digicert®

Certificate Management: The Ultimate Guide

Best practices for SSL/TLS admins managing 100s or 1000s of Certs

GUIDE

Table of Contents

Introduction	3
Take Control of Your PKI Management	3
Use a PKI Management Platform	3
Start Automating via API	4
Expose Those Neglected Certificates	5
Organize Your Team	5
Execute Timely Approvals	6
Use Notifications to Your Advantage	6
Monitor Your Network & Generate Reports	6
Use a Vulnerability Scanning Tool	7
Choose a Platform that Does It All	7

Introduction

In a certificate management role, you can't let a single certificate fall through the cracks. Forgotten or expired certificates are costly and damaging. On average, it costs large organizations $15 million per certificate outage.[1] Plus, there are repercussions for security and brand reputation, including a decline in customer trust and sales.

You're likely responsible for several of the moving parts involved in maintaining a Public Key Infrastructure (PKI): managing certificates, keeping up on best practices for SSL, and timely approvals, just to name a few.

One of biggest pain points of this role is the constant concern that there is a cert somewhere in your network that wasn't returned with scan results; one day a server is going to go down and there will be a mess to clean up.

Wouldn't it be nice if you could use some giant checklist for certificate management? Just some way to know you are focused on the most important parts of the certificate lifecycle–the ones that are essential to your network security.

One checklist won't work for every organization because network complexities vary. However, there are some things every certificate manager needs to take care of, so they can know their data, company, and employees are protected.

This guide will include everything you should be thinking about for thorough certificate management. It will help you take control of all the areas of the certificate lifecycle, while leveraging APIs and optimizing your team.

Take control of your PKI management by following best practices

Juggling the components of a PKI, like Certificate Authority (CA), Registration Authority (RA), certificate policies, and certificate management system can be stressful. Certificates can be easy to deploy but they must be deployed and managed correctly to ensure security.

SSL admins at large organizations are managing thousands (if not millions) of certificates. How do you make sure certificates are deployed and managed the right way day after day, week after week?

Maintaining control is the challenge and best practices are the solution. These best practices will increase oversight, save time, and make your life easier.

Follow them, and you won't have to think about certificates around-the-clock. Instead, you'll have the peace of mind that comes with a secure network.

Best practice: Use a PKI management platform

Managed PKI (MPKI) solutions give organizations the power to order and manage certificates without the costs of maintaining an in-house Certificate Authority (CA). Many publicly trusted CAs offer a Managed PKI solution and the majority of large organizations choose this option because of cost-effectiveness, among other reasons.

With an MPKI solution, you offload the work of maintaining a large part of a PKI to a CA, but you still get the benefit of using certificates for security. Better yet, an MPKI platform should simplify all aspects of certificate lifecycle management, namely issuance, installation, inspection, remediation, and renewal.

[1] "2015 Cost of Failed Trust Report: When Trust Online Breaks, Businesses Lose Customers." Accesses 26 June 2017. https://www.venafi.com/assets/pdf/wp/Ponemon-When-Trust-Online-Breaks-Businesses-Lose-Customers-white-paper.pdf

Overall, MPKI saves you time, so keeping track of important certificate details is more approachable:

- Expiration dates
- SSL endpoint errors
- Certificate requests from team members
- Revocation status
- Issuing CA

Up until a few years ago, many companies managed certificates manually with spreadsheets. TechTarget says, and you might know from firsthand experience, that "this can lead to mistakes, such as lost, mismatched, or mislabeled certificates."[2]

An MPKI platform eliminates the need to track certificate details in a spreadsheet and juggle requests through email, essentially automating these factors and reducing the chance of human error. It makes certificate management easier and less time-consuming.

Best practice: Start automating via API

APIs break down barriers between companies, empowering developers to use various technologies to build apps. More specifically, an API can lighten the load for IT teams who need to automate and customize certificate management functions.

An MPKI platform simplifies certificate lifecycle management

While smaller companies may find the GUI in an SSL management tool completely satisfactory, large enterprises need customization. Some PKI management tools will give you access to an API, which you can use to customize features and workflows, and automate processes to implement a more hands-off style of certificate management. When using an API, you can make SSL management truly personalized.

You could oversee thousands if not millions of devices, depending on your industry. Leveraging automation will make your life easier, and allow you to maintain security by reducing human error and certificate-caused outages.

You can save time and automate many processes in the SSL certificate lifecycle using an API, such as:

> Changing industry standards and shrinking certificate validity periods mean automation won't be an option in the future of SSL—it'll be a necessity.

- Requesting certificates
- Approving requests
- Rejecting requests
- Downloading certificates
- Renewing certificates
- Revoking certificates
- Reissuing certificates

Using an API reduces complexities that come with managing certificates from different issuing CAs. You can have more control over certificate renewals by taking the requester out of the process. If renewals are automated when a certificate comes within 90, 60, or 30 days of expiration, you won't need to worry about whether or not a team member will order from your preferred vendor—the decision is already made.

