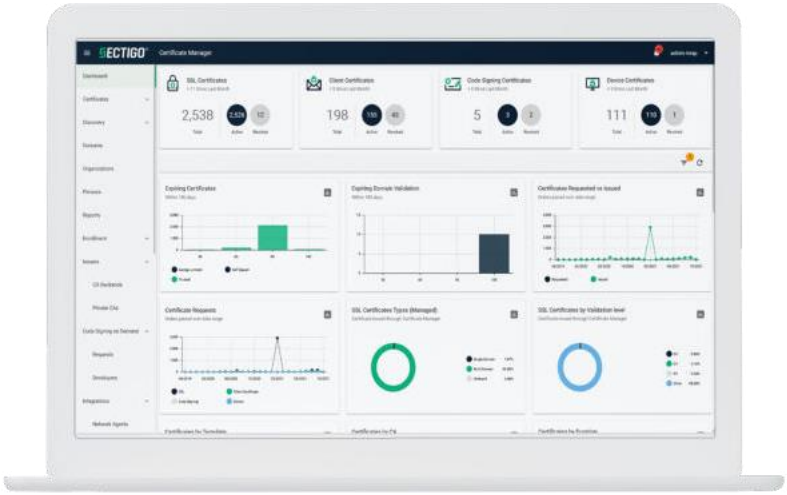
SECTIGO PRODUKTÜBERSICHT

Sectigo Zertifikatsmanagement

CA-unabhängiges Lebenszyklus-Management von Zertifikaten Management für das moderne Unternehmen

Verwalten Sie öffentliche und private Zertifikate, die von Sectigo und anderen CAs ausgestellt wurden, über eine einzige Plattform.

Sectigo Certificate Manager (SCM) ist eine branchenführende, von Zertifizierungsstellen unabhängige Plattform, speziell zur Ausstellung und Verwaltung der Lebenszyklen aller öffentlichen und privaten digitalen Zertifikate. SCM authentifiziert und sichert jede menschliche und maschinelle Identität im gesamten Unternehmen. Kunden können die Ausstellung und Verwaltung digitaler Zertifikate von Sectigo ebenso wie digitale Zertifikate anderer öffentlicher Zertifizierungsstellen (CAs) und privater CAs wie Microsoft Active Directory Certificate Services (ADCS), AWS Cloud Services und Google Cloud Platform (GCP) automatisieren.



SCM HIGHLIGHTS:

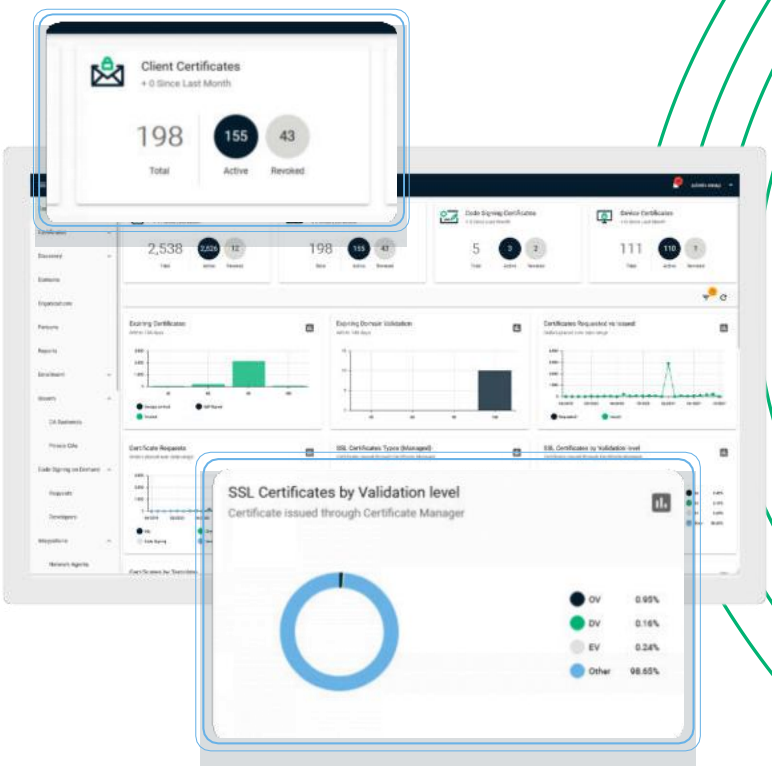
- Crypto Agility - Eine einzige Konsole für die Verwaltung privater und öffentlicher digitaler Zertifikate
- CA-unabhängig - Verwalten Sie den gesamten Lebenszyklus aller digitalen Zertifikate, unabhängig von ihrer Herkunft
- Konsolidierung von Anbietern - Offen, interoperabel und einfach zu implementieren, um sich nicht dauerhaft an einen Anbieter binden zu müssen
- Automatischer Schutz von menschlichen und maschinellen Identitäten mit einem einzigen Klick
- CLM in der Cloud - Niedrigere Bereitstellungskosten, schnellere Erkennung von Bedrohungen und erweiterte Automatisierung
- Integrationen - Verbinden Sie sich mit führenden Technologieanbietern, um mehr Flexibilität mit maßgeschneiderten Umgebungen zu erreichen
- Engagierter Support - Branchenführender Kundensupport mit "White Glove"-Service vom Onboarding bis zu fortlaufenden Kunden-Services

axians SECTIGO®

Lebenszyklus-Management von Zertifikaten

SCM macht sich das umfangreiche Portfolio öffentlicher und privater digitaler Zertifikate von Sectigo zunutze, die für eine Vielzahl von Anwendungsfällen eingesetzt werden können, darunter:

