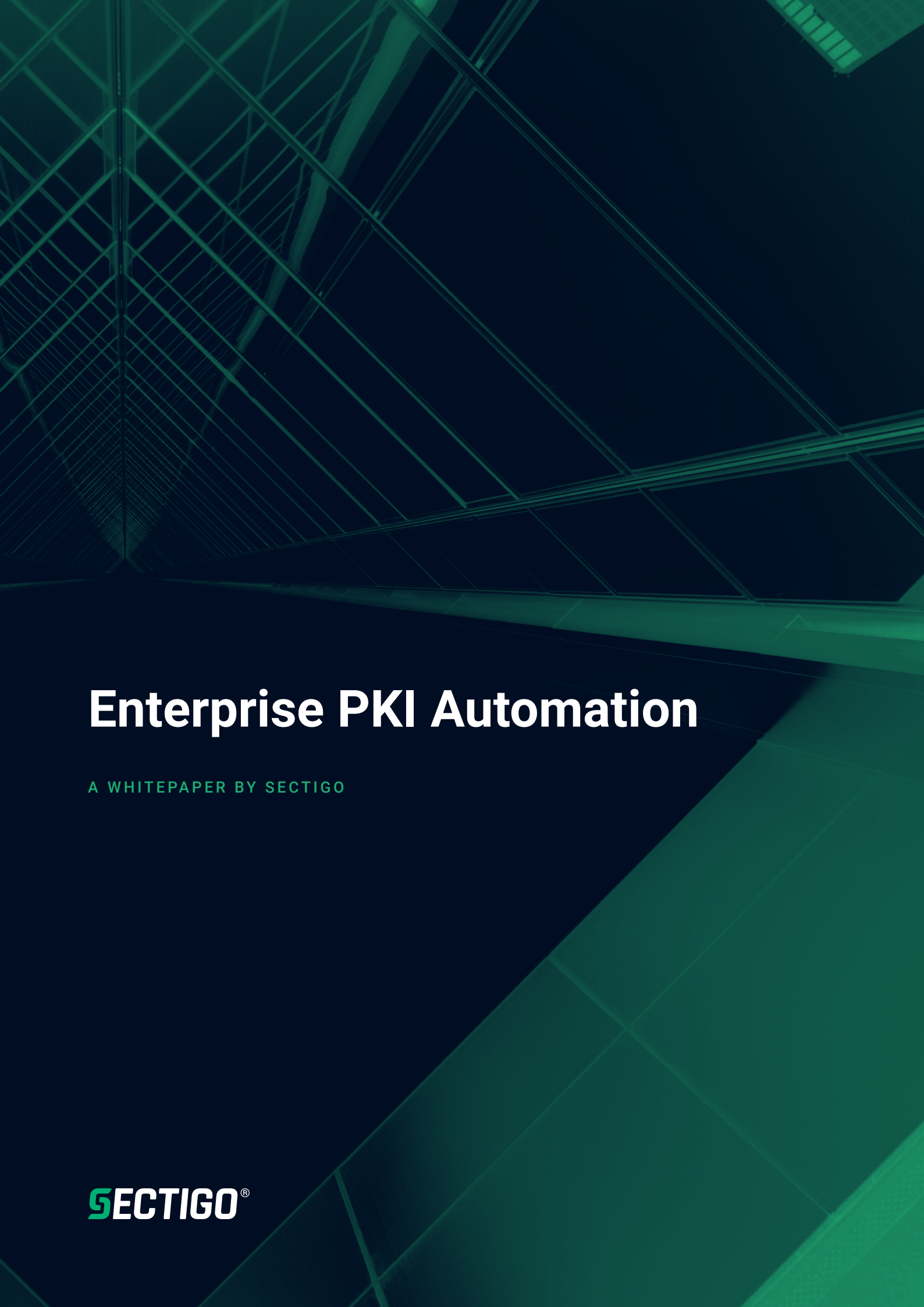


# Enterprise PKI Automation

A WHITEPAPER BY SECTIGO

SECTIGO®

# Enterprises Need an Authentication Solution to Address Increasingly Complex Requirements

**Enterprise authentication needs are becoming increasingly complex. Applications and data running across multiple cloud environments, a distributed workforce, and innovative connected devices are all intersecting in ways that demand a strong digital identity approach to protect against constantly evolving threats.**

Enterprises rely on PKI certificates as the gold standard for ensuring identity and as a foundational part of a Zero Trust, passwordless architecture for users, devices, servers and application identities.

