digicert®

47-Tage-TLS-Zertifikate: Häufig gestellte Fragen

LEITFADEN

47-Tage-TLS-Zertifikate: Häufig gestellte Fragen

Frage: Wie lauten die neuen Regeln für die Gültigkeitsdauer von Zertifikaten?

Drei wichtige Änderungen in den neuen TLS-Regeln des CA/B-Forums treten im März 2026 in Kraft:

1. Die maximale Lebensdauer für ein öffentliches TLS-Zertifikat wird von 398 Tagen auf 47 Tage reduziert.

2. Der maximale Zeitraum, in dem Validierungsinformationen zu Domains und IP-Adressen wiederverwendet werden dürfen, wird von 398 Tagen auf 10 Tage verkürzt.

3. Der maximale Zeitraum, in dem Subject Identity Information (SII, die identifizierenden Details über die Einheit, auf die das Zertifikat ausgestellt ist) wiederverwendet werden kann, wird von 825 Tagen auf 398 Tage verkürzt.

Für die Automatisierung einiger öffentlicher Zertifikate sind möglicherweise spezielle Tools oder Fachkenntnisse erforderlich, aber bei den meisten sollte die Arbeit relativ einfach sein. Es gibt dazu eine ausführliche Dokumentation, und der Dienst ist häufig kostenlos (so auch bei DigiCert).

Frage: Wie ist der Zeitplan für die Anpassungen?

Die maximale Lebensdauer für ein öffentliches TLS-Zertifikat wird in den nächsten Jahren abnehmen:

- Bis zum 15. März 2026 beträgt die maximale Lebensdauer für ein TLS-Zertifikat 398 Tage.

- Ab dem 15. März 2026 wird die maximale Lebensdauer eines TLS-Zertifikats 200 Tage betragen.

- Ab dem 15. März 2027 wird die maximale Lebensdauer eines TLS-Zertifikats 100 Tage betragen.

- Ab dem 15. März 2029 wird die maximale Lebensdauer eines TLS-Zertifikats 47 Tage betragen.

Der maximale Zeitraum, in dem Informationen zur Validierung von Domains und IP-Adressen wiederverwendet werden können, wird ebenfalls verkürzt:

- Bis zum 15. März 2026 dürfen die Informationen zur Domainvalidierung höchstens 398 Tage lang wiederverwendet werden.

- Ab dem 15. März 2026 dürfen die Informationen zur Domainvalidierung maximal 200 Tage lang wiederverwendet werden.

- Ab dem 15. März 2027 dürfen die Informationen zur Domainvalidierung höchstens 100 Tage lang wiederverwendet werden.

- Ab dem 15. März 2029 dürfen die Informationen zur Domainvalidierung höchstens 10 Tage lang wiederverwendet werden.

Frage: Was ist der Unterschied zwischen der maximalen Lebensdauer eines Zertifikats (47 Tage) und dem maximalen Zeitraum für die Wiederverwendung von Informationen zur Domainvalidierung (10 Tage)?

Die maximale Lebensdauer eines Zertifikats ist die maximale Anzahl von Tagen, für die ein Zertifikat als gültig angesehen wird. Um ein Zertifikat auszustellen, muss eine Zertifizierungsstelle (CA) bestätigen, dass der Antragsteller den im Zertifikat angegebenen Domainnamen oder die IP-Adresse kontrolliert. Wenn Sie ein Zertifikat besitzen und es einmal im Jahr erneuern (nach den derzeitigen Vorschriften), müssen Sie die Kontrolle jährlich mit Ihrem Verlängerungsauftrag erneut bestätigen.

Was aber, wenn Sie das Zertifikat vor der Erneuerung ersetzen müssen, z. B. wenn der private Schlüssel kompromittiert wurde? Die CA kann die bei der letzten Erneuerung durchgeführte Validierung wiederverwenden, so dass Sie nicht erneut validieren müssen. Dies liegt daran, dass der maximale Zeitraum für die Wiederverwendung der Informationen zur Domainvalidierung noch nicht abgelaufen ist.

