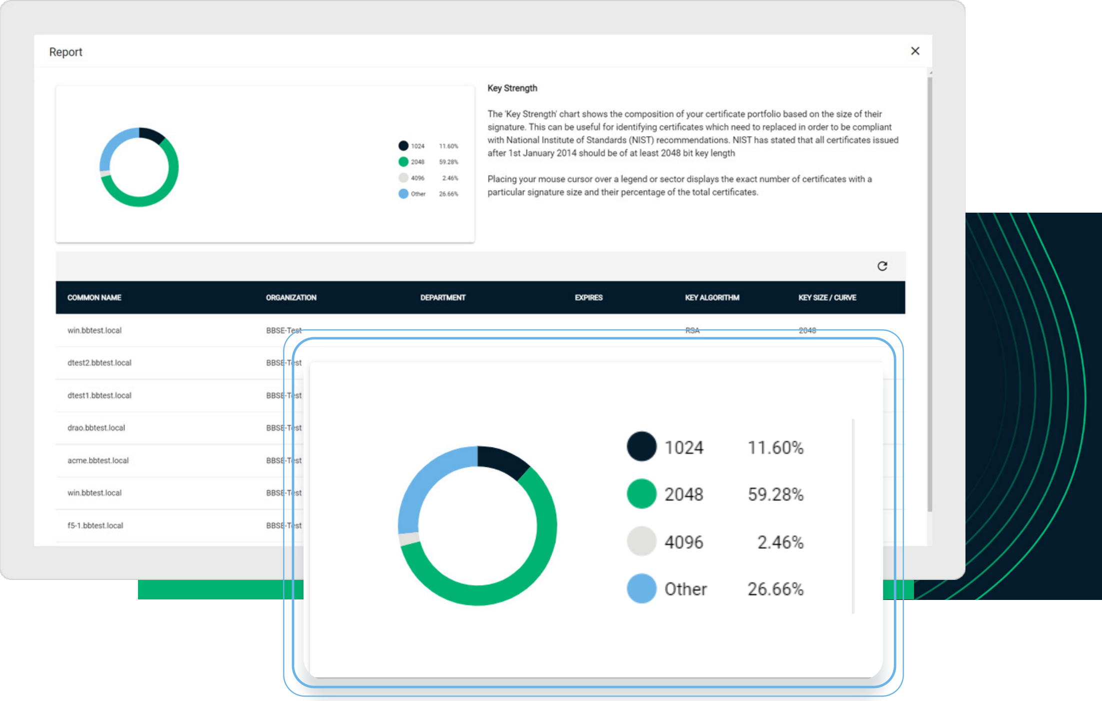
Certificate validity periods are getting shorter. SSL/TLS certificate lifespans are now required to be no longer than 13 months. Email and document signing certificates should be kept to a similar validity period to reduce risk of compromise. A digital certificate needs to be renewed before it expires to ensure continuity of service. If an enterprise only has a small number of digital certificates deployed, it may be possible to track expirations and renewals using a spreadsheet. However, as an organization scales, the task of managing the lifecycles of all digital certificates quickly becomes complex and unreliable.

Depending on manual processes to track renewals is too fraught with risk for any secure modern enterprise. IT departments must be able to visualise and quickly understand when digital certificates are expiring and take action, otherwise they may soon be dealing with the impact of a significant outage.

Certificate Governance

SCM helps organizations enforce consistent corporate policies across all digital certificates from any CA. The enterprise can define the cryptographic strength and contents of all digital certificates and enforce control by only issuing digital certificates that comply to this policy.

These same enforcement rules can be applied to digital certificates issued by other CAs and discovered by SCM. This allows the IT administrator to quickly identify digital certificates that are out of compliance.



Key Strength

The 'Key Strength' chart shows the composition of your certificate portfolio based on the size of their signature. This can be useful for identifying certificates which need to replaced in order to be compliant with National Institute of Standards (NIST) recommendations. NIST has stated that all certificates issued after 1st January 2014 should be of at least 2048 bit key length

Placing your mouse cursor over a legend or sector displays the exact number of certificates with a particular signature size and their percentage of the total certificates.

