SECTIGO

Securing the Breadth of Enterprise Use Cases with PKI

A WHITEPAPER FROM SECTIGO

Introduction: The Enterprise Security Imperative

Today, more than ever, our economy relies on data and digitally disruptive business models. Whether you are looking to improve customer experience, launch new products and services, open new routes to market, or streamline business operations, chances are data plays a key role. In fact, it's not going too far to consider data and information the lifeblood of the enterprise, and the most important thing to safeguard. Yet even as the further digitization of the enterprise and reliance on data opens new opportunities and sources of competitive advantage, it is also introducing new risks.

Never before have organizations been so vulnerable to digital threats, and never before have the risks been so great. Every year the number and type of threat vectors increase, ranging from large-scale external attacks to phishing/identity attacks to guarding against internal malicious actors. This is forcing organizations to rethink their security stances and close potential vulnerabilities.

Regulatory compliance plays a key – and growing – role. There are over 100 data privacy laws and initiatives promoted by governments worldwide, including the EU's sweeping GDPR regulations, Germany's BDSG, and new California and New York standards on data privacy. This is in addition to industry-specific regulations including PCI DSS and FFEIC for the financial services industry; HIPAA HITECH in healthcare; and FedRAMP, NIST, fisma, and FIPS in the Federal Government, just to name a few.

Never before have organizations been so vulnerable to digital threats, and never before have the risks been so great

Regulatory Compliance

And even aside from meeting data security and privacy regulations, it is simply critical for businesses to protect sensitive customer, financial, and other proprietary data. The number of high-profile data breaches and malicious attacks abounds, and grows by the month, with the costs to these businesses being quite severe. Multiple instances of data breaches directly related to mismanagement of PKI certificates include:

- **The O2 4G network outage,** in which 32 million customers and numerous organizations lost connectivity for an entire day in December 2018.
- **The Mirai botnet,** which was used in several high-profile distributed denial of service (DDoS) attacks in 2016, targeting more than 100,000 unsecured IoT devices, and bringing much of the U.S. Internet down.

One resounding lesson to come from these incidents is that no one is safe. In fact, the problem is particularly acute for large enterprises both because their high profile makes them a greater target, and because their larger customer base and deeper pockets mean there is often more at stake when breaches do occur.

Yet despite all of this, many enterprises' digital infrastructures are insufficiently secure. Too many lack secure data encryption, both for data at rest and for data in motion; too few use digital identity for a full range of enterprise use cases; and for organizations with emerging connected device/Internet of Things business models, too many of those devices represent a significant security vulnerability.

Too many enterprises lack secure data encryption and digital identity, and too many connected devices represent a significant security vulnerability

The Role of PKI in Ensuring Privacy, Integrity, and Security

Public-Key Encryption (PKI) is the gold standard in digital privacy, identity, and security, and should unquestionably be the security foundation for every device, server, user, and application in the enterprise. Encrypting data at rest and in transit guards against theft or tampering, and by guaranteeing digital identity you can more securely authenticate users and applications while guarding against identity fraud.

While this isn't news to any enterprise security officer, and practically every enterprise has incorporated PKI into its Web and device security stance in some way, not all enterprises are fully or appropriately leveraging the advantages of PKI. Two main problems stand in the way of enterprises looking to leverage PKI to the fullest possible extent.

The first is simply the complexity of managing a large pool of certificates and keys spread across the enterprise. Issuing, managing, and revoking/renewing/replacing certificates and keys numbering in the thousands, tens of thousands, or even millions (depending on the enterprise and use case) is extremely difficult. It's hard enough to manually track all of the certifications used by all the business units, departments, and organizations across the enterprise's IT infrastructure, but it's even harder to manually revoke, renew, and replace certificates when required. This makes it far too easy for organizations to operate with expired certificates, leaving them exposed to malicious actors and threats.

Public-Key Encryption (PKI) is the gold standard in digital privacy, identity, and security, and should unquestionably be the security foundation for every device, server, user, and application in the enterprise

The other problem is that many organizations are thinking about PKI too narrowly. While most use SSL PKI certificates to protect public-facing websites, there is a broad range of digital assets and use cases that can and should be protected using PKI. Some of these non-obvious use cases include securing mobile devices, DevOps/application development, cloud/multi-cloud environments, and the Internet of Things.

