Effectively Manage Your Organization's Certificates

Published 21 February 2024 - ID G00804504 - 28 min read

By Analyst(s): Paul Rabinovich, Erik Wahlstrom

Initiatives: Identity and Access Management for Technical Professionals; Build and Optimize Cybersecurity Programs

Organizations routinely experience outages stemming from unmanaged certificates. Security and risk management technical professionals must implement effective certificate life cycle management to support discovery, automation and crypto-agility.

Overview

Key Findings

- Organizations routinely experience business disruptions due to unexpected expiration of unmanaged certificates.
- Driven by diverse, hard-to-reconcile requirements, most organizations must resort to using multiple certificate authorities (CAs), making certificate life cycle management (CLM) more complex.
- Organizations are struggling to formulate their responses to developments affecting public-key infrastructure (PKI), such as advances in quantum computing and the industry's push for progressively shorter certificate lifespans. (An example of the latter is Google's proposal to shorten the maximum validity of public Transport Layer Security [TLS] certificates to 90 days.)

Recommendations

As a security and risk management (SRM) technical professional focusing on identity and access management (IAM), you should:

- Establish control over your organization's certificates by setting up a CLM practice.
- Gain visibility into your certificates by inventorying them, maintaining up-to-date information about them and implementing expiration alerts.
- Ensure uninterrupted operation in high-volume and/or short-life-span certificate use cases by implementing automation.

- Optimize machine identity management, including CLM, across your organization by establishing a machine identity working group.

Analysis

Digital certificates are playing an increasingly prominent role for most organizations because they represent an excellent credential for machine-to-machine interactions. Machine identities already outnumber human identities and continue to multiply. [1]

Certificates, of course, can be used to authenticate human users, but certificate life cycle management (CLM) as a discipline focuses primarily on the use of certificates as machine credentials. Credential management systems (CMS) support life cycle management of certificates issued to humans.

In most cases, the term "certificate" refers to an X.509 certificate (i.e., a certificate whose format, trust model and processing rules comply with the International Telecommunication Union's [ITU's] Recommendation X.509). However, in recent years, other standards have emerged that are also relevant for many organizations (see Note 1).

As certificates proliferate, small and midsize organizations eventually realize that using spreadsheets to manage them is untenable. A more scalable — and disciplined — line of action is needed for organizations of all sizes.

Importance of CLM

CLM is a set of processes supporting discovery, inventory, issuance (through appropriate certificate authorities [CAs]), storage, deployment, revocation and renewal of digital certificates.

As we noted above, manual techniques do not scale to support the number of certificates now used by most organizations.

Adoption of hybrid and multicloud architectures, PKI and CA sprawl, decreasing certificate validity periods, poorly managed legacy PKI, and emerging crypto-agility needs (see Note 2) are driving organizations to implement continuous discovery, observability and automated certificate life cycle management.

To improve security, the industry has been steadily decreasing the maximum lifespans of certain types of certificates, requiring PKI administrators to renew them more frequently. For example, in 2020, publicly facing TLS certificates moved from an 825-day to 398-day maximum validity period, and Google recently put forward a proposal to further decrease their life span to 90 days.

Most Gartner inquiries on certificate life cycle management start with clients recounting a recent outage of a mission-critical service or application caused by a certificate expiration they were unprepared for.

Applications and infrastructure components may also react unpredictably to certificate-related failures. For example, Equifax experienced a catastrophic data breach because an expired certificate caused a TLS traffic inspection appliance to stop decrypting and analyzing incoming requests (from the public internet). [2]

CLM and Machine Identity Management

Holistic machine identity management that controls machine identity life cycles, entitlements, policies and credentials is still in its infancy. As discussed in Managing Machine Identities, Secrets, Keys and Certificates, this space is fragmented. Tools are available to address specific aspects of machine identity management, but comprehensive tools and machine-identity-specific features in existing IAM tools are only emerging.

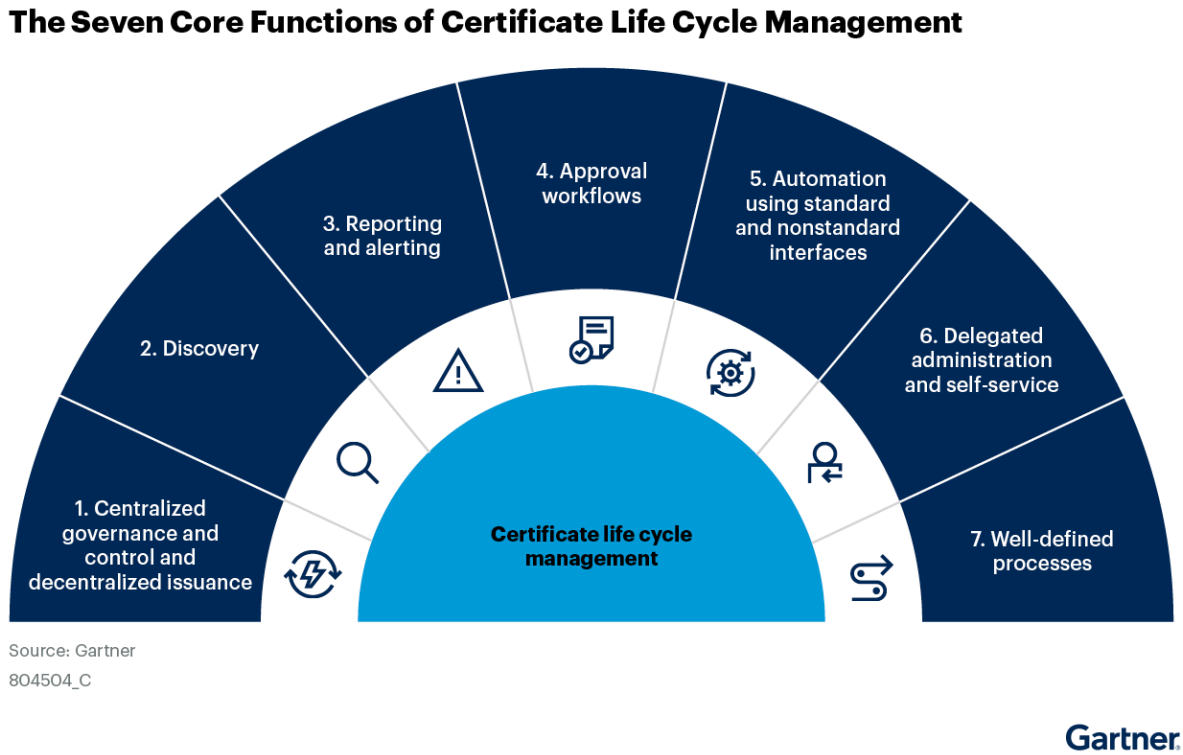
A certificate is one of several types of credentials that a machine can have. In the absence of strong machine identity governance typical of workloads and unmanaged devices, discovery becomes a key step to successful CLM implementation. CLM can further expand to support certificate issuance in a variety of use cases, securing:

- Public-facing and internal websites and applications
- DevOps pipelines
- Code-signing processes
- API-based access
- Container-based deployments

Pillars of CLM

Figure 1 shows the seven pillars, or core functions, of CLM.

Figure 1: The Seven Core Functions of Certificate Life Cycle Management



The pillars include:

1. **Centralized governance and control, and decentralized issuance.** Organizations should architect CLM in accordance with the centralized/decentralized security (CeDeSec) model (see Note 3), which stipulates centralized governance and control, and decentralized use. [3] A CLM tool can unify all aspects of certificate life cycle management for an organization by:

    - Supporting visibility and monitoring of certificates used by workloads and devices, regardless of their location (on-premises or in the cloud).
    - Bringing under a single umbrella all CAs used by the organization, including CAs used for internal IT needs, CAs issuing publicly facing TLS certificates, CAs operated by public cloud platforms and specialized CAs. This capability is sometimes called “CA agnosticism,” because these CA products and services may come from multiple vendors.
    - Providing a single orchestration framework for all certificate issuance workflows.

2. **Discovery.** At a minimum, certificate life cycle management must include CA-agnostic certificate discovery and the ability to track certificates in a centralized database. Each entry must contain all useful information gleaned from the corresponding certificate, such as the issuer, the subject name, and the not-before and not-after dates. Each entry should also contain additional metadata, such as pointers back to the certificate's locations in the environment, ownership information, and information about the certificate's users, function and usage patterns.

3. **Reporting and alerting.** CLM tools provide standard reporting common to all asset-tracking databases (data objects and their relationships, various groupings and views, trends, ownership information, etc.). In addition, CLM tools can provide information unique to certificates, such as notifications about imminent certificate expiration or notifications about violations of organizational policy (e.g., use of unauthorized cryptographic algorithms). Some CLM tools also monitor public certificate transparency (CT) logs, enabling organizations to detect TLS certificates illegally or incorrectly issued to their domains.

4. **Approval workflows.** CLM tools can support approval workflows, enabling centralized PKI operations teams to supervise certificate issuance, certificate revocation and other management functions initiated by individual certificate owners.

5. **Automation using standard and nonstandard interfaces.** CLM tools can provide a focal point for end-to-end certificate life cycle automation, from generating certificate signing requests (CSRs) to CAs to deploying certificates and private keys to end systems. A number of standard CLM management protocols are currently available, including Automatic Certificate Management Environment (ACME; see Note 5), Certificate Management Protocol (CMP), Enrollment over Secure Transport (EST) and Simple Certificate Enrollment Protocol (SCEP). However, their adoption is not universal. Certain widely deployed vendor ecosystems, such as Microsoft Windows, use proprietary mechanisms for certificate operations, and some CAs provide custom APIs that go beyond the capabilities of established protocols. CLM tools can play a mediator's role, simplifying integration and operations.

6. **Delegated administration and self-service.** Manual approvals encourage an "in-the-way" governance style, where the PKI team will be called upon to support CLM operations in real time. This approach doesn't scale. Automation is the best response to scalability challenges, but it's not possible in all situations. An "on-the-side" style of governance provides a happy medium, in essence, enabling preapprovals for certificates matching specific policies or profiles. CLM tools supporting this model focus on enablement and auditing: The centralized PKI team sets up guardrails, policies and authorizations, and delegates certificate administration to individual certificate owners.

7. **Well-defined processes.** As we discuss in the People and Processes section, technology by itself is not going to solve the challenges of effective CLM. A CLM implementation must include process components as well. Successful machine identity management relies on discovery, monitoring and reporting, formalization of best practices, cataloging and remediation of out-of-compliance systems, automation, and developer enablement. See Managing Machine Identities, Secrets, Keys and Certificates for additional information.

Discovery and reporting are the foundational components of CLM. Without them, no other function can succeed.

