SIX STEPS TO SSL CERTIFICATE LIFECYCLE MANAGEMENT

Why you need an SSL certificate management solution — and how to get started

Entrust Datacard™

+1-888-690-2424 | entrust.com

Table of contents

Introduction

Upon issuance, all SSL digital certificates have a finite lifespan and are no longer recognized as valid upon expiration. Certificates may have varying periods of validity and are often set to expire anywhere between one and three years based on company policy and/or cost considerations.

Minimally, certificates need to be replaced at the end of their life to avoid service disruption and decreased security. However, there may be a number of scenarios where a certificate needs to be replaced earlier (e.g., Heartbleed bug, SHA-1 end-of-life migration, company mergers, change in company policy).

Given the finite lifespan of SSL certificates and their widespread use throughout an organization, there are numerous reasons to take a lifecycle management approach. It's critical to maintain an accurate accounting of SSL certificates that doesn't rely on manual processes and tools.

This guide — intended for IT and security professionals — outlines the key elements of a certificate lifecycle management process and how to provide adequate tools and training to implement this process.

Take the guesswork out of certificate management and automate certificate lifecycle processes to achieve better oversight and control, lower costs, improve efficiency and reduce security risks.

Consequences of Poor Management

While the most recognizable use of SSL certificates is the "browser lock" icon displayed on transactional-based websites to protect user and payment information, it extends well beyond this to secure mission-critical enterprise infrastructure components.

For example, employees and partners use VPNs to access sensitive information, and back-end systems rely on SSL certificates to secure remote access. Virtually all browser-based cloud services require SSL certificates to transmit customer account information, business partner transactions, inventory status, time-tracking and a host of other uses.

Most internally deployed employee productivity tools and applications — such as sales quoting and document repositories — rely on SSL security as well. And use is not limited to browser-based security. SSL certificates also are used to secure server-to-server communication for applications and data exchange.

With such widespread use of SSL certificates, the consequences of an improperly configured or expired certificate can be disastrous. If an SSL certificate fails to work properly, an organization not only loses sales and places customer confidence at risk, but employees and business partners may not be able to do their jobs.

The risk of exposing confidential information rises dramatically and could result in financial losses or fines for non-compliance. Consequently, managing SSL certificates across complex networks to ensure protection and prevent unanticipated failures is a requirement for all businesses.

It's Time to Implement Lifecycle Management

While the need for ensuring SSL certificates are implemented properly is critical, it's not easy to manage individual certificates across a large organization. This quickly becomes complicated with multiple locations, divisions and the rapidly growing use of external cloud-based services.

It's not only complicated, but costly as well. Cisco estimated that prior to introducing lifecycle management, it required four hours of management per certificate — an average of $288/ certificate.[1] Applying the math in this case means that it was costing more to manage the certificate than to purchase it initially.

With many organizations employing multiple management approaches — usually varying by department and function, and are often ad hoc and manual — it becomes even more challenging to ensure against disruptions. Employing a lifecycle management system ensures a consistent approach and allows for the use of automation, which increases the efficiency and effectiveness of SSL certificate management.

While significant management is required for "routine" operations to either deploy new or maintain existing applications to prevent failures related to improper certificate configuration and expiration, major shifts in business and unplanned events can significantly increase time, costs and security risks.

Typical operational changes — such as migrations across data centers, introduction of private and public clouds, or the integration of mergers and acquisitions — place strain on decentralized manual management processes.

Likewise, unanticipated events (e.g., Heartbleed bug, accelerated end-of-life of SHA-1 hashing) requiring rapid certificate replacement are almost impossible to respond to using decentralized and manual management systems.

1 "Case Study: Scalable Key and Certificate Lifecycle Management with Cisco Systems," Session ID: SPO1-303, RSA Conference 2011, Cisco Systems Inc.

What is a Certificate Lifecycle?

As noted, SSL certificates are not evergreen software that you install and run. They have a finite lifespan and don't allow for updates in the same manner as software. SSL certificates possess the following characteristics and, when considered in aggregate, require management as follows:

- **Issuance**
  Purchase certificates from a trusted vendor and ensure internal approval and administrative oversight is in place.
- **Inventory**
  Log pertinent information about certificate type, deployment, expiration date, person and department responsible for the management of certificates.
- **Monitor**
  Continually monitor your inventory to ensure it meets current compliance rules.
- **Refresh**
  Certificate owners should track expiration, replace them prior to expiration and verify proper certificate installation.
- **Retirement**
  Status of expired certificates is recorded as either "no longer in service" or "renewed," or being able to prematurely revoke a certificate if needed.