- TLS/SSL-Zertifikate
- Benutzer-Zertifikate
- Geräte- oder Maschinenzertifikate
- Zertifikate zur Unterzeichnung von Dokumenten
- Code-Signatur-Zertifikate
- S/MIME-Zertifikate
- eIDAS-Zertifikate



SCM bietet eine Vielzahl von Funktionen, die es IT-Teams ermöglichen, den gesamten Lebenszyklus der verschiedenen im Unternehmen verwendeten digitalen Zertifikate und Schlüssel zu verwalten.

Ein modernes Unternehmen verfügt über eine Vielzahl von Zertifikaten für verschiedene Anwendungsfälle.

Dazu gehören SSL-Zertifikate für Websites und Load Balancer auf beiden Seiten der Firewall, Benutzerzertifikate zur Authentifizierung von Mitarbeitern und Gerätezertifikate zur Authentifizierung ihres Laptops oder mobilen Geräts.

Entwicklungsteams haben möglicherweise ihre eigenen Zertifikate beschafft, um die Authentifizierung von Anwendungen zu erleichtern.

In einigen Fällen wurden diese Zertifikate von anderen Zertifikatsanbietern von verschiedenen Teams und mit begrenzter Aufsicht durch die IT-Abteilung erworben. Unternehmen erkennen nun das Risiko, das mit einem solchen Ansatz verbunden ist, und sehen die zunehmende Notwendigkeit, eine größere Transparenz und Kontrolle über die Zertifikate zu erlangen, unabhängig von der Zertifizierungsstelle und unter Verwendung einer einzigen CLM-Plattform.

Der erste Schritt zur Ermöglichung von Krypto-Agilität und zur Schaffung einer soliden Grundlage für digitales Vertrauen im Unternehmen besteht darin, herauszufinden, welche Zertifikate bereits im Einsatz sind.

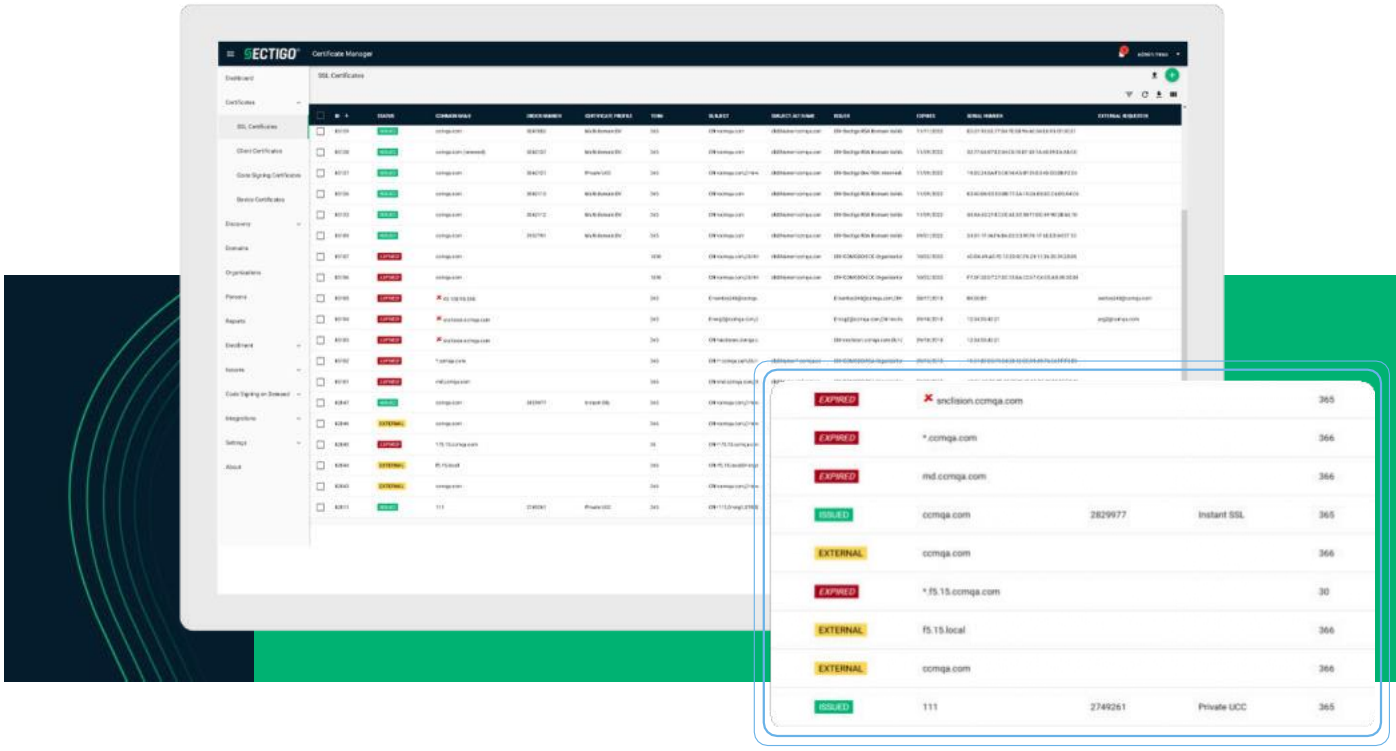
Kontinuierliche Erkennung von Zertifikaten