Sectigo offers a variety of solutions designed to solve both of these problems.

Sectigo Enterprise PKI Offerings

Sectigo provides purpose-built, automated PKI solutions securing websites, connected devices, applications, and digital identities. The Sectigo Certificate Manager provides unique capabilities to address enterprise-scale requirements. It covers five primary offerings:

- Enterprise SSL
- Private PKI
- Zero-Touch Touch S/MIME Email Encryption
- Code Signing
- Document Signing

Sectigo provides purpose-built, automated PKI solutions securing websites, connected devices, applications, and digital identities

Enterprise SSL

Sectigo Certificate Manager is a complete certificate management solution enabling enterprises to track and manage SSL certificates throughout their lifecycle, from issuance to renewal, replacement, and revocation. Its Enterprise SSL features let administrators easily manage certificate deployments regardless of the size of their deployment, both in the cloud and behind their firewall.

Sectigo Certificate Manager offers a number of capabilities to simplify enterprise SSL deployments:

- **Single-pane-of-glass management interface** speeds and simplifies the discovery, issuance, deployment, and renewal/revocation/replacement of all certificates, regardless of where they are located in the enterprise.
- **Interoperability** with all leading devices, operating systems, and load balancer/web server vendors (including APACHE, NGINX, IIS, IBM, and Oracle) as well as support for public cloud, private cloud, and on-premises environments. With Sectigo's support of ACME, no CA has a wider range of interoperability, which means Sectigo provides greater choice and allows organizations to better secure their infrastructure, regardless of their technology stack(s).
- **Automated, "zero-touch" management features** streamline certificate lifecycle management processes with the unique ability to perform initial installation, as well as revocation/renewal/replacement automatically, without manual intervention. This makes life easier on administrators, freeing up their time for more valuable tasks.

Enterprise SSL is the ideal solution to help enterprises secure a wide range of websites including:

- Ecommerce sites
- Financial services sites
- Customer service sites
- Governments' constituent relations sites
- Intranets
- Customer information sites
- Data gathering sites