In den Baseline Requirements (auch bekannt als die Regeln des CA/B-Forums für die Ausstellung von Zertifikaten) wurden immer beide Fristen festgelegt, aber im Allgemeinen mit der gleichen Zahl von Tagen. Die Änderung in der letzten Phase der neuen Vorschriften, wonach die maximale Gültigkeitsdauer von Zertifikaten (letztendlich) 47 Tage beträgt, die Informationen für die Domainvalidierung jedoch nur 10 Tage lang wiederverwendet werden können, soll sicherstellen, dass die Validierung häufig durchgeführt wird, da sie schnell veralten kann. Diese Änderung unterstreicht auch die Überzeugung des CA/B-Forums, dass die Domainvalidierung automatisiert werden muss. Bei so kurzen Fristen ist die manuelle Überprüfung eine große Herausforderung. Sobald dies automatisiert ist, sind kurze Fristen kein Problem.

Für OV- und EV-Zertifikate gilt derselbe Zeitplan für die Überprüfung der Domain. Letztendlich müssen diese nach demselben Zeitplan wie DV-Zertifikate validiert werden, d. h. alle 200/100/10 Tage. Weitere Informationen in diesen Zertifikaten (d. h. der Name und die Adresse der Organisation) müssen jedoch nur alle 398 Tage erneut geprüft werden. Die Überprüfung der Domain kann und sollte, wie bei DV-Zertifikaten, automatisiert werden, aber die anderen Informationen können nicht vollständig automatisiert geprüft werden.

Frage: Werden die Browser an den Tagen, an denen die Änderungen in Kraft treten, keine Zertifikate mit einer Lebensdauer von mehr als 200/100/47 Tagen mehr akzeptieren?

Nein, das ist so nicht richtig. Die Beschränkung bezieht sich darauf, welche Arten von Zertifikaten CAs ausstellen können, nicht darauf, was Browser akzeptieren können. Der Browser prüft, ob das aktuelle Datum innerhalb des Gültigkeitszeitraums des Zertifikats liegt.

Wenn die Regeländerungen in Kraft treten, können CAs keine TLS-Zertifikate mit einer Lebensdauer von mehr als 200/100/47 Tagen mehr ausstellen. Ein Zertifikat mit einer Laufzeit von 398 Tagen, das vor Inkrafttreten der neuen Regelung ausgestellt wurde, bleibt jedoch bis zu seinem Ablaufdatum gültig. Das Gleiche gilt für 200-Tage-Zertifikate, wenn die maximale Gültigkeitsdauer auf 100 Tage geändert wird, und für 100-Tage-Zertifikate, wenn sie auf 47 Tage geändert wird.

Frage: Was ist das CA/B Forum?

Das CA/Browser-Forum (CA/B Forum oder kurz CABF) ist ein Gremium für Industriestandards, das sich aus Zertifizierungsstellen wie DigiCert (in den Standards als Zertifikatsaussteller bekannt) und Anbietern von Anwendungen (in der Regel Webbrowser, in den Standards als Zertifikatsnutzer bekannt) zusammensetzt, die Zertifikate zur Authentifizierung einer Ressource verwenden. Andere interessierte Parteien sind ebenfalls Mitglieder, die Stimmrechte sind jedoch auf qualifizierte Zertifikatsaussteller und Zertifikatsnutzer beschränkt.

Die ersten Baseline Requirements für TLS-Zertifikate traten 2012 in Kraft. Es gibt weitere Arbeitsgruppen, die an Standards für öffentliches Code Signing und S/MIME-Zertifikate arbeiten.

Frage: Welche Möglichkeiten habe ich?

Es gibt nur einen sinnvollen Weg: Automatisieren Sie ihr Certificate Lifecycle Management (CLM). Das CA/B-Forum und die Branche (einschließlich DigiCert) weisen ihre Kunden seit vielen Jahren darauf hin, dass sich die Lebensdauer von Zertifikaten verkürzen wird und dass die manuelle Verwaltung von Zertifikaten dann keine praktikable Lösung mehr sein wird.

Die überwiegende Mehrheit der Anwendungsfälle für Zertifikate mit Domainvalidierung (DV-Zertifikate) kann mit Hilfe der Standards Automated Certificate Management Environment (ACME) und ACME Renewal Information (ARI) recht einfach automatisiert werden. Diese Funktionalität ist ohne zusätzliche Kosten in DigiCert CertCentral enthalten. Für kompliziertere Fälle bietet der Trust Lifecycle Manager (TLM) von DigiCert Automatisierungsunterstützung für eine Vielzahl von Unternehmenskonfigurationen.

