SECTIGO®

A SECTIGO WHITEPAPER

The Critical Need for Certificate Automation

sectigo.com

Short Life Certificates – A Brave New Era

Digital certificate lifespans are shrinking.

The trend of shrinking certificate lifespans, or 'short life certificates', is one Sectigo predicted as far back as 2019. In recent years the maximum term for a public TLS (also called SSL) certificate has dropped from three years, to two, to one.

Yet, on March 3, 2023, Google announced in its "Moving Forward, Together"[1] roadmap the intention to reduce the maximum possible validity for public TLS certificates from 398 days to 90 days, in a future policy update or a CA/B Forum Ballot Proposal. This drop to only 90 days maximum validity will mean major changes for the industry.

For CISOs and their teams, this step toward even shorter certificate lifespans represents a significant change in how they will approach establishing digital trust.

In this new era of short-life certificates, organizations need to understand the dangers of a manual approach to digital certificate management. The traditional approach of undertaking the lifecycle management of digital certificates with spreadsheets and siloed point-solutions is no longer sustainable. Automation will be a critical tool in the arsenal of IT teams as they look to achieve resilience and establish crypto agility.

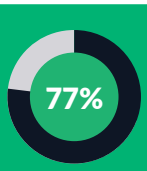
Less Than 90-Day Certificate Lifespans

Digital Certificate lifespans may become shorter, still. In a recent additional proposal to the CA/B Forum, Google has laid out its intention to revisit the concept of a "short-lived" certificate. By this proposal, any public TLS certificate of not more than ten days' term will not require for a revocation mechanism – either OCSP or CRL – to be in place. Rather, mitigation of any certificate problem will be provided by the fact that the certificate will very shortly be incapacitated by its own expiration.

[1] https://www.chromium.org/Home/chromium-security/root-ca-policy/moving-forward-together/

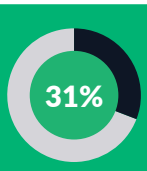
Manual Management Is Now Unsustainable

For almost all organizations, the number of digital certificates they are required to manage continues to grow rapidly - this alone has caused drastically increased levels of risk. Adding shorter digital certificate lifespans into the mix will only serve to compound this issue, bringing the likelihood of outage or breach much closer to the day-to-day reality of hard-working IT teams.



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

According to the latest Sectigo research[2], nearly half (47%) of organizations say they use spreadsheets, scripts, or CA-provided tools to manage digital certificate lifecycles. This manual approach to digital certificate management hampers visibility into all digital identities and creates an opportunity for bad actors to exploit.

Monitoring the constant additions, removals, and modifications to certificates is impossible with a spreadsheet and is difficult at best with basic tools. Just 26% of respondents to Sectigo's latest study rate their organization's visibility into all managed digital identities as "excellent."

For CISOs and their teams, the most obvious implication is how they will approach the management of digital certificates with shorter lifespans. While enterprises technically can still manage digital certificates with 90-day maximum lifespans by hand, manual renewal and deployment will rapidly become error-prone, unsustainable, and may have serious ramifications.

Sectigo's research has also pinpointed the main problem area organizations face with a manual approach to digital certificate management, with 77% of respondents citing challenges with renewing digital certificates without an outage occurring.

In the wake of short-life certificates, the traditional approach of manually handling the renewal and deployment of each server certificate more than four times per year will be incredibly difficult, more than quadrupling the work IT security teams currently spend on this already arduous task. This is a significant increase, and most enterprises do not have a small number of digital certificates.

This isn't about one certificate that must be dealt with four times per year, it's about dozens, hundreds, or thousands of digital certificates. Add in existing difficulties like rogue certificates, visibility over cryptographic decisions, and individual deployment - and manual management becomes unworkable. This is not a job that can be easily done manually today and, in the future, organizations still taking a manual approach will almost certainly pay the price.

What Is a Rogue Certificate?

A Rogue Certificate is a digital certificate that is critical to organizational security, but which has been purchased and issued by an individual outside of the IT organization. Often, these certificates are neglected as part of the organization's overall certificate management and are a source of serious outage risk.

[2] Managing Digital Identities: Tools & Tactics, Priorities & Threats, Sectigo Research, Conducted by Enterprise Management Associates (EMA), 2021.

REAL CONSEQUENCES

The Consequences Are Real

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 - outage, non-compliance and breach.

