

# Transitioning to a New Certificate Authority Isn't as Hard as You Think

## Table of Contents

- 1 Introduction
- 1 Myths about Transitioning to a New Certificate Authority
- 3 Effective Certificate Lifecycle Management
- 5 Cost
- 5 Security Implications of Transitioning CAs
- 6 Conclusion

## Introduction

You've just finished fixing some server configurations after a new OpenSSL vulnerability and you're thinking, "Why isn't my Certificate Authority (CA) making this easier?" You make a call to customer service to ask a quick question about a server license issue and you're looped into a phone queue and wait on hold for 14 minutes (Yes, you're counting). All of this leads you to start thinking about working with a new CA.

But can the daunting task of transitioning from one to another be done? Yes.

Does it have to be difficult? No.

SSL certificates are a critical part of keeping an enterprise protected from outside attacks, and if you are handling dozens, hundreds, or thousands, it can be a large undertaking—but it doesn't have to be if you are partnered with the right CA.

A CA can give you the right tools to make it easier to manage certificates and offer sage advice when you run into problems. A CA can also provide valuable systems and infrastructure that many companies can't afford to build on their own.

Contrary to popular belief, transitioning all your certificates so they are issued from one CA can make an IT security professional's job more convenient and actually alleviate burden. If you are thinking about transitioning your organization's certificates to be issued by one provider, you will want to consider what transitioning to a new CA would mean in terms of the following:

- Availability of certificate management tools
- Price of certificates
- Security risks associated with transitioning

Unfortunately, there are some myths in the security industry associated with the process of transitioning CAs, and these can slow—or even halt—the decision-making process.

This white paper will talk about all the things you should consider before transitioning to a new SSL provider. We will debunk the common myths, address the importance of certificate management tools and cost, and discuss the security risks related to making the move from one CA to another.

With some careful planning and a systematic approach, transitioning to a new CA or consolidating all your commercial certificates is easier than you think.

## Myths about Transitioning to a New Certificate Authority

We've outlined some of the common myths associated with making a transition from one CA to another (we've heard a lot through the years from customers), and want to clear some things up.

**Myth: By transitioning CAs, I will cause a service disruption to my certificates and systems.**

Transitioning CAs will not cause a disruption in service. Your current certificates and systems remain unaffected until you uninstall them. When you start the transition, you can request new certificates with your new provider for the same servers and domains, and replace the old certificates right away or as they expire.

---

## DID YOU KNOW?

You can have two certificates issued for the same domain and same server from different providers and it will cause no disruptions. This gives you time to install a new one and uninstall an older one without causing a lapse in security.

---

**Myth: If I switch to a new SSL provider, my existing certificates issued for `www.example.com` will be revoked.**

This is a common misconception. Just like in the previous example, you can have certificates from multiple providers issued for the same domain. Doing this does not create a problem nor cause one certificate to be revoked in favor of the other. Your old certificates issued from the previous provider will continue to be active until they expire or the new certificates from the new provider are installed in their place.

**Myth: Creating a new CSR on my servers and providing it to a new CA will cause downtime.**

When you have a certificate in place on your server and you create a new CSR on the same server, it does not affect the active certificate. The certificate will be unaffected until you install the new certificate. Additionally, even after installing the new certificate, it is still possible to revert back to the old certificate (or any other certificate) on the machine if the situation requires it.

**Myth: Transitioning to a new CA will cause problems because the certificates use a different root.**

DigiCert certificates are issued off of widely supported roots, which are ubiquitous with all modern browsers and devices.

Because of this, you don't need to install root certificates anywhere when installing our certificates for the first time—they will be trusted immediately and automatically.

**Myth: If I decide to transition to a new provider, I have to switch all my certificates at the same time.**

Nope. You are not obligated to replace all your certificates at a set time. If true, this would be very overwhelming. You can switch certificates one at a time as they get closer to their individual expiration dates if that is easiest for you.