SCM ermöglicht die Erkennung aller digitalen Zertifikate, die im gesamten Unternehmen ausgestellt wurden, und verschafft so einen besseren Einblick in alle digitalen Zertifikate, die im Netzwerk eingesetzt werden. Sectigo erkennt SSL/TLS-Zertifikate, die von einer beliebigen CA stammen, durch einen Port-Scan des Unternehmensnetzwerks. Die Suche nach digitalen Zertifikaten kann auch durch direkte Abfrage anderer CA-Verwaltungsplattformen wie Microsoft ADCS erfolgen.

SCM füllt das Dashboard mit einer Liste aller gefundenen digitalen Zertifikate, die wertvolle Informationen über den Status und den Besitzer jedes Zertifikats enthält.

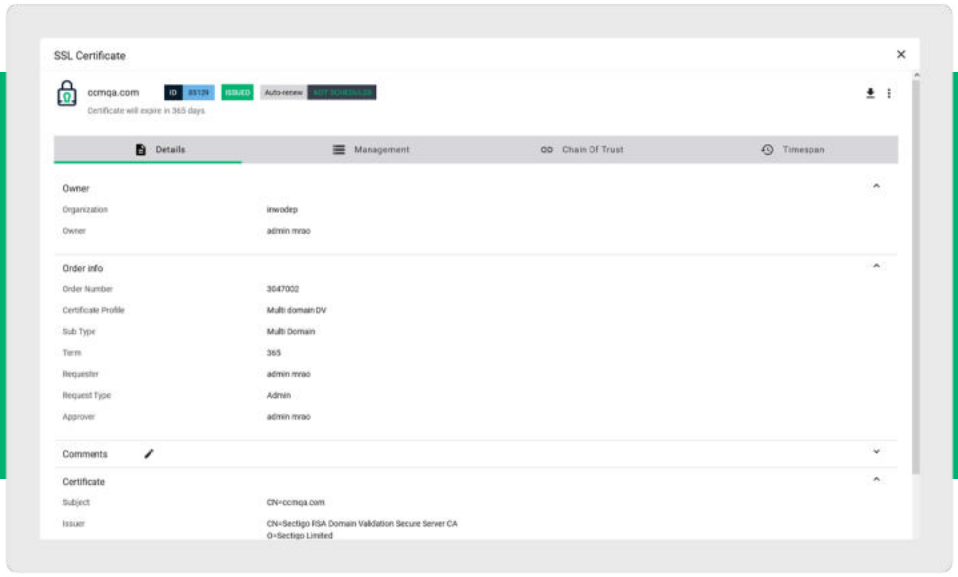
Die digitalen Zertifikate werden auf ihre Übereinstimmung mit den Unternehmensrichtlinien überprüft, wobei Benachrichtigungen ausgelöst werden, wenn ein Zertifikat abläuft, und seine automatische Erneuerung ermöglicht wird. Außerdem werden alle Menschen oder Maschinen ermittelt, die ein digitales Zertifikat besitzen, das sie nicht besitzen sollten. Zum Beispiel,

ein Webserver kann mit Hilfe eines digitalen Zertifikats mit dem Internet verbunden werden, jedoch ohne Autorisierung.



Ausstellung von Zertifikaten

SCM ermöglicht die automatische Bereitstellung und Installation digitaler Zertifikate von öffentlichen und privaten CAs. Dadurch werden die digitalen Identitäten von Menschen und Maschinen authentifiziert und gesichert, was eine sichere Kommunikation, Benutzerauthentifizierung und Verschlüsselungsfunktionen gewährleistet. Neben der eigenen CA von Sectigo kann SCM auch digitale Zertifikate von öffentlichen CAs und privaten CAs wie Microsoft Active Directory Certificate Services (ADCS), AWS Cloud Services und Google Cloud



Platform (GCP) ausstellen und verwalten. SCM erfüllt alle Anforderungen an die Ausstellung von Zertifikaten und unterstützt Flexibilität, Redundanz und Compliance.

Mit SCM können Benutzer digitale Zertifikate für zugelassene Benutzer und Geräte ausstellen und bereitstellen und so die sonst üblichen manuellen Vorgänge ersetzen. SCM ermöglicht auch die automatische Erneuerung von digitalen Zertifikaten.