CLM tools may also provide functionality in other areas:

- **Management of human user certificates.** Use of digital certificates for human-user authentication, digital signing and encryption is declining. However, it's still common in certain environments (national governments, militaries and regulated industries) and use cases (privileged access, Wi-Fi and VPN access, access from managed mobile devices, and device-as-a-user-proxy and certificate-as-an-ephemeral-credential authentication scenarios). Many organizations value solutions that provide full visibility into all certificates, regardless of who or what uses them. For instance, a centralized CLM tool could provide full visibility into certificates issued by individual CAs on behalf of unified endpoint management (UEM) and CMS tools.
- **CA migrations.** CLM solutions supporting multiple CAs can facilitate migration from one CA product or service to another. Further, an application integrated with a CLM solution doesn't even need to "know" that its certificates will be issued by a new CA.

- **Crypto-agility.** CLM solutions can monitor and report the use of obsolete CAs, cryptographic algorithms, key lengths and other security properties in organizations' certificates. Examples include the deprecation of the MD5 and SHA-1 hashing algorithms, the move to longer RSA keys, and the upcoming migration to postquantum cryptography. [4]

- **Trust management.** When others need to authenticate to resources under the control of organizations and teams, those organizations and teams must maintain trust "lists" that include trust anchors (trusted roots), certificates issued to intermediate CAs and/or pinned end-entity certificates. CLM tools can monitor these lists and help organizations keep them up to date.

- **PKI posture management.** Enterprise CAs must follow strict guidelines around certificate life cycle operations such as issuance and revocation, protection of cryptographic material, administrative processes, auditing, and change management. Third-party tools can be responsible for assessing CAs' and hardware security modules' (HSMs') security posture, hygiene, and compliance with industry guidance and specific regulations. This functionality is currently emerging.

- **Management of adjacent trust ecosystems.** Some CLM tools extend at least a portion of their capabilities to SSH keys, Pretty Good Privacy (PGP) keys and symmetric keys used for data encryption.

CLM Technology Components

Figure 2 illustrates a representative enterprise PKI ecosystem. The figure depicts workloads and devices that rely on certificates, and their integration with the public and private CAs that provide those certificates.

Although IT management tools don't focus on CLM per se, they do mediate between:

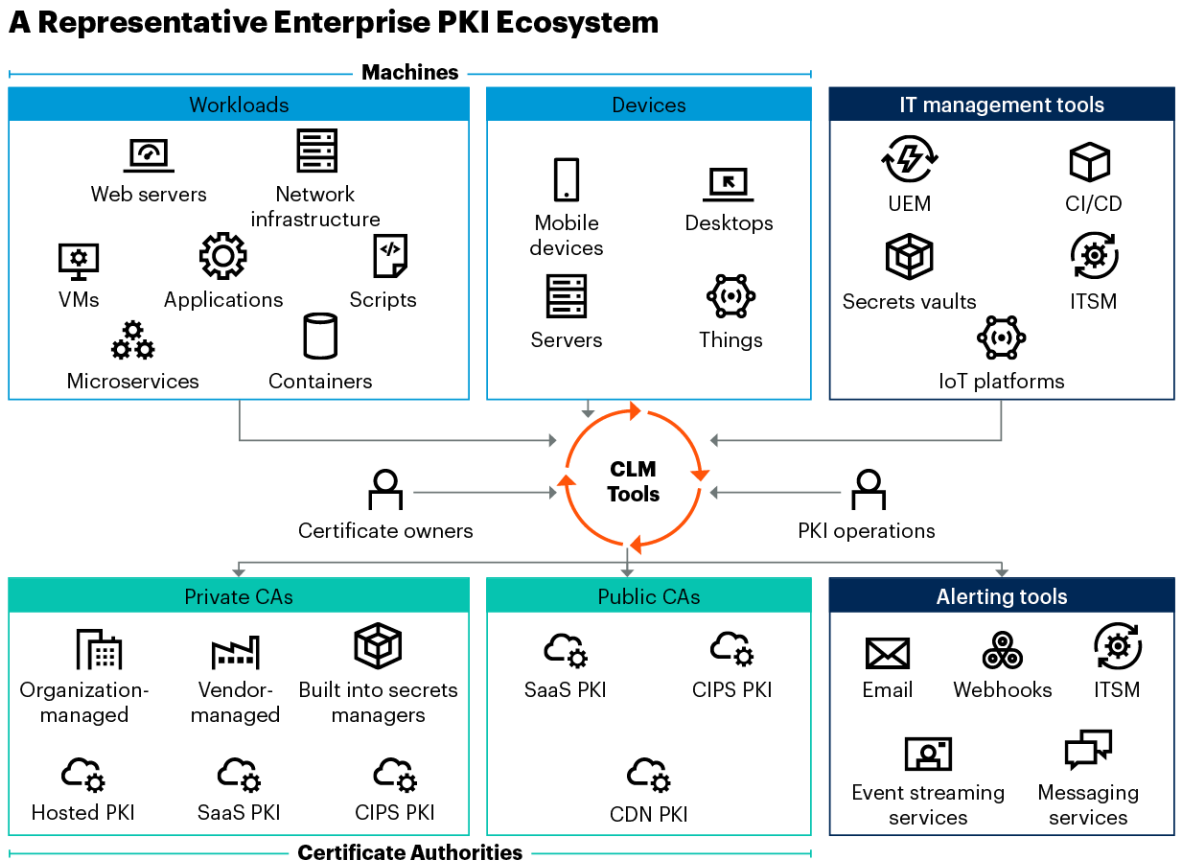
1. Workloads and devices they manage

2. CLM tools and CAs

Alerting tools are responsible for delivering alerts, events and notifications to administrators that care about certificates.