COMMON NAME	ORGANIZATION	DEPARTMENT	EXPIRES	KEY ALGORITHM	KEY SIZE / CURVE
win.bbtest.local	BBSE-Test			RSA	2048
dtest2.bbtest.local	BBSE-Test				
dtest1.bbtest.local	BBSE-Test				
drao.bbtest.local	BBSE-Test				
acme.bbtest.local	BBSE-Test				
win.bbtest.local	BBSE-Test				
f5-1.bbtest.local	BBSE-Test				

SCM's dashboard capabilities provide visibility of digital certificate status and other characteristics across the entire digital certificate inventory.

SCM includes significant reporting capabilities which can be used to facilitate audits and compliance. Having one platform with full visibility of all digital certificate activity throughout the enterprise is the only effective way of ensuring policies are being complied with. Reports can be created showing digital certificate status and activity, filtered by timeline, organization etc. This will become critical for events like quantum computing attacks, where you need to find all compromised digital certificates and replace them quickly and automatically.

SCM offers tools to help with all aspects of the certificate lifecycle including configuration, issuance, revocation, renewal, and distribution. Having one platform where all digital certificates are managed provides greater efficiencies and avoids certificate silos. SCM's modern cloud-based architecture ensures resilience, scalability, and immediate availability of the latest certificate lifecycle management capabilities.

Key Management

SCM archives private keys so that encrypted files and email can be decrypted in case the private key is accidentally destroyed or the enterprise needs access to files encrypted by the employee. The platform provides complete access control with detailed key logs for monitoring and auditing purposes to ensure the proper use of keys.

SCM automates the management process of encryption key lifecycles including key generation, key storage, and key deletion. It also automatically installs the encryption key on devices the user uses to decrypt files and emails. SCM protects the archived key from being accidentally disclosed to an unauthorized user.

With the SCM cloud-hosted platform, enterprises can scale to create and manage a portfolio of encryption keys directly from a single platform.

Certificate Use Cases

Digital certificates underpin many use cases in the modern enterprise. SSL/TLS certificates are well understood and essential to the functioning of modern cloud and web-based solutions. But there are many other applications of digital certificates that further increase the scope and scale required by a certificate lifecycle management solution. As enterprises implement new certificate-based solutions including DevOps services, Robotic Process Automation, passwordless authentication, document signing and email encryption, the number of digital certificates under management will increase significantly, placing certificate lifecycle management at the core of IT operations.

Server Certificates

In today's enterprise, the combination of the increased number of servers and more complex networks has driven the need for a modern approach to automating the lifecycle management of enterprise SSL certificates on both sides of the firewall. Certificates are also required for load balancers, a critical component of scaled web infrastructure. SCM simplifies the task by providing an automated SSL certificate management solution for every server and load balancer across your environment.