Technologiestandards, die Zertifikate wie X.509 definieren, bieten eine Reihe von Feldern und Werten, die zur Unterstützung neuer Anwendungen wie Identifizierung, Richtlinienverwaltung und Autorisierung genutzt werden können. Die meisten Plattformen für die Verwaltung des Lebenszyklus von Zertifikaten haben nur begrenzte Möglichkeiten, diese Felder auszufüllen, und beschränken sich auf die grundlegendsten Zertifikatsrollen. Nur Sectigo bietet die Möglichkeit, diese Felder zu füllen und zu verwalten und dabei komplexe Regeln anzuwenden, um die Formatierung zu kontrollieren und Doppelarbeit zu vermeiden. Dank dieser Fähigkeiten ist SCM in der Lage, komplexe Lösungen zu entwickeln, die den modernen IT-Betrieb unterstützen.

Zertifikatsmanagement

SCM ermöglicht die Verwaltung aller X.509-Standardzertifikate im Unternehmen. Dazu gehören Ausstellung, Ersatz, Erneuerung und Aufhebung von Zertifikaten. Digitale Zertifikate können manuell über die SCM-Benutzeroberfläche verwaltet oder mithilfe integrierter Tools und Funktionen automatisiert werden.

SCM ermöglicht die Verwaltung von Schlüsseln, insbesondere die Archivierung von Verschlüsselungsschlüsseln sowie die Installation in autorisierten Rechnern, und stellt sicher, dass alle Schlüssel entweder im Trusted Platfrom Module (TPM) oder im Hardware Security Module (HSM) des Rechners geschützt sind.

SCM bietet ein einziges Dashboard, um alle Metriken und den Status digitaler Zertifikate im gesamten Unternehmen anzuzeigen. Unternehmen können die Erstellung, den Ablauf und die Erneuerung von digitalen Zertifikaten nachverfolgen und kontrollieren und somit die Krypto-Agilität sicherstellen und eine solide Grundlage für digitales Vertrauen schaffen.

> “Die SCM-Funktionen zur Verwaltung des Lebenszyklus von Zertifikaten ermöglichen eine deutliche Reduzierung des manuellen Aufwands, verhindern menschliches Versagen und Serviceausfälle und verringern die Gesamtbetriebskosten.”

Die Gültigkeitsdauer von Zertifikaten wird immer kürzer. Die Lebensdauer von SSL/TLS-Zertifikaten darf jetzt nicht mehr als 13 Monate betragen. E-Mail- und Dokumentensignatur-Zertifikate sollten eine ähnliche Gültigkeitsdauer haben, um das Risiko einer Kompromittierung zu verringern. Ein digitales Zertifikat muss erneuert werden, bevor es abläuft, um die ständige Verfügbarkeit des Dienstes sicherzustellen. Wenn ein Unternehmen nur eine kleine Anzahl

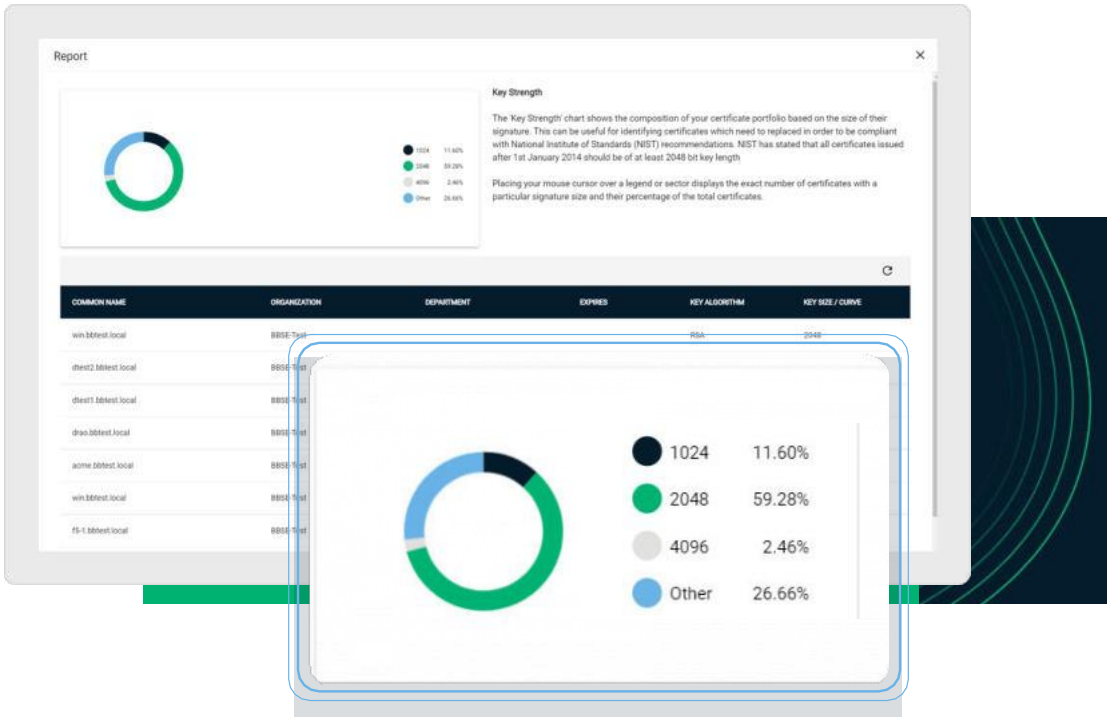
digitaler Zertifikate einsetzt, ist es unter Umständen möglich, deren Erlöschen und Erneuerung mit Hilfe eines Tabellenkalkulationsprogramms zu verfolgen. Je größer ein Unternehmen jedoch wird, desto komplexer und unzuverlässiger wird die Aufgabe, die Lebenszyklen aller digitalen Zertifikate zu verwalten.