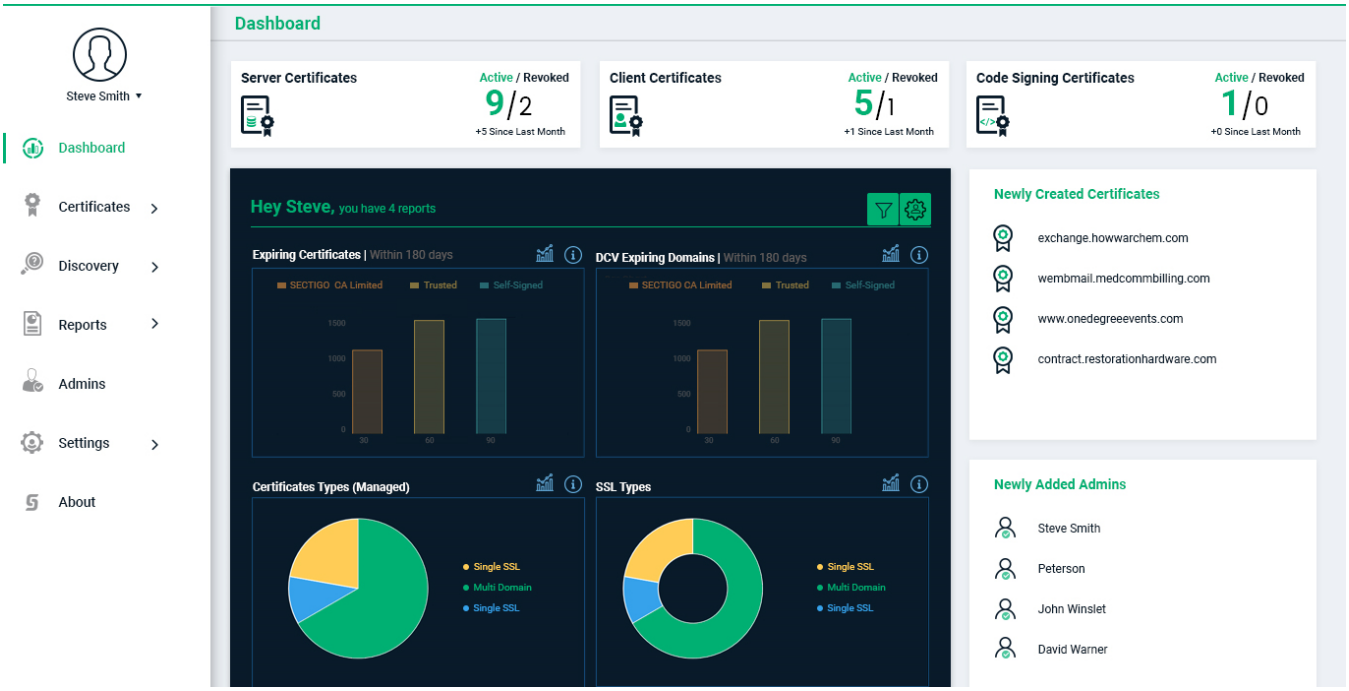


Figure: The Sectigo Certificate Manager dashboard offering single-pane-of-glass management

Private PKI

Enterprises often choose to establish their own certificate authorities, which they use to issue PKI certificates for internal use within their organization, or among their suppliers and vendors. They often use these Private CAs to support a number of use cases including mobile devices, IoT, DevOps, and cloud/multi-cloud. Microsoft Active Directory Certificate Services is a private certificate authority feature that comes with Windows servers, and many enterprises have adopted it as their Private CA. And while Microsoft Active Directory Certificate Services can be an acceptable solution for managing certificates for Windows-based servers and devices, it doesn't help with non-Windows devices.

And yet non-Windows devices proliferate across the enterprise, and many of today's use cases must work with both Windows and non-Windows devices. Microsoft Active Directory Certificate Services is not a viable option for these use cases, so Sectigo offers an enterprise Private PKI service, which lets enterprises secure both Windows and non-Windows devices and use cases.

Sectigo Private PKI secures and automates the management of internal devices and applications regardless of which internal protocols the enterprise has in place. And Sectigo

Private PKI also provides an upgrade path for enterprises to manage all Windows and non-Windows devices using a single Private CA, if they so choose.

Sectigo Private PKI is the ideal solution for a wide number of use cases across the enterprise:

- **Supplementing Microsoft Active Directory Certificate Services:** Augment your Microsoft certificate authority implementation to manage all non-Windows devices and applications – or replace it outright and manage all Windows and non-Windows device certificates with a single pane of glass.
- **Mobile devices:** Automate certificate installation on mobile devices to authenticate applications, S/MIME email encryption, mobile browsers authentication, and Wi-Fi authentication.
- **Internet of Things (IoT):** Automate the installation and management of certificates on connected embedded devices.
- **DevOps:** Ensure the identity and integrity of containers, the code that they contain, and the production applications that use that code.
- **Cloud/multi-cloud:** Secure cloud-based instances of applications and virtual servers, at a single cloud provider or across multiple providers, and both for single-tenant and multi-tenant environments.

Sectigo Private PKI

Sectigo Private PKI secures and automates the management of internal devices and applications regardless of which internal protocols the enterprise has in place

- **Web servers:** Automate the management and installation of certificates to secure web servers, load balancers, and web server farms.
- **SSH key management:** Discover keys that continue to allow access for past employees, and issue new certificates to employees, replacing the older key approach.
- **Private S/MIME:** Use S/MIME to provide identity and encryption for email and other enterprise use cases.
- **Intranet sites:** Protect your company's confidential information on internally-facing web sites.
- **Wi-Fi access:** Improve user experience with password-free Wi-Fi access, while improving security and ensuring that only authorized users are accessing your network.
- **VPN access:** Improve user experience and save money by replacing cumbersome VPN authentication solutions with password-free certificate-based authentication.
- **Point of Sale (POS) systems:** Protect POS sysems and ensure only authorized POS terminals can connect to your payment system.
- **Networking devices:** Improve authentication security for network switches and routers.
- **Windows Hello for Business:** Present users' digital identity as part of Windows' muti-factor authentication (MFA) to replace passwords while providing greater authentication security.

Zero-Touch S/MIME Email Encryption

Sectigo is the first and only certificate authority offering Zero-Touch Email Encryption to automate S/MIME email PKI deployment across the enterprise. Using S/MIME for email allows both the sender and recipient to use their existing S/MIME-capable email applications, as opposed to other approaches that require users to open a second email application or web portal and disrupt the users' experience.