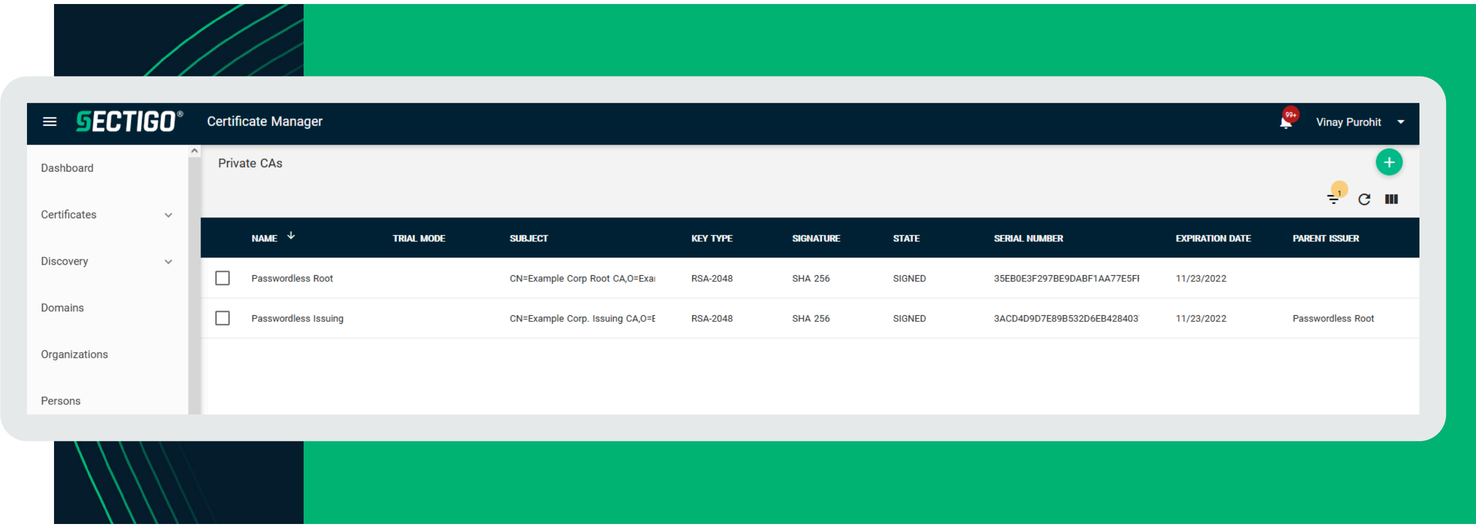
Machine Certificates

The enterprise has many machines needing to authenticate themselves and then encrypt the communication. SCM can both create those digital certificates and then automate the install and renewal. Examples include:

- DevOps micro-services
- Robotic Process Automation
- Devices connecting to the network, wired or Wi-Fi

Passwordless Authentication

Digital certificates offer the potential for replacing passwords and one-time-passwords as the primary form of user and device authentication. SCM automates the deployment of digital certificates across the enterprise resulting in cost savings, reduced IT overhead and better security. All machines manufactured since 2016 embed TPM capabilities which protect the private key from being replicated to another machine. This includes Windows, Mac, iOS, Android, and Chromebooks. SCM will requires key to be stored and renewed in this HW, so not only do you know it is the authorized user, but it is also the authorized device. This results in eliminating the password, enabling authentication for Zero Trust Network Access, and allowing windows login without a password.