Die Abhängigkeit von manuellen Prozessen, um die Erneuerungen abgelaufener Zertifikate im Auge zu behalten, ist für ein sicheres modernes Unternehmen zu risikoreich. IT-Abteilungen müssen in der Lage sein, das Erlöschen digitaler Zertifikate zu visualisieren und schnell zu erkennen und Maßnahmen zu ergreifen, da sie sonst bald mit den Auswirkungen eines erheblichen Ausfalls konfrontiert werden könnten.

Zertifikat-Governance

SCM unterstützt Unternehmen dabei, einheitliche Unternehmensrichtlinien für alle digitalen Zertifikate einer beliebigen CA durchzusetzen. Das Unternehmen kann die kryptografische Stärke und den Inhalt aller digitalen Zertifikate festlegen und die Kontrolle durchsetzen, indem nur digitale Zertifikate ausgestellt werden, die dieser Richtlinie entsprechen.

Dieselben Durchsetzungsregeln können auch auf digitale Zertifikate angewandt werden, die von anderen CAs ausgestellt und vom SCM entdeckt wurden. Auf diese Weise kann der IT-Administrator digitale Zertifikate, die nicht den Vorschriften entsprechen, schnell identifizieren.



Die Dashboard-Funktionen des SCM bieten einen Überblick über den Status digitaler Zertifikate und andere Merkmale des gesamten digitalen Zertifikatsbestands.

SCM umfasst umfangreiche Berichtsfunktionen, die zur Erleichterung von Prüfungen und zur Einhaltung von Vorschriften genutzt werden können. Nur mit einer Plattform, die einen vollständigen Überblick über alle Aktivitäten im Zusammenhang mit digitalen Zertifikaten im gesamten Unternehmen bietet, kann sichergestellt werden, dass die Richtlinien befolgt werden. Es können Berichte erstellt werden, die Folgendes zeigen

Status und Aktivität digitaler Zertifikate, gefiltert nach Zeitrahmen, Organisation usw. Dies wird bei Ereignissen wie Quantencomputer-Angriffen von entscheidender Bedeutung sein, bei denen Sie alle kompromittierten digitalen Zertifikate finden und diese schnell und automatisch ersetzen müssen.

SCM bietet Tools, die bei allen Aspekten des Lebenszyklus von Zertifikaten helfen, einschließlich Konfiguration, Ausstellung, Widerruf, Erneuerung und Verteilung. Eine einzige Plattform, auf der alle digitalen Zertifikate verwaltet werden, sorgt für mehr Effizienz und vermeidet Zertifikatsilos. Die moderne Cloud-basierte Architektur von SCM gewährleistet Ausfallsicherheit, Skalierbarkeit und sofortige Verfügbarkeit der neuesten Funktionen für die Verwaltung des Lebenszyklus von Zertifikaten.

Schlüsselverwaltung

SCM archiviert private Schlüssel, so dass verschlüsselte Dateien und E-Mails entschlüsselt werden können, falls der private Schlüssel versehentlich zerstört wird oder das Unternehmen Zugriff auf die von einem Mitarbeiter verschlüsselten Dateien benötigt. Die Plattform bietet eine vollständige Zugangskontrolle mit detaillierten Schlüsselprotokollen für Überwachungs- und Prüfungszwecke, um die ordnungsgemäße Verwendung der Schlüssel sicherzustellen.

SCM automatisiert die Verwaltung der Lebenszyklen von Verschlüsselungsschlüsseln, einschließlich Schlüsselerzeugung, Schlüsselspeicherung und Schlüssellöschung. Außerdem wird der Verschlüsselungsschlüssel automatisch auf den Geräten installiert, die der Benutzer zur Entschlüsselung von Dateien und E-Mails verwendet. SCM schützt den archivierten Schlüssel davor, versehentlich an einen unbefugten Benutzer weitergegeben zu werden.

Mit der Cloud-gehosteten SCM-Plattform können Unternehmen ein Portfolio von Verschlüsselungsschlüsseln direkt von einer einzigen Plattform aus erstellen und verwalten.