And when it comes to deployment, with other certificate authorities, users must go through a cumbersome and error-prone process of downloading and installing S/MIME certificates onto their email client. In contrast, Sectigo's Zero-Touch Email Encryption lets users deploy PKI with a single click. It automatically publishes certificates to the corporate global address list, eliminating the need for users to back up their keys and removing users' certificate renewal headaches.

Sectigo Zero-Touch S/MIME Email Encryption is the ideal solution for:

- **Email signing:** Ensure emails actually came from the intended sender, guarding against fraud vectors such as phishing and business email compromise (BEC).
- **Email encryption:** Safeguard against emails or attachments being altered in transit, so malicious actors cannot intercept or read email.
- **Mobile email encryption:** Encrypt and establish email identity on Apple and Android devices, while removing users' burden to install certificates and keys.

Zero-Touch S/MME Email Encryption

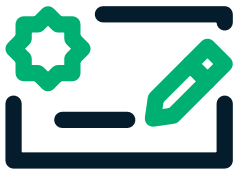
Sectigo is the first and only certificate authority offering Zero-Touch Email Encryption to automate S/MIME email PKI deployment across the enterprise

- **Mobile Wi-Fi access:** Improve user experience with password-free Wi-Fi access for Apple and Android devices, while improving security and ensuring that only authorized users access your network.
- **Mobile website authentication:** Eliminate the need to use passwords to authenticate to cloud services or single-sign-on via mobile devices.

Code Signing

Sectigo Code Signing certificates enable developers to digitally sign applications and software programs to verify the source of the file and ensure that it has not been altered in any way. Unlike code signing products from many other vendors, Sectigo assists with the entire software lifecycle from managing approval to signing operations to subsequent maintenance.

Sectigo Code Signing supports 32-bit or 64-bit code and supports all file types from drivers and firmware to scripts and applications. And with our enterprise-scale issuance, management, and renewal/revocation/replacement features, development teams have greater cryptographic flexibility and improved time to market.



Code Signing

Sectigo Code Signing certificates enable developers to digitally sign applications and software programs to verify the source of the file and ensure that it has not been altered in any way

Enterprise Code Signing is the ideal solution for:

- **Application development:** Digitally sign software to protect end users from downloading and installing compromised software.
- **DevOps:** Ensure containers and the code developed within them are the code you intended it to be.
- **Connected devices (Internet of Things):** Enable secure boot, letting you verify devices' bootloader, microkernel, OS, and applications and reducing malicious actors' ability to compromise them.
- **Mobile devices:** Improve security and trust associated with mobile applications and the devices they run on.

Connected Devices and Internet of Things (IoT)

Sectigo's IoT Platform is the first and only security solution that combines comprehensive hardening technology for embedded devices with third-party certificate issuance and management purpose-built for the Internet of Things. Sectigo's IoT Platform features embedded security solutions for device hardening including secure boot, embedded firewall, TPM integration, and secure firmware updates with alerts, along with certificate issuance and management from cloud native or on-premise CAs, purpose-built for IoT.

Part of the Sectigo IoT Security Platform, 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 Manager uses a secure, cloud-based portal to issue trusted, third-party PKI certificates to be assigned to devices for

IoT Platform

Sectigo's IoT Platform is the first and only security solution that combines comprehensive hardening technology for embedded devices with third-party certificate issuance and management purpose-built for the Internet of Things

authentication and lifecycle management. This is all in a solution that's cost-effective, efficient, and automated.

IoT Manager's high-availability, batch-issuance system allows administrators to easily enroll, download, and decrypt certificate batches quickly and efficiently. It meets requirements for many industry standards, including WiMAX Forum, GSMA, Zigbee, OCF, and Joint Venture-Silicon Valley.

