

Certificate Lifecycle Manager



Trustwave® CLM centrally manages your organization's certificate lifecycle to ensure up-time and protect your assets and brand.

Managing Numerous SSL Certificates is Resource Intensive

Managing the barrage of SSL certificates that organizations need to secure their Web sites and network resources limits an IT staff's ability to focus on other business objectives. However, certificate lifecycle management is a critical task. Without it, an organization's network assets can become unavailable leading to a decrease in staff productivity and damage to an organization's brand and reputation.

Many organizations now institute Managed Public Key Infrastructure (MPKI) initiatives to assure the validity of their certificates in general, and SSL certificates in particular, and the availability of network resources.

An MPKI initiative increases the efficacy of the end-user experience and improves the productivity of staff members, but each network component can require multiple certificates to facilitate communication across an entire network infrastructure. The average enterprise deploys hundreds if not thousands of network assets and to manage credentials across such a vast infrastructure requires the management of hundreds, if not thousands, of certificates.

The number of tasks that IT staff members must perform to manage the lifecycle of an enterprise's entire portfolio of SSL certificates creates a time-consuming and resource-intensive process:

- Tracking all deployed certificates
- Maintaining certificates to ensure their compliance with regulatory and industry standards
- Requesting, installing, revoking and renewing certificates

While tedious, each task is critical to business operations. The expiration or improper configuration of just one certificate on a business-critical network asset can put an organization out of compliance or take an entire network infrastructure offline, putting an organization at risk.

Automated Management Ensures Security and Availability

Trustwave Certificate Lifecycle Manager (CLM) automates the entire process and is available via either software executable at the client site or as a managed, on-demand security solution accessed via Web browser. Trustwave CLM automates the three major phases of your organization's certificate lifecycle management:

- **Discovery** via an automatic audit of your IT infrastructure for deployed certificates
- **Analysis** via monitoring assets and then applying your policies
- **Management** via issuance, revocation and renewal of certificates

About Trustwave

Trustwave is a leading, global provider of information security and compliance management solutions to large and small businesses and the public sector. Trustwave offers and supports SSL certificates, proprietary security appliances, managed security services and compliance management solutions to help organizations simplify, accelerate and validate their compliance with industry standards and regulations such as PCI DSS, HIPAA, SAS-70, GLBA and ISO 27002 (formerly 17799) among others. Trustwave's clients include financial institutions, large and small retailers, global electronic exchanges, educational institutions, business service firms and government agencies. Trustwave is headquartered in Chicago with offices throughout North America, South America, Europe, the Middle East, Africa, Asia and Australia.

www.trustwave.com 1-888-878-7817



Discovery

Trustwave CLM detects all certificates used on the network by performing IP, port, host and DNS scanning. The scans allow users to determine which assets are associated with which certificates and the Certificate Authorities (CAs) that issued those certificates. Users can then quickly locate and decommission non-compliant certificates and trigger renewal processes if necessary.

Analysis

To complement existing policy and compliance initiatives, Trustwave CLM provides key storage, key recovery and an auditing platform. The solution compares all deployed certificates to internal policy parameters and industry or regulatory requirements. Trustwave CLM also logs every action taken by the system and users to provide an audit trail for each certificate and key to provide a compliant and auditable key management infrastructure.

Management

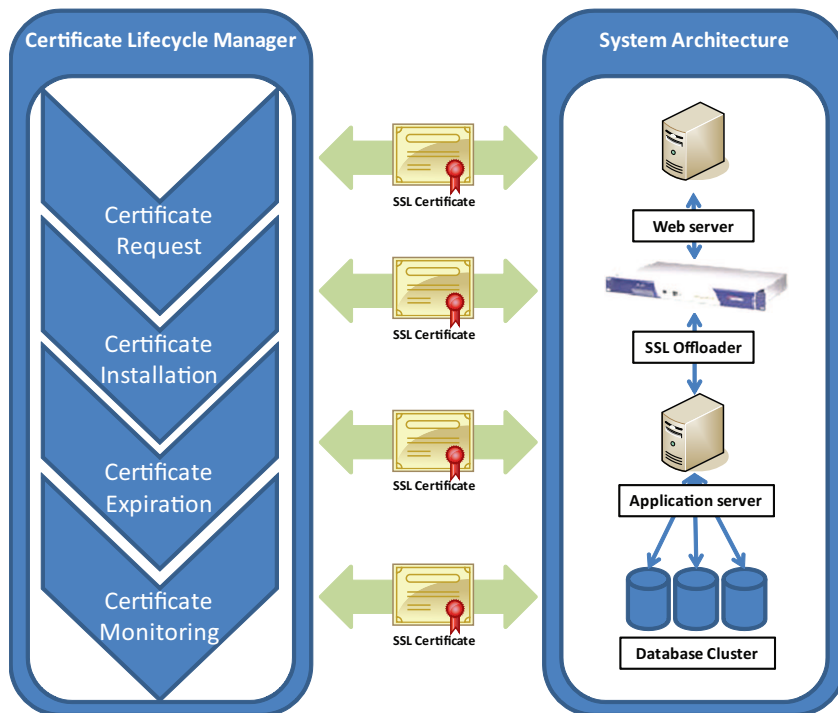
Trustwave CLM centralizes management of certificates and, through an integrated Certificate Authority (CA), can issue, revoke and renew any certificate. Through its automated certificate provisioning and installation capabilities, CLM reduces or eliminates manual certificate management tasks to streamline the process and increase or maintain availability, productivity and efficiency.

Trustwave CLM: How it works

Trustwave CLM has a state-of-the-art script and template system that allows your organization to model the specific change processes that are required to efficiently manage your digital certificates. Upon deployment, CLM will immediately inventory your deployed SSL assets and can then be connected to your various CA's to begin managing your certificate lifecycle. Certificate renewal can be automated throughout the entire lifecycle or just a specific aspect of it based on your organization's needs. In addition, every aspect of CLM is protected by access control technology to ensure that only system administrators have access to configurations and scripts that can affect your systems.

A significant portion of certificate lifecycle management involves monitoring remote assets. CLM has a highly flexible network scanning and monitoring engine with a fully customizable notification engine to provide information to interested parties. The types of scans supported by CLM include:

- SSL certificate by host
- SSH keys by host and address
- SSL certificate by address
- Location of deployed Microsoft CAs



Trustwave CLM facilitates management of most components of SSL deployment:

- Apache SSL
- Apache Tomcat SSL
- IBM WAS SSL
- Trustwave certificate request
- Comodo certificate request
- OpenSSL certificate request

System Requirements	
Processor	2.0 Ghz
Memory	512 MB/1 GB
Disk	2.0 GB
Network	10/100 Base-T
Operating Environment	VM-Ware Server, ESX or Player