Anwendungsfälle für Zertifikate

Digitale Zertifikate bilden die Grundlage für viele Anwendungsfälle in modernen Unternehmen. SSL/TLS-Zertifikate sind allgemein bekannt und für das Funktionieren moderner Cloud- und webbasierter Lösungen unerlässlich. Es gibt jedoch noch viele andere Anwendungen für digitale Zertifikate, die den Umfang und die Skalierbarkeit einer Lösung für die Verwaltung des Lebenszyklus von Zertifikaten weiter erhöhen. Indem Unternehmen neue zertifikatsbasierte Lösungen, einschließlich DevOps-Dienste,

Robotic Process Automation, passwortlose Authentifizierung, Dokumentensignierung und E-Mail-Verschlüsselung einführen, wird die Zahl der verwalteten digitalen Zertifikate erheblich steigen, wodurch die Verwaltung des Lebenszyklus von Zertifikaten in den Mittelpunkt des IT-Betriebs rückt.

Server-Zertifikate

In den Unternehmen von heute hat die Kombination einer gestiegenen Anzahl von Servern und komplexeren Netzwerken dazu geführt, dass ein moderner Ansatz zur Automatisierung des Lebenszyklusmanagements von Unternehmens-SSL-Zertifikaten auf beiden Seiten der Firewall erforderlich ist. Zertifikate sind auch für Load Balancer erforderlich, eine wichtige Komponente einer skalierten Webinfrastruktur. SCM vereinfacht die Aufgabe, indem es eine automatisierte Lösung zur Verwaltung von SSL-Zertifikaten für jeden Server und jeden Load Balancer in Ihrer Umgebung bereitstellt.

Maschinen-Zertifikate

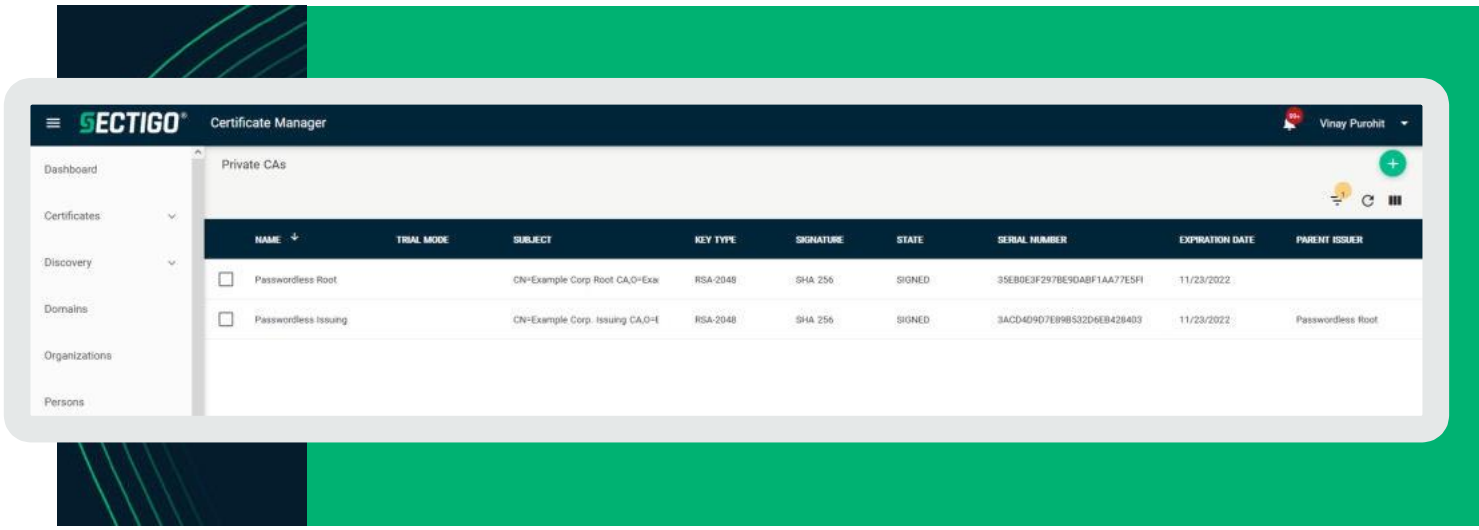
Unternehmen haben viele Rechner, die sich authentifizieren und die Kommunikation verschlüsseln müssen. SCM kann diese digitalen Zertifikate erstellen und anschließend die Installation und Erneuerung automatisieren. Beispiele hierfür sind:

- DevOps-Mikrodienste
- Robotergestützte Prozessautomatisierung
- Geräte, die sich mit dem Netzwerk verbinden, sowohl kabelgebunden als auch über Wi-Fi

Passwortlose Authentifizierung

Digitale Zertifikate bieten das Potenzial, Passwörter und Einmal-Passwörter als primäre Form der Benutzer- und Geräteauthentifizierung zu ersetzen. SCM automatisiert die Bereitstellung von digitalen Zertifikaten im gesamten Unternehmen, was zu Kosteneinsparungen, geringerem IT-Aufwand und besserer Sicherheit führt. Alle seit 2016 hergestellten Geräte verfügen über TPM-Funktionen, die den privaten Schlüssel davor schützen, auf ein anderes Gerät kopiert zu werden. Dazu gehören