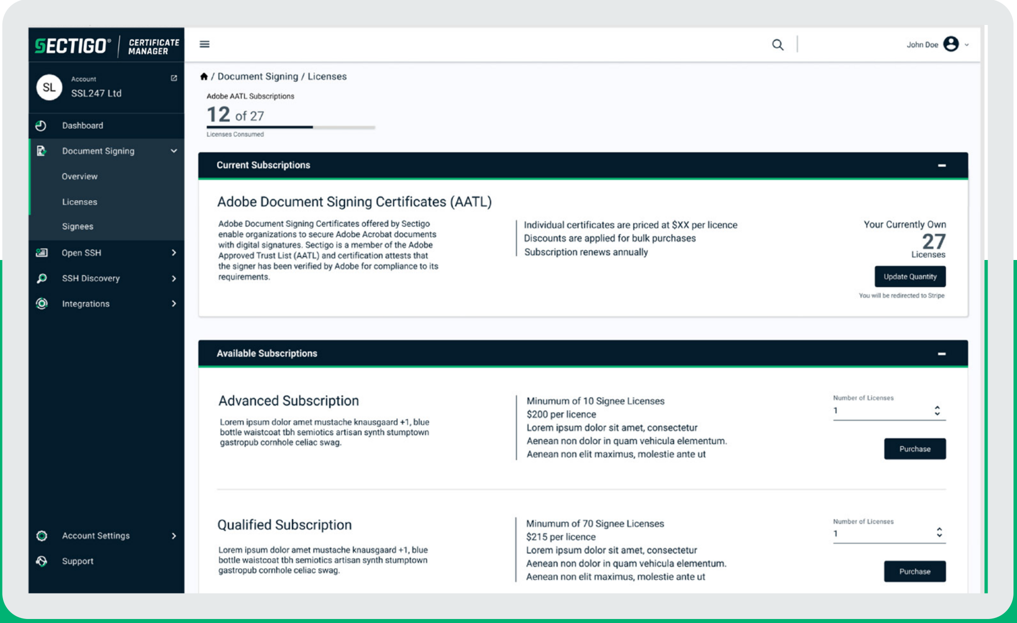


Private CAs

	NAME ↓	TRIAL MODE	SUBJECT	KEY TYPE	SIGNATURE	STATE	SERIAL NUMBER	EXPIRATION DATE	PARENT ISSUER
□	Passwordless Root		CN=Example Corp Root CA,O=Exa	RSA-2048	SHA 256	SIGNED	35EB0E3F297BE9DABF1AA77E5F	11/23/2022	
□	Passwordless Issuing		CN=Example Corp. Issuing CA,O=E	RSA-2048	SHA 256	SIGNED	3ACD4D9D7E89B532D6EB428403	11/23/2022	Passwordless Root

Document Signing

Digital signatures for documents are becoming mandatory for many transactions and offer a compelling approach to reducing business fraud while improving the productivity of employees working from home. Certificate lifecycle management is an essential element in a document signing solution and SCM provides mechanisms to help scale document signing across an entire business. Digital Signatures are no longer limited to finance and legal departments but can be easily leveraged by individuals at every level in the organization. Sectigo's document signing certificates save enterprises money while providing a more resilient information transfer infrastructure. These signatures are trusted by Adobe PDF reader anywhere in the world.



/ Document Signing / Licenses

Adobe AATL Subscriptions

12 of 27

Licenses Consumed

Current Subscriptions

Adobe Document Signing Certificates (AATL)

Adobe Document Signing Certificates offered by Sectigo enable organizations to secure Adobe Acrobat documents with digital signatures. Sectigo is a member of the Adobe Approved Trust List (AATL) and certification attests that the signer has been verified by Adobe for compliance to its requirements.

Individual certificates are priced at $XX per licence
Discounts are applied for bulk purchases
Subscription renews annually

Your Currently Own
27
Licenses

You will be redirected to Stripe

Available Subscriptions

Advanced Subscription

Lorem ipsum dolor amet mustache knausgaard +1, blue bottle waistcoat tbh semiotics artisan synth stumptown gastropub cornhole celiac swag.

Minumum of 10 Signee Licenses
$200 per licence
Lorem ipsum dolor sit amet, consectetur
Aenean non dolor in quam vehicula elementum.
Aenean non elit maximus, molestie ante ut

Number of Licenses: 1

Qualified Subscription

Lorem ipsum dolor amet mustache knausgaard +1, blue bottle waistcoat tbh semiotics artisan synth stumptown gastropub cornhole celiac swag.

Minumum of 70 Signee Licenses
$215 per licence
Lorem ipsum dolor sit amet, consectetur
Aenean non dolor in quam vehicula elementum.
Aenean non elit maximus, molestie ante ut

