SECTIGO

A WHITEPAPER FROM SECTIGO

Product Guide

Sectigo Web Security Solutions

SECTIGO

Intro

Trusted by enterprises globally for more than twenty years, Sectigo (formerly Comodo CA) provides web security solutions 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.

Sectigo provides the most complete range of web security solutions for businesses of all sizes to protect their entire online environment. Building off the foundation of the world's most chosen commercial digital certificate provider, Sectigo has constructed a world-class solutions portfolio to identify, prevent, remediate, and combat the growing and ever-evolving cast of web-based threats.

This guide explains Sectigo's web security solution portfolio, features, and the value each solution provides. Whether implementing a single solution or a multi-layered approach, Sectigo's diverse range of web security products complement each other to deliver a full spectrum of protection.

SECTIGO

Table of Contents

SECTIGO

Web Security Solution Portfolio

TLS/SSL Certificates

Enable encrypted transmission and avoid browser security warnings through industry-leading SSL certificates including wildcard, Extended Validation (EV), and multi-domain certificates.

Certificate Manager

Take the worry out of certificate management with Sectigo's full-featured certificate management console for discovery, monitoring, and replacement of certificates.

IoT Manager

Trusted, mutual-authentication solutions for all IoT devices and networks, enabling companies to securely build out and scale their IoT ecosystems and manage the full device lifecycle.

Signing Certificates

Show that your code hasn't been tampered with through Code Signing and Email (S/MIME) certificate solutions.

- **Code Signing Certificates** enable trust for program files downloaded or updated across the internet. Signing your code enables the receiving party to validate the identity of the code's author and to know for a fact that this code is bit-for-bit identical to how it was when signed.
- **S/MIME Email Certificates** enable encrypted email and allow recipients to verify the true email sender. These certificates help to protect your online identity against use in email spoofing attacks and prevent unwanted third parties from reading the contents of your email.

Website Backup and Recovery

Track all changes and instantly restore your site to any previous version, including automatic detection and removal of malware.

PCI Compliance and Website Vulnerability Scanning

Your simple, automated way to ensure compliance with the Payment Card Industry Data Security Standard (PCI DSS). Approved by the PCI Security Standards Council.®

SECTIGO

SSL Certificates

SSL — or Secure Sockets Layer — is the commonly used term for the Transport Layer Security (TLS) standard. SSL certificates enable encrypted communication over the internet and allow a client system to trust it is connected to the intended server and not a Man-in-the-Middle (MITM) attacker. Popular browsers make it possible for users to ensure they are on SSL-enabled sites through a variety of interface mechanisms, including the padlock icon, HTTPS in the address, and the color green.

All SSL certificates must be issued by a Certificate Authority (CA) with roots that are trusted by client operating systems and browsers. By regulation, CAs must follow a codified, minimum vetting process before issuing any SSL certificate.

The browser will check if the CA is verified and if the SSL certificate is being used for the correct site. If the certificate has been tampered with or doesn't match the domain on which it appears, the user will receive a warning that the site is not secure.

SECTIGO

Product Comparison

Features	Domain Validation Single Domain	Domain Validation Multi-Domain/UCC	Domain Validation Wildcard	Organization Validation Single Domain	Organization Validation Multi-Domain/UCC	Organization Validation Wildcard	Extended Validation Single Domain	Extended Validation Multi-Domain/UCC
Secures	Single Domain	Multiple Domains	Single Domain and All Sub-Domains	Single Domain	Multiple Domains	Single Domain and All Sub-Domains	Single Domain	Multiple Domains
Validity Period	1-2 Years	1-2 Years	1-2 Years	1-2 Years	1-2 Years	1-2 Years	1-2 Years	1-2 Years
Validation Level	Domain Validation	Domain Validation	Domain Validation	Organization Validation	Organization Validation	Organization Validation	Extended Validation	Extended Validation
Green Address Bar	—	—	—	—	—	—	✓	✓
Avg. Issuance Time Frame	Minutes	Minutes	Minutes	1-5 Business Days	1-5 Business Days	1-5 Business Days	1-5 Business Days	1-5 Business Days
Unlimited Server Licenses	✓	✓	✓	✓	✓	✓	✓	✓
Strongest SHA2 & ECC Encryption	✓	✓	✓	✓	✓	✓	✓	✓
Major Browser & Mobile Device Compatibility	✓	✓	✓	✓	✓	✓	✓	✓
Average Issuance Time Frame	✓	✓	✓	✓	✓	✓	✓	✓
Priority Support	—	—	—	—	—	—	✓	✓
Warranty	$500,000	$500,000	$500,000	$1,000,000	$1,000,000	$1,000,000	$1,750,000	$1,750,000
Trust Logo	SECURED BY SECTIGO	SECURED BY SECTIGO	SECURED BY SECTIGO	SECURED BY SECTIGO	SECURED BY SECTIGO	SECURED BY SECTIGO	SECURED BY SECTIGO	SECURED BY SECTIGO