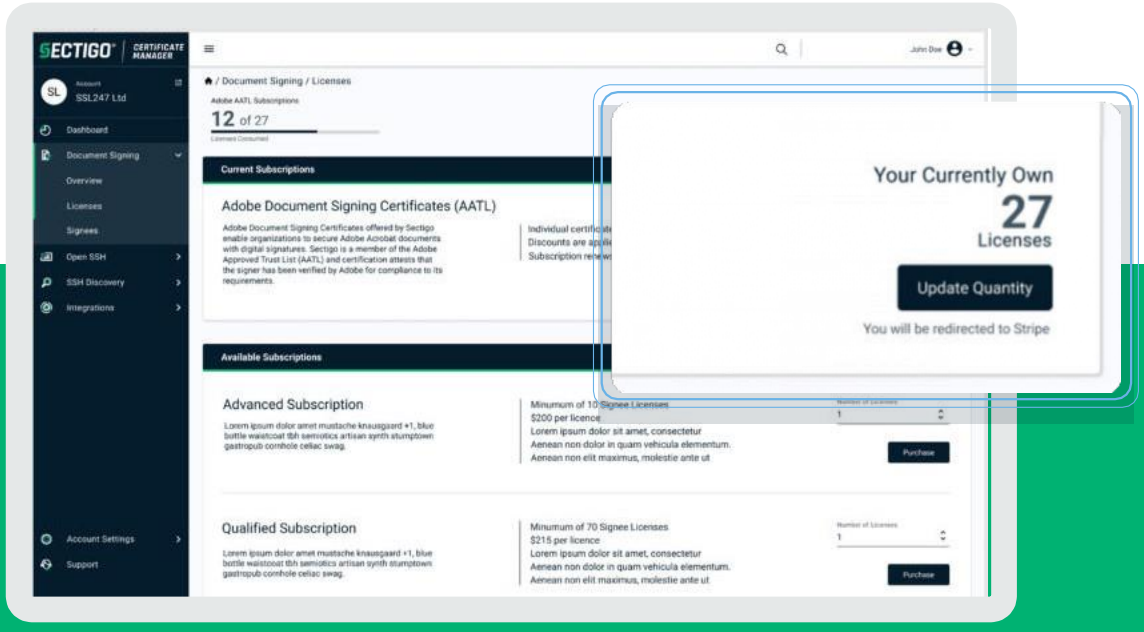
Windows, Mac, iOS, Android und Chromebooks. Der SCM verlangt, dass der Schlüssel in dieser HW gespeichert und erneuert wird, damit Sie nicht nur wissen, dass es sich um den autorisierten Benutzer handelt, sondern auch um das autorisierte Gerät. Dadurch entfällt das Kennwort, die Authentifizierung für den Zero Trust Network Access wird aktiviert und die Windows-Anmeldung wird ohne Kennwort ermöglicht.



Unterzeichnung von Dokumenten

Digitale Signaturen für Dokumente werden für viele Transaktionen obligatorisch und bieten einen überzeugenden Ansatz zur Verringerung von Geschäftsbetrug bei gleichzeitiger Verbesserung der Produktivität von Mitarbeitern, die von zu Hause aus arbeiten.

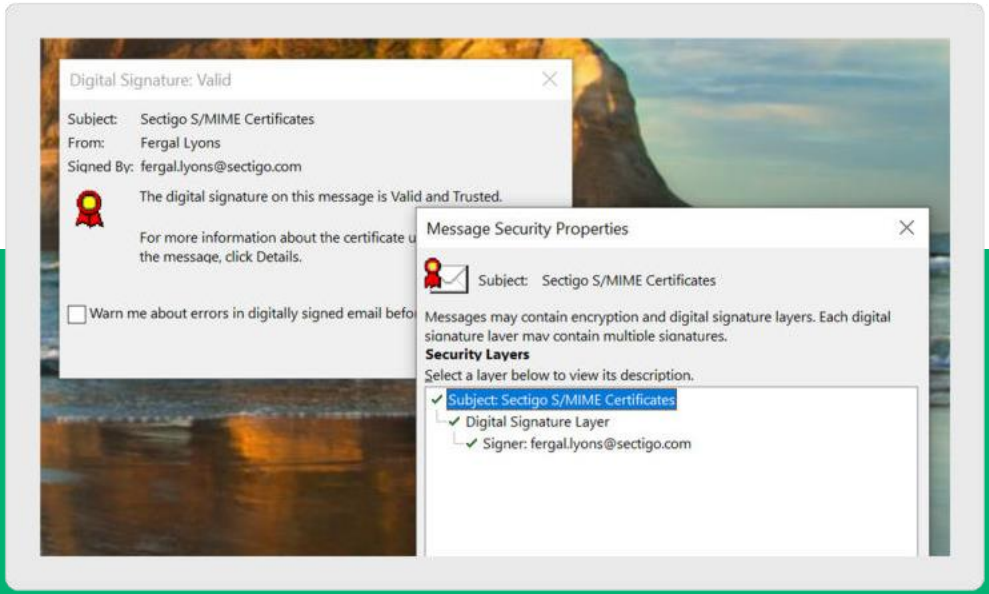
Die Verwaltung des Lebenszyklus von Zertifikaten ist ein wesentliches Element einer Lösung für das Signieren von Dokumenten, und SCM bietet Mechanismen, die die Skalierung des Signierens von Dokumenten über das gesamte Unternehmen hinweg unterstützen. Digitale Signaturen sind nicht mehr auf Finanz- und Rechtsabteilungen beschränkt, sondern können von Personen auf allen Ebenen des Unternehmens genutzt werden. Mit den Dokumenten-Signaturzertifikaten von Sectigo ermöglichen Unternehmen, Geld zu sparen und gleichzeitig eine stabilere Infrastruktur für die Informationsübertragung zu schaffen. Diese Signaturen werden von Adobe PDF-Readern überall auf der Welt als vertrauenswürdig eingestuft.