Eine interne PKI, auch bekannt als Private PKI, ist eine weitere Option für einige Anwendungen. Viele öffentlich vertrauenswürdige Zertifikate werden zum Schutz von Ressourcen verwendet, die keinen öffentlichen Zugang benötigen und gemäß bewährten Verfahren nicht über das Internet zugänglich sein sollten. Administratoren verwenden manchmal öffentliche Zertifikate für diese Ressourcen, weil es am einfachsten ist, aber der richtige Ansatz ist die Verwendung einer internen PKI.

Eine interne PKI stellt Zertifikate aus, die nur innerhalb Ihres Unternehmens für die Kommunikation zwischen privaten Ressourcen „gültig" oder vertrauenswürdig sind. Sie können also Ihre eigenen Regeln für die Lebensdauer von Zertifikaten und viele andere Parameter festlegen.

Sie könnten die gesamte Software für eine interne PKI selbst ausführen und verwalten, aber das ist eine komplexe und fehleranfällige Aufgabe. DigiCert bietet verschiedene interne PKI-Lösungen für Unternehmens-, Cloud- und Produktionsanwendungen an.

Frage: Wirken sich diese Änderungen der Standards auf interne (private) PKIs aus?

Nein, die Baseline Requirements sind nur für öffentliche Zertifizierungsstellen verbindlich.

Eine interne PKI läuft innerhalb Ihres Netzwerks oder Ihrer Clouds. Es umfasst Zertifizierungsstellen, aber die von den internen Zertifizierungsstellen durchgesetzten Richtlinien, einschließlich der Ablaufdaten von Zertifikaten, können Sie selbst festlegen. Auch für interne PKI kann es sinnvoll sein, kurze Gültigkeitsdauern zu wählen, aber das ist nicht obligatorisch.

Sie könnten die gesamte Software für eine interne PKI selbst ausführen und verwalten, aber das ist eine komplexe und fehleranfällige Aufgabe. DigiCert bietet verschiedene interne PKI-Lösungen für Unternehmens-, Cloud- und Produktionsanwendungen an.

Frage: Muss ich mehr bezahlen, um Zertifikate häufiger zu ersetzen?

Nein, zumindest nicht mit DigiCert CertCentral. Sie zahlen für Zertifikate im Jahresabonnement. Während der Laufzeit Ihres Abonnements fallen keine Kosten für die Erneuerung oder den Austausch von Zertifikaten an, so oft Sie diese benötigen, und die Abonnements beinhalten die ACME/ARI-Automatisierung ohne zusätzliche Kosten. Wir haben Entwicklungen wie diese vorhergesehen und sind unter anderem deshalb auf ein Abonnementmodell umgestiegen.

Wir haben festgestellt, dass Kunden, die ihre Zertifikatserneuerung automatisieren, freiwillig zu schnelleren Erneuerungszyklen übergehen, weil es einfach ist und es keinen Grund gibt, es nicht zu tun. Sie können z. B. direkt dazu übergehen, Ihre Zertifikate alle 30 Tage zu erneuern und wissen dann, dass Sie für 2029 bereit sind.

Frage: Wirken sich die neuen Regeln auf Zwischen- und Root-Zertifikate aus?

Nein, sie betreffen nur Anwenderzertifikate, die von einer Zwischen-CA ausgestellt wurden.

Es gibt keine Regeln des CA/B-Forums oder anderer Normungsgremien, die die Lebensdauer von Root- und Zwischenzertifikaten einschränken, aber es gibt allgemein akzeptierte Best Practices, und Softwarehersteller, die Zertifikate verwenden, legen ihre eigenen Regeln für ihre vertrauenswürdigen Root-Zertifikate fest, die sehr unterschiedlich sein können.

Die Mozilla Root Store Policy besagt (Abschnitt 7.4), dass Mozilla Root-Zertifikaten 15 Jahre, nachdem der Schlüssel erzeugt wurde, nicht mehr vertraut.

