

SECTIGO PRODUCT BRIEF

Sectigo Certificate Manager

CA Agnostic Certificate Lifecycle Management for the Modern Enterprise

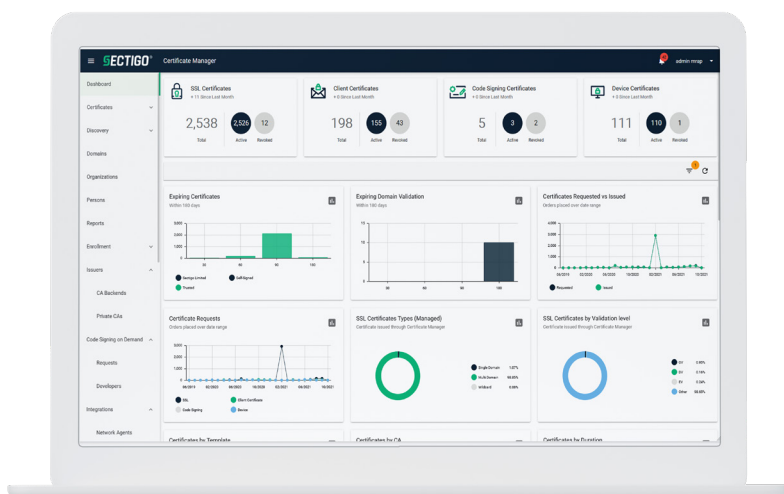
Manage Public and Private Certificates Issued by Sectigo and Other CAs From a Single Platform.

Sectigo Certificate Manager (SCM) is a universal platform, purpose-built to issue and manage the lifecycle of public and private digital certificates to secure every human and machine identity across the enterprise, all from a single platform. With SCM, customers can automate the issuance and management of Sectigo certificates, alongside their certificates from other publicly trusted Certificate Authorities (CAs) and private CAs, like Microsoft Active Directory Certificate Services.



SCM HIGHLIGHTS:

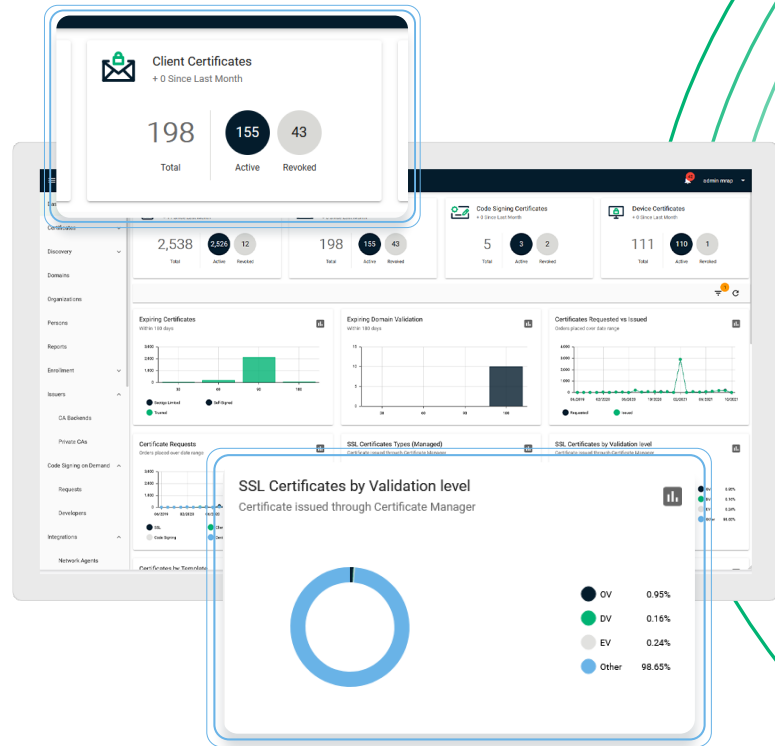
- ✓ Industry-leading certificate portfolio
- ✓ Modern cloud deployment for instant setup and lower operating costs using audited industry best practices
- ✓ Integrations with popular enterprise applications
- ✓ Provides 100% automation for customer's Active Directory Certificate Services
- ✓ CA agnostic to issue and manage certificates from other public and private CAs
- ✓ Operates multiple CAs to maintain redundancy and quickly implement automation for existing certificates
- ✓ Automated certificate and key installation and renewal
- ✓ Enables new and emerging certificate-based use cases
- ✓ Single platform management across all X.509 and SSH certificates



Certificate Lifecycle Management

SCM leverages Sectigo's extensive portfolio of public and private certificates which can be employed to address an extensive 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
- SSH certificates



SCM offers a variety of functions to manage the entire lifecycle of the diverse set of certificates and keys used in the enterprise.

