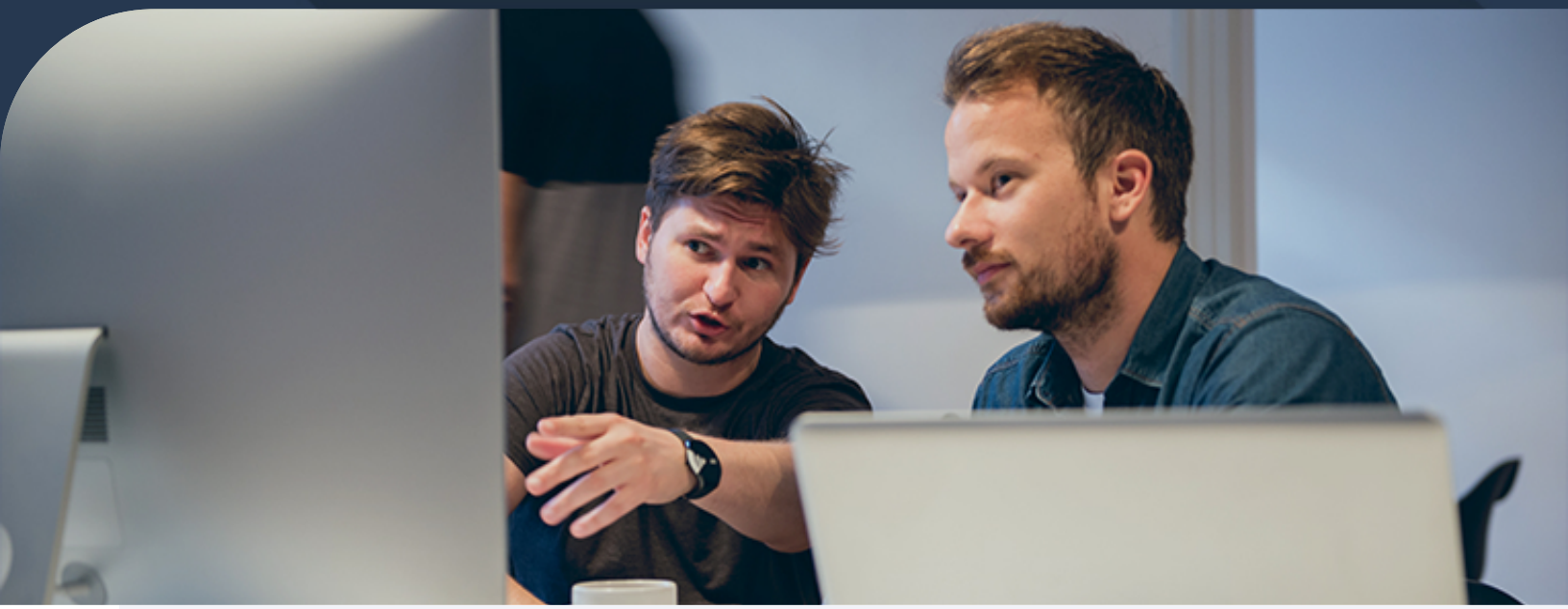
SEVEN BEST-PRACTICES FOR SSL MANAGERS



The growth of a corporation often comes with the need for issuing more digital certificates to encrypt all the new websites, cloud infrastructure, mobile connections, and IoT devices.

Digital certificates, commonly referred to as SSL or TLS, have reached the point that they have become a necessary part of doing business. In fact, not having a digital certificate management system in place can lead to catastrophic consequences such as, expensive outages and downtime, regulatory penalties, or worse yet — critical data breaches.

Despite the ubiquitousness of digital certificates, many business owners and IT managers have found themselves in need of better guidance around how to manage the certificates effectively and efficiently.

A recent survey conducted by Digicert, one of the premier Certificate Authorities, identified the top five challenges corporations face when dealing with SSL certificates to be the following:

1. Discovering all certificates in your network
2. Managing certificate expirations
3. Determining certificate access
4. Keeping up with vulnerabilities
5. Utilizing private SSL certificates

To address these challenges and reduce risk, we have assembled a list of seven best practices for your corporation's digital certificate manager to implement. Let's begin!

1. Create a Certificate Management Operations Policy

If your corporation already has a certificate management policy in place, congrats as you are a step ahead of the game! If not, today is a great day to begin putting one together. To help you get started, here is an outline of what a robust certificate management operations policy should address:

- Specify each of the ways you use digital certificates in your organization
- Who are the individuals and/or roles involved in certificate management
- What permissions each individual or role has/needs
- Your primary and backup Certificate Authorities (CAs)
- The specific certificates used for each use case, including:
  - Validation level (DV, OV or EV)
  - Public/private
  - Device/internet-of-things
  - Email and code signing
- Certificate coverage (i.e. single name) - we recommend minimizing the use of multi-domain and wildcard certificates where possible as they expand the scope of risk across multiple sites

2. Centralize Your Certificate Management

When it comes to your certificate management, there are multiple aspects to making sure it is centralized.

Centralize Purchasing — Streamlining which type of certificates your organization uses and where you purchase them from will make management much simpler as well as ease your accounting and PO (purchase order) management.

