MODERNIZING YOUR SSL CERTIFICATE MANAGEMENT

A Selection Guide to SSL Certificate Lifecycle Management Platforms

Entrust Datacard™

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

Table of contents

About this guide

Deciding on the right SSL management platform for your organization can be daunting. This step-by-step guide is will not only you help you along the path to finding the right service, but then ensure you execute a successful implementation.

If you are in the market for SSL certificate management services, the next 15 minutes of reading will save you weeks of work and prepare you to decide upon the right solution — and ensure you get the maximum value from the SSL management platform you purchase.

Why SSL management is critical

While the most recognizable use of SSL certificates is the “browser lock” icon displayed on transactional-based websites to protect user login information, ordering and credit card submissions. But it extends well beyond this use case and protects mission-critical enterprise infrastructure components.

For example, employees and partners using VPNs that access sensitive backend systems and information use SSL certificates to secure remote access. Virtually all browser-based cloud services require SSL certificates when used to display 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. And use is not limited to browser-based security. SSL certificates secure server-to-server communications for applications and data exchange, wireless access points and a host of other uses.

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, a company 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 of 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 has become mission critical to all businesses.

Businesses that have used manual management processes and/or multiple services to manage their SSL certificates typically experience a high level of cost and complexity. These organizations can expect to see a dramatic reduction of both through consolidation into a single master management system.

Organizations with as few as 10 certificates, or those managing 10,000 or more certificates, will realize a number of benefits to include:

- Greater operational efficiencies
- Higher availability of critical business applications
- Lower, more predictable costs
- Greater productivity
- Decreased risk of compromised information

This guide will walk you through the key steps to selecting an SSL certificate management platform. Included checklists explore product, implementation, service and business requirements — all of which impact the benefits received and total cost of ownership (TCO) of an SSL certificate management platform.

Define your SSL needs

Support for complete lifecycle management

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. They have the following characteristics and, when considered in aggregate, require management as follows:

- Purchase

  Purchase certificates from a vendor or re-issue existing certificates, following established Certificate Service Request (CSR) policy with approval and administrative oversight.

- Install

  Automatically install SSL Certificates and configure servers. Auto-install speeds up the deployment process and provides a hassle-free way to support Always-On SSL by reducing installation and server configuration errors.

- Inventory

  Log pertinent information about certificate type, deployment, expiration date, person and department responsible for management of certificates.

- Refresh

  Track expiration and replace prior to expiration and verify proper installation of certificates.

- Retirement

  Record status of expired certificates as either no *longer in service or renewed*.

Modern certificate management requires the ability to monitor and manage certificates throughout their lifecycle in accordance with your organization's policies and procedures. In such a system, all certificates need to be consolidated into one management system.

Once consolidation takes place, configure the system based on established procedures and process owners. Once complete, administrators can perform continuous monitoring of systems and certificates and generate an audit for governance and compliance purposes. A modern certificate management system requires the ability to centrally manage and automate much of the required processes during the certificate lifecycle.

Business considerations

When implementing an SSL solution for your organization, consider its ability to support your business operations and flexibility to change, as necessary. For example, major shifts in business operations — such as migrations across data centers, private cloud and public clouds, or the integration of mergers and acquisitions — will place a significant strain on decentralized manual management processes and reduce business agility.

One of the primary business benefits of consolidating SSL certificate management is the ability to purchase in bulk. This typically includes volume discounts and stock an inventory certificates that allow line-of-business-level access and management. Also consider your organization's budgeting and accounting methods and understand whether the vendor offers CAPex and OPex payment options when purchasing multi-year services.

Technical considerations

There are numerous technical considerations based on the diverse number and types of certificates, roots, encryption strength, private keys and hashing algorithms, as well as operational environments and integration points.

Support for a wide variety of applications — ranging from consumer sites requiring highly recognizable extended validation (EV) certificates to back-end utility certificates for securing server-to-server communication — need to be taken into account.

It's important to be able to deploy the right types certificates for the right use cases based on company policies and the ability to ensure certificates are properly configured and installed. It's also essential to have API support for integration with company systems such as billing, enterprise resource planning (ERP) and configuration management database (CMDB).

Examine your options

As you explore your SSL management options, you may discover three types of solutions: services that will find but not manage certificates; those that will manage but not procure certificates; and those that can manage but not discover certificates.

Trying to patch together a number of products is generally less effective and more costly than a single solution. The field can be narrowed to two main options: enterprise key management systems and SSL certificate management platforms. There are differences to consider that ultimately affect the level of effort, resources required and cost of deploying a certificate management system.

1

Option 1

Enterprise key & certificate management (EKCM)
Your first option is to use an automated enterprise key and certificate management (EKCM) solution. These will offer improved security and save time and money. They offer the ability to manage each process in the digital certificate lifecycle, reducing its risk of breach, failed audits and unplanned system downtime.

