ManageEngine
Key Manager Plus

Certificate management 101

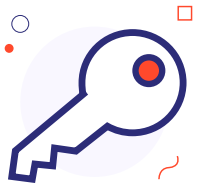
Certificate management is the process of monitoring and managing the life cycles—from acquisition and deployment to tracking renewal, usage, and expiration—of all SSL/TLS certificates deployed within a network. This process provides IT administrators with complete visibility and control over their SSL/TLS environments and helps them pre-empt security breaches, outages, and compliance issues.

Before understanding why SSL/TLS certificate management should form an integral component of your organization's IT security strategy and how to build an enterprise-wide certificate management program, let's take a look at how certificates work to keep online communications secure.

SSL certificates and their role in securing online communications.

An SSL certificate, also known as a public key certificate, is an electronic document that verifies one's ownership of a public key. When site owners install SSL certificates onto their web servers, all web traffic between their servers and users' browsers gets encrypted, ensuring confidentiality of the information exchanged. The application protocol HTTP automatically changes to HTTPS in the browser's omnibox and a padlock icon appears, indicating that all connections to the website remain private.

You can view the SSL certificate of any website that runs on HTTPS and you will find the following information:



Public key: Shows details of which public key and cryptographic algorithm are used for signing the certificate.

Site owner identity: Identifies the site owner who has installed the certificate on his website.

Digital signature: Shows the signature of a trusted third party that authorizes the legitimacy of the site owner's identity and their website.

SSL certificates are usually signed and issued by entities called certificate authorities (CAs). These are third-party organizations that play a pivotal role in internet security by acting as the epitome of trust for both parties—site owners purchase SSL certificates to gain their customers' trust and site visitors rely on SSL for their data privacy. Browser companies trust only those SSL certificates issued by internationally acknowledged CAs and will throw error messages when connecting to websites that use locally generated SSL certificates.

How do SSL certificates work?

When browsers attempt to establish an encrypted session with a website that's secured with SSL, the following sequence of operations occurs in the background:

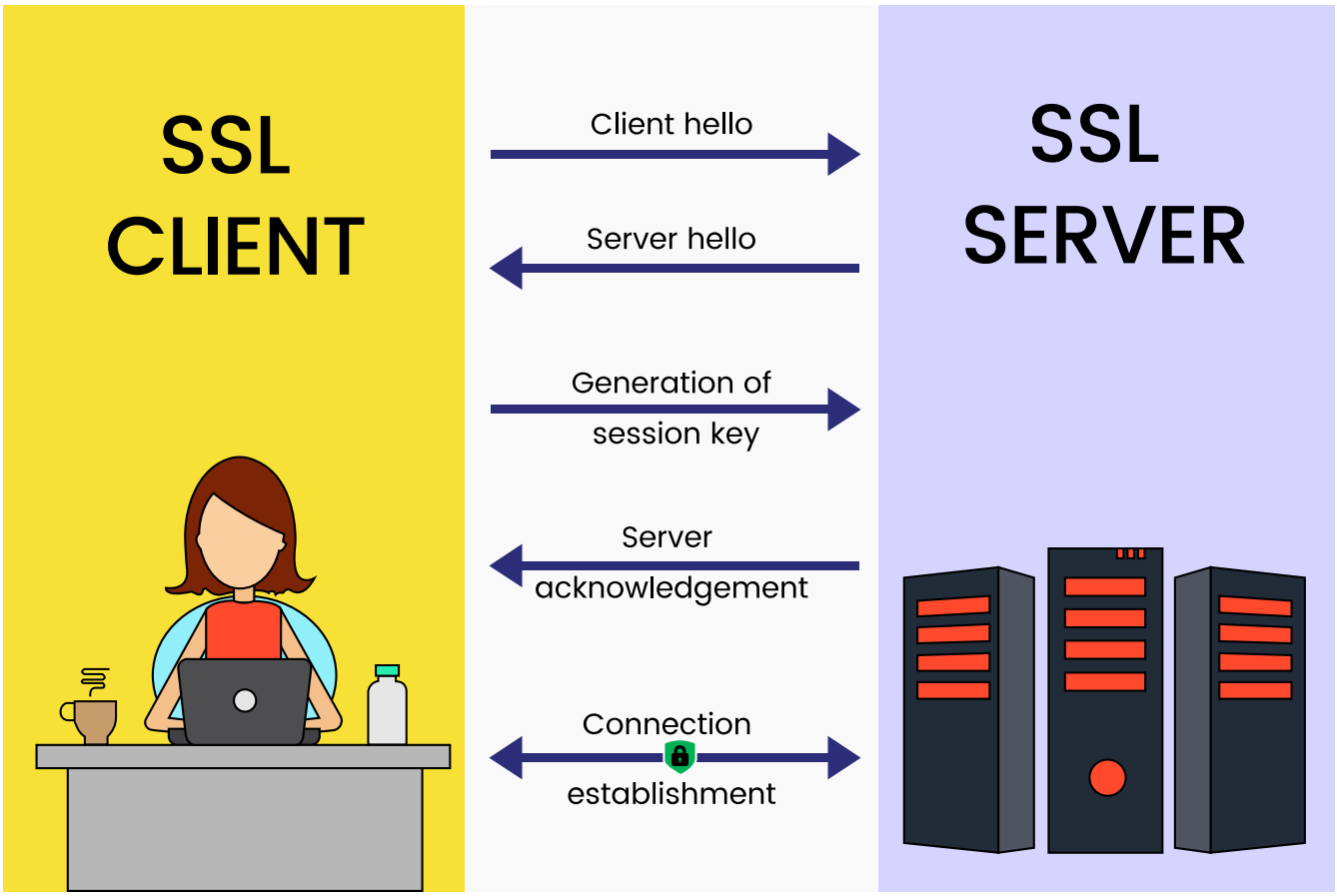
1. The browser connects to a web server secured with SSL and requests the server to prove its identity.

