digicert®

47-Day TLS Certificates: FAQs

GUIDE

47-Day TLS Certificates: FAQs

Q: What are the new rules for certificate lifetimes?

Three major changes in the CA/B Forum's new TLS rules will begin taking effect in March 2026:

1. The maximum lifetime for a public TLS certificate will decrease from 398 days to 47 days.

1. The maximum period during which domain and IP address validation information may be reused will decrease from 398 days to 10 days.

2. The maximum period during which Subject Identity Information (SII, the identifying details about the entity to which the certificate is issued) may be reused will decrease from 825 days to 398 days.

Automation for some public certificates may require special tools or expertise, but for most of them the work should be relatively straightforward. There's extensive documentation, and the service is often free (as it is from DigiCert).

Q: What's the schedule for the changes?

The maximum lifetime for a public TLS certificate will decrease over the next several years:

- Until March 15, 2026, the maximum lifetime for a TLS certificate is 398 days.
- As of March 15, 2026, the maximum lifetime for a TLS certificate will be 200 days.
- As of March 15, 2027, the maximum lifetime for a TLS certificate will be 100 days.
- As of March 15, 2029, the maximum lifetime for a TLS certificate will be 47 days.

The maximum period during which domain and IP address validation information may be reused is also going down:

- Until March 15, 2026, the maximum period during which domain validation information may be reused is 398 days.
- As of March 15, 2026, the maximum period during which domain validation information may be reused is 200 days.
- As of March 15, 2027, the maximum period during which domain validation information may be reused is 100 days.
- As of March 15, 2029, the maximum period during which domain validation information may be reused is 10 days.

Q: What's the difference between maximum certificate lifetime (down to 47 days) and maximum domain validation reuse period (down to 10 days)?

The maximum lifetime of a certificate is the maximum number of days for which a certificate is considered valid. To issue a certificate, a certificate authority (CA) must validate that the applicant controls the domain name or IP address identified in the certificate. If you have one certificate and renew it once a year (under the current rules), you will reverify control annually with your renewal order.

But what if you need to replace the certificate before you renew it—for instance, if the private key is compromised? The CA can reuse the validation performed at the most recent renewal, saving you from having to revalidate. This is because the maximum domain validation reuse period has not run out.

The Baseline Requirements (aka the CA/B Forum rules for certificate issuance) have always specified both time limits, but they've generally set them at the same number. The change in the final phase of the new rules so that the maximum certificate lifetime will (eventually) be 47 days but domain validation can only be reused for 10 days is meant to ensure that validation is performed frequently in the belief that it quickly gets stale. This change also underscores the CA/B Forum's belief that domain validation must be automated. With such short timelines, manual verification is a major burden. Once it's automated, short timelines are no problem at all.

The same schedule for domain verification will apply to OV and EV certificates. Eventually, these will need to have their domain validation performed on the same schedule as DV certificates, i.e., every 200/100/10 days. But the other information in those certificates (i.e., the organization name and address) will only require renewal every 398 days. The domain verification can and should be automated, as with DV certificates, but the other information cannot be fully automated.

Q: On the dates the changes take effect, will browsers no longer accept certificates with lifetimes greater than 200/100/47 days?

No, not exactly. The restriction is on what kinds of certificates CAs can issue, not on what browsers can accept. The browser checks whether the current date is within the validity period for the certificate.

When the rule changes take effect, CAs will no longer be able to issue TLS certificates with lifetimes greater than 200/100/47 days. But a certificate with a 398-day lifetime issued before the rule change takes effect will still be valid until it expires. The same is true of 200-day certificates when the rule changes to 100 and 100-day certificates when the rule changes to 47.

Q: What is the CA/B Forum?

The CA/Browser Forum (CA/B Forum or CABF, for short) is an industry standards body consisting of certificate authorities like DigiCert (known under the standards as certificate issuers) and applications (usually web browsers, known in the standards as certificate consumers) that use certificates for authenticating a resource. Other interested parties are also members, but voting is limited to qualified certificate issuers and consumers.

The first TLS Baseline Requirements (BRs) for TLS certificates went into effect in 2012. There are other working groups working on standards for public code signing and S/MIME certificates.

Q: What are my options?