---

## DID YOU KNOW?

If you want to switch all your certificates at the same time, DigiCert offers free replacements for certificates you currently have with different providers. (Replacement certificates expire on the same date as the certificates they replace.) We also offer credit in cases where you may have pre-purchased certificates with another provider.

---

It can't be this simple. There must be something you're forgetting—how can there be no downtime?

The whole process of getting a certificate—from requesting a CSR to obtaining the certificate to installing the certificate—causes no downtime. When you install a new certificate and uninstall the older one, the change from one to the other is instantaneous and invisible to anyone connecting to your server.

**Myth: If I transition to a new CA, it will be hard to keep track of all my new certificates.**

If you switch to a CA that has tools and a platform designed to simplify tracking and managing certificates, it won't be difficult to transition. For example, using Certificate Inspector, a free DigiCert tool, allows you to scan any machine (Windows/Mac/Linux) and finds all the certificates deployed in your environment. The tool lets you know where they are installed, the issuing CA, which domains are secured, and any vulnerabilities or weak configurations. (We discuss this tool later.)

Now that we've addressed common myths associated with transitioning to a new SSL provider, it's time to talk about other aspects that should play a role in your decision such as management tools, the cost of transitioning, and impact to security.

## Effective Certificate Lifecycle Management

Many of the myths associated with transitioning to a different CA are related to concerns about how to manage certificates. Understandably so, because lack of effective management results in weaker security—sometimes a complete lapse in security, which means loss of customer trust, and ultimately loss in revenue.

On average, businesses lose \$15 million per certificate outage, according to a Ponemon study in 2015. And in the same survey, nearly two-thirds of the respondents admitted to losing customers because they failed to manage their certificates effectively.

Poor certificate management introduces many security risks to enterprises. You may be considering switching

SSL providers because your current CA doesn't offer many management tools or a centralized platform. Lack of management tools force many IT security professionals to waste time tracking certificate details by hand, causing a lot of unnecessary headaches.

Manually tracking actions for individual certificates is overwhelming and time-consuming, which means certificate details, like expiration dates or a server address, can easily fall through the cracks without reminders, or even be changed unintentionally by human error. However, managing certificates should—and can—be simple.

IT security professionals are better off choosing an all-in-one platform that allows you to maintain a secure network, oversee your certificate landscape, run reports, issue and renew certificates, and remediate vulnerabilities.

In particular, many SSL managers choose to transition to DigiCert because of the ease of management and effective vulnerability remediation.

### EASE OF MANAGEMENT

DigiCert believes optimized SSL security goes beyond installing a certificate. IT security professionals cannot risk forgetting about certificates until the expiration date. Continuous monitoring and diligent oversight are crucial during the lifecycle of the certificate to ensure there are no lapses in security. Effective management is truly a full-time job.

Because of this, DigiCert aims to make certificate lifecycle management as easy as possible for customers. An enterprise-grade managed PKI platform, CertCentral®, is available and includes tools designed to streamline lifecycle tasks, improve oversight, and customize workflows.

During the certificate lifecycle, an SSL manager will need to do a number of tasks including, but not limited to, issuing, revoking, remediating, and renewing. CertCentral brings these tasks to one platform and tracks all the certificate details, eliminating human error.

### DISCOVER EVERY DETAIL

Without an automation tool, the only way to gather details about your certificates is by examining your certificates one by one and then checking in periodically to make sure nothing has changed. Doing this manually is nearly impossible when you are managing more than a handful of certificates. The ideal solution is to use a tool for inspection.

Certificate discovery or inspection means knowing about all the certificates in your network, staying on top of vulnerabilities, and making smart decisions based on the analysis of network reports.

CertCentral is equipped with a tool that does all of this. After running a scan, Certificate Inspector pulls all certificate details into a dashboard, where users can visually see the health of their network. From the scan, Certificate Inspector displays the information for each certificate issued for your organization in charts and converts it to downloadable reports. The dashboard gives the user a top-level view of the entire certificate landscape and you can dive into individual certificates to get to the nitty-gritty.

Certificate Inspector plays a key role in helping SSL managers identify when there are vulnerabilities that compromise security, which brings us to another reason why you might consider switching to a new CA.