Finally, CLM tools orchestrate certificate life cycle management, from discovery to data persistence, alerting and reporting, and automation.

Figure 2: A Representative Enterprise PKI Ecosystem



Source: Gartner

CDN = content delivery network; CI/CD = continuous integration/continuous delivery; CIPS = cloud infrastructure and platform services; IoT = Internet of Things; ITSM = IT service management

804504_C

Gartner

To discover certificates in an environment, a CLM tool may:

- Perform network scans against TLS endpoints, most frequently web servers, but also servers supporting nonweb protocols, such as SMTPS, secure Lightweight Directory Access Protocol (LDAP) and FTP Secure (FTPS). The CLM tool can also leverage agents deployed in different networks to help facilitate both discovery and automated life cycle management.
- Receive updates from agents installed on end systems (e.g., Linux and Windows machines). The agents may provide information about locally discovered certificates stored in Privacy-Enhanced Mail (PEM)- and Public-Key Cryptography Standards (PKCS)-formatted files, Java key stores, Windows certificate stores, etc.

- Allow administrators to manually import certificates from end systems, IT management tools and third-party discovery tools, in bulk or individually.
- Interrogate IT management tools, such as UEM tools, secrets vaults and ITSM tools, for information on certificates managed by them.
- Connect to individual CAs, through proprietary APIs, to receive information about certificates issued by them.
- Look up certificates in enterprise directories, such as Microsoft Active Directory or LDAP-based repositories.

As mentioned earlier, one of the principal reasons for organizations to acquire a CLM tool is to receive notification of impending certificate expiration. Out-of-the-box CLM tools typically use email or webhooks as the primary notification mechanism. They can also open tickets in organizations' ITSM systems and/or forward alerts to their SIEM tools. Most vendors provide APIs and software development kits (SDKs), enabling customers to integrate alerts with third-party data streaming and workflow management tools.

Gartner clients with large active certificate bases tell us that lost alerts are a recurring problem in their environments. [6] Some vendors support reliable notifications with feedback and escalations. Organizations whose tools support only a "fire-and-forget" style of notification must themselves design stateful, persistent notification flows using third-party tools.

Certificate issuance and renewal processes may take several different forms, depending on an organization's requirements. Multiple flows may coexist in any given deployment. In Figure 2, we distinguished the flows based on who or what initiates them:

- **CLM initiates.** The CLM tool, typically in response to an upcoming certificate expiration event, starts the process, requests and receives a certificate from the appropriate CA, and deploys it to the endpoint system. To deploy, the CLM tool pushes the new certificate and, where needed, the private key to the endpoint system itself or to a repository used by it (possibly, the local filesystem). The tool then modifies the system's configuration to point to the new certificate, notifies it that a new version of the certificate is available, and/or restarts it to force reconfiguration. Local agents and custom connectors typically enable fine-grained control over the deployment process.

- **Endpoint (workload or device) initiates.** Many endpoints are certificate-life-cycle-aware and can request their own certificates, either from a CA or from a CA-agnostic CLM tool. In the latter case, the CLM tool acts as an orchestrator, single point of visibility and control, and protocol translator. Examples of this flow include:
  - Mobile OSs, such as Apple iOS, Apple iPadOS and Android, using Simple Certificate Enrollment Protocol (SCEP)
  - Windows devices using Windows certificate autoenrollment
  - IoT devices using Enrollment over Secure Transport (EST)
  - Apache HTTP Server using ACME (see Note 5)

- **Owner initiates.** Certificate owners may use the end systems themselves or third-party tools to generate CSRs and submit them to the CLM tool. The CLM tool executes applicable workflows with automated or manual approvals. Owners can then download the new certificate once it's issued by the appropriate CA. Certain end systems, such as Microsoft IIS, F5 BIG-IP and Kubernetes, can generate and export CSRs, and import certificates. Those that cannot allow administrators to import externally generated certificates and private keys. To generate CSRs, administrators can use:
  - Any readily available utilities, such as the Java keytool, OpenSSL or CloudFlare's CFSSL
  - Tools provided by their CLM vendor
  - Any standards-compliant third-party software

- **IT management tool initiates.** IT management tools can mediate between end systems and CLM tools. For example, UEM tools and IoT platforms can configure devices for direct interaction with CLM tools. They can also take over key pair and CSR generation, manage the request-response cycle, and push certificates and private keys into the endpoints.

Secrets managers and secrets vaults can also automate interactions with CLM tools. Most treat certificates as first-class objects. In other words, they "understand" the certificate format, can extract useful information from certificates, are aware of the notion of certificate expiry and can initiate renewal requests. Some products come with their own CA (indicated in Figure 2 as "built into secrets managers" under "Private CAs").

People and Processes

In the absence of an overarching process and governance framework, CLM technology won't be able to accomplish much.

First and foremost, Gartner recommends that technical professionals help to establish, and subsequently participate in, a machine identity working group. A machine identity working group is a cross-functional team that brings together representatives from the following domains to optimize machine identity management within the organization:

- IAM
- PKI
- Infrastructure and operations
- Cloud
- Security
- DevOps
- Platform engineering
- Applications
- Business

The working group, typically initiated and governed by security leaders, must:

- Define common policies, procedures, roles and responsibilities
- Establish guidance related to the organization's compliance requirements
- Provide integration and architecture guidelines
- Establish consistent approaches to managing different types of machine credentials (certificates, SSH keys, symmetric keys, etc.) and different types of machine identities

The working group should be responsible for implementing the CeDeSec strategy for CLM. It won't own all the tools involved in CLM, but will provide centralized governance and oversight of distributed certificate use and life cycle management.