SECTIGO

Extended Validation (EV) Certificates

Featuring the highest level of protection offered by an SSL certificate, Extended Validation (EV) is the industry standard for business websites. When an EV SSL certificate is loaded on a site, browsers will display an additional trust indicator, which is the authenticated name of the company adjacent to the web address, often in the color green. Commonly referred to as the "green address bar" or "branded address bar," this interface element helps users distinguish between the online businesses they intend to deal with and potential imposters attempting to scam them.

To obtain an EV certificate, a company must go through a rigorous, standardized authentication process that has not been defeated in more than ten years of common use.

Displaying the company name in the browser has been shown to build visitor confidence and therefore improve engagement with sites, increasing purchases, use of online services, and the sharing of personal information.

Multiple ecommerce sites are finding a significant increase in transactions when testing green address bars, including:

- Time on site
- Page views
- Bounce rates
- Collateral downloads
- Mailing list signups
- Form completions
- Log ins
- Service usage
- Return visits

By giving your customers peace of mind, not only will you increase engagement and satisfaction, you'll also build brand awareness and preference, helping to spread your message and draw new customers to your business.

Transaction type	% of users more likely to engage*
Engage in financial transactions	50%
Share personally identifiable information	57%
Make a purchase	37%
Use a credit card	28%
Sign up for a new account	43%
Fill out and submit an online form	38%
Use a payment service like PayPal	41%
Add recommended items to a shopping cart	32%

**DevOps, July 2018*

EXTENDED VALIDATED SSL CERTIFICATES AVAILABLE IN:

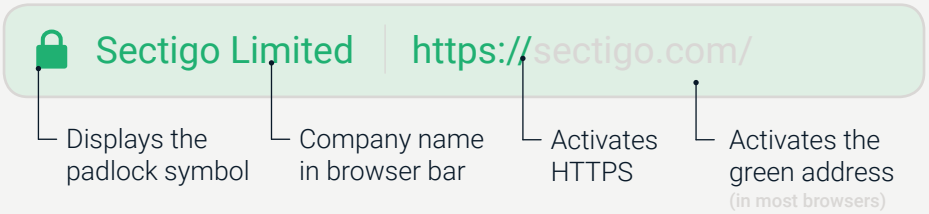
Single

Secure one Fully Qualified Domain Name (FQDN) on a single certificate.

Multi-Domain

Secure multiple, distinct domains with a single solution.

VISIBLE TRUST INDICATORS



SECTIGO

KEY FEATURES

Increase site transactions
The green address bar helps boost transactions, form completions, new user signups and engagement. When internet users see the green address bar, 50% are more likely to make a financial transaction and 37% are more likely to make a purchase.

Protect users against phishing attacks
Provide extra security for your customers by prominently displaying your company name in the browser interface, so they know it's your site — not an imposter.

Help you to stay compliant
Extended Validation provides the strongest protection an SSL certificate can offer, meeting many standards and regulations for online businesses, such as PCI-DSS, HIPAA/HITECH, GDPR, and others.

Browser Trust
Compatible with all popular browsers, Sectigo certificates are a no-worry option for maintaining trust in a company's site.

Certificate Management
Included in every Sectigo SSL purchase is a free subscription to our certificate management tool that allows companies to perform certificate discovery, generate CSRs, install and configure certificates in a few clicks, and set renewals to replace certificates before they expire.

Show customers you care
EV SSL certificates let your customers know you're employing best-of-breed security measures to keep their transactions safe. More than 50% of site visitors believe an online business with the green address bar is trustworthy, secure, and safe to do business with.

SECTIGO

Organization Validated (OV) Certificates

Organization Validation (OV) SSL certificates authenticate connections, enable encryption, and activate web browser trust indicators while offering validation of the organization's identity.