### VULNERABILITY REMEDIATION

Vulnerabilities are inevitable in the security world. BEAST,

Logjam, and Heartbleed are just a few examples of recent endpoint vulnerabilities. SSL certificates can also be vulnerable when they have missing fields, use internal names, or are using an outdated hashing algorithm.

A CA needs to react quickly whenever there is a new vulnerability. Organizations—no matter the size—cannot live with the possibility of an attack looming. Patches need to be implemented quickly. Customer data, intellectual property, and revenues are on the line.

Certificate Inspector scans for weaknesses in configurations based on the latest vulnerabilities affecting SSL and assigns a letter grade to each certificate. If a certificate is compromised by a vulnerability or has a weak configuration, Certificate Inspector offers remediation suggestions, so you know exactly what steps to take to bring your network back up to the highest standard of security.

But there still may be times when you have questions or want help and you need to be able to call support. Technical support plays a big part in vulnerability remediation and overall decision to switch SSL providers. An SSL manager needs a CA who stays on top of vulnerabilities and updates tools to look for the latest bugs and weaknesses. Sometimes security can't wait. And a CA that offers easy access to knowledgeable support personnel shows a customer-first attitude.

---

On average, DigiCert customer support answers live chat inquiries within 45 seconds and phone calls within 20 seconds.

---

## Cost

No matter what line of business you're in, you care about the bottom line. When considering a new SSL provider, you will certainly compare certificate pricing models, but make sure you look at more than just the price tag. When evaluating the cost of the certificate, you'll want to consider features and benefits that increase the overall value to ensure you stretch your dollars the farthest.

There are some free or very cheap certificate options out there. Unfortunately, free SSL certificate providers often skip authentication checks to keep costs low. Authentication and identity verification are crucial to online trust. Authentication provides the assurance that you're visiting the real DigiCert.com and not a fake DigiCert phishing site.

When thinking about price vs. overall value, consider what a CA can offer you in these areas:

- SSL management tools (and if it costs you anything to use them)
- A certificate management platform
- Dedicated account representatives
- Support staff availability
- Customizable options

DigiCert stands up to cheaper competitors by offering exceptional value with free tools, a management platform, account reps, 24-hour support, and fully customizable options. Beyond that, DigiCert offers flexible pricing for large/bulk orders and accommodates special circumstances. For example, DigiCert offers a free replacement option if you choose to transition all your certificates at the same time.

## Security Implications of Transitioning CAs

Should you decide to use a new CA, keeping your organization secure during the transition is a top priority.

While debunking myths, we addressed the fact that there are no inherent lapses in SSL security during a transition from one CA to another as long as you use best practices. Some of these include the following:

- Do not uninstall a certificate until you have its replacement certificate properly installed on the server
- Renew certificates before expiration to avoid costly lapses in security
- Run regular scans of your environment using Certificate Inspector to keep track of all your certificates, regardless of issuer
- Make sure certificates use SHA-2 algorithms

If you transition to a CA, such as DigiCert, SSL certificates are automatically trusted by all major browsers, mail systems, operating systems, and mobile devices because it has one of the oldest root certificates in the industry. This allows you to transition your certificates to the DigiCert CA without worrying about managing trust relationships.

Following these best practices will keep your enterprise secure during the transition from your current SSL provider to a new CA. The way we see it, there are more security implications if you choose to stay with a low-cost certificate provider that doesn't allow you to effectively manage your certificates.

## Conclusion

Transitioning your SSL certificates to a new CA isn't going to be as hard as you think. There are many myths associated with the idea of switching, but they are just myths!

While it may seem like a daunting task when you first think about it, consolidating your certificates to be issued by one provider will not cause a disruption in service and can ease administrative burden, especially if the new CA provides around-the-clock support and a certificate management platform. A CA should make your life easier—not more complicated.

**For more information about transitioning your certificates to DigiCert, contact sales at 1.855.800.3444 or email [sales@digicert.com](mailto:sales@digicert.com).**