SRM technical professionals should provide the working group with institutional knowledge on PKI and CLM. The working group brings together certificate “producers” (those who run the organization’s PKI) and certificate “consumers” (owners and relying parties). Even the most powerful CLM tool cannot operate in a vacuum. For instance, a tool cannot assuredly discover all certificates in the organization unless it’s guided by a high-level understanding of the applications, networks, services and infrastructure that use them.

Although it’s appealing to have a single centralized solution serving all the CLM needs of an organization, this strategy is not always practical. For example:

- Specialized PKIs, such as those dedicated to IoT use cases, may need to be managed separately.
- Server, client and human-user CLM typically have different requirements and call for different technical approaches. For example, many CLM tools focus exclusively on machine identity. They do not support certain functions required for human-user certificate life cycle management, such as integration with CMS tools.
- Public cloud platforms offer full certificate life cycle management for the workloads they manage on behalf of their customers (e.g., load balancers).
- Organizations may prefer to directly integrate their workloads and/or devices with individual CAs for certificate issuance, but still use a CLM tool for discovery, monitoring and centralized governance.
- Non-CLM tools may provide good-enough functionality for a subset of certificates used by an organization (see the CLM Tools and Vendors section).

Thus, an organization may need to use several approaches to CLM at the same time, depending on use cases and environments. The responsibility for orchestrating a fragmented CLM implementation and designing consistent policies and processes across multiple tools also lies with the machine identity working group.

Finally, as discussed in the Pillars of CLM section, a CLM implementation may need to support automation, in-the-way governance and/or on-the-side governance for certificate life cycle management processes. Most organizations with a large and heterogenous active certificate base will implement all three.

The decision to automate or stay manual is typically based on a simple ROI calculation: You need to compare the total cost of ownership for both approaches and decide whether investing in automation is worth it. With automation, organizations also need to implement additional monitoring and exception handling to ensure that no failed CLM operation remains unaddressed.

For manual processes, organizations should give preference to on-the-side flows, which do not require real-time approvals by a centralized (typically small) team. However, this approach hinges on the CLM tool's ability to enable sufficiently granular authorization rules that support the organization's security and accountability requirements.

CLM for SMBs

Small and midsize businesses (SMBs) are experiencing CLM challenges similar to those of larger organizations, albeit on a smaller scale. Their difficulties are exacerbated by lack of resources and lack of PKI-related expertise. The needs of SMBs can be addressed through:

- **Combined PKI and CLM offerings.** Leading CLM vendors now offer stand-alone CA products and/or services. In addition, PKI vendors increasingly offer lightweight CLM functionality, and some now provide general-purpose CLM. See the Tools and Vendors section for more details.
- **Managed and cloud-delivered CLM services.** Cloud delivery has become the norm: CLM vendors universally provide at least some cloud capabilities. SMBs will benefit from simplified operations and administration afforded by cloud-based and managed CLM. See the Future of CLM section for more details.
- **CLM solutions specifically targeting SMBs.** Several vendors told Gartner that they are working on CLM offerings for SMBs.

CLM Tools and Vendors

Figure 3 shows categories of vendors with products and/or services that support CLM.