The dangers posed by haphazard, manual digital certificate management can compromise the entire lifecycle of an organization's digital presence and break digital trust. Unexpected certificate expirations can cause a set of cascading failures, leading to mission critical systems becoming offline. With today's complex and interwoven IT environments this is a serious concern as these failures are rarely restricted to a single system or process. In this scenario, typically, other interdependent systems will become affected, sometimes causing a much more widespread and long-lasting outage. These consequences will only be more likely as short-life certificates become commonplace.

- **Outages, Outages and More Outages** - Sectigo's latest research study revealed that 94% of respondents see digital certificates as core to their organizational security. With this in mind, it is vital for CISOs and their teams to avoid outage by eliminating reliance on outdated manual certificate management processes.
- **Increased Risk of Breach** - With shorter certificate lifespans, organizations will need to renew certificates more frequently and are likely to have five or six times as many certificate lifecycles. For those still relying on manual certificate management, the risk of failure to correctly install or renew a digital certificate will also increase five, or sixfold. Errors with the installation or renewal of certificates at scale massively increase the risk of breach.
- **Poor UX** - Users may encounter error messages or warnings if they attempt to connect to a site or enable a process with an expired or invalid certificate. This can be particularly problematic for e-commerce sites, where users may abandon their shopping carts if they encounter any security warnings.
- **Increased Cost** - Shorter digital certificate lifespans can have significant financial implications for companies. In reality, expensive System Administrators will be the ones tasked with manually renewing digital certificates. This is time-consuming work that can only be carried out by expensive resources. Organizations that are committed to manual management will need to invest in additional, expensive resources to cope with managing increased amounts of digital certificates, with shorter lifespans.

REAL BENEFITS

The Benefits Are Real, Too

Despite these challenges, it is important to recognize the benefits of short life certificates. Shorter certificate lifespans will reduce the impact of a security breach by limiting the amount of time that a compromised certificate can be used for malicious purposes. However, the benefits don't stop there.

The Major Benefit - Crypto Agility

In its “Moving Forward, Together” roadmap, Google made clear the benefits of shorter certificate lifespans: “Reducing certificate lifetime encourages automation and the adoption of practices that will drive the ecosystem away from baroque, time-consuming, and error-prone issuance processes. These changes will allow for faster adoption of emerging security capabilities and best practices, and promote the agility required to transition the ecosystem to quantum-resistant algorithms quickly. Decreasing certificate lifetime will also reduce ecosystem reliance on “broken” revocation checking solutions that cannot fail-closed and, in turn, offer incomplete protection. Additionally, shorter-lived certificates will decrease the impact of unexpected Certificate Transparency Log disqualifications.”

At Sectigo, we concur with this assessment. Ultimately, the primary benefit of short life certificates is increased agility. Shorter certificate lifespans force organizations to keep their certificate management practices current. With the so-called ‘Quantum Apocalypse’ edging closer to reality, now is the time for organizations to be focused on establishing a strong approach to crypto agility. Though, there are other benefits.

- **Shortened Risk Window** – In the event of certificate mis-issuance or compromise, the total time during which negative consequences can result is lower.
- **Encouraging Automation** – Short-Life Certificates will increase the motivation to deploy automation, which will benefit organizations with accurate and current certificate usage throughout the ecosystem.
- **Faster Route to Post-Quantum Cryptography (PQC)** – Once PQC is ready for use in public certificates, the rollout of these important cryptographic primitives will be greatly shortened, reducing the burden on organizations making the changeover.
- **Aligned Certificate and Domain Ownership** - It is possible for a domain to change hands while active certificates are still available for that domain. Shortening the lifespan of certificates decreases the amount of time that can occur.

  However, to see these benefits, CISOs and their teams must be empowered with automation technology to ensure the lifecycles of ALL digital certificates across an enterprise network are properly governed.

The Critical Need for Automation

To reduce risk and take advantage of the benefits of short life certificates, automation is crucial. As digital transformation continues to revolutionize the way we do business, the use of digital certificates has become increasingly essential for the authentication and verification of all human and machine identities deployed across an enterprise network. The increasing ubiquity of digital certificates cannot be ignored. Equally, the benefits of an automated approach to Certificate Lifecycle Management also cannot be ignored.