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 under a single CLM platform.

The first step in getting control of certificates in the enterprise is to find what certificates are already active.

Continuous Certificate Discovery

SCM provides discovery of certificates throughout the enterprise enabling greater visibility into certificate assets deployed in the network. Sectigo discovers SSL/TLS certificates from any CA using a port scan, and certificates of any type issued by ADCS. Additional discovery mechanisms will be added in upcoming releases.

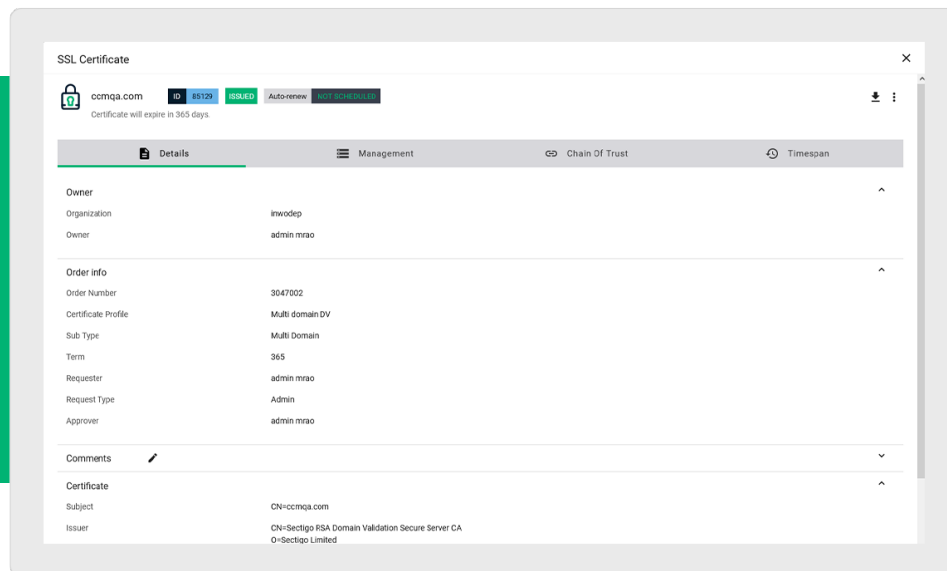
SCM populates the dashboard with a list of discovered certificates, providing valuable information about the status and owner of each certificate.

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

| ID | Status | Issuer | Subject | Validity | Details |
|-------|---------|---------------------|---------------------|---------------------|---------|
| 80100 | EXPIRED | scnclison.ccmqa.com | scnclison.ccmqa.com | 1/1/2022 - 1/1/2023 | 2829977 |
| 80101 | EXPIRED | *.ccmqa.com | *.ccmqa.com | 1/1/2022 - 1/1/2023 | 365 |
| 80102 | EXPIRED | md.ccmqa.com | md.ccmqa.com | 1/1/2022 - 1/1/2023 | 366 |
| 80103 | EXPIRED | *.fs.15.ccmqa.com | *.fs.15.ccmqa.com | 1/1/2022 - 1/1/2023 | 30 |
| 80104 | EXPIRED | fs.15.local | fs.15.local | 1/1/2022 - 1/1/2023 | 366 |
| 80105 | EXPIRED | ccmqa.com | ccmqa.com | 1/1/2022 - 1/1/2023 | 366 |
| 80106 | ISSUED | 111 | Private UCC | 1/1/2022 - 1/1/2023 | 365 |

Certificate Issuance

SCM provides automated delivery and installation of certificates from Public and Private CAs. This enables digital identities for humans and machines, driving secure communication, user authentication and encryption capabilities. SCM can also issue certificates from 3rd party CAs such as MSCA. It addresses all certificate issuance needs, supporting flexibility, redundancy, and compliance.