While there is no stronger, easier to use authentication and encryption solution than the digital identity provided by PKI, the challenge for busy IT teams is that manually deploying and managing certificates is time-consuming and can create unnecessary service outages. Whether an enterprise deploys a single SSL certificate for a web server or manages millions of certificates across all its networked device and user identities, the end-to-end process of certificate issuance, configuration, and deployment can take hours per certificate. Manually managing certificates also puts enterprises at significant risk of certificates being forgotten until expiration and of exposure to gaps in ownership, resulting in sudden outages of critical business systems.

# The Financial Cost of Manual Certificate Management

As already-complex environments expand to include mobile devices, cloud infrastructure, DevOps, Internet of Things, and more, the financial cost to effectively manage PKI certificates has increased dramatically.

The most effective security investment is security that is both easily deployed and easily used by employees. But security solutions like passwords often burden individual users with remembering, updating, and managing their own security. And IT teams are inundated with time-consuming password reset requests, and training employees not to surrender their passwords to sophisticated phishing schemes. As an example, if the employees cannot encrypt/decrypt on their mobile device, they will simply bypass using email encryption.

Additionally, your customers as well as internal users rely on critical business systems to be always on. Expired certificates have already led to numerous high-profile website and services outages. resulting in billions of dollars in lost revenue, contract penalties, and lawsuits as well as the significant loss of brand reputation.

Insufficient certificate management can also put enterprises in jeopardy of noncompliance with regulatory mandates. To guard against information theft, regulations such as HIPAA/HITECH, GDPR, and the U.S. federal government acquisition rules (DFARS) require data encryption to mitigate or minimize the consequences of a breach or accidental disclosure. Not meeting compliance requirements can result in substantial fines. Further, GDPR mandates that fines are not only based on the scale of an individual breach, but also on the level of negligence. So putting strong protection on your systems and devices not only helps reduce the risk of a breach itself but helps reduce the amount of the fine should a breach occur.

# Administration Costs Add up Quickly

Certificate management may be perceived as a simple, day-to-day task for an IT or web administrator, but ensuring certificates are valid one at a time is costly. Using manual processes to discover, install, monitor, and renew all the PKI certificates in an organization is labor-intensive and technically demanding.

For example, even a minimal manual SSL certificate installation with a single web domain involves multiple steps and can easily add up to over $50 per web server. Figure 1 breaks down each step a web administrator is required to perform to correctly install a single SSL certificate. For an organization with 2,000 web servers, it would require one person working full time to just replace certificates before they expire.

**Figure 1** – Steps Required to Manually Install SSL Certificates

| Steps | Time |
|---|---|
| Selection/Purchase of SSL Certificates | Minutes to Hours |
| SSH Login to the web server | < 2 Minutes - Look up of server address & credentials. |
| Enter a set of commands to achieve domain control validation (for new domains) | Minutes to Hours - Read documentation, type appropriate commands. Web admin forums are filled with Q&A and troubleshooting, suggesting that many have problems with this step. |
| Request issuance of the certificate and download | Up to 5 to 10 Minutes - Read documentation, type appropriate commands. |
| Copy the certificate files to the appropriate server file location (varies based on web server) | <2 Minutes - Look up of server file location, type appropriate commands. |
| Modify the web server configuration file to enable the web server to utilize the SSL certificate and publish https | Minutes to Hours - Read documentation, type appropriate commands, save file. Web admin forums are filled with Q&A and troubleshooting, suggesting that many have problems with this step. |
| Refresh//Restart the web server in order to recognize the configuration | <1 Minute |
| Test | Minutes to Hours - If no error messages then testing will be quick. Responding to error messages will require re-modifying the web server configuration file. |
| All of the above steps must be done precisely. Otherwise, human time and effort is wasted, and critical business systems will be taken out of service. | |

# Cryptographic Evolution Creates New Enterprise Security Challenges

Now enterprises face another new security threat as cryptography evolves. Within a few short years, quantum computing will render the current RSA and ECC encryption algorithms that our digital systems depend on worthless. While NIST and Certificate Authorities like Sectigo's Quantum Labs are developing quantum-safe X.509 certificates that use encryption algorithms to withstand quantum computing, it is clear that enterprises will have to adopt entirely new families of cryptography with unprecedented speed.