Root Issues Leading to Security Gaps

- Lack of visibility for installed certificate base
- Certificate managers don't have effective processes, tools or training
- Certificates obtained from external sources are not recorded in central system or readily accessible
- Lack of understanding regarding risk and responsibility associated with certificate procurement and management
- Certificate renewal processes, information and verification are inadequate

Addressing SSL Certificate Management Gaps

Organizations without proper certificate lifecycle management typically have limitations — at one or more stages — that can be addressed as follows.

Lifecycle Phase	Without Lifecycle Management	With Lifecycle Management
Issuance	Multiple, disjointed interfaces and authorization mechanisms	Single common interface and authorization mechanism
Inventory	Limited to information collected at issuance, often stale and inadequate	Certificate information continually updated by automated systems
Monitor	Certificates get lost in the system, expire and cause lost revenue and reputation	Customizable email notifications will alert you with messages at various points during the certificate's lifecycle to make sure you don't overlook any important issues
Refresh	Limited to email notification attempts based on information collected at time of issuance; no verification of certificate installation	Notification and escalation are combined to create a closed-loop process; verifiable certificate installation
Retirement	No formal retirement	Certificates either renewed or formally retired

End-to-End Lifecycle Management — What's Involved?

At the core of an effective certificate lifecycle management system is defining an administration process for your organization. This requires establishing ownership of procurement and management, and ensuring all departments and personnel who depend upon or directly manage certificates are involved.

There should be a process for requesting new or renewing certificates, approval of requests and backups, and contingencies in the chain to account for people temporarily (e.g., sick, vacation) or permanently (e.g., no longer employed) unable to participate in the process and/or respond in a timely manner.

An audit of all domains and certificates is required to provide an inventory and may need to occur prior to establishing an administration process. Certificates in use might not be properly inventoried because there is no centralized repository.

All certificates need to be consolidated into a single management system. Once consolidation takes place, configure the system based on established procedures and process owners.

With this solution in place, administrators may perform continuous monitoring of systems and certificates, and generate an audit for governance and compliance purposes.

Accelerate the Process

A certificate discovery tool may be used to speed and automate the process and catalogue key certificate information and attributes such as location, expiration date, validity period, issuer and key size. The audit should, minimally, include the following:

- Identify all certificates in your infrastructure, regardless of vendor
- Discover certificates across all servers, local and remote
- Include all certificates and chains, including CA and intermediate CA certificates
- Identify fraudulent or corrupted certificates
- Locate unauthorized "rogue" certificates in use
- Ensure all certificates are properly installed
- Validate that certificates have appropriate validation, encryption and authentication levels
- Identify all servers that should be secured with SSL

Getting Started in 6 Steps

1 Start Scanning

Scan your whole environment: audit all applications, domains and certificates.

To start, you need to know where your SSL certificates are located to gain comprehensive insight into all SSL certificates deployed in the enterprise. This is critical for securing online transactions and communications, as well as back-end operations and applications.

Even if you have a certificate management service and approval process, most certification authority (CA) discovery tools only find SSL certificates issued by that CA or of a particular type. If this is the case, then the audit will miss certificates purchased outside of the approved process — often the ones that cause problems that administrators should be concerned about.

Confirm you're using a universal certificate discovery tool that will find all certificates, regardless of whether they are issued in-house or by outside vendors. The discovery tool should also verify that SSL certificates have been properly installed. Investing in a universal tool will ultimately save time, reduce risk and simplify the audit process. A thorough audit will help identify the need for additional tools and policy/process improvements.

2 Begin Consolidation

Consolidate all certificates into a centrally managed system.

As the use of public and private cloud services, applications and platforms increases, so does the need for SSL certificates. This, in turn, increases the number of administrators and accounts for different types of SSL certificates. Management of these silos becomes inefficient and ineffective unless you have a single point of control.

It's likely you acquired SSL certificates from a range of vendors with different encryption strengths and validation levels, and each are accompanied by their own management consoles.

Based on the results of your audit, you'll have more complete information to evaluate the use of SSL in your environment. This will help identify where you may have silos and fragmentation, which will allow you to consolidate certificate management under a single managed account for better control.

Establish a single master account to use going forward. As current certificates approach their expiration date, replace them with certificates from a primary managed account that supports all types of certificates.

3 Build a Process

Define an organization-wide administrative process for oversight and control policies.

The No. 1 priority: clearly identify who is responsible, accountable and authorized to act regarding certificate management.

With a primary managed account in place, you'll need to establish who can act as authorized administrators to oversee the lifecycle process — from issuance to retirement — and implement controls within the management system.