With SCM, users can issue and deploy certificates to approved users and devices replacing manual operations typically used to install the certificate. SCM also enables automatic renewal of 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 management platforms have only limited ability to populate these fields, restricting their value to management of only the most basic certificate roles. Only Sectigo provides comprehensive capabilities 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 provides management of any X.509 or SSH certificate in the enterprise. This includes issuance, replacement, renewal and revocation. Certificates can be managed manually, using the SCM UI or can be automated using built in tools and capabilities.

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

SCM offers a single dashboard to view all certificate metrics and status across the entire enterprise. An enterprise can track and control certificate creation, expiration and renewal ensuring ongoing manageability of certificate resources.

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

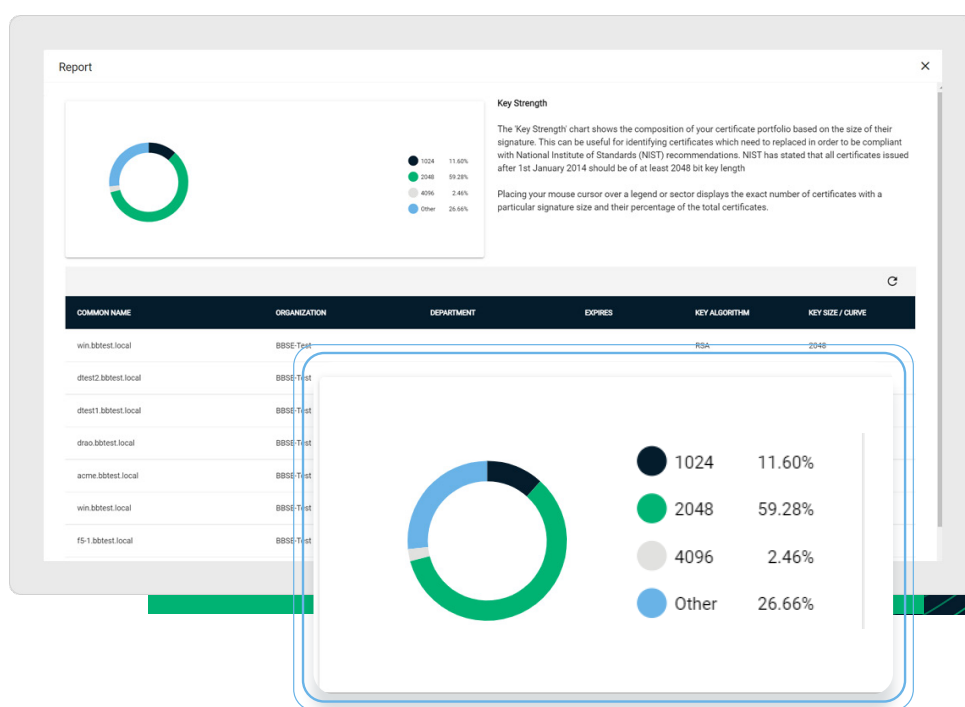
Certificate validity periods are getting shorter throughout the industry. SSL/TLS certificates are now required to be no longer than 13 months. Email and document signing certificates should be kept to a similar validity schedule to reduce risk of compromise. A certificate needs to be renewed before it expires to ensure continuity of service. If an enterprise only has a small number of certificates, it may be possible to track expirations and renewals using a spreadsheet. But very quickly the task 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 certificates are expiring and take action, otherwise they may soon be dealing with the impact of a significant outage.

Certificate Governance

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

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



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

SCM includes significant reporting capabilities which can be used to facilitate audits and compliance. Having one platform with full visibility of all certificate activity throughout the enterprise is the only effective way of ensuring policies are being complied with. Reports can be created showing 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 certs 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 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 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

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 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 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 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

