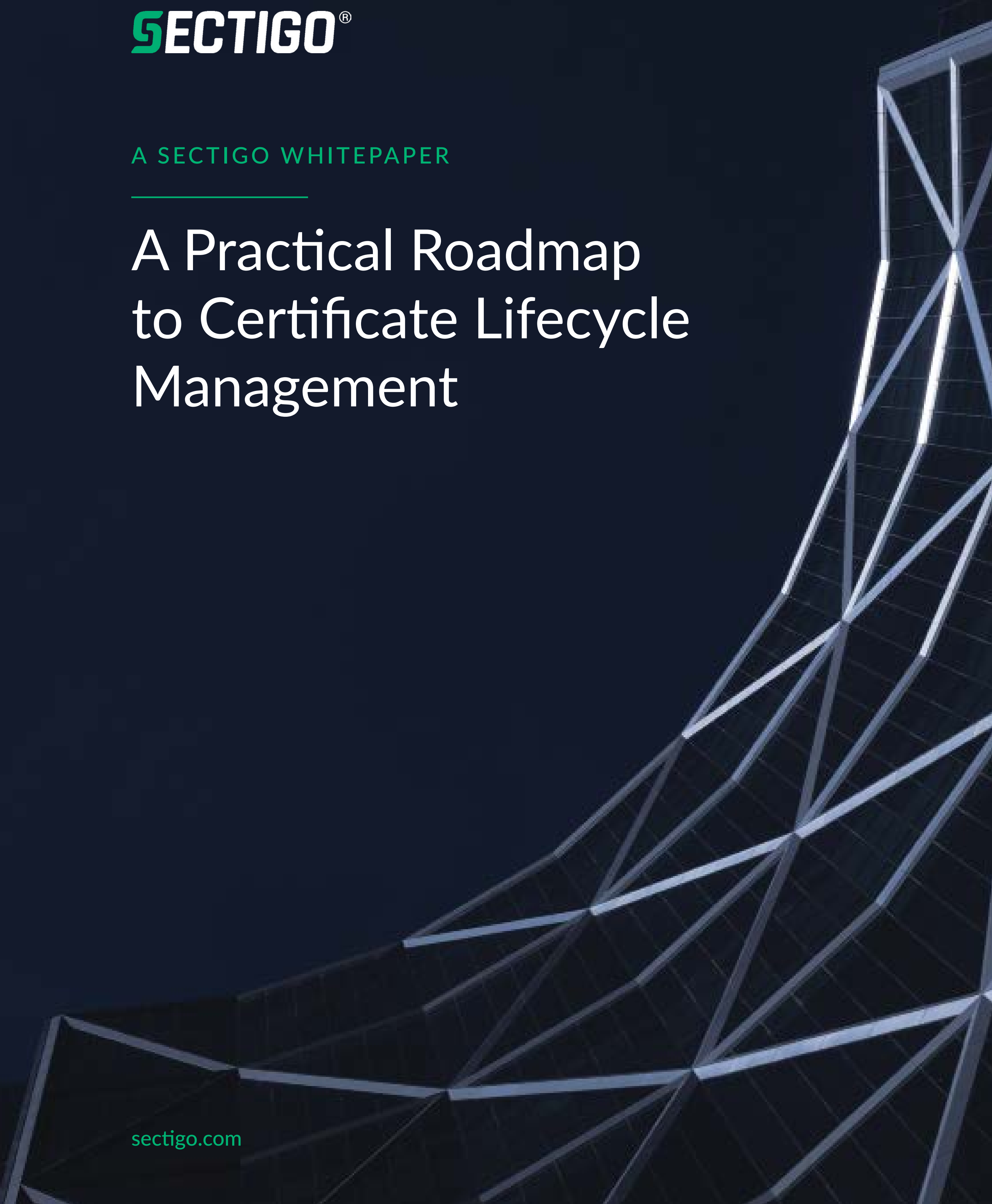
SECTIGO®

A SECTIGO WHITEPAPER

A Practical Roadmap to Certificate Lifecycle Management



sectigo.com

Enterprises face fundamental IT security challenges with the management of human and machine identities

The walled digital fortresses enterprises spent decades building are now empty. Or rather, they have undergone a profound change in the recent past. The IT architecture we all rely so heavily on has become increasingly complex. Multiple operating systems, cloud and hybrid multi-cloud environments, vast swathes of applications, devices, and emerging technology each add layers of complexity for the average enterprise IT team to contend with.