For a company that has 10,000 certificates manually installed across users, servers, devices, and applications, it would take up to five people one year to find and replace all the certificates. Before they are done, the bad guy will exploit the weak cryptography to impersonate the rightful owner or decrypt sensitive information.

# The Modern Enterprise Needs Automated Solutions

With the pitfalls and financial ramifications inherent in managing PKI certificates manually, the return on investment for automated certificate lifecycle management is clear. IT professionals must rethink their certificate lifecycle management strategy. Particularly as enterprises go to market more quickly with new services enabled by DevOps, organizations need an automated solution that ensures certificates are correctly configured and implemented without human intervention. This automation not only eliminates service outages but allows IT departments to control operational costs and launch services to market faster.

Recently, PKI has evolved to become even more versatile. Interoperability, high uptime, and governance are still key benefits. But today's PKI solutions are also functionally capable of improving administration and certificate lifecycle management through:

### Automation

Speed up deployment of certificates while eliminating costs and errors

### Scalability

Managing certificates numbering in the hundreds, thousands, or even millions

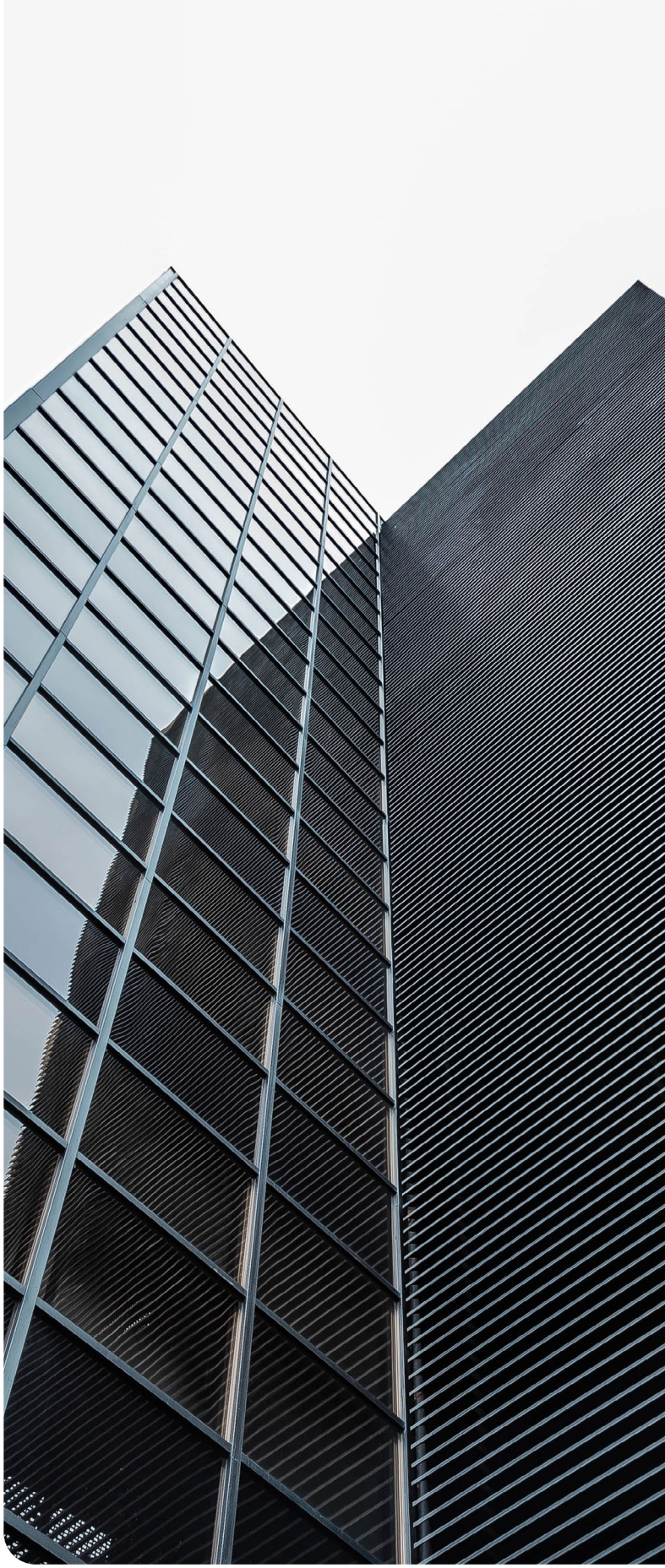
### Crypto-agility

Updating cryptographic strength and revoking and replacing at-risk certificates with quantum safe certificates very quickly in response to new or changing threats

### Visibility

Viewing certificate status with a single pane of glass across all users, devices, servers and applications

# Save Time and Maintain Control With Sectigo PKI Automation



Given the disparate systems, applications, and devices that use digital certificates, IT teams often manage distinct automation services from many different vendors, with different user interfaces, and quality of support. A single certificate management dashboard that automates discovery, deployment, and lifecycle management across all use cases and vendor platforms creates the efficiency that automation promises. And IT teams still maintain control of configuration definitions and rules so that automation steps are performed correctly.