Code Signing on Demand

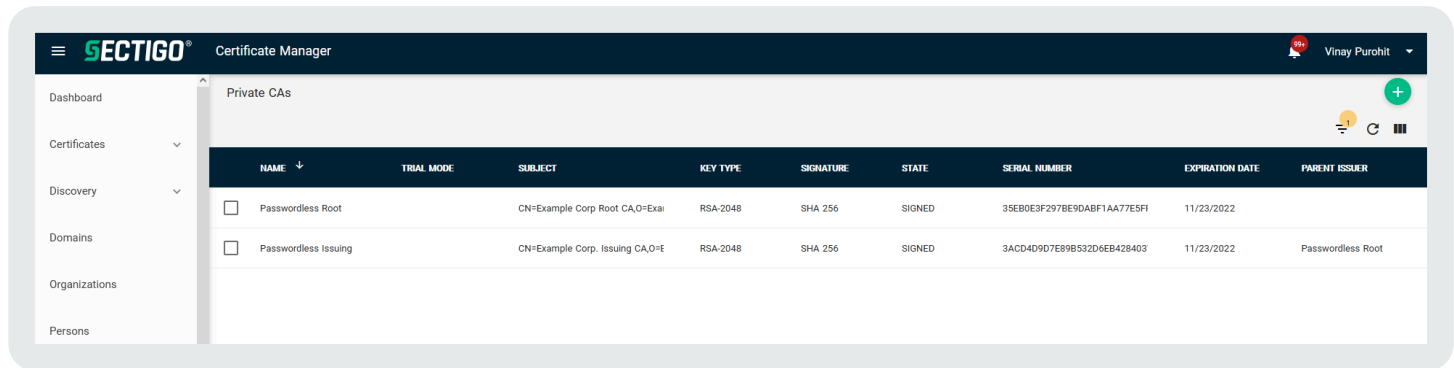
Modern development organizations have complex certificate demands driven by rapid development cycles and software containerization. SCM provides a flexible and responsive certificate-based solution for Code Signing, enabling applications to be signed on demand and at scale.

This could be signing an application delivered to your customers or signing the code running in a DevOps container. Signing code reduces the possibility of rogue code from unapproved providers being deployed in the enterprise.

| Sectigo Certificate Manager | | | | | | | | | | |
|-----------------------------|----------|--------------|---------------------|------|----------------------|-----------------------|------------|----------------------|----------------|------------|
| Code Signing Certificates | | | | | | | | | | |
| | STATUS | ORDER NUMBER | CERTIFICATE PROFILE | TERM | REQUESTED VIA | SUBJECT | EXPIRES | SERIAL NUMBER | ORGANIZATION | DEPARTMENT |
| <input type="checkbox"/> | EXPIRED | | SECTIGO Publ... | 365 | Discovery | | 04/02/2020 | 68:00:00:00:26:14... | Solidude Inc | |
| <input type="checkbox"/> | REVOKED | 499059076 | SECTIGO Publ... | 365 | PKCS10 | CN=Comodo CA Ltd... | 08/06/2022 | 4D:81:4E:D7:04:75... | Comodo CA Ltd. | |
| <input type="checkbox"/> | REJECTED | 265675455 | SECTIGO Publ... | 1 | Signed Public Key an | | | | Comodo SE | |
| <input type="checkbox"/> | REVOKED | 257235377 | SECTIGO Publ... | 1 | Signed Public Key an | CN=Comodo CA Ltd... | 07/08/2020 | 35:4A:35:6A:77:8C... | Comodo CA Ltd. | |
| <input type="checkbox"/> | REVOKED | 447905453 | SECTIGO Publ... | 365 | PKCS10 | CN=Sectigo,O=Secti... | 09/02/2022 | 27:F1:6F:8D:0B:F2... | Sectigo | |
| <input type="checkbox"/> | INVITED | | SECTIGO Publ... | 1 | PKCS10 | | | | Comodo CA Ltd. | |
| <input type="checkbox"/> | EXPIRED | 271927388 | SECTIGO Publ... | 1 | PKCS10 | CN=Comodo CA Ltd... | 25/09/2020 | D2:3A:4D:D6:3B:BE... | Comodo CA Ltd. | |
| <input type="checkbox"/> | APPLIED | 819276573 | Code Signing | 365 | PKCS10 | | | | Sectigo | |
| <input type="checkbox"/> | INIT | | Code Signing | 365 | PKCS10 | | | | Sectigo | |