A simpler, faster certificate option for registered organizations, a company can receive an OV certificate by proving it owns the domain it is seeking to secure and is a legally registered business. Through visual trust indicators — like the appearance of HTTPS, the padlock icon, and a dynamic site seal — visitors will know the site is secure.

Requiring only one to three days for validation, OV SSL certificates are business validated and ideal for confirming your ownership of your organization's website. With Sectigo's 24/7 dedicated support, unlimited free server licensing, and free certificate reissuance, OV certificates offer the strongest SHA2 and ECC encryption available. Plus, Sectigo SSL certificates are mobile friendly.

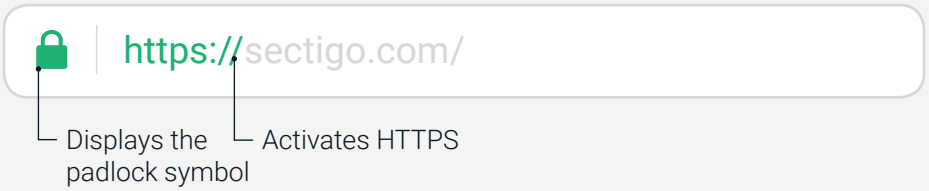
ORGANIZATION VALIDATED SSL CERTIFICATES AVAILABLE IN:

Single
Secure one Fully Qualified Domain Name (FQDN) on a single certificate.

Wildcard
Secure a single domain and unlimited subdomains.

Multi-Domain
Secure multiple, distinct domains with a single solution.

VISIBLE TRUST INDICATORS



SECTIGO

KEY FEATURES

Value
Sectigo OV certificates are a cost-effective way to secure your website. Sectigo's unique, real-time assurance seal helps to boost customers' confidence in a company's site.

Strongest Encryption
Sectigo OV certificates offer the strongest SSL encryption available, with SHA-256, 2048-bit RSA keys, and ECC support.

Server Licensing
Each SSL certificate includes unlimited server licensing, allowing companies to secure all physical servers.

Browser Trust
Compatible with all popular browsers, Sectigo certificates are a no-worry option for maintaining trust in a company's site.

Certificate Management
Included in every Sectigo SSL purchase is a free subscription to our certificate management tool, which allows companies to perform certificate discovery, generate CSRs, install and configure certificates in a few clicks, and set renewals to replace certificates before they expire.

Sectigo Trust Seal
Every Sectigo SSL certificate comes with a free Sectigo trust seal. With real-time identity assurance through our point-to-verify technology, the Sectigo trust seal enhances assurance in your online identity and gives customers confidence to buy from your site.

SECTIGO

Domain Validated (DV) Certificates

Domain Validation (DV) SSL certificates provide the quickest, easiest, most cost-effective way to receive industry-standard encryption for websites and internal systems. To attain a DV certificate, a company must prove ownership of the domain being secured. Issued in just minutes, DV certificates display trust indicators in browsers, like the padlock icon and HTTPS.

Offering express five-minute certificate issuance — the fastest of any Sectigo certificate — DV SSL certificates offer strong 256-bit encryption and come with Sectigo's 24/7 dedicated support as well as free unlimited server licensing and free reissuance. In addition to offering the strongest SHA2 and ECC Encryption, Sectigo DV SSL certificates are also mobile friendly.

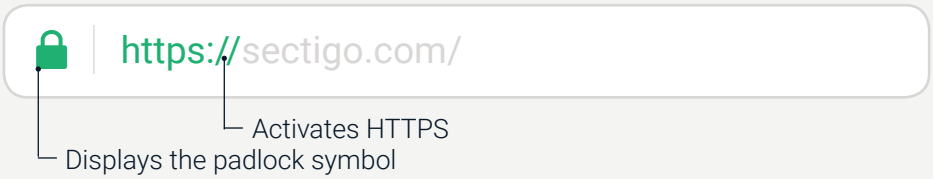
DOMAIN VALIDATED SSL CERTIFICATES AVAILABLE IN:

Single
Secure one Fully Qualified Domain Name (FQDN) on a single certificate.

Wildcard
Secure a single domain and unlimited subdomains.

Multi-Domain
Secure multiple, distinct domains with a single solution.

VISIBLE TRUST INDICATORS



SECTIGO

KEY FEATURES

Value
Sectigo DV certificates are a cost-effective way to secure your website. Sectigo's unique, real-time assurance seal helps to boost customers' confidence in a company's site.