Sectigo provides certificate automation solutions that allow enterprises to be agile and efficient, and maintain control of all the certificates in their environment. Sectigo supports automated installation, revocation, and renewal of SSL/TLS and non-SSL certificates via industry standard protocols, APIs, and third-party integrations.

Moreover, with Sectigo, you will never run into a certificate volume cap, as you might with open source alternatives. Sectigo's automation solutions enable your security team to easily enforce cryptographic security policy; protect communications; prevent data loss via unauthorized access; and future-proof systems, applications, and devices across the enterprise.

# Automating Management of SSL/TLS Certificates

For SSL/TLS certificates, Sectigo provides automated certificated management through:

- **Support for Automated Certificate Management Environment (ACME) protocol:** Sectigo Certificate Manager supports the protocol ACME, allowing you to automate certificate issuance, installation, and revocation for a wide range of web servers and load balancers. The ACME protocol requires very little time for IT teams to configure and execute their certificate management automation, making it an increasingly adopted component of enterprise security.

Sectigo supports DV, OV, EV and private SSL certificate types via ACME and provides full control to IT administrators. Sectigo provides the ACME server and works with ACME-compliant clients, including Certbot by the Electronic Frontier Foundation (of which Sectigo is a sponsor). See Figure 2 for how certificate authentication works using ACME.