Further complicating these changes is the dramatic increase in the volume of digital identities and their variety over the past few years. The driving forces behind this growth are threefold:

1. Global digital transformation efforts over the past decade have caused the digitization of vast numbers of business processes.
2. New use cases that support critical business outcomes have skyrocketed.
3. The COVID-19 pandemic, which ushered a new era of remote working accelerated the already explosive growth of human and machine identities, all requiring remote access to enterprise networks.

Foreword by

David Mahdi

Chief Strategy Officer and CISO Advisor, Sectigo

Establishing digital trust – that is, trust in machines, software, devices, and humans interacting with digital services that now power our world – is essential to conducting business successfully and securely. This has resulted in a notable change of perspective for IT teams, forcing them to view identity as the new perimeter.

Digital trust is not a new concept. Even before the massive shift to remote and hybrid work environments, everyone possessed digital identities, which helped enable basic digital trust. The difference today is that digital identities are even more prevalent.

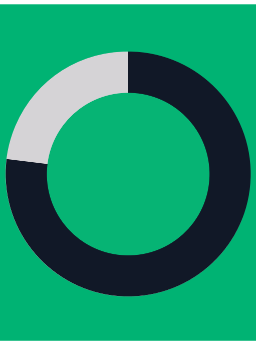
So, how can enterprises establish digital trust, prevent an identity management breakdown and protect the network and data against breaches and theft? A 2021 Sectigo research study of IT executives found 81% of enterprises find it challenging to manage digital identities. Yet, bad actors continue to use identity as an attack vector. This whitepaper will explore the main issues enterprise IT teams face with identity management, and will detail why an identity-first Security posture is the only way to establish digital trust in a rapidly changing business landscape.

Ineffective Digital Identity Management

Digital certificates issued by Certificate Authorities (CAs) establish digital trust and are the proven approach used to secure and authenticate human or machine identities. However, while critical, digital certificates require proper care and management.

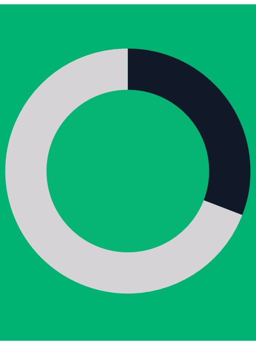
The IT security challenges associated with digital identity management can lead to an astounding number of costly consequences—from the obvious, such as erroneous provisioning and installation, to the less visible and far-reaching: certificate expiration and non-compliance. The dangers posed by haphazard digital identity management can compromise the entire lifecycle of an organization's digital presence. Ineffective identity management can also result in serious business outages, fines, a loss of time and reputation damage.

Recent research by Sectigo pinpoints the main problem areas enterprises face when approaching digital identity management.



of enterprises reported they find it challenging to successfully renew digital certificates without an outage

EMA IT Security Research, 2021



of enterprises have experienced outages due to expired, stolen or revoked certificates

EMA IT Security Research, 2021

ISSUANCE AND INSTALLATION

Identity management begins with the issuance and installation of digital certificates. A mistake, such as an incorrect validity period for a certificate, can have serious consequences. In fact, 52% of enterprises find error-free provisioning and installation of certificates to be difficult, according to Sectigo research.

MONITORING, REVOCATION, AND RENEWAL

In order to maintain a secure and compliant environment, robust certificate management must be performed effectively for each and every device, user, and application process. Yet 77% of enterprises reported that they struggle to successfully renew digital certificates.

MANUAL MANAGEMENT

Nearly half (47%) of organizations say they use spreadsheets, scripts, or CA-provided tools to manage digital identities. This manual approach to identity management hampers visibility into all digital identities and potentially creates an opportunity for bad actors to exploit. Monitoring the constant additions, removals, and modifications to certificates is impossible in a spreadsheet and is difficult at best with basic tools. Just 26% of respondents to the 2021 Sectigo research study rate their organization's visibility into all managed digital identities as "excellent."

OUTAGES

Outages to critical business systems can have a devastating impact on an organization's bottom line. Unfortunately, outages due to expired, forgotten, or simply improperly installed certificates are all too common. In fact, our research study shows that 31% of enterprises have experienced outages due to expired, stolen, or revoked certificates.

Global Regulatory Landscape

Compounding the already complex process of managing swathes of human and machine identities, enterprises today need to be aware of the growing number of wide-ranging legislation designed to safeguard Personally Identifiable Information. Compliance with multiple data protection regulations is no mean feat for even the largest of enterprises and ongoing adherence requires long-term commitment. Regardless of sector or geography, identity management is a critical aspect to get right for many regulations.