2. The web server receives the request and sends back a copy of its SSL certificate along with its public key.

3. The browser receives the certificate and checks its legitimacy by comparing it with a predefined list of trusted CAs. If the browser trusts the certificate, it creates a symmetrical key called the session key, encrypts the key using the server's public key, and sends it back to the server.

4. The web server decrypts the message using its private key, sends an acknowledgement—that is encrypted using the session key—back to the browser to start the session.

5. The browser and server then begin the session afterwards, in which all exchanged information is encrypted using the session key.

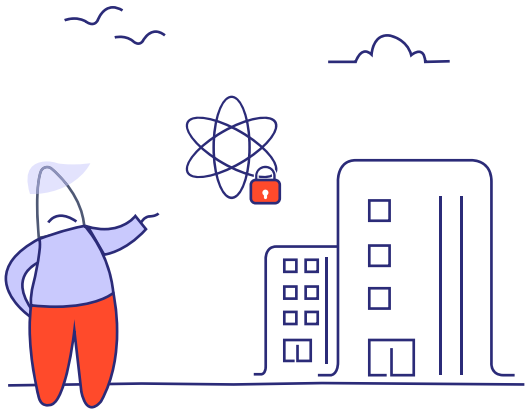


However, implementing SSL encryption for websites is not a one-time process. SSL certificates expire after a predefined duration and have to be constantly renewed. Failing to renew will cause browsers to lose trust in that website's legitimacy, which is shown as error messages. Worst case scenario, expired certificates may also pave the way for security breaches. Therefore, organizations need to maintain surveillance on the life cycles of all certificates deployed within their network and constantly monitor their usage to ward off any chances of data breaches or website outages.

Current state of certificate management in enterprise IT*

61% of enterprises are deploying more keys and certs because of shorter certificate lifespan

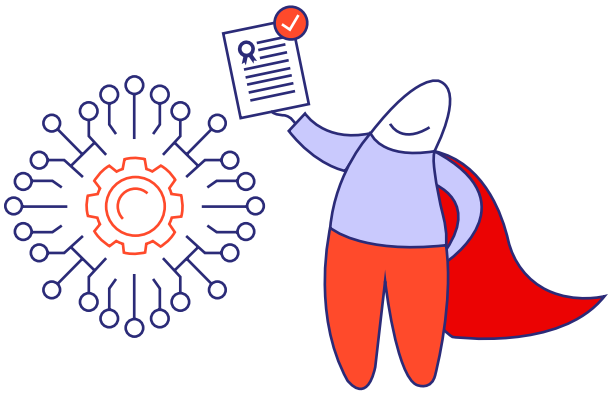
60% of enterprise don't have an enterprise-wide cryptographic strategy for deploying keys and certs