Strongest Encryption
Sectigo DV certificates offer the strongest SSL encryption available, with SHA-256, 2048-bit RSA keys, and ECC support.

Server Licensing
Each SSL certificate includes unlimited server licensing, allowing companies to secure all physical servers.

Browser Trust
Compatible with all popular browsers, Sectigo certificates are a no-worry option for maintaining trust in a company's site.

Certificate Management
Included in every Sectigo SSL purchase is a free subscription to our certificate management tool that allows companies to perform certificate discovery, generate CSRs, install and configure certificates in a few clicks, and set renewals to replace certificates before they expire.

Sectigo Trust Seal
Every Sectigo SSL certificate comes with a free Sectigo trust seal. With real-time identity assurance through our point-to-verify technology, the Sectigo trust seal enhances assurance in your online identity and gives customers confidence to buy from your site.

SECTIGO

Solutions

Single-Domain Certificates

The standard SSL certificate, single-domain certificates are the most cost-effective solution for securing a business's internal servers and consumer-facing pages.

Wildcard Certificates

Wildcard SSL certificates allow companies to secure their main domain and unlimited subdomains under a single certificate. Cost effective and efficient, the Wildcard SSL certificate makes it easy to maintain a website's security without the hassle of managing multiple SSL certificates. Wildcards also provide the most flexibility, as additional subdomains can be added without requiring a new certificate to be issued.

Wildcard certificates work the same way as a standard SSL certificate, allowing a company to secure the connection between their website and a customer's browser, with the added ability to secure unlimited sub-domains with one certificate. All SSL certificates enable encryption for the information between the server and the browser and ensure the integrity of the transmitted information. Plus, using Sectigo Wildcard SSL certificates provides compatibility with all popular browsers.

KEY FEATURES

Ease of Administration
Wildcard SSL certificates enable protection for any number of sub-domains with a single certificate, greatly easing administrative burdens, especially in complex environments with many domain names or changing domain structures.

Value
Because a single wildcard certificate can secure any number of sub-domains, wildcard certificates can prove highly cost effective for certain use cases.

Certificate Management
Included in every Sectigo SSL purchase is a free subscription to our certificate management tool that allows companies to perform certificate discovery, generate CSRs, install and configure certificates in a few clicks, and set renewals to replace certificates before they expire.

Sectigo Trust Seal
Every Sectigo SSL certificate comes with a free Sectigo trust seal. With real-time identity assurance through our point-to-verify technology, the Sectigo trust seal enhances assurance in your online identity and gives customers confidence to buy from your site.

Browser Trust
Compatible with all popular browsers, Sectigo certificates are a no-worry option for maintaining trust in a company's site.

Server Licensing
Each SSL certificate includes unlimited server licensing, allowing companies to secure all physical servers.

Multi-Domain Certificates

Multi-domain certificates (also known as SAN/UCC certificates) use Subject Alternate Names (SANs) to secure up to 100 distinct domain names or IP addresses. They are a great solution for managing complex environments with a single SSL certificate. For example, a single multi-domain certificate can be used to secure domain-1.com, domain-2.com, domain-3.co.uk, and domain-4.net.

Multi-domain certificates are available in Extended Validation (EV), Organization Validated (OV), and Domain Validated (DV) certificates, providing protection and trust for all a company's domains. Plus, using Sectigo Multi-Domain SSL certificates provides compatibility with all popular browsers.

Multi-Domain SSL Certificate Options

With DV, OV, and EV multi-domain certificate options, companies can secure up to 100 domains with one SSL certificate.

EV Multi-Domain SSL Certificates

The highest level of protection offered by an SSL certificate, EV multi-domain certificates utilize proven, highly trusted authentication methods to give the best possible assurance of a website's legitimacy, allowing you to protect up to 100 fully qualified domains on a single certificate. With the EV SSL certificate's visible trust indicators, EV multi-domain certificates help improve customer trust and interactions across company's domains.

- Up to 256-bit SSL encryption
- Company validation
- Company name identified in browser
- Green label in browser address bar
- Free trust seal

Unified Communication Certificates

Unified Communications Certificates (UCC) are TLS/SSL certificates intended specifically for the Microsoft® Exchange and/or Microsoft® Office Communication Server (OCS) environments. Also referred to as Exchange certificates, these multi-domain certificates use Subject Alternate Name (SAN) fields to secure the full set of addresses required to operate Microsoft email servers.

