Certificate Management

BEST PRACTICES CHECKLIST

14 best practices to
avoid downtime, protect your brand,
maintain compliance, and
avoid data breaches.

SECTIGO
FORMERLY COMODO CA

Store
AUTHORIZED
PLATINUM PARTNER

Certificate Management Checklist

14 best practices to avoid downtime, protect your brand, maintain compliance, and avoid data breaches.

Yahoo, Equifax, Home Depot, LinkedIn, Ericsson—Nearly every week, yet another well-known brand makes headlines-for all the wrong reasons: hackers gained access to customer data, a certificate-error caused their website to go down, or investigators fined them for compliance violations. This checklist will help you implement certificate management best practices to avoid similar problems for your company.

Whether it's SSL/TLS, S/MIME, Code Signing, Client, Device or IoT – certificates are the foundation of the trust that makes business work in the digital age. Mismanaging certificates can lead to catastrophic consequences:

Expensive Outages & Downtime

When certificates expire, websites break, applications go down, and business comes lurching to a halt. And not just your business. Anyone relying on your organization will experience outages and downtime, too. For example, Ericsson had a certificate expiration in 2018 that cut cellular service for 32-million people – for just a few hours.

Angry Customers & Partners

In business, on- or offline, trust is currency. Your customers, your partners – they trust you to be open, easily identified, with your services available. When that doesn't happen, your brand and reputation can suffer long-lasting damage. Over a year after the Ericsson incident, their customers are still angry. In fact, one of their partners was reported to be receiving up to £100 million from Ericsson as compensation for the downtime.

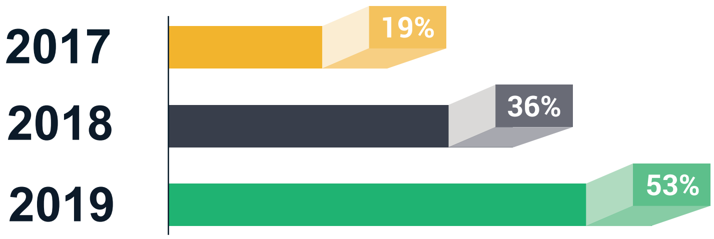
Regulatory Penalties & Non-Compliance Fines

Encryption and authentication are critical components of just about every compliance and regulatory framework. That means digital certificates are, too. A Ponemon Institute study found that certificate mismanagement costs the average enterprise just over $7.2 million per year due to failed audits and regulatory penalties.

Critical Data Breaches

Certificate expiration is far more treacherous than just an HTTP browser warning. It can open the doors for far greater attacks. The Equifax data breach wasn't detected for 76 days because an expired certificate knocked out traffic inspection. Two years later the credit bureau is still reeling, with costs at $1.4 billion and still rising!

Adoption of SSL/HTTPS



Visualizing 82,833 Certificates

If each certificate took one seat, **that's enough to fill up Wembley Stadium,** one of the largest sports stadiums in the world.

Companies Are Managing More Certificates Than Ever

Digital certificate usage has skyrocketed dramatically from what it was just half a decade ago, and it's only going to get worse. According to a study by the Ponemon Institute, the average Enterprise is now managing an average of 82,833 certificates and keys (and 71% of organizations don't even know how many certificates they have).

That's why it's so important for companies to get on top of their certificate management needs now. To get you started, we've compiled this list—14 actionable pieces of advice that can transform your certificate management from an unruly burden to a finely tuned machine.

14 Certificate Management Best Practices

1 Start by Creating a Certificate Management Operations Policy

Set parameters. Figure out who is authorized to do what, what you want deployed and how things should escalate. The fewer cooks in the kitchen, the better. Keep it simple though, a one-pager should work. Make sure to cover:

- ✓ Each of the ways you use digital certificates in your organization
- ✓ The individuals and/or roles involved in certificate management
- ✓ The permissions each individual or role has
- ✓ Your primary and backup CAs (using 1-2 CAs makes management simpler; we recommend enforcing your a choice with CAA record)
- ✓ The specific certificates used for each use case, including:
  - ✓ Validation level
  - ✓ Certificate coverage – we recommend using single name certificates to minimize risk

2 Centralize Your Certificate Management

Unless you're a high-maturity security organization with adequate technical sophistication, spinning up your own management solution is going to invite a lot of unwanted problems. It's the #1 cause of certificate management mistakes. And by not having the right solution, you'll fail to prevent the #2 cause of problems – shadow certificates. We recommend a cloud-based certificate management platform that gives you full visibility and control of all types of X.509 certificates in a single dashboard.

3 Scan Your Network Weekly for Unknown Certificates

Shadow certificates, which are digital certificates acquired outside of your standard procedures, cause countless unplanned expirations and cost millions of dollars each year. Fortunately, shadow certificates are easily preventable:

- ✓ Run a discovery scan internally and externally at least once a week to ensure shadow certificates don't escape your oversight.
- ✓ Monitor CT logs for your domains, either via API or email notifications.
- ✓ When you find a shadow certificate, talk with the requester to educate them on the procedures they should use in the future.