Poor digital identity management can put enterprises in jeopardy of non-compliance with regulatory mandates. Failure to meet compliance requirements can result in substantial fines. HIPAA laws, for example, are designed to protect sensitive patient health information and require a series of technical safeguards, specifically around data access control.

Additionally, the US federal government's DFARS defines instances and use cases that require data encryption to mitigate or minimize the consequences of a breach. If an organization falls out of compliance with these regulations, it can face significant financial penalties.

$888M

Amazon was recently fined $888 million by a European privacy watchdog over data violations

DFARS is not the only regulatory mandate with which an organization must contend. GDPR, or the General Data Protection Regulation, captured the enterprise world's attention when it went into effect on May 25, 2018. The regulation requires data encryption to protect against information theft vulnerabilities and stipulates significant fines for organizations that do not protect the personal data of their customers. For instance, Amazon was recently fined $888 million by a European privacy watchdog over data violations.

However, GDPR is merely the first of many privacy and security regulations that are expected to impact enterprises in the coming years. California's CCPA, Virginia's CDPA, and Vermont's Act 171 of 2018 Data Broker Regulation are all state-level regulations that will require certificate management for compliance. And that's just in the United States. International regulations are also on the horizon, including the UK's National Data Strategy (UK GDPR and DPA18); Canada's Consumer Privacy Protection Act (CPPA); India's planned Personal Data Protection Bill; and Singapore's Personal Data Protection Act (PDPA). Breaches of these regulations can result in substantial fines as well.

Identity-First Security and Digital Trust

‘Identity-first security’ is a term increasingly referenced by cybersecurity practitioners including leading industry analysts. It is now a top priority for every IT security department as the post-COVID technology landscape and threat factors have dramatically changed and continue to shift.

In light of the many challenges and high-risk consequences associated with digital identity management, enterprises need a way to automate their identity-first security stance, thus establishing digital trust. Yet with every identity requiring a certificate and the need for end-to-end management of the massive volume of certificates, regardless of the certificate origin, a new automated approach is required: **Certificate Lifecycle Management (CLM).**

CLM automates the certificate lifecycle, from provisioning to revocation. With CLM, enterprises can ensure that all certificates are properly installed, monitored, and renewed, providing organizations with the visibility and control they need to keep their digital environments safe and compliant.

CLM Needs Openness and Interoperability

For CISOs, CIOs, and their teams to successfully operate strong identity-first security, they cannot rely on a growing list of security products to function. To truly solve cybersecurity threats and help practitioners, identity and cybersecurity solutions need to break down existing silos and interoperate. For a CLM solution to meet the needs of enterprise IT leaders today, it must work with a host of different on-premise, hybrid, and multi-cloud IT environments, a multitude of certificate types and use cases, and various certificate origins.

It is essential for CLM to integrate with leading technology providers for everything from network hardware devices to mobile device management to DevOps container environments, as well as support automation standards like ACME, SCEP and EST. Only with this level of openness and interoperability can organizations truly secure their digital identities across all environments and protect their data.

Interoperability applies to CAs as well. The reality is organizations use an ever-growing number of certificates issued by different public-trusted CAs and often their own private CA solutions. On the face of it, this approach uses the best certificate solution for each use case. But each of these different CAs have their own proprietary management solution. Once again, IT administration and identity management complexities creep back in.

An effective CLM solution must be CA agnostic in order to manage the ever-growing number of certificates issued by different CAs. This means that the CLM platform must provide a single interface for certificate discovery and end-to-end lifecycle management, regardless of the CA that issued the certificate. With this capability in place, IT leaders can reduce management complexity and better secure their digital identities. A CLM solution that does not openly work with the rest of the organization's CAs, nor their cybersecurity stack, is not a viable option.

A FOUR STAGE CLM APPROACH

Sectigo Research found that the top benefits of CLM are high availability of systems (68%), easier access to information on demand (66%), and improved ability to meet demanding compliance requirements (61%). These benefits and more are found within the four features of CLM, which largely occur simultaneously:

DISCOVERY: A dynamic CLM enables an automated, continuous discovery process to search and find all certificates across the enterprise, as well as to proactively ensure that certificates follow company policies. This is where organizations that rely on manual discovery and monitoring of certificates across various CAs begin to struggle. Alarmingly, 97% of organizations claim that lack of visibility is a risk. When someone changes their name or leaves the company, when a machine is disposed of, or when a cryptographic algorithm is compromised, a larger corporation must quickly find and revoke those certificates in a sea of other certificates.