APIs are the best way to save time by automating and customizing your certificate management.

[2]Shapland, R. "SSL certificate management: Avoiding costly mistakes." Accessed 26 June 2017. http://searchsecurity.techtarget.com/tip/SSL-certificate-management-Common-mistakes-and-how-to-avoid-them

Best practice: Expose those neglected certificates

Certificate managers all have concerns about finding rogue and unknown certificates. This happens because of scaling certificate landscapes, multiple individuals ordering and installing certificates, and the standard employee turnover rate in a large enterprise. The problem is you can't manage a certificate if you don't know it exists.

By using an inspection tool for certificate discovery, you will gain a broad overview of your certificate landscape and be able to dig deeper when you need to see granular certificate details. Many CAs offer an inspection tool or agent that discovers certificates and aggregates information from each scan. Ideally, the tool will find all certificates used on your network, regardless of issuing CA, so you know about all certs deployed. Discovery tools help you avoid mistakes in manual tracking and save you time on inventory.

Running regular scans (we recommend at least once a week) ensures you have a full view of all the certificates in use and gives you more insight into possible weaknesses, including finding rogue certs that may be putting your brand at risk. Once you find forgotten or neglected certificates, you can act to remediate weaknesses.

Best practice: Organize your team

A fundamental part of certificate management is managing the individuals involved with your PKI.

You want to have the right key players, segment them by department or team, assign each person the right level of access, ensure he/she knows what they are responsible for, and keep each individual up-to-date on the processes you have in place.

Divide your business

Managing certificate requests from across the country or across the world becomes a much more manageable task when you divide (organize) individuals into departments, divisions, or units. Regardless of what option you choose, it allows you to segment requests based on location, IP address, internal team, or another classification.

These small details help when you have incoming requests with incomplete information—you'll know who to go to retrieve the rest of the information. It also helps track down the right person when there is an expired certificate.

Assign user roles

Assigning user roles to each member of your team is crucial to maintaining control of your PKI. If each person has the correct level of access to your management platform, you'll enjoy a less stressful renewal process and more streamlined tracking.

Evaluate each person, where they become part of the process, and what role they play. Whether they are a regular user or should be an admin to approve requests, assigning each person with a role within your certificate management platform gives each person the right capabilities. When users are given the power to make requests on their own, it frees up more of your time by not needing to do tasks that could be accomplished by another capable team member.

There may be times when a one-time user needs to make a request. Manage their access by giving them guest access, which will only give them temporary and limited admittance. This further safeguards your certificates by only giving information on a need-to-know basis.

Educate your team

Keeping your team up-to-date on your processes and educating them about new technology or implementations is a continuous process.

Your system admins and developers need a technical knowledge of how to maintain and deploy certificates. They're allies and you should consult with them for input about all these components when appropriate.

They also need to be kept in-the-loop about changes to requirements or policies. You can stay informed about industry trends and changing standards by following the CA/Browser Forum as well as your preferred SSL provider's blog.

Best practice: Execute timely approvals

Streamlined and fast approvals are critical for high-volume issuance and are another important part of maintaining control of your PKI. Assuming you work with a CA with quick validation times, the only typical hold up in the issuance process falls on a certificate administrator, who has to approve the request.

Once you have organized your users and departments, verification emails should be sent to the appropriate admin(s) for approval to accelerate issuance. The segments you have in place speed up the approval process because all the admin will have to do is verify the accuracy of information and then approve. This saves you time not needing to hunt down anyone to get answers and avoids prolonging deployment.

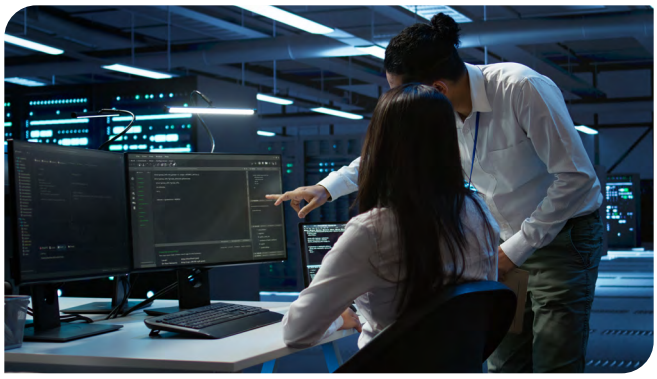
Best practice: Use notifications to your advantage

The absence of notifications is a common problem for SSL managers and often affects security when it's time to renew a certificate. You should be notified—at the very least—about certificate expiration; but notifications can also be helpful in other parts of the certificate lifecycle, like when there are pending cert requests, recent revocations, or when certs need to be reissued.

Managing certs in spreadsheets doesn't scale and there's no notification process. Some managers set calendar reminders in Outlook to remind them when it's time to renew, but this has several downsides, like the creator of the event forgetting to set a reminder or leaving the company without passing on the info, or some other malfunction. Spreadsheets are not 100% reliable.