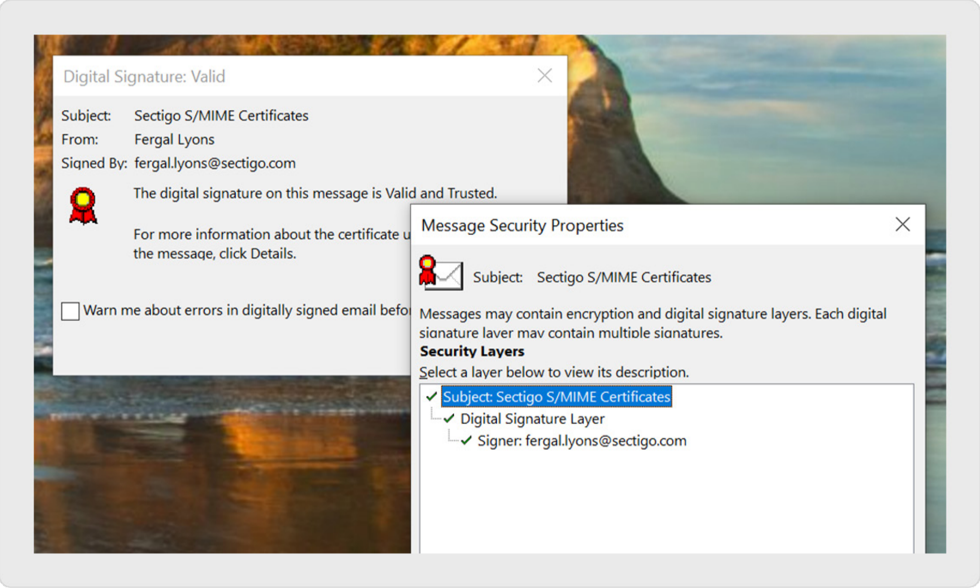
Number of Licenses: 1

The European eIDAS standard for qualified trust services is leading to broader usage of signed and sealed documents between European companies. Sectigo offers eIDAS compatible digital certificates as a QTSP (Qualified Trust Service Provider). These can also be managed via SCM.

Email Security

Email security is becoming increasingly important for compliance with privacy regulations such as GDPR and HIPAA. Enterprises can secure corporate email accounts by digitally signing and encrypting communications with Secure/Multipurpose Internet Mail Extensions (S/MIME) email certificates. These types of certificates validate the digital identity of the user and encrypt and decrypt emails and attachments. Sectigo's secure enterprise email certificates are supported by all the major email providers and mail applications, including Microsoft Outlook, Exchange, Gmail, popular mobile operating systems, and more.

Sectigo offers automated S/MIME encryption to simplify the deployment of user certificates across the enterprise. With SCM, IT professionals can seamlessly deploy and maintain email certificates for any user across any device - all with a single click.



Digital Signature: Valid

Subject: Sectigo S/MIME Certificates
From: Fergal Lyons
Signed By: fergal.lyons@sectigo.com

The digital signature on this message is Valid and Trusted.

For more information about the certificate u
the message, click Details.

□ Warn me about errors in digitally signed email befo

Message Security Properties

Subject: Sectigo S/MIME Certificates

Messages may contain encryption and digital signature layers. Each digital signature layer may contain multiple signatures.

Security Layers

Select a layer below to view its description.