Figure 3: Categories of Vendors Delivering CLM Functionality

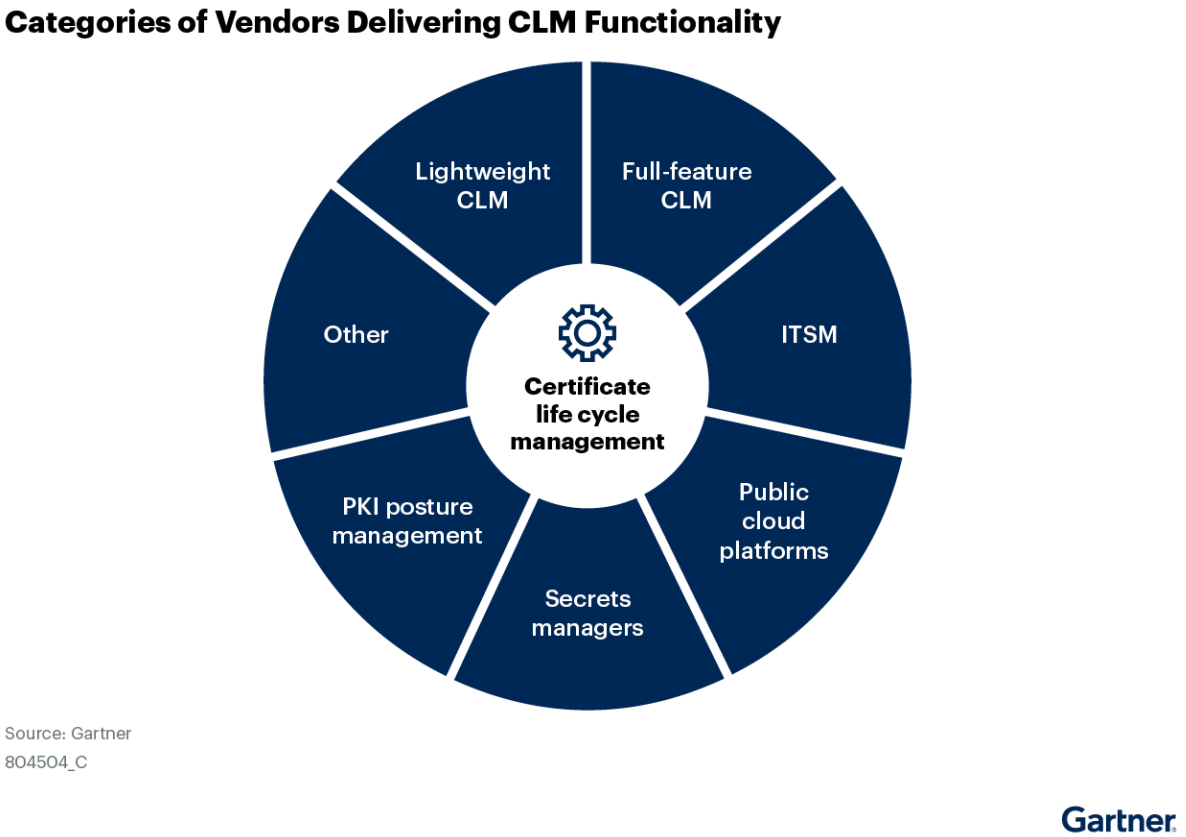


Table 1 explains each vendor category and provides a list of example vendors.

Table 1: CLM Vendors

(Enlarged table in Appendix)

Vendor category	Description	Example vendors
Lightweight CLM	Vendors supporting limited-scope CLM that focuses on one of the following: ▪ Specific CA products (e.g., their own and/or Microsoft Active Directory Certificate Services) ▪ Specific types of certificates (e.g., TLS) ▪ Specific use cases (e.g., DevOps) ▪ Specific CLM functionality (e.g., discovery or automation)	▪ Data-Warehouse ▪ eMudhra ▪ GlobalSign ▪ Smallstep
Full-feature CLM	Vendors with broad-scope CLM products and services supporting out-of-the-box integration with multiple CA products.	▪ AppViewX ▪ Cogito Group ▪ Cybersec Innovation Partners ▪ Entrust ▪ DigiCert ▪ Digitalberry ▪ EverTrust ▪ Keyfactor ▪ Sectigo ▪ senhasegura ▪ Venafi
ITSM	IT platforms that enable organizations to design, automate, manage and deliver integrated IT services and digital experiences. ITSM tools view certificates as one more type of enterprise asset to manage. They typically emphasize discovery and reporting for TLS certificates. In addition, ITSM portals can integrate with CLM tools, providing single-console visibility and the ability to trigger back-end workflows (e.g., for certificate issuance).	▪ Ivanti ▪ ManageEngine ▪ ServiceNow
Public cloud platforms	Cloud infrastructure and platform services (CIPS). CIPS providers typically support full automation for workloads they manage on behalf of their customers and lightweight CLM for customer-managed workloads.	▪ Alibaba Cloud ▪ Amazon Web Services (AWS) ▪ Google ▪ Microsoft ▪ Oracle
Secrets managers	Secrets managers providing vaults for application passwords, API keys and other secrets. Secrets managers support vaulting services for certificates and private keys. Some vendors support expiry notifications and/or renewal workflows, and some ship integrated CA products.	▪ Akeyless ▪ BeyondTrust ▪ HashiCorp
PKI posture management	Tools for assessing CAs' security posture, hygiene and compliance with industry best practices and specific regulations.	▪ PKI Solutions
Other	Vendors in adjacent markets whose non-CLM products use or manage certificates. These vendors typically provide lightweight CLM capabilities focusing on discovery, reporting and integration with ITSM tools.	▪ Difenda ▪ ExtraHop ▪ Qualys ▪ Quest ▪ SolarWinds ▪ Tenable

Source: Gartner (February 2024)

In addition, organizations may want to evaluate open-source tools for smaller environments and/or to address specific use cases or aspects of CLM. Examples of open-source CLM tools include:

- **Certbot**. Developed by the Electronic Frontier Foundation (EFF), Certbot automates TLS certificate renewal using the ACME protocol. It was designed to work with Let's Encrypt, a popular not-for-profit public CA, but can support other CAs as well. The tool supports many common web servers and features a pluggable architecture to accommodate other endpoints.

- **cert-manager**. cert-manager facilitates management of TLS certificates in Kubernetes clusters. Originally developed by Jetstack, it is now maintained by Venafi, which acquired Jetstack in 2020.

- **Lemur**. Lemur is a tool for simplified certificate issuance and deployment in DevOps environments. It supports simple approval and notification workflows, and can integrate with multiple CAs and end systems. Netflix developed Lemur and contributed it to the open-source community.
- **mod_md**. mod_md, an Apache HTTP Server module, monitors and renews TLS certificates used by the server. It utilizes the ACME protocol.

These tools do not address core CLM requirements such as discovery and governance. However, they can complement a larger CLM implementation or help automate CLM in small-scale or homogeneous PKI environments.

Future of CLM

Due to the confluence of forces discussed in the Importance of CLM section, the CLM space is undergoing a significant shift. While many large organizations have a formal CLM practice and deploy CLM tools, few SMBs do. Based on client interest, Gartner predicts rapid adoption of CLM tools in the next 12 to 24 months.

In the short to medium term, several technology trends will influence the capabilities of CLM tools and their use:

- **Advances in machine learning (ML) and generative AI (GenAI).** An April 2023 Gartner survey of technology provider leaders showed that more than 80% are either utilizing or considering utilization of GenAI in the next six months. [5] In CLM, analytics and ML techniques can enable natural language interactions between administrators and tools, help reconcile and enrich certificate metadata using multiple data sources, and assist with troubleshooting. As one early example, Venafi has released a chatbot that helps administrators configure and integrate Venafi's tools. It is also working on a GenAI-based tool for Q&A and reporting on customers' certificate real estate.
- **Expansion of platform engineering initiatives.** As companies mature and expand services provided by their platform engineering teams, they should incorporate guidance, standards, components (such as common libraries) and tools addressing CLM needs. Web applications, microservices and containers, and API gateways increasingly rely on certificate-based authentication and will benefit from standardized building blocks that can speed up software development and delivery.