KEY FEATURES

Include Wildcards in SANs

It is possible for SANs in a multi-domain certificate to contain wildcards. For example, a multi-domain certificate could be acquired for cart.domain1.com, login.domain1.com, and *.domain2.com.

Official Microsoft UCC vendor
Sectigo is an approved Microsoft UC certificate provider. Multi-domain certificates can be used to secure Microsoft Exchange and Lync.

Certificate Management
Included in every Sectigo SSL purchase is a free subscription to our certificate management tool that allows companies to perform certificate discovery, generate CSRs, install and configure certificates in a few clicks, and set renewals to replace certificates before they expire.

Sectigo Trust Seal
Every Sectigo SSL certificate comes with a free Sectigo trust seal. With real-time identity assurance through our point-to-verify technology, the Sectigo trust seal enhances assurance in your online identity and gives customers confidence to buy from your site.

Strongest Encryption
Sectigo certificates offer the strongest SSL encryption available, with SHA-256, 2048-bit RSA keys, and ECC support.

SECTIGO

Signing Certificates

Sectigo offers S/MIME and Code Signing certificates to secure your email and distributed software.

Sectigo Code Signing

Every internet transaction provides an opportunity for malicious hackers to intercept and corrupt the information passing between the two unsuspecting parties. One such attack vector is through code that is downloaded or automatically updated online. Sectigo Code Signing enables developers to add a layer of assurance, informing users the software they're receiving can be trusted.

Utilizing certificates that allow developers to digitally sign software before distribution,
Code Signing lets end users downloading digitally signed 32-bit or 64-bit programs know the code actually comes from the developer and has not been modified by a third party since it was signed.

File types that need code signing:

- Drivers
- Firmware
- Scripts
- Applications

By digitally signing the executable software with a publicly trusted X.509 certificate, code developers can increase confidence in their software. If hackers do inject malicious code into a piece of software, Sectigo Code Signing will catch the infestation and alert the user prior to software installation, preventing any damage.

- Enables file reputation in Microsoft's SmartScreen Application Reputation filter.
- Builds trust with the end user.

Code Signing Variations

Unlike code signing products from many other vendors, Sectigo Code Signing assists you with the entire software lifecycle, delivering everything you need in one integrated solution:

- Managing approval
- Signing operations
- Subsequent maintenance

SECTIGO CODE SIGNING ALSO OFFERS ON-DEMAND SERVICE IN TWO VARIATIONS.

1. **In-House Hosted Mode**
   Sectigo runs the back end on the cloud, while the developer utilizes its in-house team to run the rest of the lifecycle.

   Ideal for companies that are more comfortable holding and protecting their own private keys than they are using a third party.

2. **Cloud Service Mode**
   Sectigo runs everything at the back end, so developers can spend minimum time and attention managing their certificates.

   Sectigo Code Signing is available in both Organization Validated (OV) — commonly referred to as "Standard Code Signing certificates" — and Extended Validated (EV) Code Signing certificates.

EV Code Signing certificates give developers and end users all the benefits of Standard Code Signing certificates and are additionally compatible with higher security operating system features, including Microsoft SmartScreen and Windows kernel mode.

Additionally, the EV certificate reduces the possibility that the certificate could be exported and used by an unauthorized entity by using two-factor authentication and requiring that private keys be stored on an external hardware token needed for code signing.

The Sectigo Difference

Verifying your software with Sectigo Code Signing not only builds trust in your product, it also delivers value-added capabilities for implementing and managing your certificates. Code Signing allows you to designate and authorize which users can sign the code on behalf of your organization and to approve a second authorized entity, if required by company policy.

Sectigo Code Signing allows your company to:

Send a hash of the file to the Sectigo Cloud for signing instead of the entire executable file. The developer simply has to embed the signed hash within the file.

- Generate and store the private key in an HSM for added security
- Host the non-CA components at your premise, including local key generation

By implementing Sectigo Code Signing, you'll increase the security of your software and build trust with your customers — all while partnering with a company that's synonymous with reliability and security.

SECTIGO

Secure Email Certificates (S/MIME)

Posing as legitimate employees, servers, or devices, hackers can utilize email to infiltrate an organization's digital infrastructure and wreak havoc on its business — potentially resulting in theft of intellectual property and capital as well as damage to the business and brand. You can combat these potential attacks by signing email using Sectigo S/MIME Email certificates.