MANAGEMENT: The process of revoking and automatically provisioning new valid certificates switching out the old ones must be streamlined and straightforward. Enterprises cannot afford to do this manually for every certificate; it should happen seamlessly and at scale, with easy reporting for visibility and a way to enforce a common cryptographic policy across the organization. Automated Certificate Lifecycle Management creates a reliable and consistent touchless process for the entire lifecycle of certificates, from provisioning and registering to revoking and replacing or renewing, and all the subtasks in between. It eliminates interference from individual contributors and reduces labor costs, speeds up the process, and decreases the potential for errors.

RENEWAL: Certificates always have an expiry date. It is set based on when the keys or certificates may have been compromised or when the identity described in the certificate needs to be vetted again. In some cases, the expiry date is enforced by a governing body such as Browsers, Adobe, and eIDAS. Automated renewals are enabled by CLM. Manually tracking expiration dates and revoking and renewing certificates is likely to lead to the outages of critical business systems and potential non-compliance.

GOVERNANCE: Ensuring trust policies and reporting for compliance audits is a challenge when an organization has complex sets of certificate types, multiple vendors, and various lifecycles that require revocation and renewal at different times. Performing governance requires a single pane of glass view that provides a clear map of the complex environment and the status of every certificate.

Below is a list of standards that every CA must adhere to. Since your CLM solution will automate the process of managing your organization's digital certificates, it only makes sense that a trustworthy CLM tool includes:

1 **AUTOMATIC CERTIFICATE MANAGEMENT ENVIRONMENT (ACME):** ACME is a communications protocol for automating interactions between certificate authorities and web servers and load balancers. ACME is based on JSON-formatted messages and was designed by the Internet Security Research Group (ISRG RFC 8555).

2 **SECURE CERTIFICATE ENROLLMENT PROTOCOL (SCEP):** SCEP is a communications protocol that increases flexibility when enrolling new devices for digital certificates. This includes requirements for a shared secret and a URL to communicate with PKI. SCEP is also an industry standard.

3 **ENROLLMENT OVER SECURE TRANSPORT (EST):** EST is a protocol for automating x.509 certificate issuance to networking gear and IoT devices. The EST protocol is defined in RFC 7030. One attractive attribute of EST is the ability to use an existing certificate to authenticate the request for a new certificate. Also, unlike SCEP, it supports elliptic curve cryptography.

4 **REST API:** REST is a universal standard for APIs—the standard method to get certificates to your applications.

Cloud Native

The cloud delivers the digital identity management solution that today's enterprise needs. Cloud-based CLM solutions provide the scalability and flexibility needed to manage a massive volume of certificates while maintaining the control needed to ensure enforcement of an organization's security policies and procedures. Enterprises can easily add digital identities for new users, devices, and applications as their business grows and changes. Simultaneously, organizations can securely store and maintain their root key and private keys without the daily headaches of managing themselves.

From a total cost of ownership (TCO) perspective, scaling an on-premise infrastructure to meet tomorrow's inevitable threats is simply not cost-effective in terms of capital expenses for datacenters, salaries for specialized labor, and ongoing hardware and software investments. The lower TCO and operational expense model of cloud-based CLM make financial sense as well. With the interoperability, high uptime, and governance benefits of a cloud-based CLM solution, the business case for cloud-based CLM is strong.

Modern Certificate Management With Advanced CLM

While a CLM investment gives companies of all sizes the ability to discover, manage, automate, renew, and govern certificates, each organization brings specific requirements. A practical guide to implementing CLM is needed.

Here is a starter checklist of questions to answer when looking to deploy a sophisticated CLM and evaluate identity management platforms.

CAN IT SUPPORT TRADITIONAL USE CASES?

❑ TSL/SSL certificates

❑ S/MIME certificates

❑ Device authentication

❑ User authentication

❑ Document signing

❑ Code signing

❑ eIDAS

CAN IT SUPPORT NEW TRANSFORMATIONAL USE CASES?

❑ Mobile/IoT/Endpoints

❑ DevOps

❑ Passwordless Network Access

❑ SSH

❑ Robotic Process Automation

❑ Zero Trust Network Architecture

❑ Digital Trust Architecture

❑ Remote Identity Validation

❑ Quantum cryptography

IS IT ROBUST ENOUGH TO SCALE WITH YOUR NEEDS?

❑ Does it offer complete **Certificate Lifecycle Management automation**?