You're going to find shadow certificates eventually. Scanning ensures you don't find them too late.

4 Set and Manage Granular Permissions

The principle of least privilege applies to certificate management, too! Assign permissions for users (request, approve, and revoke), giving them only the permissions they need. This is where the Operations Policy you created in step one comes in handy. Everything should already be documented there. You can assign highly granular permissions (by user, role, department, company, branch, etc.) very easily from within your certificate management platform.

5 Create Approval and Escalation Workflows

Because you're limiting employee permissions, 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. Start with the lowest-level employee with permissions to fulfill the request and escalate over the next few hours, days or weeks to ensure that things are dealt with in a timely manner. This is especially critical for renewals, to ensure there's no margin for downtime due to an expired certificate.

6 Issue all Certificates From a Fully Managed PKI / Avoid Self-Signed Certificates

For most organizations, the simplest, most secure option is to always use certificates issued by a publicly-trusted certificate authority, even within your private network. This gives you maximum visibility and control (including revocation) over all certificates, while minimizing management workload. If your company has a use case that requires issuing your own certificates (for example, a non-existent domain) be sure that you're issuing certificates from a fully-managed private CA complete with certificate logging, certificate revocation list (CRL), issuance policies, issuance auditing, and vulnerability testing.

7 Use OV or EV SSL Certificates

OV and 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. It's also just more professional. Some may argue for free 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.

8 Streamline Validation to Issue All certificates Instantly

Everyone knows you can automate DV issuance. Did you know you can automate business authentication, too? Whether you want to automate Organization or Extended Validation, the right certificate management solution lets you validate with your CA(s) of choice one time, then skip doing it again for the next 12 months. When you don't have to wait 2-3 days for validation, certificate issuance becomes instant!

9 Automate the Entire Issuance Process

Being able to get the certificate validated instantly is great, but what about the rest of the process –generating key pairs, creating and submitting the CSR, waiting for the certificate to be emailed to you, and collecting it for installation? Save time by automating those processes via a pre-built server agent, API, Active Directory integration, the ACME protocol, and/or key management tools.

10 Automate Installation, Too

Again, leveraging an integration (API, server agent, Microsoft CA/Active Directory or the ACME protocol) can completely eliminate the burden of manually installing certificates. The specifics vary, but the concept is the same. A client/agent is installed on your server(s) and/or end point(s) and handles all aspects of installation and configuration for client and server certificates.

11 Automate All Renewals

Once again, regardless of what mechanism you're using to achieve Zero-Touch capabilities (API, Active Directory, ACME, etc.), you'll be able to automate the renewal cycle, too. Simply configure your management platform to renew (and even rotate keys) at set intervals and it takes care of everything else in the background.

12 Set Up the Right Notifications

At minimum, two parties should be notified for every certificate expiration at least 30-60 days in advance. Even though you've automated, you still need to know: this can act as a safeguard in case anything fails. If you're renewing 30 days before expiration, set a notification for 15 days before the expiration. If you get the notification, something went wrong and you still have two weeks to address it. You'll typically also need notifications for pending requests, revocations, reissuances, etc.

13 Generate and Review Reports

Compliance reporting is a headache for just about every organization nowadays, regardless of industry. The right certificate management platform can ease this burden, too. Be sure that you're regularly generating and reviewing comprehensive reports that include:

- ✓ Upcoming expirations
- ✓ Summarized data on all active certificates
- ✓ Revoked certificates
- ✓ Pending requests
- ✓ Newly discovered certificates
- ✓ Any found vulnerabilities

14 Scan for Vulnerabilities

Certificates and TLS implementations can have vulnerabilities, too. That's why a critical part of certificate management is vulnerability scanning. There are a variety of certificate-related vulnerabilities that enterprise security teams need to stay on top of, such as SHA-1 hashing algorithm, 1024-bit key size, and outdated protocols like SSLv3. Schedule regular vulnerability scans and ensure notifications are sent to at least two parties for issues identified.

How To Make Certificate Management Completely Painless

Having the right certificate management platform and knowing how to leverage it properly makes your certificate management easier, faster, and more accurate. And we're here to help. We've been implementing the best certificate management solutions (at the best prices) for enterprises and companies of all sizes for over a decade. We can help you, too.

- ✓ Audit your certificate usage and identify your organization's needs.
- ✓ Assess best-in-class solutions that have the capabilities you need.
- ✓ Identify the solution that best fits your needs and budget.
- ✓ Create a discount package customized with your chosen solution.
- ✓ Implement the certificate management solution across your organization.

Like we said at the top: we'll help you implement a certificate management system that makes your job easier while improving your company's security posture, reducing risk, and improving efficiency.

Get started with a free consultation with one of our PKI experts.

Schedule A Free Consultation

Get Started Today!
Call +1 (888) 481-5388 or email sales@SectigoStore.com

SECTIGO FORMERLY COMODO CA | Store AUTHORIZED PLATINUM PARTNER

146 2nd St. N. #201, St. Petersburg, FL 33701 US

V 1.0 | SEPT 2020