There's only one course that makes sense: Automate your certificate lifecycle management (CLM). CA/B Forum and the industry (DigiCert included) have been advising customers for many years that certificate lifetimes would shorten and that manual certificate management would no longer be a workable solution.

The vast majority of use cases for Domain Verified (DV) certificates can be automated fairly easily using the Automated Certificate Management Environment (ACME) and ACME Renewal Information (ARI) standards. This capability is included at no added cost in DigiCert CertCentral. For more complicated cases, DigiCert's Trust Lifecycle Manager (TLM) provides managed automation support for a wide variety of enterprise configurations.

An internal PKI, also known as a private PKI, is another option for some applications. Many publicly trusted certificates are used to protect resources that need no public access and, under best practices, should not be accessed from the internet. Administrators sometimes use public certificates for these resources because it's the easiest course, but the proper approach is to use an internal PKI.

An internal PKI issues certificates that are only "valid" or trusted within your enterprise for communication among private resources. As such, you can set your own rules for certificate lifetimes and many other parameters.

You could run all the software for an internal PKI yourself, but it's a complex and error-prone task. DigiCert offers several different internal PKI solutions for enterprise, cloud, and manufacturing use cases.

Q: Do these standards changes affect internal (private) PKIs?

No, the baseline requirements are binding only on public certificate authorities.

An internal PKI runs inside your network or clouds. It includes certificate authorities, but the policies enforced by the internal certificate authorities, including the expiration dates of certificates, are yours to set. It may be best to choose short expiration dates even for internal PKI, but that's not required.

You could run all the software for an internal PKI yourself, but it is a complex and error-prone task. DigiCert offers several different internal PKI solutions for enterprise, cloud, and manufacturing use cases.

Q: Will I have to pay more to replace certificates more often?

No, at least not with DigiCert CertCentral. You pay for certificates as an annual subscription. During the term of your subscription, there's no cost for renewing or replacing certificates as often as you need, and subscriptions include ACME/ARI automation at no additional cost. Our anticipation of developments like this is one of the reasons we moved to a subscription model.

We find that once customers automate certificate renewals, they voluntarily move to faster replacement cycles because it's easy and there's no reason not to. You may, for example, move straight to renewing every 30 days and know that you're ready for 2029.

Q: Will the new rules affect intermediate and root certificates?

No, they only affect leaf certificates issued by an intermediate CA.

There are no rules from the CA/B Forum or other standards bodies restricting the lifetimes of root and intermediate certificates, but there are generally agreed-upon best practices, and certificate-consuming software vendors set their own rules for their trusted root programs, which can vary wildly.

The Mozilla Root Store Policy says (section 7.4) that Mozilla will distrust root certificates 15 years after the key was generated.

The lifetime rules in the Chrome Root Program Policy, version 1.6 (February 15, 2025), are more complicated. There's no hard lifetime limit, but "[a]ny root CA certificate with corresponding key material generated more than 15 years ago will be removed from the Chrome Root Store on an ongoing basis." Roots containing keys created before April 16, 2014 will be deleted on a fixed annual schedule defined in the Root Program Policy.

The Microsoft Trusted Root Program says that "[n]ewly minted Root CAs must be valid for a minimum of eight years, and a maximum of 25 years, from the date of submission." The difference in rules between Microsoft's and other policies is rooted in the variety of applications Microsoft supports in their PKI, which is far broader than any of the other browsers.

One common-sense best practice is that a root CA certificate should not expire before any intermediate CA certificates that chain up to it.

Mismanagement of root and intermediate CA certificate lifecycles can have severe consequences, as happened recently when an apparently forgotten Google intermediate CA certificate expired, leaving many Google Chromecast devices without service.

Q: How do I automate my certificate lifecycle management?

For common and straightforward cases, such as web servers and public TLS certificates, automation is free for CertCentral customers using the widely supported Automated Certificate Management Environment (ACME) and ACME Renewal Information (ARI) standards.

Of course, not all certificates are public TLS, and not all technologies support ACME. For those cases, DigiCert's Trust Lifecycle Manager provides advanced automation capabilities and integrations.

Automation with ACME involves more than just checking a box. There are changes you need to make on the device or application (typically a web server) that requests the certificate. But for most administrators, the process is uncomplicated and well-documented.

Q: What are ACME and ARI?