- **Evolution of cloud-first and cloud-smart strategies.** Organizations are increasingly looking to the cloud to satisfy their security and IAM requirements. CLM vendors typically support cloud delivery models, either hosted (single-tenant) or SaaS (multitenant), in addition to software delivery in the form of server software or appliances. (Some organizations, such as governments, aerospace and defense companies, and financial institutions, still prefer to run their CLM tools on-premises.) Most vendors' SaaS implementations stemmed from their software-delivered products and required significant redevelopment. Some vendors are still working on achieving functional parity between the two offerings. SMBs should prioritize cloud-based implementations, provided they do not violate their compliance and security requirements.

- **Blurring of boundaries between machine identity management tools.** In Managing Machine Identities, Secrets, Keys and Certificates, we mentioned that vendors do not necessarily stay in their respective "lanes." They expand into adjacent areas. For example, secrets managers typically can perform limited CLM functions and integrate with third-party CLM tools. Some ship CA modules as well. Some privileged access management (PAM) vendors (e.g., ManageEngine and senhasegura) also ship CLM tools. Gartner expects this trend to continue. Secrets management and PAM vendors, CIPS platforms, and identity governance and administration (IGA) providers will increasingly offer CLM functionality through integrations, partnerships, in-house development and acquisitions.

Recommendations

- **Establish control over your organization's certificates by setting up a CLM practice.** Do not wait for a business disruption caused by a certificate whose expiration went unnoticed. Proactively set up a CLM practice that, at a minimum, can help you inventory all certificates and maintain actionable data about them. Historically, Gartner has recommended that organizations maintain a single PKI framework, even if they need to maintain multiple PKIs. Such a framework enables consistent policies and processes across use cases while accommodating requirements and exceptions specific to each use case. Centralized certificate life cycle management enables this approach by providing centralized control in a decentralized environment and implementing management workflows, automation, ownership tracking and delegated administration. CLM may also include non-X.509 certificates that use different formats and trust models, such as SSH certificates (see Note 1).

- **Gain visibility into your certificates by inventorying them, maintaining up-to-date information about them and implementing expiration alerts.** You cannot manage what you cannot see. Therefore, you should establish discovery processes (plural, because most organizations need to deal with multiple types of certificates) and consolidate all collected information in a centralized database. Document locations, ownership information, information about entities that use certificates and, of course, expiration dates. Note that, even when you are using mature CLM tools, some information may be ambiguous or incomplete, and manual reconciliation may be required.

- **Ensure uninterrupted operation in high-volume and/or short-life-span certificate use cases by implementing automated CLM.** As certificate lifespans get shorter and the number of certificates grows, manual certificate life cycle management processes reach their scalability limits. Some environments (Active Directory-centric Windows networks, UEM-managed mobile devices and "things" integrated with IoT platforms) have already found practical solutions to this problem. However, other use cases (most obviously, web server certificates) are not well-addressed, and comprehensive approaches that support heterogeneous use cases require implementing a third-party CLM tool. Open-source tools, which primarily support the ACME protocol, can help automate the life cycle of TLS certificates. However, to deal with other types of certificates — and to scale TLS operations — you will need to invest in a commercial product or service.

- **Optimize machine identity management (including CLM) across your organization by forming a machine identity working group.** As a discipline, certificate life cycle management is part of credential management. As mentioned in the introduction to the Analysis section, some organizations continue to use certificates for human-user operations (authentication, digital signatures and encryption), but their number is dwindling. On the other hand, certificates are widely used as a machine credential. While focusing on the immediate needs of CLM (such as discovery and avoidance of disruptions due to expired certificates), organizations should take a broader view of machine identity management. They should leverage a machine identity working group, often led by an SRM leader, that enables the organization to:
  - Bring together all teams that have a stake in efficient and secure machine identity life cycle management
  - Implement consistent policies and processes across multiple types of credentials (certificates, SSH keys, application passwords, API keys, OAuth 2.0 client secrets, etc.)
  - Mature machine identity governance and administration over time to effectively manage machine identities wherever they exist in the environment

Conclusion

PKI is playing a progressively important role in securing organizations' machine identities. Most enterprise identities belong to machines, and the number of machine identities is growing. Certificates represent an excellent credential for machines. However, unmanaged certificates routinely cause business disruption and security incidents.

CLM, through discovery and capture in a centralized repository, can provide visibility into an organization's certificate real estate and facilitate uninterrupted use of certificates. Organizations can further improve their CLM by implementing:

- Unified governance
- Reporting and auditing
- Approval workflows
- Certificate life cycle automation
- Ownership tracking

- Delegated administration

Evidence

[1] CyberArk 2023 Identity Security Threat Landscape Report, CyberArk.

[2] The Equifax Data Breach, U.S. House of Representatives.

[3] See, for example, 2024 Planning Guide for Identity and Access Management.

[4] See Preparing for the Quantum World With Crypto-Agility for additional information.