These certificate managers are certification authority (CA) agnostic, allowing you to bring any certificate from any CA (including internal CAs) under an automated EKCM system. This will allow you to manage all encryption assets centrally.

2

Option 2

Certificate management platform
A second option is to use a certificate management platform from a CA vendor. The best of these typically include most of the functionality provided by EKCM solutions. Others are very rudimentary in their approach and don't come close to offering the functionality of an EKCM solution.

The ECKM solution depends on procuring certificates from a CA. Deploying an EKCM can be redundant and significantly more costly when compared to a CA-delivered management platform that includes the cost of the certificates and offers similar functionality as an EKCM platform.

Since the CA-based solution will meet the needs of most organizations, and given the broader applicability, ease of deploying one platform and lower costs, this is the recommended approach. This paper will provide the essential "must-haves" and considerations for purchasing this option.

Feature requirements

To best select an SSL management solution, it is imperative to assess the security capabilities of the products you are considering so that you're gaining the level of security necessary to protect client trust and your company's brand.

It is also important that your SSL management solution offers enhanced performance capabilities to allow your infrastructure to scale with the growth of your cloud-based environment.

Finally, evaluate the flexibility of the product to assess whether it can accommodate modifications as your business needs change. Determine whether it is interoperable with the broad suite of technology and infrastructure tools that are needed to successfully operate a Web-based business.

The following is a list of critical business and technical features that should be present in any capable SSL management service.

Cloud-based service

The ideal SSL certificate management solution lives in the cloud so organizations don't have to bear the high costs of managing servers, PKI software, hardware security modules and key management.

While there are still some organizations that run premise-based PKI deployments to issue publicly trusted SSL certificates, this approach is costly and impractical for any organization that isn't currently using this approach. All of the major certification authorities (CA) have been offering cloud-based services for over 10 years and is by far the best option for the majority or organizations.

Universal centralized control

A robust certificate management system should allow you to consolidate purchasing and management across business units and locations to reduce costs. It should have the capability to manage SSL certificates from multiple CAs, including self-signed certificates. There should be no need for multiple CA management tools and you should be able to manage all certificates from a single console.

Secure Web-based management portals

Using a cloud-based service offers the flexibility of easy anywhere, anytime access, giving you the ability to manage certificates from desktops as well as mobile devices. Because certificates are mission-critical services, you want capabilities to manage certificate inventory via Web-based access. This gives accredited company administrators the capability to issue certificates on demand for immediate availability, as well as revoke certificates instantly from anywhere in the world.

Vendors should offer the ability to secure access to all management portals using multifactor authentication to prevent unauthorized access to certificate issuance and revocation operations.

Five Essential Elements of an SSL management service

1 **Certificate Discovery —** identifies every certificate across all systems, inspects for expiry, and notifies about potential misconfigurations.

2 **Certificate Monitoring Policy —** provides an overview of all SSL certificates for your domains so you can detect and stop unauthorized issuance and protect your brand.

3 **SSL Server Testing —** identifies vulnerabilities and grades your level of compliance.

4 **Malware Scanning —** detects and removes harmful malware while identifying other vulnerabilities to common attacks.

5 **Best Practices Approach —** provides the tools and resources needed to keep up-to-date on the latest threats and to help properly install SSL and configure your servers.

Bulk purchase & pre-verification

The challenge of Web-enabling both internal- and external-facing business applications — as well as mission-critical applications such as enterprise resource planning (ERP), supply chain management (SCM) and customer relationship management (CRM) — is the need to have them constantly available. This leaves little time for the testing, deployment and maintenance of these applications — tasks often restricted to small windows of time during off-peak and/or weekend hours. Given the small windows of opportunity for maintenance, it is critical to have valid SSL certificates available.

If an administrator can’t obtain a new certificate or renew an existing one, then deployment of the application may be delayed or, worse, put into use without adequate security. Bulk purchasing and inventory of pre-verified certificates provides administrators with the ability to quickly fulfill requests within small time windows and keep operations running smoothly.

Full range of SSL certificates

Because you will likely be deploying certificates across a variety of applications — ranging from external consumer websites, to internal server-to-server communications, to mail servers and VPNs — you need to ensure that your service allows you to issue a full complement of certificates and allow for varying validity periods.

If a user needs a certificate that’s not available through the service, then it will likely result in “rogue“ certificates being purchased for specific uses or environments that fall outside of a centralized management system. This increases security and outage risks, as well as adds additional costs for administration.