Define super-administrators, administrators' requestors, approvers and any other roles that may be required in your organization. This will make it easy to deploy a management process that operates with checks and balances, and delegates ownership according to the required level of control and responsibility.

Workflows should be designed to streamline management and eliminate any bottlenecks or dead ends. Take into account who has what privileges, how enrollment works and who receives what types of notifications.

Using role-based access and flexible, real-time assignment of privileges helps enforce the administrative process and enables users to manage certificates based on their role and organization. Audit logs should record a detailed history of all administrator actions related to every issued certificate and can be used to uncover any policy violations.

4 Be On Alert

Establish alerts and reporting to monitor inventory.

Your organization needs to be able to notify and escalate certificate issues — based on authoritative and current information — to a chain of command via an actionable process.

Treat impending critical certificate expirations as incidents in real-time to prevent service disruption. Relying on manual reports with incomplete and static information (e.g., spreadsheets calendars or alert logs) will not suffice.

Set up your certificate management platform to run automated reports for the system administrators to better manage time and resources. Run dynamic, real-time reports to show the actual SSL certificate inventory across the enterprise by certificate status:

- All certificate requests
- Pending
- Approved
- Rejected
- Valid
- Revoked
- Deactivated
- Expired or expiring

Publishing renewal reports at regular intervals — starting as far out as 90 days and progressing to 60 days, 30 days and up to daily alerts — helps an administrator plan for SSL certificate renewals and prevent disruption.

These reports should have a distribution list for failover and escalation paths as expiration dates approach and no action has been taken. Historical reports can provide administrators with valuable insight into past usage for future planning and management.

You should also run the SSL Server Test by Qualys SSL Labs frequently. This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. Please note that the information you submit here is used only to provide you the service. They do not use the domain names or the test results.

5 Revoke & Replace

Revoke, replace or retire certificates as necessary based on policy.

A centralized certificate inventory and management tool makes it easier to revoke and replace certificates in conjunction with established polices for certificate issuance life, key strength, validation type, etc. This system and process will support both routine updates and replacement, but also support more non-routine scenarios.

For example, when servers are taken offline, moved or replaced, administrators should have access to a management system to take actions to either revoke and/or replace SSL certificates, as necessary. This type of system will also support situations such as the Heartbleed bug remediation, where it's critical to replace a certificate with compromised private key.

In the event a private key is lost, or if a server crashes and a certificate is deleted, the administrator should be able to revoke the certificate and issue a replacement.

6 Maintain Diligence

Enable continuous discovery and monitoring through established processes.

There is the continuous threat that rouge certificates will be deployed, placing your organization at risk. Common scenarios include someone legitimately procuring a certificate in a test or development environment; an outside vendor deploying unapproved certificates; or a malicious actor installing a rouge certificate for their benefit.

Continually monitor and scan the environment using Discovery and the SSL Server Test to ensure the integrity of the whole process and prevent against outages and security risks. Regularly review current practices against regulatory and other policies to ensure the process is evolving with industry standards, compliance requirements, new threat vectors, technology shifts and business objectives.

Conclusion

By adopting a certificate lifecycle process supported by a single, comprehensive SSL certificate management method, organizations can get out of “fire-drill” mode, gain enterprise-wide visibility and ensure enterprise security.

A key component of this solution is the use of an SSL certificate management system that supports a process-driven approach that simplifies SSL certificate discovery and monitoring, and automates certificate renewal and transfer.

An effective SSL certificate management solution enables organizations to know what kinds of certificates they have, help them renew certificates in a timely fashion, and manage certificates across multiple vendors.

The implementation of a lifecycle management system will, ultimately, result in the agility to respond to security events (e.g., Heartbleed), perform updates such as SHA-1 migration, prevent service outages and maintain compliance.

This proven approach reduces the overall cost and complexity of managing SSL certificates across a distributed environment.

About Entrust Datacard

Consumers, citizens and employees increasingly expect anywhere-anytime experiences — whether they are making purchases, crossing borders, accessing e-gov services or logging onto corporate networks. Entrust Datacard offers the trusted identity and secure transaction technologies that make those experiences reliable and secure. Solutions range from the physical world of financial cards, passports and ID cards to the digital realm of authentication, certificates and secure communications. With more than 2,000 Entrust Datacard colleagues around the world, and a network of strong global partners, the company serves customers in 150 countries worldwide.

For more information about Entrust products and services, call **888-690-2424**, email **entrust@entrust.com** or visit **www.entrust.com**.

Headquarters
Entrust Datacard
1187 Park Place
Shakopee, MN 55379
USA

EMEA:
+44 (0) 118 953 3000

Twitter Facebook Youtube LinkedIn Google+ RSS