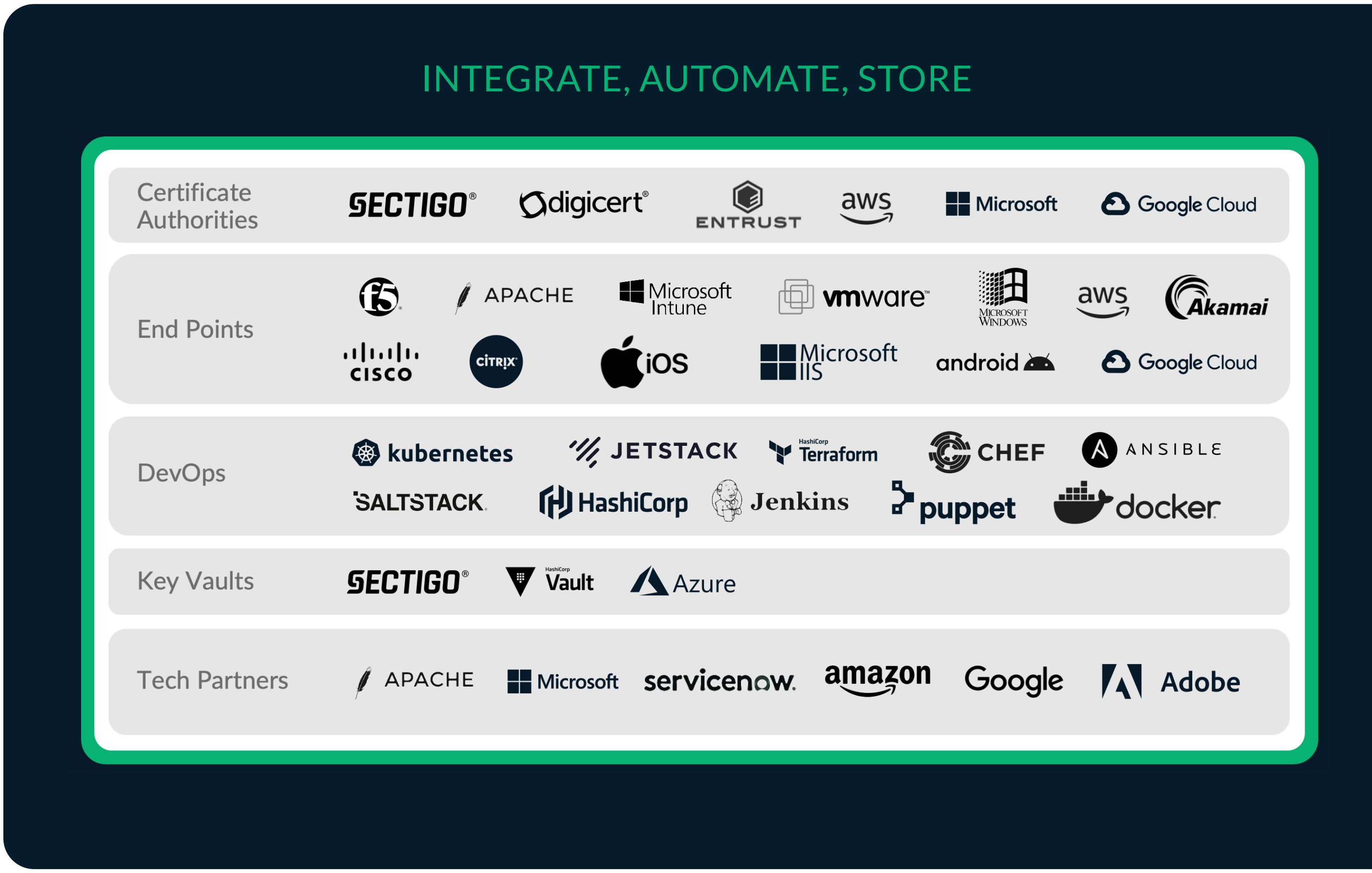
✓ Subject: Sectigo S/MIME Certificates
  ✓ Digital Signature Layer
    ✓ Signer: fergal.lyons@sectigo.com

Integrations

SCM has integrations with all the popular application used within the enterprise. Some examples:

- DevOps containerization & orchestration tools.
- Automation standards to integrate with applications using that same standard, such as Universal Endpoint Managers & networking gear using SCEP, IoT devices using RFC 7030 and ACME.
- Cloud vendor applications such as AWS Certificate Manager, CloudFront, Elastic Load Balancer, Azure Key Vault.

These integrations automate certificate deployment and compliance


INTEGRATE, AUTOMATE, STORE

Subscription Pricing

ensuring alignment of your certificate strategy across the enterprise.

Sectigo offers subscription pricing, where customers pay for the certificate subscription term rather than per issuance. SCM subscription provides the customer the freedom to issue certificates with any lifetime and change what human or device the certificate is used for. For example a customer could:

- Issue 52 one-week certificates in sequence
- Issue a one-year certificate
- Issue a certificate for a new or replacement employee with no additional fees

The subscription can bundle the digital certificate and certificate management/automation to provide an even greater value to the customer, eliminating the need for a more expensive CLM vendor.

An optional Enterprise Subscription model allows for growth in the number of active certificates without the need for additional purchases.

About Sectigo

Sectigo is a leading provider of digital certificates and automated certificate lifecycle management solutions to leading brands globally. As one of the longest-standing and largest Certificate Authorities (CA), Sectigo has over 20 years of experience delivering innovative security solutions to over 700,000 businesses worldwide. Sectigo is the leading certificate lifecycle management provider supporting multiple CA vendors and integrating with the largest software ecosystems in the world.