Root ubiquity & certificate compatibility

Root ubiquity refers to how widely a CA’s Root Certificate is installed in browsers, devices and applications using SSL. Root ubiquity is critically important because a browser or application will only recognize SSL certificates if the Root Certificate of the CA is present within the “trusted Root Certificates” store. And with more and more devices being Internet-enabled, this extends to mobile devices, mobile apps, email clients, micro-browsers, gaming devices, set-top boxes and printers.

CA Root Certificates are added into the trusted Root Certificate store by the application, browser or operating system vendor, such as Microsoft or Mozilla. In general, SSL vendors need to be audited to WebTrust-complaint standards set by the AICPA.

If you use an SSL certificate that has been issued by a CA Root Certificate not present in the trusted Root Certificate store (in one of the commercially available browsers), then the visitor’s browser will display a warning message or an application may fail to establish service. Clearly, it’s important to avoid such situations.

Ensure you avoid such warnings by selecting an SSL provider with the highest acceptance level across all applications and browsers. Ubiquity rates should exceed 99.99 percent to make sure that users with older browsers and devices can access your services.

Since newer or smaller CAs may not have had their roots included in the root store for some browsers or devices (e.g., gaming consoles, smart devices, set-top boxes), you should avoid using vendors with limited ubiquity. This is especially an issue for older browsers, which maintain popularity outside North America and Europe.

Scalability use case

Your operation in India, for example, needs to issue a certificate locally to bring a development server online, but the time difference means they'll have to wait 24 hours for your approval.

The delay is a costly and redundant requirement for a pre-approved use of a certificate in an authorized domain by an authenticated user. Delegated administration will allow instant issuance of the certificate.

Scalability of administration

In addition to performance and availability, scalability also refers to the ability to manage and administer an ever-changing and expanding user population. Delegation is the answer to making administration scalable. While you want to centralize access policy definition, monitoring, enforcement and auditing, you want to decentralize day-to-day decisions about who can manage certificates.

Without losing control, push such responsibilities into your lines of business and operations centers to people working directly with service providers and/or developing Web applications. These are the people who can make the best and fastest decisions.

Automated certificate discovery

There should be no need to manually search for the number or types of SSL certificates that exist in your environment. Enterprise-wide visibility of all certificate types, from all CAs, reduces risk of down time and deployment of rogue certificates. Consequently, you should ensure that a platform has capabilities to automate discovery and monitoring.

Support for certificate installation

Installing intermediate certificates can be challenging for system administrators unfamiliar with SSL certificates. An SSL certificate management system, with automated transfer and renew capabilities for intermediate certificates, will help avoid incorrect installation and ensure business continuity.

Customizable & robust reporting

Your system needs to provide strong reporting capabilities to be able to satisfy internal operations management as well as internal and external governance and compliance reporting. You need to ensure you can report on all SSL certificates in the inventory for accountability and compliance verification, and can provide both detailed and executive-level reporting. You will need to make sure you can maintain reports that monitor the security of SSL certificates, such as private information and hashing algorithms. Finally, you will need to be able to customize your reports and receive them by email according to a set schedule.

This capability will help to makes sure you are adhering to industry best practices and standards as well as simplify certificate replacement in situations such as the Heartbleed vulnerability and SHA1 to SHA2 migration process.

Customizable audit trails

Keep an audit trail on all actions performed on certificates. This will include statistics quantifying the number and types of certificates issued, revocation actions and analysis of these activities using exportable certificate revocation list (CRL) files, which are helpful for organizations using governance, risk management and compliance (GRC) applications. The ability to monitor certificate requests using comprehensive search functionality on certificates and certificate signing requests should also be available to administrators.

Customizable alerts & notifications

To reduce the risk of expired certificates alarming users or website visitors, and to ensure against operational outages and security vulnerabilities, it's critical to have an escalation path that notifies a number of people across the organization when a certificate is about to expire.

You must be able to maintain the ability to view upcoming expiration dates for certificates and plan for timely renewal. Your system should also be able to provide automatic email and/or SMS notifications at predetermined intervals of your choosing (e.g., one, seven or 30 days) before certificate expiration. Route notifications to backup administrators in the event the primary administrator is unable to respond.

Customization & application integration

A complete SSL software management service should allow you to extend your operations and brand with a minimal amount of effort. It should provide the ability to be integrated with existing application and GUIs to deliver services to your users in the manner you require.

You may want your certificate request system to have your own look, feel and branding, but that doesn't mean you need to write custom code for the whole application. You may need it to integrate with your ERP system for cost allocation and internal billing, or connect with enterprise CMDB ITL process applications or services such as ServiceNOW. If that's the case, find out if the services have APIs or can work using HTTPS post front-end integrations.

Implementation & delivery support

Providing the management platform is not where vendor responsibilities stop. To ensure rapid implementation, the vendor should provide detailed documentation, including release notes, integration guides, issuance instructions and API help files. Proper implementation may also require access to vendor support teams. Ensure that the vendor is available to support customers throughout the duration of the implementation and life of the service.