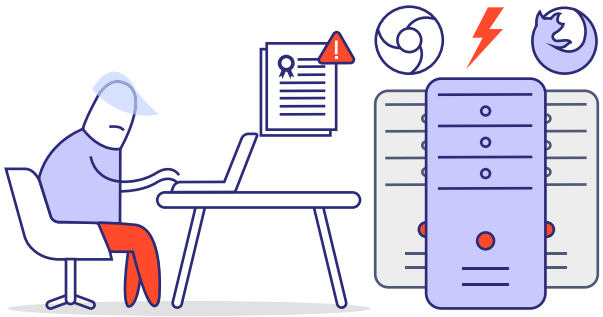


51% of enterprises mark crypto agility as a tope strategic priority for IT security

* State of Machine Identity Management, Ponemon Institute, 2021

82% of organizations feels SSL/TLS certificates are the most crucial machine identity





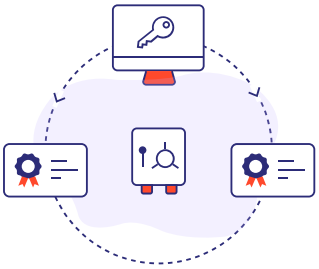
41% of companies experienced 4 or more service outages due to expired certs in the last 24 months.

Take the guesswork out of SSL/TLS certificate management

With digital transformation and cloud adoption taking over almost every industry, organizations are witnessing a splurge of certificates scattered across their networks. In addition, browser communities are increasingly moving towards short-lived certificates with an intent to improve the baseline security of online services. These factors have left IT administrators with the huge responsibility of tracking the life cycle of every security certificate deployed within their network, monitoring these certificates for any unusual activity, and renewing them before expiration. This is very daunting, especially for large organizations that juggle a lot of certificates. A centralized platform that can automate certificate management operations and provide insights on an organization's SSL environment is exactly what IT administrators need. Here are a few of the many advantages of deploying a centralized certificate management solution:

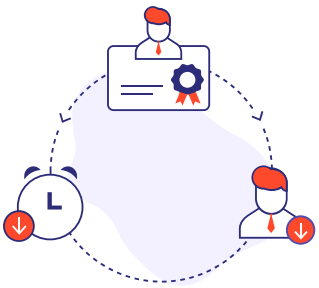
1. Timely alerts to prevent outages and protect brand reputation.

It's not uncommon for organizations to let a certificate or two expire by mistake. But one expired SSL certificate is all it takes for visitors to lose trust in your brand's credibility. Implementing a centralized certificate management solution alerts administrators when certificates are about to expire and reduces the possibility of website outages due to unexpected certificate expiration.



2. Centralized inventory and increased transparency.

Quite often, SSL certificates are requested and deployed by teams locally, as needed, but then their existence is soon forgotten. Centralized management consolidates all of an organization's certificates in a single repository and streamlines the acquisition, deployment, and renewal processes. This provides administrators with complete transparency and control over their SSL environments.