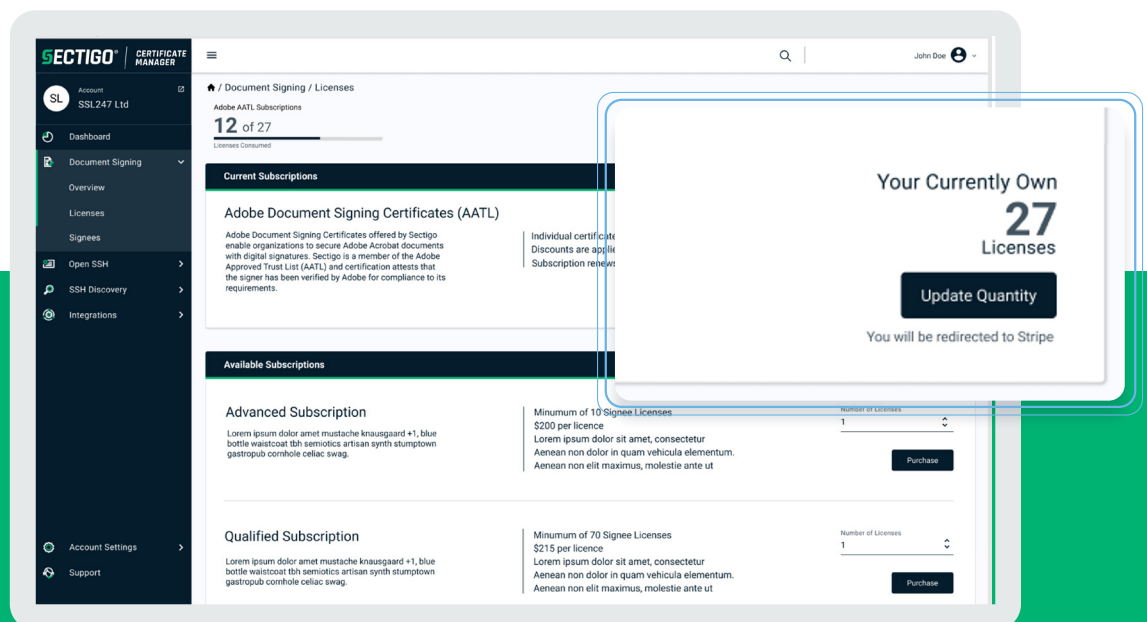
Passwordless Authentication

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 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 force the 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. All while eliminating the password, enabling authentication for Zero Trust Network Access, and allowing windows login without a password.



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 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 solution saves enterprises money while providing a more resilient information transfer infrastructure. These signatures are trusted by Adobe PDF reader anywhere in the world.