## How the ACME Protocol Works for Automated PKI Certificate Management

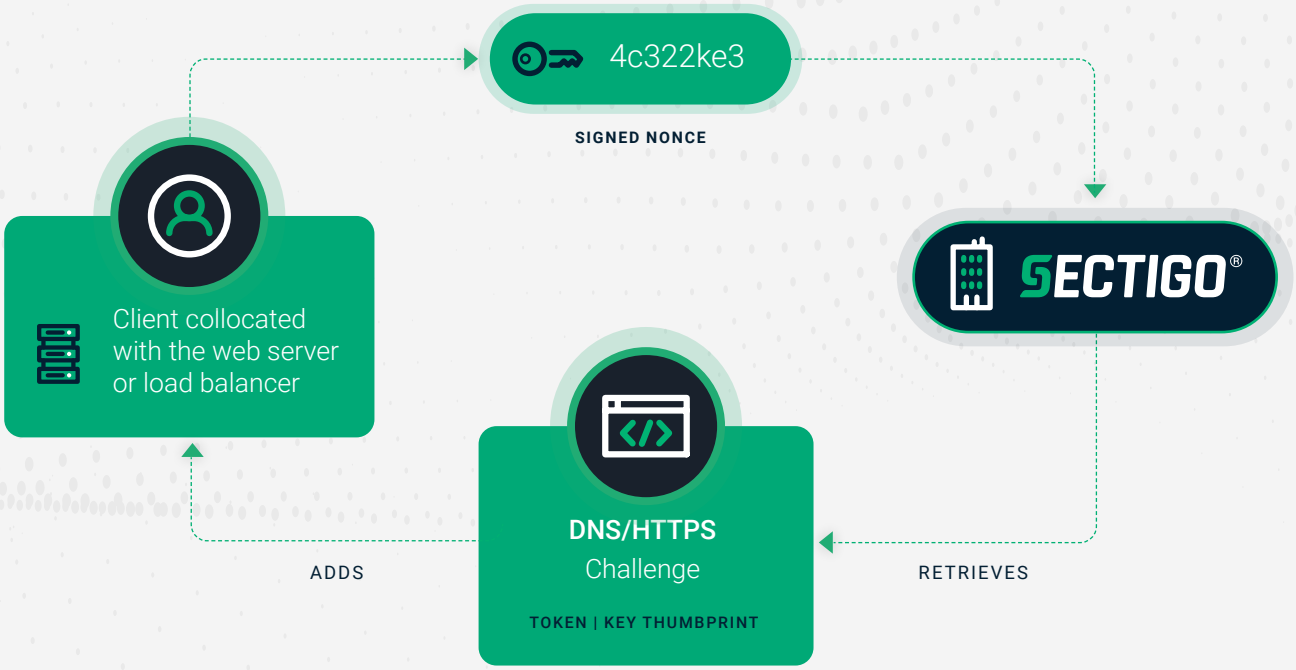



**Figure 2** – Authentication process using ACME protocol

# Automating Management of SSL/TLS Certificates

- **REST API:** In some instances, companies prefer to integrate applications with Sectigo using Sectigo's REST API. While this requires additional development on the application side, it allows you to leverage certificate management and customize your workflow.

  Additionally, through the REST API, Sectigo has direct integrations with all leading containerization and automation tools environments, such as Docker, Chef, Ansible, Salt Stack, Terraform, Puppet, and Jenkins. We also include mechanisms to incorporate PKI into the continuous integration and continuous deployment (CI/CD) pipeline, orchestration frameworks such as Kubernetes, and third-party key vaults such as HashiCorp's Vault.

- **A customer premise automated install agent:** Using Sectigo's Network Agent, you can automate certificate management for a variety of systems, including Apache, Tomcat, IIS and F5 web servers. The customer premises Network Agent is integrated with Sectigo Certificate Manager to schedule issuance, installation, and renewal of certificates.
- **Integration with Third Party Vendors:** Sectigo directly integrates with leading third party vendors to help customers achieve full certificate automation using popular technologies already in place in IT environments, like F5's Big-IP load balancer, Citrix's ADC application delivery controller, and ServiceNow's IT workflow platform.

  See Figure 3 for a list of currently supported platforms and technologies.