❑ Does it operate continuously and have a **high-availability** track record?

❑ Is it a **cloud solution**, and does it support your cloud adoption strategy?

❑ Does it allow **quick implementation to passwordless authentication** for thousands of users?

❑ Does it have a comprehensive set of **integrations with the applications you use**?

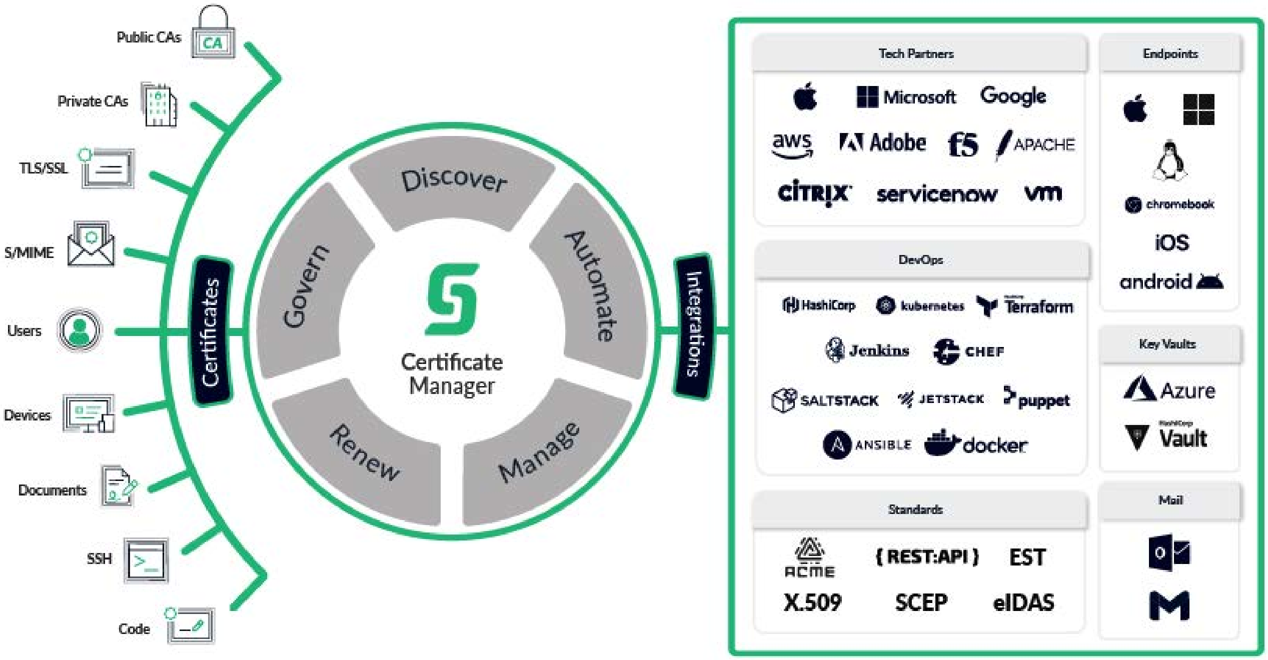
❑ Does it use industry standards to **avoid vendor lock-in**?

❑ Does it have a toolkit to **integrate your custom applications**?

BUILD A POWERFUL DIGITAL PLATFORM WITH SECTIGO CLM

There's no looking back. At a time when establishing digital trust is no longer a "nice to have," enterprises across the globe need to invest in CLM that leverages open standards and can easily interoperate with existing technology solutions. From seemingly simple use cases like securing a website or remotely signing documents to more complex situations like systems controlled by thousands of connected IoT devices, all require a strong digital identity. And digital certificates are at the center of it all.

The Sectigo Certificate Lifecycle Management Platform



The modern approach to CLM is Sectigo's CA agnostic cloud-based solution that delivers a single administration portal to secure and manage growing numbers of digital identities, both human and machine, with integrations into leading technology providers that work efficiently in any IT environment.

About Sectigo

Sectigo is the leading provider of digital certificates and automated Certificate Lifecycle Management (CLM) solutions trusted by the world's largest brands. Its cloud-based universal CLM platform issues and manages the lifecycles of digital certificates issued by Sectigo and other Certificate Authorities (CAs) to secure every human and machine identity across the enterprise. With over 20 years of experience establishing digital trust, Sectigo is one of the longest-standing and largest CAs with more than 700,000 customers, including 36% of the Fortune 1000. For more information, visit www.sectigo.com.