When a certificate is up for renewal and the owner has not renewed within the set timeframe, you'll need to immediately know who the owner is, whether the cert is being used, and which server it is being installed on. The sooner the notification, the sooner you can follow-up.

Establish an escalation path for specific, potential certificate issues. For example, you should be notified directly if a certificate will expire within the next 7 days. Escalation at the right time brings awareness before it's too late. Setting these types of checks will help you avoid outages caused by expiring certificates.



Best practice: Monitor your network & generate reports

Lack of visibility into your network results in more worry for you. An MPKI platform may have the capability to pull certificate information from your network scans into a comprehensive dashboard view. Use the dashboard for more thorough inspection.

A dashboard view gives you quick insights into your certificate network. Just from a glance, you can assess your overall network health. You can also see upcoming certificate expirations, vulnerable certificate endpoints, and pending certificate requests from other team members. These are just a few examples of the insights gained from using a dashboard to monitor your network.

Monitoring your network this way, with continual discovery and reviewing reports on findings, might be the most important part of helping you gain visibility. Discovery and reporting are two components that work together to give you the most insight and control of your certificate landscape.

Use these tips for exceptional monitoring:

- Deploy an agent to scan your network and generate a report at least once every 30 days
- Automate scans with a script if possible
- Remediate vulnerable endpoints after each and every scan
- Approve cert requests as soon as possible
- Opt-in for auto renewals to avoid outages

Closely watching your certificate landscape from a bird's-eye view as well as scrutinizing specific details is are parts of the ongoing inspection step in the certificate lifecycle.

Best practice: Use a Vulnerability Scanning Tool

A new vulnerability can come onto the scene at any time, making remediation a time-sensitive aspect of certificate lifecycle management.

According to a 2017 report by Bay Dynamics, 74% of security teams feel overwhelmed by vulnerability maintenance work at very large enterprises. In fact, at any given time you could be managing more than one million vulnerabilities across your systems.

"Ensuring all vulnerabilities are appropriately managed and mitigated causes a significant amount of pressure."[3]

Some of these vulnerabilities may be lurking in your SSL network right now. A certificate isn't enough to protect an SSL service if you are using outdated ciphers or vulnerable versions of SSL/TLS. You can reduce the stress of managing vulnerabilities for SSL endpoints when you choose to use tool that scans your network, searches for vulnerabilities, and delivers information about weaknesses.

These tools are most helpful when they identify specific vulnerabilities and match them to the affected endpoints, so you can remediate quickly and without confusion.

Best practice: Choose a platform that does it all

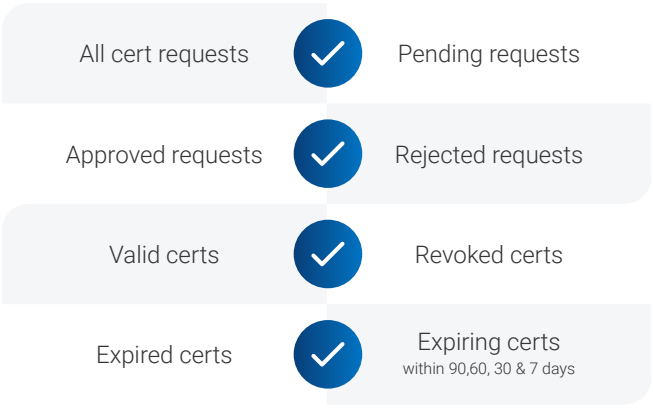
Make things easier for yourself and choose a certificate management platform that allows you to:

- Use an MPKI solution
- View a comprehensive dashboard
- Automate via API
- Discover certs
- Segment and assign user roles
- Set up notifications and escalation paths
- Scan for vulnerabilities

The platform is the key to maintaining control of your PKI and managing the certificate lifecycle including issuance, installation, inspection, remediation, and renewal.

The CertCentral® platform from DigiCert is an enterprise-grade certificate management software suite designed to simplify management, customize workflows, and automate issuance.

You should monitor all parts of your networks. For certificates, you should generate reports for:



Through the DigiCert Services API, SSL managers can automate virtually any desired process. The API integrates with third-party applications and can be branded to fit in with your other tools.

Using an all-in-one platform to help you monitor, manage, discover, and scan for vulnerabilities eliminates the worries associated with not knowing what's going on in your network. It increases visibility. Organizing your team members, assigning roles, and segmenting when necessary expands control.

CertCentral will be your most valuable asset for ensuring no certificates fall through the cracks.

Want to learn more about CertCentral® or our API? Contact sales at 1.855.800.3444 or email sales@digicert.com.

[3]Monahan, D. "A Day in the Life of a Cyber Security Pro." Accessed 26 June 2017. https:// baydynamics.com/content/uploads/2017/05/4-19-17-FINAL-EMA-A-Day-in-the-Life-of-a- Security-Pro.pdf