**Figure 3** – Currently supported automation solutions for SSL/TLS certificates

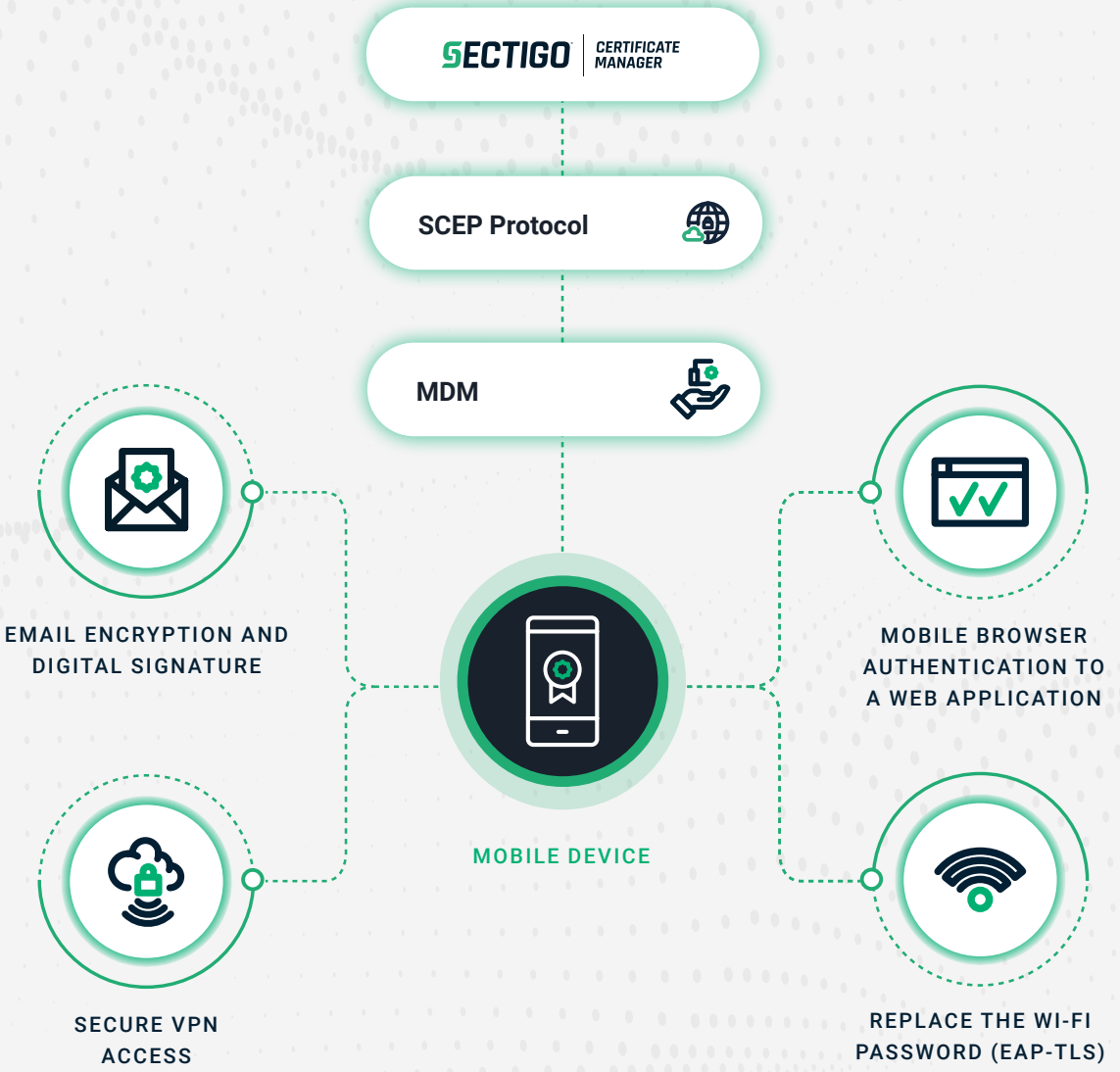
| Web Server/Network Gear/DevOps Tools | | Customer Choice | | | |
|---|---|---|---|---|---|
| **Type** | **Platform** | **Sectigo Installation Agent** | **ACME** | **Sectigo REST API** | **Custom Integration** |
| Web Server | Apache HTTP Server | Yes | Yes | Available | |
| | Apache Tomcat | Yes | Yes | Available | |
| | IIS | Yes | Yes | Available | |
| | NGINX | | Yes | Available | |
| | Other Certbot supported web servers | | Yes | Available | |
| Load Balancer | F5 | Yes | Yes | Available | Yes |
| | Citrix ADC (formerly NetScaler) | | Yes | Available | Yes |
| IT Service Management | ServiceNow | | | Available | Yes |
| DevOps Tools | Ansible | | | Available | |
| | AWS ELB | | Yes | Available | |
| | Chef | | | Available | |
| | Docker | | | Available | |
| | HashiCorp Vault | | | Available | |
| | Jenkins | | | Available | |
| | Kubernetes | | Yes | Available | |
| | Puppet | | | Available | |
| | SaltStack | | | Available | |
| | Terraform | | | Available | |

# Automating Non-SSL Certificate Installation

Many systems, applications, and devices utilize non-SSL certificates, an example being identity certificates for mobile devices. For non-SSL Certificate Installation, Sectigo provides:

- **Enrollment over Secure Transport (EST) protocol:** Sectigo supports the EST protocol, which is used for managing networking gear from many vendors. In fact, a number of vendors have EST support already built in. EST is also popular in Internet of Things (IoT) environments given the efficiency of the protocol and support of Elliptic Curve Cryptography (ECC) keys. Sectigo offers a commercial EST client and supports the several open source EST clients available as well.
- **Simple Certificate Enrollment Protocol (SCEP):** SCEP has been around for nearly two decades and has gained significant traction with businesses. As the SCEP protocol has no licensing fees and requires very little time for IT teams to configure and execute, it has become an almost ubiquitous component of enterprise security. Mobile Device Management (MDM) systems like Microsoft Intune and AirWatch use SCEP for PKI certificate enrollment. This allows mobile devices to replace the Wi-Fi password and authenticate for VPN. Most networking gear, including routers, load balancers, Wi-Fi hubs, VPN devices, and firewalls, also support the SCEP protocol for certificate enrollment.

**Figure 4** – SCM uses SCEP to pass certificates to the MDM which installs them into the mobile device




In the Sectigo environment, SCEP can be used to enroll certificates in Linux, MacOS, and other operation systems.

- **Microsoft Agent:** A Sectigo Proxy Server can sit between the Microsoft Desktop and the Active Directory Certificate Service. It intercepts certificate requests made over the Windows Client Certificate Enrollment Protocol (WCCE) and automatically provides the certificate to the desktop without any employee intervention.
- **Sectigo Mobile Certificate Manager (MCM):** Sectigo MCM issues and manages certificates and keys across iOS, Chrome OS and Android mobile devices with little or no user intervention. It supports all certificate types and is interoperable with all leading devices, operating systems, and enrollment protocols. Sectigo uses an MDM built into our Certificate Manager or a self-service web portal approach, depending on customer requirements.