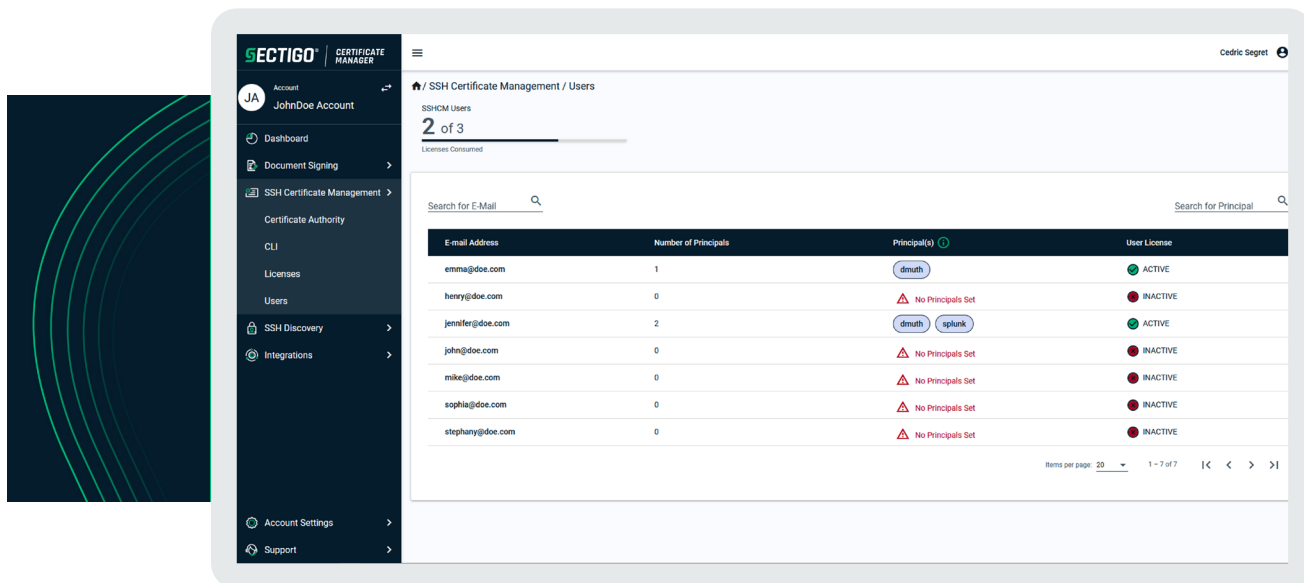


The European eIDAS standard for qualified trust services is leading to broader usage of signed and sealed documents between European companies. Sectigo offers eIDAS compatible certificates as a QTSP (Qualified Trust Service Provider). These can also be managed via SCM.

SSH Certificates

Certificate-based SSH authentication provides tremendous benefits over traditional key based approaches. SCM provides the tools to create and distribute SSH certificates resulting in clear advantages for the enterprise including reduced costs, controlled validity periods and a simple revoke and replace process. Better yet, it works with the OpenSSH product you already have deployed.

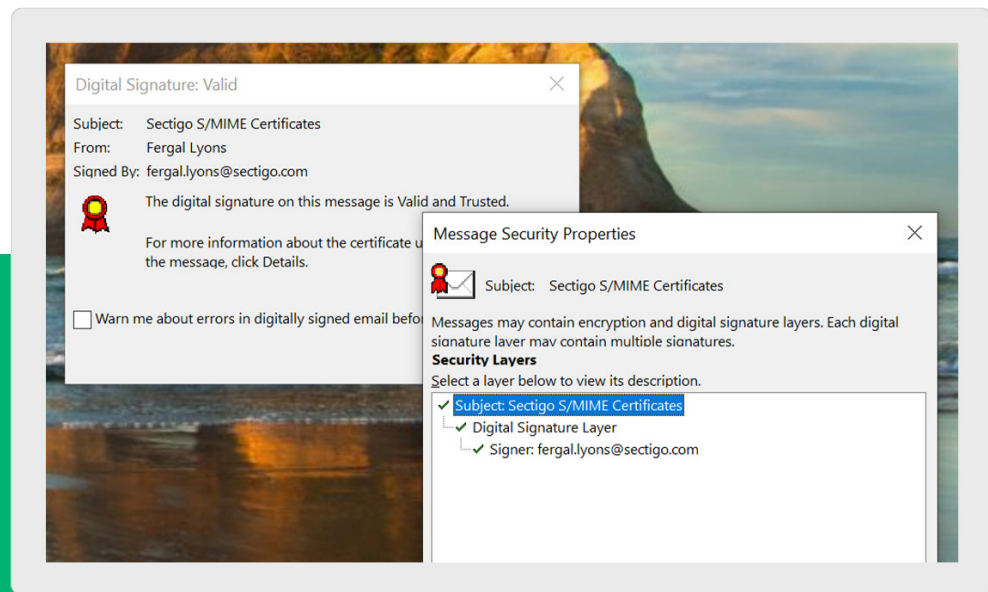
Investing in certificate based SSH authentication will save any organization from numerous headaches and pitfalls.



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 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 Zero-Touch 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.



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 ensuring alignment of your certificate strategy across the enterprise.

INTEGRATE, AUTOMATE, STORE

Tech Partners   Microsoft  Adobe  f5  APACHE  CITRIX  servicenow.

Endpoints  MCM Portal  iOS  Microsoft Intune  aws  Google Cloud  vmware  android

DevOps  HashiCorp  kubernetes  Terraform  Jenkins  CHEF
 SALTSTACK  JETSTACK  puppet  ANSIBLE  docker

Key Vaults  Azure  Google  aws

Mail  

Standards  ACME  {REST:API}  SCEP  EST  X.509  eIDAS

Subscription Pricing

SCM subscription provides the customer the freedom to issue certificates with any lifetime and change what human or device the certificate subscription is used for. For example:

- issue 52 one-week certificate in sequence
- issue a one-year certificate
- issue a certificate for the replacement employee with no additional fees

The subscription can bundle the 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.