A core pillar in Google's "Moving Forward, Together" roadmap is focused on automation and mentions specific methods of automating digital certificate issuance and management such as The Automatic Certificate Management Environment (ACME). Google lays out the benefits of automation in the context of shorter certificate lifespans as increased agility and resiliency as well as easing the transition to quantum-resistant algorithms. However, the benefits of automation don't stop there.

- **Avoid Outage and Breach** - Reduce the risk of human error. Manual processes are prone to mistakes, such as misconfiguration or missing a renewal deadline, which can result in security vulnerabilities, outage and breach. Automation can help ensure that all digital certificates across a network are deployed correctly, and critical tasks such as key rotation and certificate revocation are performed promptly and without error.
- **Reduce Cost** – Spend less by automating certificate management. It could easily take over an hour for an administrator to manually renew a single digital certificate. This is incredibly costly at scale and error-prone. Automation removes the need for this time-intensive manual approach and allows administrators to focus on more important tasks.
- **Compliance** - Comply with industry regulations and standards. Automated certificate management processes can provide organizations with better visibility into their certificate inventory, making it easier to track and manage certificates across the organization.
- **Scalability** - Easily manage growing numbers of digital certificates and scale them across increasingly complex enterprise network environments.

  CISOs and their teams need a solution that reliably streamlines the entire digital certificate management process, from issuance and installation to renewal and revocation. They need the power of technology to simplify and automate complex processes, such as certificate lifecycle management, key generation, and provisioning, thus reducing human errors and eliminating the need for manual intervention.

A Capable Solution to Automated Certificate Lifecycle Management

Now is the time to look for CA agnostic Certificate Lifecycle Management (CLM) solutions. These solutions help with the automated discovery of digital certificates across vast enterprise environments, regardless of the issuing Certificate Authority, notifying you of impending expirations, and automatically provisioning and installing renewal and replacement certificates. In so doing, they help avoid outages and breaches due to the incorrect use or renewal of digital certificates.

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 five primary features of CLM:

- **Deployment** – A modern CLM solution will enable automatic certificate deployment, including ordering, issuance and installation - through a single pane of glass. With shortening certificate lifespans, system administrators can no longer be expected to manually order, issue and deploy digital certificates one by one – this is not sustainable. With a CLM solution, organizations benefit from powerful automation capabilities that ensures the accurate, compliant and predictable deployment of digital certificates, reducing the burden of time-consuming and repetitive work on system administrators. With accurate and predictable results, organizations can prevent unexpected outages, plan and manage certificate renewals with accuracy, optimize spend and ultimately, gain a strong handle on the governance of all certificates deployed in the ecosystem.
- **Discovery** - 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, is vital. This is where organizations that rely on manual discovery and monitoring of certificates across various CAs begin to struggle. The latest Sectigo research revealed that 97% of organizations claim a 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. Such an exercise is near impossible to carry out with a manual approach.
- **Revocation & Replacement** - 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.
- **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 Trust Store Operators, Browsers, Adobe, and eIDAS. Automated renewals are enabled by CLM. Manually tracking expiration dates and revoking and renewing certificates with shorter lifespans is likely to increase the risk of outage and potential non-compliance.
- **Visibility** – All digital certificates and certificate qualities deployed across an ecosystem, must be visible, regardless of their origin. It is vital that organizations have a reliable view of all digital certificates across the enterprise at the touch of a button. Automated CLM achieves this with robust reporting, alerts for non-compliant, problematic and expiring certificates through a single pane of glass. This is the only way CISOs and their teams can have the confidence they need to rectify issues before they become problems.

It's Time to Automate With ACME

Automated CLM 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. Now is the time to automate.

As mentioned earlier in this whitepaper, one of Google's main pillars in its "Moving Forward, Together" Roadmap is focused on automation. Specifically, the roadmap lays out Google's intention to encourage the use of automation, and highlights ACME as core to the automation of digital certificate lifecycles.

In its roadmap, Google states: “Today, over 50% of the certificates issued by the Web PKI rely on ACME. Furthermore, approximately 95% of the certificates issued by the Web PKI today are issued by a CA owner with some form of existing ACME implementation available for customers.”

In addition, a future planned policy update by Google will require that all Chrome Root Store applicants must:

- Be part of PKI hierarchies that offer ACME services for TLS server authentication certificate issuance and management.
- Support ACME Renewal Information (ARI, Draft RFC) to further improve ecosystem agility.