[5] 2023 Gartner Technology and Service Provider Generative AI Survey. This survey was conducted online from 28 March through 10 April 2023 to explore how technology and service providers (TSPs) utilize generative AI in content marketing. In total, survey participants included 43 TSP leaders utilizing or considering utilization of generative AI in the next six months. Forty-two TSP leaders were members of Gartner's Research Circle, a Gartner-managed panel, and one was from an external survey link shared via social channels and analyst contacts. Research Circle member participants were from EMEA (n = 19), North America (n = 17) and Asia/Pacific (n = 6). Disclaimer: The results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

[6] Based on Gartner client inquiries over the last 12 months. Note that we are not referring to unreliable transports (though many common communications technologies, such as email, are "best effort" only and do not provide delivery guarantees). The pain point here is that administrators do receive notifications, but misplace them or fail to act. Change management may also be a problem. For example, when a certificate changes owners, the CLM tool may not reflect the change in ownership.

Note 1: Non-X.509 Certificates

In inquiries, Gartner clients express interest in the following types of non-X.509 certificates:

- **Secure Shell (SSH) certificates.** These certificates are compliant with an alternative model proposed and implemented by OpenSSH. SSH certificates occupy an intermediate place between X.509 certificates that also can be used in SSH access (uncommon) and SSH keys (common but difficult to manage at scale). Although proprietary, SSH certificates are widely supported by SSH servers and clients.

- **Institute of Electrical and Electronics Engineers (IEEE) 1609.2 certificates.** These certificates are compliant with the IEEE standard for wireless access in vehicular environments (WAVE), IEEE 1609.2. The automotive industry uses WAVE certificates to authenticate component-to-component communications.

Note 2: Crypto-Agility

Crypto-agility is the ability to switch to new, more secure cryptographic algorithms with minimal impact to applications and systems. As technology evolves, new attacks become practical that render once-secure algorithms unsafe.

Note 3: Centralized/Decentralized Security (CeDeSec)

Gartner defines a centralized/decentralized security (CeDeSec) pattern as a shift toward centralized governance and control in a decentralized security environment. There are already many established IAM examples of this pattern that showcase the power of CeDeSec, such as:

- Centralized life cycle management and provisioning of identities in decentralized user stores using System for Cross-Domain Identity Management (SCIM), a provisioning protocol
- Centralized authentication via single sign-on in a decentralized application environment using OpenID Connect or SAML
- Centralized certificate life cycle management across decentralized certificate authorities using certificate life cycle management tools

Note 4: Automatic Certificate Management Environment (ACME)

A common misconception is that deploying ACME-based certificate renewal fully addresses CLM. The ACME protocol is an increasingly popular technical method for automated issuance of certificates. However, it does not satisfy all CLM needs:

- ACME, as currently implemented, focuses only on web server (TLS) certificates and domain validation.
- ACME does not support discovery and monitoring (e.g., of certificate expiry).
- ACME does not address certificate deployment.

- ACME, by itself, doesn't promote CeDeSec. It is architecture-agnostic, supporting both centralized and distributed client architectures.
- ACME, as a technical protocol, is not concerned with governance, processes and policies.

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Architect a Modern API Access Control Strategy

Hype Cycle for Digital Identity, 2023

Managing Machine Identities, Secrets, Keys and Certificates

Market Guide for Identity Governance and Administration

Table 1: CLM Vendors

Vendor category	Description	Example vendors
Lightweight CLM	Vendors supporting limited-scope CLM that focuses on one of the following: ■ Specific CA products (e.g., their own and/or Microsoft Active Directory Certificate Services) ■ Specific types of certificates (e.g., TLS) ■ Specific use cases (e.g., DevOps) ■ Specific CLM functionality (e.g., discovery or automation)	■ Data-Warehouse ■ eMudhra ■ GlobalSign ■ Smallstep
Full-feature CLM	Vendors with broad-scope CLM products and services supporting out-of-the-box integration with multiple CA products.	■ AppViewX ■ Cogito Group ■ Cybersec Innovation Partners ■ Entrust ■ DigiCert ■ Digitalberry ■ EverTrust ■ Keyfactor ■ Sectigo

		■ senhasegura ■ Venafi
ITSM	IT platforms that enable organizations to design, automate, manage and deliver integrated IT services and digital experiences. ITSM tools view certificates as one more type of enterprise asset to manage. They typically emphasize discovery and reporting for TLS certificates. In addition, ITSM portals can integrate with CLM tools, providing single-console visibility and the ability to trigger back-end workflows (e.g., for certificate issuance).	■ Ivanti ■ ManageEngine ■ ServiceNow
Public cloud platforms	Cloud infrastructure and platform services (CIPS). CIPS providers typically support full automation for workloads they manage on behalf of their customers and lightweight CLM for customer-managed workloads.	■ Alibaba Cloud ■ Amazon Web Services (AWS) ■ Google ■ Microsoft ■ Oracle
Secrets managers	Secrets managers providing vaults for application passwords, API keys and other secrets. Secrets managers support vaulting services for certificates and private keys. Some vendors support expiry	■ Akeyless ■ BeyondTrust ■ HashiCorp

	notifications and/or renewal workflows, and some ship integrated CA products.	
PKI posture management	Tools for assessing CAs' security posture, hygiene and compliance with industry best practices and specific regulations.	■ PKI Solutions
Other	Vendors in adjacent markets whose non-CLM products use or manage certificates. These vendors typically provide lightweight CLM capabilities focusing on discovery, reporting and integration with ITSM tools.	■ Difenda ■ ExtraHop ■ Qualys ■ Quest ■ SolarWinds ■ Tenable

Source: Gartner (February 2024)