With your priary and backup CAs established (see Best Practice #1), you should look for a vending partner whose portfolio includes both your primary and secondary. Webnames actually offers both Digicert and Sectigo, the two most trusted CAs in the industry.

Centralize Visibility — By consolidating the purchasing options, you can more easily manage your certificates through a single dashboard which will give you a top level view to track your certificates across the network.

For your public digital certificates, Webnames provides customers with a dashboard to manage the full lifecycle of a certificates (enrollment, configuration status, renewal and more).

When it comes to private certificates, many companies choose to utilize a separate management system—including even spreadsheets. While spreadsheets may be free, it is always important to recognize the cost and risks of manual management especially as your certificate inventory grows.

3. Scan Your Network Weekly for Unknown Certificates

Until your corporation has an airtight strategy for how you acquire and issue new certificates, it's a good practice to scan your network weekly for any new certificates. With different departments in a corporation who might not yet be abiding by your new Certificate Management Operations Policy, it's not uncommon for rogue or shadow certificates to be issued within an organization.

There are numerous tools available to scan your network, such as Google's Certificate transparency logs. While it can be a bit of a manual process, you can get a quick – albeit limited - understanding of how many certificates you have to manage. While these tools cannot show whether an SSL certificate has been installed correctly or provide a full-picture of the properties under a Wildcard SSL certificate for example, they can be helpful in a more limited scope. The ultimate scanning solution would come in the form of an Enterprise Certificate Management dashboard that integrates your entire network.

4. Set and Manage Granular Permissions

As your Certificate Management Operations Policy takes precedence in your corporation, you'll be able to assign permissions for users, giving them only the permissions they need.

For security compliance, you may already have a segregation of duties policy for your finance, dev-ops, and IT departments—if not for your entire company. This policy should also include the use of digital certificates. As should have been discovered from Best Practice #1, you will want to recognize which departments and staff utilize certifications and for what purpose. Then you will want to decide who should have what permissions (e.g. request, approve, procure, reissue, install, and revoke). Employing the permission settings will be dependent on the sophistication of your certificate management tool.

5. Create Approval and Escalation Workflows

As you limit employee permissions, any requests for issuance, renewal and revocation will need to be routed to the right parties. To ensure there's no bottlenecking – should an employee be absent or leave the company – there needs to be an escalation path, too. This is especially critical for renewals, to ensure there's no margin for downtime due to an expired certificate.

6. Use OV or EV SSL Certificates

Organization Validation (OV) and Extended Validation (EV) certificates give you greater control over who can issue certificates for your properties and make it easier to get full visibility into all the certificates being issued. Frankly, it's just more professional. Some may argue for free Domain Validation (DV) SSL certificates, after all – they're free. But so is email, yet you wouldn't use Gmail addresses for your company's communication. OV and EV certificates build trust, offer better authentication and show customers you did more than just the bare minimum for connection security.

7. Set Up the Right Notifications

It's good practice to have two parties notified for the major milestones of every certificate. These include renewals, revocations, reissuances, etc. With two contacts in place, the risk of notifications being missed or ignored is reduced. In this regard, it's important that these contact emails be email accounts that are regularly checked and that have someone specifically responsible for them.

With Webnames, notifications are sent to the account owner, in addition to either the technical, admin, or billing contact, as specified by the account owner. An additional party can also be CC'd on the emails for another layer of accountability. In addition to the three email notifications sent a 1-month, 2-weeks and 1-week ahead of expiry, hardcopy renewal letters are sent, in addition to a personal phone call 3-days ahead of expiry.

Did you know you can renew up to 60 days before expiration and roll over any left-over time to the new certificate?

Even if you've automated the process, make sure you are tracking the timeline and the progress of your SSL renewals. If you're renewing 30 days before expiration, use the 15-day notification as a check-in point to make sure the process in underway and/or scheduled, and 7-day mark to ensure it's complete.

Conclusion

As the velocity of domains, apps, devices and certificate usage continues to ramp up — businesses will need to find better, more scalable way to manage it all and more resources appointed. This can be achieved in a few different ways.

At Webnames, all corporate clients can leverage our team of SSL experts to monitor and manage their renewals, reissuances and new configurations, so nothing is missed. We can also help to uncover their broader SSL footprint, providing a better understanding of how many SSL certificates have been issued in their name and what they are - all critical components to developing a strong certificate management policy.

Additionally, automated solutions can also be leveraged by corporations with hundreds-to-thousands of SSL certificates. With the right tools and integrations, the certificate lifecycle process can be automated for all major environments (e.g. Windows, Linux, F5, ACME, Active Directory, Azure, Cisco, AWS, Kubernete, etc.), and be used for discovery/research, risk mitigation, issuance, installation, renewals and more. According to Gartner Research, where large SSL portfolios are concerned, it's been estimated that "certificate management platforms with automation capabilities can reduce management time by up to 60%".

Every corporation managing certificates manually must determine the appropriate time to transition to enterprise certificate management tools. Until that point, it benefits corporations to have trusted external experts, in addition to in-house staff, to turn for full-service SSL support, troubleshooting and management. For those who are ready to explore automation platforms, Webnames can help provide you with an industry-leading solution.