Hackers target weak points in an organization's email infrastructure using several common tactics.

OCTOBER 2013 – MAY 2018

78,000 BEC fraud incidents

$12 billion in corporate losses worldwide

Business Email Compromise (BEC)

A sophisticated type of scam targeting companies that regularly perform wire transfer payments with suppliers. Hackers disguise themselves as known suppliers using spoofed email addresses in order to dupe companies into wiring funds to them instead of the real recipients.

By requiring email communication with suppliers and vendors to be certificate-signed from their true sources, companies can radically decrease their exposure to BEC attacks.

Interception

By sending essential documents and information unsecured through the internet, users expose these properties to interference by malicious actors — which can result in the loss of business secrets or employee personally identifiable information (PII), reputational damage to the company, and legal exposure.

Phishing & Malware

Hackers can use the simple strategy of bombarding employee inboxes with malware and phishing attacks to infiltrate a company's digital infrastructure or gain access to assets. Without a Secure Email Gateway in place, it is easy to slip malicious messages into employee mailboxes.

With Sectigo S/MIME Email certificates, companies can protect themselves against attacks by rogue actors. Automatically installed into all mail clients, the public S/MIME certificate adds a layer of defense by encrypting emails both in storage and in transit. The encryption key archive is accessible to the secure email gateway, enabling signing, encryption, and decryption of emails at the gateway. Utilizing publicly trusted digital signatures, Sectigo is the first company to deliver this capability.

Through a slew of sophisticated security features, Sectigo S/MIME Email certificates give users the confidence they need to trust their digital correspondence and help their company thrive. S/MIME Email certificates:

- Automatically encrypt and decrypt emails
- Display encryption via a lock symbol in popular mail programs
- Tell users emails are authentic and unmodified via check mark icon
- Decrypt incoming attachments
- Automatically encrypt replies
- Encrypt all sent attachments
- Deliver the same user experience as plain text email
- Utilize the same email repository and search

Consolidation of Certificate Management

Offering a single management console for all enterprise identities, Sectigo S/MIME Email certificates are available alongside public SSL, Code Signing, and private certificates. By scanning servers using an SSL handshake and searching the active directory for Microsoft CA issued certificates, Sectigo Certificate Manager automatically discovers existing certificates.

With automated enrollment and renewals, certificates are renewed without the need to manually manage the task — reducing cost and the risk of outages due to human error. And with Sectigo's predictable fee and the ability to issue certificates for temporary projects, we can help your company grow. While other venders don't offer public and private certificates in the same console, Sectigo Certificate Manager stands alone in offering an unlimited enterprise license.

SECTIGO

Certificate Manager

With many potential pitfalls inherent in managing certificates in-house, companies need a simple, automated, robust certificate management solution to discover, monitor, and renew their digital certificates. Sectigo Certificate Manager is the cloud-based platform that gives businesses complete visibility and lifecycle control over any certificate in their environments, helping them reduce risk, quickly respond to threats, and control operational costs.

Too many companies still use the spreadsheet method of managing their certificates. Manually tracking and managing certificates carries serious disadvantages:

- Risk of certificates being forgotten until expiration, resulting in sudden failure of critical business systems
- Considerable effort in tracking and managing certificates
- The presence of rogue certificates in use for necessary systems without the knowledge of central IT
- Potential compliance gaps with internal policies or regulations requiring specific protections for data collected and used by the enterprise

Sectigo Certificate Manager automates the management of the entire certificate lifecycle, from issuance to expiration and replacement. Sectigo Certificate Manager even scans the network for expired and rogue certificates that could lead to unexpected vulnerabilities. By enabling organizations to manage, track, and run reports on their entire certificate portfolios from one portal, companies no longer need to worry about unexpected — and unwelcome — certificate issues.

With customizable administration settings that allow for multiple administrators to quickly issue certificates across the globe, Sectigo Certificate Manager also provides:

- Certificate discovery
- Customer notifications
- Self-enrollment/streamlined workflow/ certificate process
- Rapid enrollment, approval, issuance, revocation, and renewal of all certificates
- Real-time status checking
- Same day expiration for all issued certificates
- Auto CSR generation
- Auto installation (ISS, Apache)
- Auto renewal
- Customizable device certificates
- SCEP support for device certificates
- S/MIME enrollment by interface

Supporting all validation levels — from DV to OV to EV — Sectigo Certificate Manager performs certificate discovery though MS AD-MS CA-IIS.