Building and securing your company's connected devices using Sectigo IoT Platform provides:

- **Peace of mind:** No one wants to suffer the next botnet catastrophe. PKI is the best approach to identity security, and incorporating it onto your devices protects what could otherwise be a major vulnerability for your business and a threat to your connected device business model. Choosing a partner with the experience, scale, and commitment to embedded device security of Sectigo will let you rest better at night.
- **Future-proofing for IoT business models:** By removing security as a barrier, you can fully unlock the data on your devices and maximize their value to your business. Whether you are using data for predictive maintenance, analytics, visibility, or control, Sectigo will help you maximize the value of your IoT business model. And many IoT products have lifetimes measured in decades. With the possible arrival of post-quantum computing in the not-too-distant future, today's cryptographic algorithms could be rendered obsolete. Sectigo IoT Platform enables you to update certificates over the air, on the fly, providing the cryptographic agility to ensure your devices are secure not only today, but for the remainder of their lifecycle.
- **Ease of operation:** Our device-hardening technologies and certificate issuance, provisioning, and lifecycle management are purpose-built for connected devices, and are widely interoperable. This removes the pain associated with securely building, provisioning, and running embedded devices, both within your own enterprise and across complex device supply chains.

Sectigo IoT Platform is the ideal solution for:

- **Certificate issuance and provisioning:** Sectigo IoT Manager is purpose-built for IoT certificate issuance and provisioning. It is quick to implement, highly scalable, and rich in provisioning technologies such as EST, REST API, and a lightweight embedded agent, enabling you to adjust your provisioning depending on your needs.
- **Certificate lifecycle management:** Use our lightweight embedded agent to perform certificate lifecycle management in the field.
- **Secure Boot:** Ensure the code running on your devices is the code you authorize. Multi-phase secure boot verifies the integrity of the device bootloader, microkernel, OS, and apps.
- **Monitoring and control:** Perform anomaly detection and identify traffic variances against pre-defined conditions.
- **Secure key storage:** Securely store certificates on your devices, using our integration library to the Trusted Platform Module (TPM) or use our software-based secure certificate storage.
- **Data at rest encryption:** Encrypt the data on your devices and protect it from malicious actors.
- **Data in transit encryption:** With TLS library support, protect data as it's transmitted across network boundaries.
- **Over-the-air updates:** Enable secure firmware updates in the field.

Securing your company's connected devices using Sectigo IoT Platform provides peace of mind, future-proofing for IoT business models, and ease of operation

Conclusion: Gain Peace of Mind by Making Sectigo PKI the Foundation of Your Enterprise's Digital Security

Securing your enterprise digital infrastructure is vitally important, but it is also hard. Sectigo is one of the world's leaders in PKI, having been a pioneer in SSL and related security technologies, and it continues to invest in new technologies, standards, and solutions to remain at the leading edge of security.

Let Sectigo play a key role in securing your enterprise. With Sectigo, you get greater:

- **Choice:** Sectigo's core philosophy revolves around interoperability and the use of open standards as our foundation. We can support any situation, any protocol (such as ACME, REST, and EST), and any use case, regardless of your IT infrastructure. And if anything should go wrong, you have a single, 24/7 point of contact.
- **Ease of use:** Unlike other companies, Sectigo is laser-focused on PKI, both as a public CA and as a leading provider of private PKI. Take advantage of our certificate deployment automation and single-pane-of-glass management/reporting technologies to centralize and simplify the tedious tasks associated with certificate lifecycle management and free your team's time up to focus on more valuable tasks.
- **Future-proofing:** Sectigo is the world's leading commercial CA, and is constantly investing in new technologies and solutions. When you partner with us you can rest assured your organization will remain at the leading edge of cryptographic technologies, and our automated certificate renewal technologies provide cryptographic agility, helping you guard against a possible post-quantum computing "crypto-apocalypse."
- **Peace of mind:** All of this leads to greater peace of mind. Sectigo is used by 700,000 businesses in all industries and corners of the globe, including 35 percent of the Fortune 500. Our size, scale, leadership, and continued investment in PKI means there is no better partner to secure the foundation of your digital infrastructure. And with the addition of Icon Labs, we offer a unique ability to secure connected (IoT) devices not only through our automated certificate lifecycle management purpose-built for IoT, but also through our comprehensive technology to harden the devices themselves.

About Sectigo

Sectigo provides purpose-built, automated PKI solutions that secure websites, connected devices, applications, and digital identities. As the largest commercial Certificate Authority trusted by enterprises globally for more than 20 years, and more than 100 million SSL certificates issued in over 200 countries, Sectigo has the proven performance and experience to meet the growing needs of securing today's digital landscape. For more information, visit **www.sectigo.com.**