The Top 5 Challenges You'll Face as an SSL Manager

With the ever-growing number of connected devices, online portals, and internal networks that enterprises manage, the number of use cases for digital certificates to secure information communicated between devices and users is rapidly increasing. It is not unusual for enterprises to have thousands (even millions) of SSL certificates in use.

Certificates provide essential security and trust for organizations of any scale, but they do not come maintenance-free. Tracking and renewing expiring certificates, dealing with potential vulnerabilities, and managing all stages of a certificate's lifecycle can be extremely complicated, resulting in costly consequences if not done properly. Fortunately, you're not alone in the daunting task of SSL management, and since DigiCert understands the complications involved, we've drawn out some answers to a few of the most common problems SSL IT professionals deal with daily.

1. Keeping up with Vulnerabilities

SSL certificates can be vulnerable for various reasons—they could have missing fields, use internal names, be using an outdated hashing algorithm, or have weak cypher suites compromising SSL endpoints. Vulnerabilities are inevitable in any security landscape, and it can get overwhelming to keep track of everything. An SSL manager needs something that can stay on top of any new bugs and weaknesses that come up.

With Certificate Inspector, a tool in our certificate management platform CertCentral, you can easily scan for weaknesses in configuration. If one or more certificates is compromised by any vulnerability, Certificate Inspector will also provide remediation suggestions so you can maintain the highest level of network security.

2. Discovering all Certificates in Your Network

Manually gathering details about your certificates one by one to check that everything is in order is not practical for enterprises with thousands of certs. This is why companies often don't have a good handle on how many certificates they have, where they are installed, or if they are still functioning correctly. However, with an automated tool for certificate discovery, you can easily know about all the certificates in your network.

DigiCert Certificate Inspector not only finds vulnerabilities, it tracks and discovers all certificates issued for your domain by any CA. After running a scan, Certificate Inspector inputs all certificate details into a dashboard where you can view your entire certificate landscape, as well as any issues it may have.

3. Managing Certificate Expirations

Effectively monitoring certificate expiration dates is another key difficulty in managing SSL certificates. We often see IT security professionals working off excel spreadsheets to track their certificate expirations, and it is very easy to make mistakes and miss renewal this way. Because of this, DigiCert aims to make continuous monitoring and oversight easier with CertCentral, where you will receive notifications when a certificate is going to expire and how you can renew it.

4. Determining Certificate Access

Once you have a handle on tracking everything, how do you know who in your company is authorized to approve and issue a certificate? Instead of wondering if your CSR applicant should also approve the certificate or which admin should be renewing all your client certificates, DigiCert has implemented enhanced access control functionalities in CertCentral. Be it user management, divisions, whitelists, product settings, and custom order fields, we have you covered so you can decide exactly who can request a certificate, who can order a certificate, who can approve a certificate, and more.

5. Utilizing Private SSL Certificates

Enterprises often need both public and private certificates to secure all their data in transit. To issue private certificates, you need a private PKI solution. Many companies are managing their own home-grown internal CA to provide private certificates without the proper management tools that allow for seamless revocation or reissuance.

However, with our hosted Private PKI solution, you can issue private certificates without any maintenance hassle—we host your dedicated intermediate, help you customize your certificate profiles, provide revocation mechanisms, and ensure your security is tailored to your needs. Our private PKI is integrated with CertCentral, so you can manage your private and public certificates from a single interface, which will save you time, effort, and cost.

Want to talk more about how CertCentral can make your SSL management simpler? Call 1.855.800.3444 or contact sales@digicert.com for further information.

digicert®