Certificate Management Tools

Through Sectigo Certificate Manager's slew of sophisticated tools, this solution helps to effectively and easily manage the certificate lifecycle.

Certificate Discovery provides in-depth scanning to uncover and monitor all certificates installed across an entire environment, regardless of the Certificate Authority (CA). For each certificate, Sectigo Certificate Manager shows:

- Your issuing CA
- Expiration date
- Signature Algorithm
- Ciphers

Certificate Lifecycle Management delivers simplified control over certificate lifecycle management across the entire environment through one cloud-based portal. Providing rapid enrollment, approval, issuance, revocation, and renewal of all certificates from one console, Certificate Lifecycle Management also allows organizations to search and run reports using custom data parameters.

Automation gives admins the ability to automate monitoring, notifications, renewals, and installation while quickly provisioning and issuing certificates to users or devices anywhere by leveraging APIs and Active Directory integration.

Private Certification Authority Service (Private CA) provides a cost-effective way for customers to avoid the risks associated with self-signed certificates, while providing security and management capabilities. By outsourcing the PKI operation to Sectigo, organizations can be assured their Private CAs are being managed using industry best practices.

Code Signing in the Cloud secures and manages code signing certificates by storing the keys in the Sectigo Certificate Manager PKI infrastructure. With its fast, simple interface, developers can upload, sign, and collect signed software, ensuring cost-effective deployment. Providing a safe ecosystem — where certificate keys are securely stored and only available to authenticated users — this tool allows customers to track code signing history, create audit reports, manage lifecycles, get notifications, and assign code signing admins.

Compatible signing formats:

- .EXE
- .DLL
- .CAB
- .MSI
- .OCX
- .SYS
- .JAR
- .APK

SECTIGO

IoT PKI Manager

With more than one billion devices deployed today, Internet of Things (IoT) is among the most important growth areas for technology in the coming years. Research predicts the deployment of as many as 50 billion IoT devices by 2020 with companies of all sizes and industries planning IoT strategies to improve productivity, responsiveness, and their ability to delight customers.

Unfortunately, after several years of highly damaging attacks exploiting vulnerabilities in IoT networks, it has become clear that security has not kept up with the growth of this new platform. Too often, IoT device networks are susceptible to rogue, infected, and malicious software, which can inflict harm on companies' operations, their customers, and the online community at large. One result of this trend is recent legislation requiring companies creating and operating IoT networks to provide protection against exploits.

Sectigo's IoT Manager provides trusted, mutual-authentication solutions for all IoT devices and networks, enabling companies to securely build out and scale their ecosystems and manage the full device lifecycle.

IoT 2018:

1 Billion Devices

IoT 2020:

50 Billion Devices

Challenges

Recent history has proven that for an IoT implementation to be secure, it must include unique, fool-proof identifiers for all devices on the network. Weak identity options, like providing access control strictly through passwords, do not rise to this level of protection. Even one-and-done certificates are not effective. From manufacturers to network service providers to consumers, maintaining IoT ecosystems in-house has become too daunting a task — especially for those managing hundreds to millions of devices.

FROM DEVICE CREATION THROUGH CUSTOMER USE, EVERY STAGE PRESENTS POSSIBLE DANGERS FOR THE ECOSYSTEM.

- Manufacturers worry about device integrity and ecosystem standards as well as what could happen to their brand reputation should issues occur.
- Network service providers face issues of DDOS and botnet attacks, customer outages caused by these assaults, and compromised data and consumer privacy.
- Enterprises operating IoT networks must be comfortable that their devices follow best practices in device integrity and ecosystem standards.

While the ideal solution is a PKI management system, most products on the market are seen as too expensive and time consuming for many companies to implement.

Solution: Sectigo IoT Manager

To protect an IoT ecosystem against outside threats, Sectigo IoT Manager utilizes a secure, cloud-based portal that issues trusted third-party PKI certificates for authentication and lifecycle management of the IoT network to protect it throughout its lifespan. All in a solution that's effective, efficient, and easy to manage.

