Information Sheet

DIGITAL CERTIFICATES

Frequently Asked Questions

Sectigo intermediate expiration

On September 9, 2024, CSC's SubCA (Intermediate) Certificate with Sectigo will expire. To give clients the maximum amount of time to prepare for this, we now deliver a new extended life Intermediate Certificate.

If clients are not pinning certificates, there should be no impact at all. If clients are pinning, they'll need to be sure to add all intermediates included in the zip files CSC provides if they don't have them installed already.

What is "pinning?" Why is it considered risky?

Pinning is the practice where a client installs the root and intermediate certificates of a digital certificate chain on their server or device. This forces their installed certificate to accept connections only when that specific chain is used. If that chain is not used, their connection will be denied.

Originally pinning was used as an attempt to prevent Man in the Middle (MITM) attacks, however certificate authorities (CAs) now request all clients to **"STOP CERTIFICATE PINNING."** Unfortunately, pinning is not very effective in preventing MITM attacks, and the additional risks introduced far outweigh the benefits.

As the CA/B Forum (the governing body for digital certificates) continues to lobby for reduced certificate lifetimes. The CAs are now heavily recommending all clients work on improving their certificate agility.

Pinning makes it difficult to replace certificates and chains quickly when needed. Additionally, if a key is compromised, the CA may be required to revoke it with zero advanced notice. Having pinned certificates could create downtime on your sites or devices.

It's very important that clients update their server software and devices to versions that don't require pinning as soon as possible. The urgency to reduce pinning and increase certificate agility continues to grow as certificate lifetimes will inevitably shorten.

90-day certificate lifetimes

In the past, we've seen digital certificate lifetimes get shorter and shorter. In 2020, the maximum term of a digital certificate dropped from three years to one year. Our partner CAs expect that we may get an announcement that lifetimes will further drop from one year to 90 days this year. That means that clients will need to renew and install new certificates every 90 days or less, possibly starting as soon as 2025.

The ultimate goal of the CA/B Forum is to reduce digital certificate lifetimes so low that there will be no need to manage a Certificate Revocation List (CRL) as compromised keys would be replaced so frequently, it would almost eliminate risk. It wouldn't be completely unexpected to see weekly certificates—though that would be (likely) years away.

Another concern driving the digital certificate lifetime reduction is the emergence of quantum computers, which will potentially be able to decrypt RSA and ECC certificates in a matter of days if not hours. Reducing certificate lifetimes reduces the harm this can cause.

As digital certificate lifetimes reduce, the greater the requirement to be able to order, replace, and install certificates at a moment's notice with as little effort as possible.

The importance of automation

As mentioned, the need for certificate agility and removing manual processes is great. The best way to accomplish this is to implement automation.

Automation can manage the entire life cycle of a digital certificate including:

1. Monitoring expiration dates of existing digital certificates.
2. Ordering replacements for expiring certificates with CSC.
3. Validating the domain control validation (DCV) automatically.
4. Installing the digital certificates.

This removes manual human interaction from the process, and as an added benefit, eliminates human error. When certificate lifetimes reduce, automation is ***the*** way to futureproof a client's critical systems.

CSC is ready to assist in cataloguing clients' digital certificate portfolio (a vital first step) and has top-of-the-line automation options to offer.

CAA records—another tool in reducing risk

In all the sections above, the driving force behind all the changes have been to reduce the risk to domain holders, hosting companies, and also visitors who trust them to manage their data safely and securely. Digital certificates are a security product, so everyone should do everything they can to make sure every precaution is taken.

CAA records on a domain can help do just that. CAA records can perform a couple functions:

1. CAA records can limit WHAT CAs can be used to order certificates. For example, this could make it that only Sectigo Trusted Secure certificates can be ordered for the domain. Bad actors will usually try to order certificates through a CA that has less-than-stellar security standards if they try to take over a subdomain. That CAA record would look something like this:

   yourdomain.com. CAA 0 issue "sectigo.com"
   yourdomain.com. CAA 0 issuewild "sectigo.com"

2. CAA Records can send a notification if someone tries to violate the policy that has been set. This could give the domain holder early warning that someone might be trying to take over a subdomain. This might look like:

   yourdomain.com. CAA 0 iodef mailto:youremail@yourmaindomain.com

The system would send an email to the address provided every time anyone tries to order from a company not on the allowed list.

Master Account 2.0—simplifying and increasing speed of certificate issuance

CSC, in partnership with Sectigo, has created a process called Master Account 2.0, which allows Organization Validated (OV), or Extended Validation (EV) certificates to be issued faster than ever before. While automation is the most important way to simplify certificate issuance and remove the possibility of human error, Master Account 2.0 is the key to speeding up the process. With Master Account 2.0 CSC can enroll a client so they'll only need to complete a single email every year no matter how many OV or EV certificates they order, instead of an email or callback with every single order.

For most certificates, being enrolled in Master Account 2.0 will make the OV and EV ordering process feel almost like a Domain Validated (DV) certificate—very quick and easy, only requiring the ownership of the domain be proven.

CSC has tested Master Account 2.0 with about 150 clients in the past year, and has had great success getting digital certificates issued in **record time**. As CSC continues to enroll more and more clients into Master Account 2.0, they can expect a speedy yet secure OV and EV ordering process unlike anywhere else.

CSC's renewal process and why it's important to pay attention

On the first of every month, CSC emails digital certificate renewal contacts about all their certificates expiring in the next 45 days. It's very important to pay attention to the notices and be aware of the upcoming renewals.

Here are some important things to consider:

1. If an expired certificate isn't replaced, it can stop visitors from viewing a website, take down email, make vital services in a network stop responding, and generally cause a business to not be able to perform important functions until it is replaced.

2. Digital certificates need to be ordered, delivered, installed, and tested BEFORE the expiration date of the existing certificate. That means they must be ordered in advance. Ordering the same day or even only a couple days in advance puts the business at risk.

3. A digital certificate can actually have a term of up to 397 days. That means a business can order a certificate up to a month BEFORE it is actually needed. This gives more than ample time to receive the certificate, install it, and test it before it becomes urgent.

Don't forget you can set up multiple digital certificate renewal contacts so it becomes more difficult for a renewal to slip through the cracks. CSC highly recommends having multiple contacts for extra protection.

SHA-256—what is it and why use an older version?

Digital certificates use different encryption algorithms to make sure that communication between a client and a server cannot be intercepted and deciphered. From time to time, new encryption algorithms are created to keep ahead of bad actors and the new methods they invent to decode sensitive data.

Earlier in this communication, it was mentioned that quantum computers are quickly entering the purview of security professionals. They're able to decrypt some existing algorithms quicker than they'll be replaced under current certificate lifetimes.

A few years ago, Secure Hash Algorithm 1 (SHA-1) was the standard that everyone used for digital certificates. Unfortunately, as technology progressed it was no longer considered secure and no CAs will issue leaf certificates that way any longer. Today's most common algorithm is one of the SHA-2 family.

The SHA-2 family includes SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, and SHA-512/256. Sectigo's goal is always to provide maximum security tempered by enough compatibility to make their digital certificates still useable on most systems. So they're now issuing certificates by default to SHA-384.

However, the unfortunate news is that some small amount older systems were hard-coded to only accept SHA-256 certificates such as Okta (an identity provider). In other cases, companies have not updated an existing server to be able to use newer algorithms.

Whenever possible, CSC and Sectigo highly recommend updating systems to versions that allow the SHA-384 algorithm (and higher). It's ALWAYS more secure to keep up with current standards.

Contact your CSC representative for more information about digital certificates.