The backdrop of short life certificates is one organizations cannot ignore for long. Shorter digital certificate lifespans have real-world consequences for those still approaching certificate lifecycle management manually which include outage and breach, cost implications, non-compliance and an inability to scale. A fully-fledged automated CLM platform enables organizations to avoid these worries, and will integrate with the ACME protocol (as well as others) to facilitate the automatic deployment, discovery, revocation, replacement and renewal of all digital certificates across the enterprise ecosystem, regardless of origin.

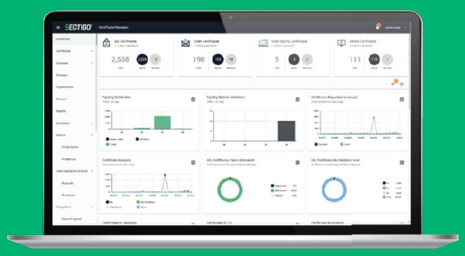
The time to move to automated Certificate Lifecycle Management is now. Sectigo’s CLM provides customers with a strong foundation of digital trust and integrates with the ACME protocol, as well as other popular automation protocols to enable an accurate and reliable approach to the lifecycle management of short-life certificates.

What Is ACME?

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

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.

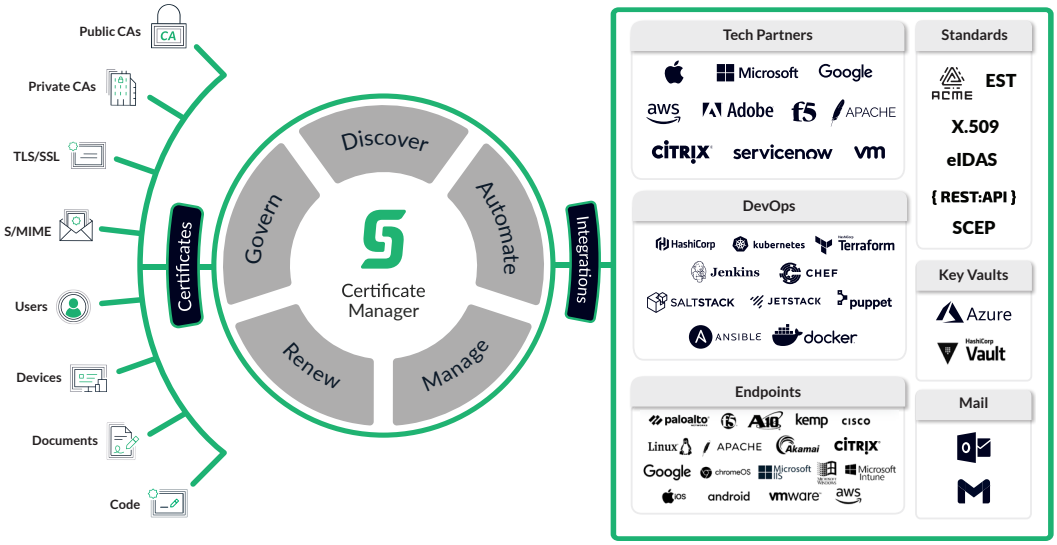


Sectigo Certificate Manager (SCM) is an industry leading, CA agnostic platform, purpose-built to issue and manage the lifecycles of all public and private digital certificates through a single pane of glass. SCM authenticates and secures every human and machine identity across enterprise.

With SCM, customers can automate the issuance and management of Sectigo digital certificates, alongside digital certificates originating from other public Certificate Authorities (CAs) as well as private CAs such as Microsoft Active Directory Certificate Services (ADCS), AWS Cloud Services and Google Cloud Platform (GCP).

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.

CA Agnostic Certificate Lifecycle Management



Get in touch to book a demo of Sectigo Certificate Manager today! Sectigo.com/clm

About Sectigo

Sectigo is a leading provider of Certificate Lifecycle Management (CLM) and digital certificates – establishing a strong foundation of digital trust for companies of all sizes. Sectigo's universal CLM platform is CA agnostic and automates the lifecycles of both public and private digital certificates, regardless of origin, within a single platform. Sectigo integrates across the tech stack and enables organizations to easily secure all human and machine identities across vast networks. With over 20 years of experience, Sectigo's heritage as a Certificate Authority is uniquely positioned to provide over 700,000 customers the confidence they need in an increasingly challenging cybersecurity landscape. For more information, visit www.sectigo.com.