Through the use of a third-party PKI solution, device registration certificates are installed by the PKI provider at the first point of network connection, thus helping to protect devices from interception or malicious software installation. Once connected to the private network ecosystem, devices can link only to those authorized on the network. Any device without the proper authentication credentials will not be allowed to connect.

By building an ecosystem of trusted devices for customers and partners, Sectigo's IoT Manager helps organizations bring secure devices to the market quickly and contributes to the company's security throughout the product lifecycle. Working with our partners to deliver a platform that's built to scale, quick to implement, easy to manage, and cost effective, Sectigo has created a solution that's available across a wide range of industries:

- Smart cities
- Medical device ecosystems
- Point of sale
- AeroMACs ecosystem
- Industrial automation

Using x.509 PKI certificates and custom hybrid TSL/SSL certificates, the IoT Manager's high-availability, batch-issuance system allows administrators to easily enroll, download, and decrypt certificate batches quickly and efficiently. Plus, it meets requirements for many industry standards:

- WiMAX Forum
- GSMA
- Zigbee
- OCF
- Joint Venture — Silicon Valley.

Sectigo's IoT Manager offers:

- CA signing and hosting services
- Batch PKI certificate issuance
- Identity and registration certificates
- Device authority partnership for KeyScaler
- Automated certificate installation and provisioning
- Certificate lifecycle management
- HSM provisioning and management

Support centers spanning the globe:

- U.S.
- Canada
- UK
- India

Support in many languages:

- English
- Spanish
- Simplified Chinese
- Korean
- Arabic
- German
- Russian
- Hebrew

And with data centers in Manhattan, NY and Manchester, UK, Sectigo has an issuance capability of 250 million certificates per day.

Whatever your industry and wherever your company, Sectigo IoT Manager can help to secure your IoT ecosystem — protecting your data, your customers, and your brand reputation.

SECTIGO

Website Backup and Recovery

The fastest, most reliable website backup service tracks all of your changes daily. CodeGuard scales to your business and your client's business needs. Offering essential backup, malware remediation, and rollback capabilities, CodeGuard makes it easy for you to keep your site safe and backed up.

- Malware monitoring & remediation
- Enterprise-grade backups made easy
- WordPress plugin
- One-click restore

ALL CODEGUARD PLANS INCLUDE:

Daily Backup
We back up your site every day, saving only what has been changed or modified to save you space.

MalwareGone™
Sectigo's patented functionality automatically scans, discovers, and fixes threats your site encounters.

Client Access & Reports
Use CodeGuard as a service to your customers. White-label offering helps give clients a personal portal to their information.

WordPress Plugin Updates
CodeGuard takes care of automatically updating and working with all WordPress updates.

ChangeAlert™ Notifications
CodeGuard notifies you by email any time anything changes within the source code of your website.

CodeGuard

SECTIGO

PCI Compliance and Website Vulnerability Scanning

A simple, automated way to ensure your website is compliant with the PCI DSS. Approved by the PCI Security Standards Council.®

The PCI DSS, aka the Payment Card Industry Data Security Standard, has been formulated by the five major credit card companies — VISA, Mastercard, American Express, Discover, and JCB — to mitigate risks involved through online purchases and transactions and prevent data loss. Compliance to the PCI DSS standard is required by these five credit card companies for any business that accepts, processes, or stores credit card payment data.

PCI DSS mandates that companies take specific actions to ensure they are protecting credit card information. Merchants and processors failing to meet these standards can be subject to fines or loss of the ability to accept credit card charges.

Introducing HackerGuardian PCI Compliance Scanning

PCI compliance scanning enables merchants to validate PCI Compliance quarterly on up to five servers using the full complement of HackerGuardian plugins (over 30,000 individual vulnerability tests). The HackerGuardian Additional IP Address Pack allows HackerGuardian to grow with your external and internal PCI scanning needs.

SECTIGO

Benefits of PCI Scan Compliance

- Ensure ongoing PCI compliance thanks to vulnerability scanning by a PCI-approved scanning vendor.
- Receive ready-to-submit PCI compliance reports to send to your merchant bank.
- Review HackerGuardian's detailed reports identifying security holes exposed by HackerGuardian's 30,000+ tests and containing actionable fix recommendations.
- Start with an easy PCI self-assessment questionnaire available in our online wizard.
- Schedule up to ten PCI scans per quarter on up to five servers through a secure web-based interface.
- Add IP address packs to your license to allow scanning of additional, external, IP addresses.

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**