# Automating the Installation of Certificates Issued by ADCS

Using Microsoft's Active Directory Certificate Service (ADCS), IT administrators can instruct all desktops and servers to automatically enroll and renew certificates issued by active directory certificate services. But this automation only applies to applications using a Windows operating system. Today's enterprises have devices that do not utilize Microsoft operating systems, meaning the administrator and employee share the burden of manually renewing and installing certificates for any non-Microsoft applications or devices. For these certificates, administrators often employ an error-prone method using spreadsheets to manually track when certificates were issued, where they were installed, their cryptographic strength, when they expire, and who is responsible for them.

**Sectigo offers these options:**

- Continue to utilize ADCS as your Root CA, establish Sectigo as the CA which issues certificates and automatically installs the certificates into the device or application. The enterprise does not need to embed the root CA again.
- Continue to utilize ADCS as the CA which issues the certificates. Sectigo certificate manager will discover the ADCS issued certificates, report on certificate attributes/ ownership, and send notifications prior to expiry.
- Replace both the ADCS root and issuing CA with the Sectigo CA. This eliminates the cost of operating ADCS, while fully automating certificate issuance and installation.

**ADCS cannot automatically install certificates for many common enterprise use cases, including:**

- Web servers
- Apple, Android, Chromebook mobile devices, without a mobile management system
- Azure key vault
- People or device identities not in the Microsoft Active Directory
- Load balancers
- Networking gear
- Code signing
- DevOps containers
- Authentication of server administrators using SSH
- Publicly trusted Secure/Multipurpose Internet Mail Extensions (S/MIME)
- Document signing trusted by Adobe Reader, Adobe Sign
- Internet of Things devices
- Ability to provision the same encryption key history to all devices owned by the same user

Sectigo Certificate Manager augments ADCS by automating the installation of certificates, removing the need for costly, error prone manual management. Certificate Manager ensures the enterprise certificates are properly managed and won't unexpectedly expire.

# Conclusion: Gain Peace of Mind by Automating PKI with Sectigo

**PKI is the best technology for eliminating passwords and ensuring only authorized devices and users access enterprise systems.**

Sectigo pioneered SSL and related technologies and is now a world leader in PKI. Sectigo continues to invest in new technologies, standards, and solutions to remain at the leading edge of security, and protect your business from digital threats.

## With Sectigo, you get greater:

### Choice

With Sectigo's core philosophy around interoperability and the use of open standards such as ACME, SCEP, and EST as our foundation, you can rest assured you will have a wide degree of choice and control over your PKI solution. 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 digital identity, both as a public CA and as a leading provider of private PKI. By taking 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, you will be able to free your team to focus on higher value tasks.

### Value

Under the Sectigo licensing model, we do not charge per issuance, but rather per usage. Certificates that are no longer in use (e.g., when someone leaves your company) can be transferred.

### Futureproofing

Sectigo is the world's leading commercial CA, and we are constantly investing in new technologies and solutions. When you partner with us, you can rest assured your enterprise will remain at the leading edge of cryptography as your needs change and grow. Our automated technologies will ensure cryptographic agility to adjust for advances in computing and cryptographic techniques that require updates to your hashing and encryption algorithms.

### Peace of Mind

All of this leads to greater peace of mind. Sectigo is WebTrust and SOC 3 compliant, and our connections with the CA/Browser Forum and select government entities help ensure we receive early alerts on PKI security concerns. In addition, our open source approach helps reduce security vulnerabilities. With Sectigo's size, scale, leadership, and continued investment in PKI, there is no better partner to secure the foundation of your digital infrastructure.

Sectigo is a cybersecurity technology leader providing digital identity solutions, including TLS/SSL certificates, web security, DevOps, IoT, and enterprise-grade PKI management. As the world's largest commercial Certificate Authority, with more than 700,000 customers worldwide and 20 years of experience delivering online trust solutions, Sectigo provides proven public and private trust solutions for securing web servers, digital identities, connected devices, and applications. Recognized for its award-winning innovations and best-in-class global customer support, Sectigo delivers the technologies required to secure the digital landscapes of today, as well as tomorrow.

For more information, visit www.sectigo.com and follow @SectigoHQ