Der europäische eIDAS-Standard für qualifizierte Vertrauensdienste führt zu einer breiteren Verwendung von signierten und versiegelten Dokumenten zwischen europäischen Unternehmen. Sectigo bietet eIDAS-kompatible digitale Zertifikate als QTSP (Qualified Trust Service Provider) an. Auch diese können über SCM verwaltet werden.

E-Mail-Sicherheit

E-Mail-Sicherheit wird immer wichtiger für die Einhaltung von Datenschutzbestimmungen wie GDPR und HIPAA. Unternehmen können ihre E-Mail-Konten schützen, indem sie die Kommunikation mit Secure/Multipurpose Internet Mail Extensions (S/MIME)-E-Mail-Zertifikaten digital signieren und verschlüsseln. Diese Arten von Zertifikaten validieren die digitale Identität des Benutzers und ver- und entschlüsseln E-Mails und Anhänge. Die sicheren Unternehmens-E-Mail-Zertifikate von Sectigo werden von allen wichtigen E-Mail-Anbietern und -Anwendungen unterstützt, darunter Microsoft Outlook, Exchange, Gmail, beliebte mobile Betriebssysteme und mehr. Sectigo bietet eine automatisierte S/MIME-Verschlüsselung, um die Bereitstellung von Benutzerzertifikaten im gesamten Unternehmen zu vereinfachen. Mit SCM können IT-Experten E-Mail-Zertifikate für jeden Benutzer und jedes Gerät nahtlos bereitstellen und verwalten - mit einem einzigen Klick.



Integration

SCM lässt sich in alle gängigen Anwendungen, die im Unternehmen verwendet werden, integrieren. Einige Beispiele:

- DevOps-Tools für Containerisierung und Orchestrierung.
- Automatisierungsstandards zur Integration mit Anwendungen, die denselben Standard verwenden, wie z. B. Universal Endpoint Managers und Netzwerkgeräte, die SCEP verwenden, IoT-Geräte, die RFC 7030 und ACME verwenden.
- Anwendungen von Cloud-Anbietern wie AWS Certificate Manager, CloudFront, Elastic Load Balancer, Azure Key Vault.

Diese Integrationen automatisieren die Bereitstellung von Zertifikaten und deren Einhaltung Abstimmung Ihrer Zertifikatsstrategie auf das gesamte Unternehmen.

Abonnement-Preise

Sectigo bietet Abonnementpreise an, bei denen die Kunden für die Laufzeit des Zertifikatsabonnements und nicht pro ausgestelltem Zertifikat bezahlen. Das SCM-Abonnement bietet dem Kunden die Freiheit, Zertifikate mit beliebiger Laufzeit auszustellen und zu ändern, für welchen Mitarbeiter oder welches Gerät das Zertifikat verwendet wird. Zum Beispiel könnte ein Kunde:

- 52 einwöchige Zertifikate der Reihe nach ausstellen
- Ein Zertifikat für ein Jahr ausstellen
- Ein Zertifikat für einen neuen Mitarbeiter oder einen Ersatzmitarbeiter ohne zusätzliche Gebühren ausstellen

Das Abonnement kann das digitale Zertifikat und die Zertifikatsverwaltung/-automatisierung bündeln, um dem Kunden einen noch größeren Nutzen zu bieten und einen teureren CLM-Anbieter überflüssig zu machen.

Ein optionales Enterprise-Abonnementmodell ermöglicht die Erhöhung der Anzahl aktiver Zertifikate, ohne dass zusätzliche Anschaffungen erforderlich sind.

Über Sectigo

Sectigo ist ein weltweit führender Anbieter von digitalen Zertifikaten und automatisierten Lösungen für die Verwaltung des Lebenszyklus von Zertifikaten. Als eine der ältesten und größten Zertifizierungsstellen (CA) verfügt Sectigo über mehr als 20 Jahre Erfahrung in der Bereitstellung innovativer Sicherheitslösungen für über 700.000 Unternehmen weltweit. Sectigo ist der führende Anbieter für das Management des Lebenszyklus von Zertifikaten, der mehrere CA-Anbieter unterstützt und in die größten Software-Ökosysteme der Welt integriert ist.