Account models & support for multiple licensing models

As the number of Web-enabled applications grows, so too does the number of certificates required to secure those applications, which can often lead to increased and unpredictable procurement costs.

In many organizations, purchasing certificates is done on an as-needed basis across multiple locations, departments and personnel. This results in multiple POs, credit card transactions and multi-day wait times to receive certificates. In addition, purchasing may be spread across multiple vendors with different licensing options, some of which may require minimum purchases that result in paying for certificates that go unused. Without cost predictability, budgets can be exceeded and profitability decreased.

Consider options that will best fit your budgets and whether you are better served with Opex- or Capex-friendly services. Some vendors offer flexible pooling accounts or a budget-oriented, non-pooling account model. The different models allow organizations to tailor their certificate purchases with their specific security or budget requirements. From up-front investments to structured certificate lifetimes, carefully consider the subscription models to find one best

Feature checklist

The following is a list of specific features and functionality that should minimally be included in SSL software applications. This list takes into account backwards compatibility and emerging, near-term technology requirements.

Audit capabilities

Identify all certificates in your infrastructure	
Discover all certificates across all servers (local and remote)	✓
Include all certificates and chains, including CA and/or intermediate CA certificates	
Identify fraudulent or corrupted certificates	
Identify unauthorized "rogue" certificates in use	
Validate all certificates are properly installed	✓
Validate certificates have the appropriate level of validation, encryption and authentication	✓
Identify all servers that should be protected and secured with SSL	✓

Administration capabilities

Multifactor user authentication	
Support for multiple user roles	✓
Multiple access privileges	✓
Escalation path	✓
Delegated administration	✓
Segregation of duties	✓
Administrative audit	✓

Security

Multifactor authentication for administrative access	✓
WebTrust certification	✓
Advanced key management	✓
Rapid revocation	✓
Secure console	✓
Segregation of duties	✓

Certificate support

Extended Validation	✓
Standard Validation	✓
Unified Communications	✓
Wildcard	✓
Secure Email/Document	✓
Mobile Device	
PDF Signing	
Code Signing	
SHA-1 and SHA-2 Hashing	
1028-Bit and 2048-Bit Encryption	✓
OCSP and CRL Validation	
Intranet Certificates	✓
99.99 Percent Browser Ubiquity (both Desktop and Mobile)	✓
ECC Support, Intel VPN Support	

Other

On-Demand Issuance	✓
Customizable Request Forms	✓
API Support	✓
Customizable Reporting	✓
Customizable Alerts	✓
Global Support	✓
SSL Server Test	✓

Critical strategic considerations

SSL is a unique industry, requiring understanding of browsers, mobile platforms, servers, applications, standards and advanced security. In addition to making sure the features map to your requirements, you want make sure the vendor has the experience and expertise to deliver today and going forward.

The following list covers the strategic and qualitative considerations that form a solid vendor relationship.

1. How well does the solution satisfy your most important requirements?
2. How user-friendly is the solution?
3. How compelling are the vendor's references?
4. How easy/complex is the implementation?
5. How customizable is the solution?
6. Does the vendor offer excellent support and speedy service?
7. Does the vendor have customers similar to you?
8. What are the vendor's security qualifications?
9. How innovative is the solution compared to others on the market?

Review pricing carefully

When evaluating vendors, be sure all feature pricing is considered and, optimally, not offered piecemeal, which can become costly. Some vendors charge extra for verifying additional domains, keeping certificates in offline cold or warm backups, and replacing corrupted certificates. Some functionality, such as adding administrators, can also be a hidden cost.

One of the most significant surprises organizations face is centered on certificate replacement or re-use. Be sure to understand whether certificates are purchased on a "use-it-or-lose-it" basis or can be recycled or carried forward if not issued.

When making a selection, it's important to consider this list of essential features and be sure that there is no hidden pricing for critical components.

Conclusion

In the final analysis, you want a complete certificate provisioning solution that gives your organization full control over certificate issuance, suspension and revocation.

It should allow employees to request certificates, and empowers accredited company administrators to directly manage certificates requests with minimal technical know-how that will ultimately require flexibility.

It's unlikely any product is going to meet 100 percent of your requirements out-of-the-box. In order to get a "best-fit" for your needs, you will require a tool that is powerful, but also flexible enough to be molded into your environment.

The platform you select needs a robust suite of capabilities so that your operations are efficient and effective, and the user experience remains the way you want across your organization. Also ensure it offers the necessary hooks and APIs to seamlessly integrate into a variety of applications and workflow environments.

If you consider the above criteria — and select a platform with demonstrable success under real-world conditions — you will find a significant reduction in the cost and complexity of managing SSL certificates.

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