digicert®

# THE TLS CERTIFICATE MANAGEMENT BEST PRACTICES CHECKLIST

In the last year, 60% of organizations suffered a certificate related outage that impacted their critical business applications[1]. These outages are now costing large corporations an average of $5,600 per minute[2], damaging reputation and growth rates.

It's more important than ever to set up and maintain the uncompromising standards that will help you manage your organization's digital certificates.

That's why we put together these guidelines: by breaking down the industry best practices into these necessary steps, you can keep your business safe from the damaging outages that result from lack of knowledge or poor coverage and control of your certificate lifecycles.

# IDENTIFY

## Get a baseline of all your certificates issued

Without a stringent inventory of your certificates, you open yourself up to security risks, so start in the right place by creating a list of all the issued certificates from your Certificate Authority (CA). Ensuring you've captured everything, from internal CAs to any network devices, can be challenging - using a network scanner to detect your TLS certificates is the easiest solution.

## Locate where all your certificates are installed

Knowing that you own an issued certificate is only part of the story — if a rogue certificate is installed, it can leak encrypted data without notifying you. Locate the verified server locations of all your certificates and plug them into your inventory.

## Name the owners of all your certificates and domains

Unexpected expiration is a big factor in the rise in certificate related outages, making it paramount to both identify who is buying your certificates and ensuring processes are in place to renew and transfer ownership should they leave.

## Identify the web server OS and application versions

Hackers can exploit certain weaknesses in operating systems, for example Heartbleed; a vulnerability in the OpenSSL cryptographic library that allows anyone on the internet to access your system. This makes it vital to include the details of your Operating Systems and apps in your inventories.

## Pinpoint the web server cipher suites and TLS versions

A cipher suite is a collection of algorithms that work with your TLS encryption to secure a network connection. Hackers tend to target outdated versions of TLS or insecure cipher suites, making it critical for your inventories to include which versions of each you're running.

[1] https://www.venafi.com/blog/majority-businesses-still-experience-outages-are-you-protecting-your-certificates

[2] https://www.venafi.com/blog/what-if-you-could-guarantee-eliminating-outages-your-organization

# REMEDIATE

- [ ] **Remove weak keys, cipher suites and hashes**

  Old hashing algorithms like MD5 or SHA-1 could still be on your internal websites and will need updating. The only recommended versions of TLS are TLS 1.2 and TLS 1.3 and ensure you are using modern ciphers such as AES.

- [ ] **Control wildcard certificate issuance and distribution**

  Although wildcard certificates can be attractive for their multiple sub-domains and ease of management, it's important to be aware that if its private keys are compromised, hackers can manipulate any system within that domain space — making revoking and reissuing complex and costly. However, if the strict conditions are met, wildcard certificates can be secure and flexible.

- [ ] **Deploy appropriate certificate types**

  When it comes to certificates, you need the right tool for the job. For internal systems, your private TLS certificates can be used, but for public sites you need either Organization Validation (OV) or Extended Validation (EV). Basic Domain Validation (DV) certificates are low-assurance and not recommended if you're transporting sensitive information

- [ ] **Control all default vendor certificates**

  Vendor certificates are not trusted by browsers because they're usually self-signed, expired, or operate with weak keys and were never intended for use on a production network. And yet, it's common for organizations to have thousands of them. Streamline the removal and replacement of vendor certificates using the latest automation tools on a cutting-edge certificate management platform.

- [ ] **Ensure all web services have latest patches installed**

  In order to protect your operating systems and web servers from the most malicious attacks as they develop, it's vital they're updated with the latest patches.

# PROTECT

- [ ] **Standardise and automate issuance and renewal process**

  By deploying automated and standardised protocols into your TLS procedure, including certificate issuance and renewals, you can remove user error and save time. This is made easy with a quality certificate management platform.

- [ ] **Install and renew all certificates in a timely manner**

  It's important to tailor your certificate renewals to the time constraints of your business. We recommend renewing at regular intervals and leaving a minimum of 15 days between renewing your certificates and the date they expire, but other businesses may need up to 90 days.

- [ ] **Ensure that private keys are not reused when certificates are renewed**

  Regardless of if you're using DV, OV or EV certificates, reusing private keys leaves you at risk of the keys being compromised. Always create a new key pair during the renewal process.

- [ ] **Install certificates and private keys in a secure manner**

  Create your private keys on a secure computer and ensure you're only distributing them through encrypted emails on a system in which they can be disposed of automatically.

- [ ] **Address certificate the decommissioning process**

  Ensure you have the appropriate processes in place that manage the removal and revocation of your certificates when your systems change hands, are decommissioned or reach their end-of-life.

# MONITOR

- [ ] **Scan networks for changes**

  Manually managing your certificates is becoming increasingly difficult — your networks are constantly changing and the sheer number of certificates owned by most businesses is rising rapidly. Using network scanning tools will highlight any issues as they arise, saving you time and keeping you protected.

- [ ] **Check Certificate Transparency (CT) logs for rogue certificates**

  Any of your public certificates that aren't logged will be flagged up as untrustworthy to your customers. Similar to a credit report, a CT monitor will detect any of these rogue certificates and remediate them before any damage is done to your data or reputation.

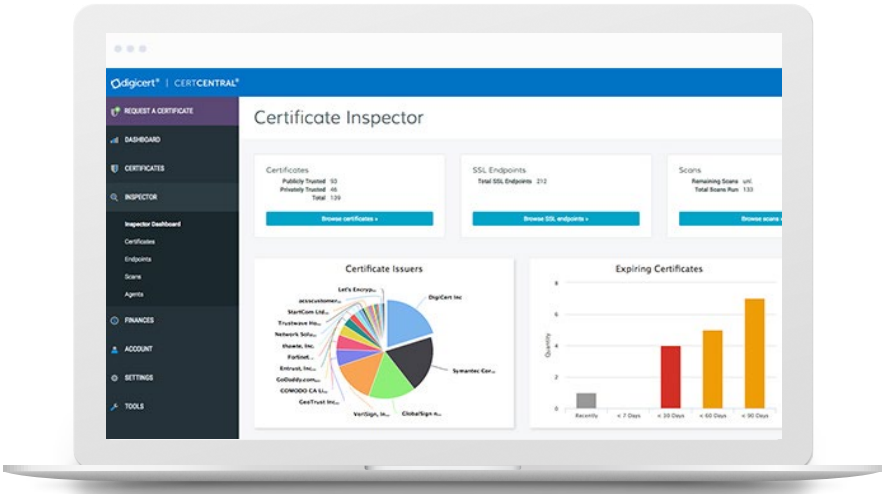
- [ ] **Use CAA to prevent unauthorized certificate requests**

  A Certificate Authority Authorization is a DNS record that dictates which CAs can issue certificates to you. By using a CAA, you control which CAs can issue certificates to your domains, meaning you can prevent requests from unauthorised and insecure CAs.

# CONCLUSION

Now you know what's required to keep your organization secure online, you can consider the most trusted solution:

## CertCentral by DigiCert




### Certificate management made easy

With DigiCert CertCentral®, you'll have all the tools and capabilities you need to identify, remediate, protect and monitor all your certificates, as well as customizing and automating your entire certificate ecosystem. Enabling you to:

- Scan your networks for new systems and changes
- Monitor CT logs for unauthorized certificates
- Use CAA to detect and prevent unauthorized certificate requests

All of this from a single screen.

### To learn more visit: digicert.com/certificate-management