SECTIGO

A WHITE PAPER FROM SECTIGO

The Value of Automatic SSL Certificate Installation

Introduction

The installation of SSL certificates is labor intensive, requires scarce skills, and poses a risk to the enterprise. What may be perceived as a day to day task that is expected of a web administrator, these costly and risky steps should be automated. This document outlines the value of automating SSL certificate installation and renewal.

Installing SSL Certificates Manually Requires Work

The following steps will be done by a web admin or equivalent with a technical skillset. A minimal SSL Certificate installation (single webserver and domain instance) requires the web admin to do the following steps at a cost of $50 to $100 per web server.

Work	Description
Selection/Purchase of SSL Certificates	Minutes to Hours – Read
SSH Login to the web server	< 2 Minutes – lookup of server address & credentials
Enter a set of commands to achieve domain validation (for new domains)	Minutes to Hours – Read documentation, type appropriate commands. Web admin forums are filled with Q&A and troubleshooting, suggesting that many have problems with this step
Request issuance of the certificate and download	Up to 5 to 10 Minutes – Read documentation, type appropriate commands.
Copy the certificate files to the appropriate server file location (varies based on web server)	< 2 Minutes – lookup of server file location, type appropriate commands.
Modify the web server configuration file to enable the web server to utilize the SSL certificate and publish https	Minutes to Hours - Read documentation, type appropriate commands, save file. Web admin forums are filled with Q&A and troubleshooting, suggesting that many have problems with this step
Refresh/Restart the web server in order to recognize the new configuration	< 1 Minute
Configuration of certificate renewal mechanism (e.g., cron job / scripting)	5 to 10 Minutes - Read documentation, type appropriate commands.
Test	Minutes to Hours – If no error messages then testing will be quick. Responding to error messages will require re-modifying the web server configuration file.

The work described in the previous chart multiplies if the web server utilizes any of the following:

- Multiple Domains or Wildcard, which requires propagation of the private key to all servers
- Multiple Instances per Web Server
- Reverse Proxy
- Load Balancer(s)

All of the above steps need to be done precisely, otherwise the risk of downtime (at worst) or wasted human time (at least) could result. Mistakes by human error are very easily made.

Skillsets Required to Perform Manual SSL Certificate Installation

In order to perform the steps described in the previous section, a web administrator needs to have adequate knowledge of the Linux shell environment, or the Windows equivalent (Powershell / IIS). An administrator experienced with Linux shell will still need to spend time reading documentation to learn the commands. A web administrator who is more skilled with html coding and web site building and less experienced in Linux shell may have significant difficulty performing the necessary steps, and/or spend a great deal of time teaching themselves what is necessary.

Risks Associated with Manual SSL Certificate Installation are as follows:

- **Misconfiguration**
  - Downtime and Time spent troubleshooting
  - Introduction of security flaws
- **Lack of visibility to installed certificates**
  - Certificate expiry leading to unexpected downtime

Solution

Sectigo provides a certificate management solution which uses the industry standard ACME protocol between the Certification Authority and Web Server or Load Balancer to fully automate the process of key generation, domain control validation, and certificate creation/install in the server. The 3rd party ACME client is sometimes built into the Web Server, or is a sperate client co-located with the server to reach out to the CA for certificates. The web admin username and password does not need to be configured into the ACME client.

In addition, Sectigo developed a proprietary automated method which is designed to handle the duplication of the private key to servers sharing the same key for wild card or multi-domain certs.

The Sectigo certificate management system will notify the administrator if for some reason the automated system failed to update the certificate in a timely fashion, or automation was not configured for the specific certificate. As well, the certificates could be updated prior to expiry to improve cryptography, or naming within the certificate. This is true for SSL and non-SSL private CA certificates, all from the same pane of glass.

The Sectigo certificate management system will notify the administrator if for some reason the automated system failed to update the certificate in a timely fashion, or automation was not configured for the specific certificate.

Contact a Sectigo website security specialist to find out how EV SSL can help your business.

SECTIGO

sales@sectigo.com