ACME is Automated Certificate Management Environment. ARI is ACME Renewal Information.

ACME is a standard supported by all large certificate authorities by which certificate client software (typically a web server) requests a certificate from the CA and installs it on the client. (The web server is the client in this scenario.)

The client software also has to support ACME. Support is widespread, but not universal. The ACME client program usually runs on the client system on a schedule using the Linux cron or Windows Scheduled Tasks, but there are other solutions that integrate the schedule into larger products.

ARI is a related standard by which the server can suggest a schedule so the client knows to renew the certificate before it expires. Properly configured, ARI can instruct the client to renew if the certificate has been revoked, preventing an outage.

Q: How will this affect my Organization Validated (OV) and Extended Validation (EV) certificates?

Under the new rules for TLS certificates, as of March 15, 2026, validations of Subject Identity Information (SII) can only be reused for 398 days, down from 825.

This means the main effect on your OV and EV certificates will be that you will have to reverify the Subject Identity Information (SII)—the information in the certificate that identifies your organization—annually rather than every other year.

Under the TLS Baseline Requirements, this requires an annual phone call with a DigiCert representative and therefore cannot be fully automated.

Note that OV and EV certificates also protect domain names, so the lifetime of the OV and EV certificates will change at the same schedule as DV certificates: To 200 days in 2026, to 100 days in 2027, and to 47 days in 2029. The need for automating the management of these certificates is every bit as great as that of DV certificates.

This model of setting an odd time period with wiggle room added has long been standard operating procedure for the CA/B Forum

Q: Why 47 days?

47 days might seem like an arbitrary number, but it's a simple cascade:

- 200 days = 6 maximal months (184 days) + 1/2 30-day month (15 days) + 1 day wiggle room
- 100 days = 3 maximal months (92 days) + ~1/4 30-day month (7 days) + 1 day wiggle room
- 47 days = 1 maximal month (31 days) + 1/2 30-day month (15 days) + 1 day wiggle room

This model of setting an odd time period with wiggle room added has long been standard operating procedure for the CA/B Forum. The current 398-day limit was chosen as 1 maximal year (366 days) + 1 maximal month (31 days) + 1 day wiggle room.

Q: Are these changes related in any way to threats to cryptography from quantum computing?

Not directly, but we expect them to have the effect of improving readiness for post-quantum cryptography (PQC) by forcing organizations to adopt automated certificate management solutions.

In the years to come, the move to PQC will involve many changes to cryptographic systems in the infrastructure (certificate authorities, for example), at customer sites (web servers and other applications that use digital certificates), and to software itself (web browsers, network devices, and so on). To stay current with these changes, organizations will have to be able to make changes in their software quickly and without disruption to their operations. Automated certificate lifecycle management facilitates an important part of this.

Certificates are just one part—albeit an important one—of PQC. Many other software and hardware products you use, from many different vendors, will also need to be updated to support PQC. It's worth noting that 2029, the year when the full force of these changes take effect, is also the year by which Gartner says organizations need to be quantum ready.

Q: How are non-browser clients (like network devices) affected?

The public TLS certificate market overwhelmingly supports browser-facing certificates installed on a web server of some kind, but there are others. VPN gateways and some IoT devices are good examples of these.

These devices will also have to increase their CLM cadence. Many of them support ACME or some other automation protocol directly, so changing parameters may not be a major task. In other cases, there may be support for an alternative automation mechanism or none at all, in which case the user has some programming to do in order to automate.

Accommodating the new schedule on these devices will be a common problem. It's important to create a complete inventory of your affected assets, a process DigiCert can help with.

Can I renew my certificates before the 2026 deadline and still get 398 days out of them?

Yes, it's within the rules to get another 398 days by renewing before March 15, 2026. This is a one-time extension—the next time you renew your certificates, the maximum lifetime have been reduced to 100 days. Be sure to establish automation using CertCentral or Trust Lifecycle Manager ahead of time to prepare.

If you need to rekey the certificate on or after March 15, 2026, DigiCert (or any public CA) will have to conform to the rules in effect at that time, giving you, at best, a 200-day certificate.

The best time to automate your certificate management is as soon as you can to ensure you're prepared to do so without risking outages—from expiration or any other cause.

Learn more about how DigiCert can help you automate certificate management to prepare for shorter certificate lifetimes.