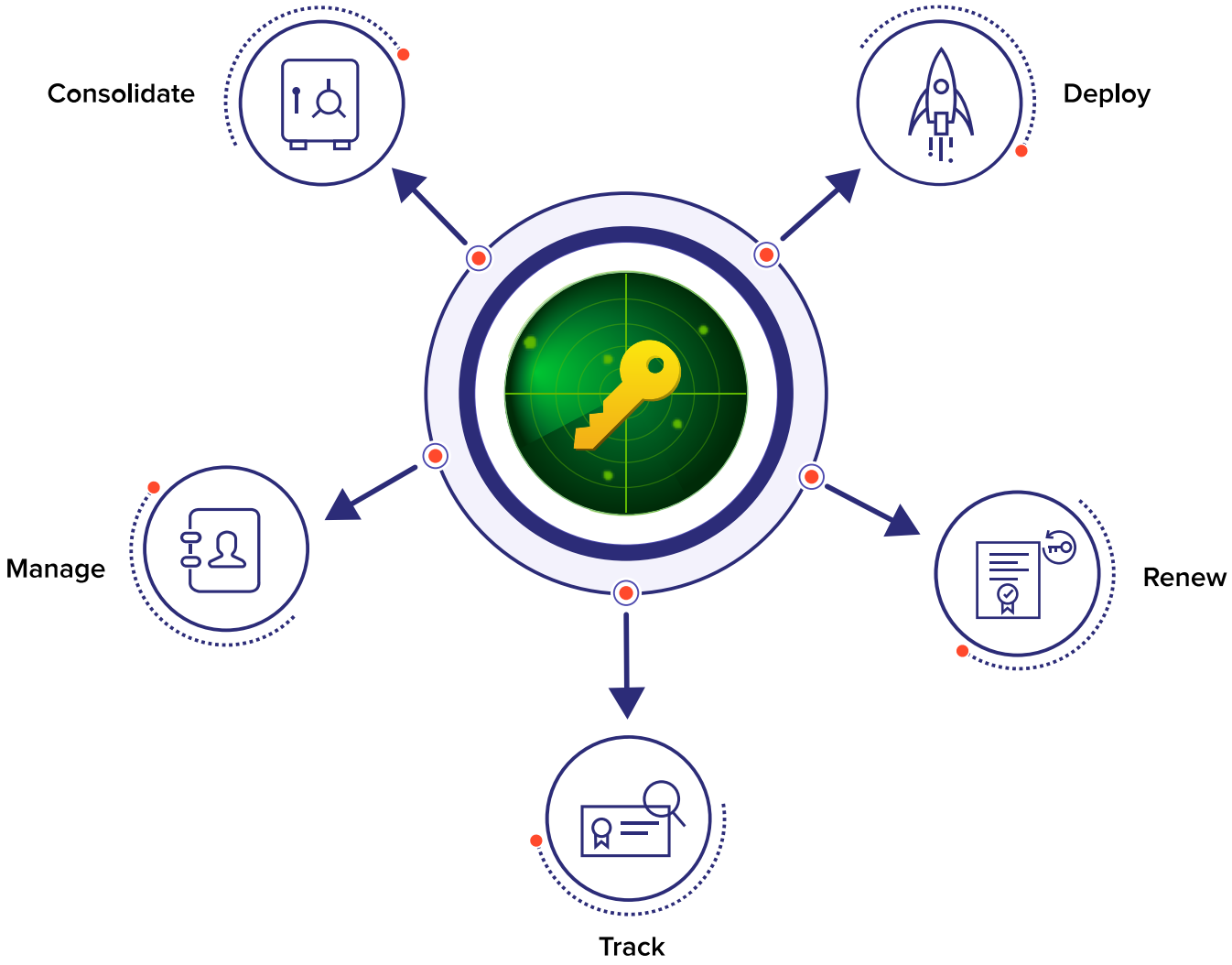


3. Reduced time and effort.

Most of all, centralizing and automating certificate management greatly reduces operational costs and staff time associated with managing individual certificates.

Eliminate certificate fatigue by centralizing life cycle management with Key Manager Plus.

Key Manager Plus, our web-based key and certificate management solution,provides administrators with much-needed visibility and control over their SSL environment. It centralizes and automates operations related to managing certificate life cycles and helps pre-empt security attacks, compliance issues, and site outages due to unexpected certificate expirations. Here's a quick summary of Key Manager Plus' features:



- Centralized SSL certificate discovery and inventory
- Built-in CSR generation tool
- Streamlined certificate request workflow
- End-to-end life cycle management through third-party CA integrations
- Active Directory and MS Store integrations
- Instant, comprehensive reports on all certificate management operations
- Intuitive dashboard view

www.keymanagerplus.com

4141 Hacienda Drive Pleasanton,
CA 94588, USA
US +1 888 204 3539
UK : +44 (20) 35647890
Australia : +61 2 80662898
www.keymanagerplus.com

ManageEngine
Key Manager Plus