Die Lebenszeitregeln in der Chrome Root Program Policy, Version 1.7 (15. Juli 2025), sind komplizierter. Es gibt keine feste Obergrenze für die Lebensdauer, aber „jedes Root-CA-Zertifikat, das vor mehr als 15 Jahren generiert wurde, wird (mit dem dazugehörigen Schlüsselmaterial) in einem fortlaufenden Prozess aus dem Chrome Root Store entfernt." Root-Zertifikate mit Schlüsseln, die vor dem 16. April 2014 erstellt wurden, werden nach einem festen jährlichen Zeitplan gelöscht, der in der Root Program Policy festgelegt ist.

Das Microsoft Trusted Root Program besagt, dass „neu erstellte Root-CAs mindestens acht Jahre und höchstens 25 Jahre ab dem Datum der Einreichung gültig sein müssen". Der Unterschied zwischen den Regeln von Microsoft und denen anderer Anbieter liegt in der Vielfalt der Anwendungen begründet, die Microsoft in seiner PKI unterstützt, die weitaus umfangreicher ist als die der anderen Browser.

Zu den einleuchtenden Best Practices gehört, dass ein Root-CA-Zertifikat nicht vor den Zwischenzertifikaten ablaufen sollte, die mit ihm verkettet sind.

Eine unzureichende Verwaltung der Lebenszyklen von Root- und Zwischenzertifikaten kann schwerwiegende Folgen haben, wie kürzlich geschehen, als ein offenbar vergessenes Google-Zwischenzertifikat ablief, was dazu führte, dass viele Google Chromecast-Geräte nicht mehr funktionieren.

Frage: Wie kann ich die Verwaltung meines Zertifikatslebenszyklus automatisieren?

Für gängige und einfache Fälle, wie Webserver und öffentliche TLS-Zertifikate, ist die Automatisierung für CertCentral-Kunden kostenlos, wenn sie die weithin unterstützten Standards Automated Certificate Management Environment (ACME) und ACME Renewal Information (ARI) verwenden.

Natürlich sind nicht alle Zertifikate öffentliche TLS-Zertifikate, und nicht alle Technologien unterstützen ACME. Für diese Fälle stellt der Trust Lifecycle Manager von DigiCert fortschrittliche Automatisierungsfunktionen und Integrationen bereit.

Die Automatisierung mit ACME erfordert mehr als nur das Ankreuzen eines Kästchens. Auf dem Gerät oder der Anwendung (in der Regel ein Webserver), die das Zertifikat anfordert, müssen Sie einige Änderungen vornehmen. Für die meisten Administratoren ist das Verfahren jedoch unkompliziert und gut dokumentiert.

Frage: Was sind ACME und ARI?

ACME steht für Automated Certificate Management Environment. ARI steht für ACME Renewal Information.

ACME ist ein von allen großen Zertifizierungsstellen unterstützter Standard, bei dem die Zertifikats-Clientsoftware (in der Regel ein Webserver) ein Zertifikat von der Zertifizierungsstelle anfordert und es auf dem Client installiert. (Der Webserver ist in diesem Szenario der Client.)

Die Client-Software muss auch ACME unterstützen. ACME wird von sehr vielen, aber nicht von allen Client-Softwarelösungen unterstützt. Das ACME-Client-Programm läuft normalerweise auf dem Client-System nach einem Zeitplan, unter Verwendung von cron auf Linux oder dem Windows Aufgabenplaner, aber es gibt auch andere Lösungen, die den Zeitplan in größere Produkte integrieren.

ARI ist ein verwandter Standard, mit dem der Server einen Zeitplan vorschlagen kann, damit der Client weiß, dass er das Zertifikat erneuern muss, bevor es abläuft. Richtig konfiguriert, kann ARI den Client auch anweisen, das Zertifikat zu erneuern, wenn es widerrufen wurde, um einen Ausfall zu vermeiden.

Frage: Wie wirkt sich dies auf meine Zertifikate mit Unternehmensvalidierung (OV) und Extended Validation (EV) aus?

Nach den neuen Regeln für TLS-Zertifikate können Validierungsdaten für Subject Identity Information (SII) ab dem 15. März 2026 nur noch 398 Tage lang wiederverwendet werden, vorher waren es 825.

Die wichtigste Konsequenz für Ihre OV- und EV-Zertifikate wird daher sein, dass Sie die Subject Identity Information (SII) – die Informationen im Zertifikat, die Ihre Organisation identifizieren – jährlich statt alle zwei Jahre neu validieren müssen.

Gemäß den Baseline Requirements für TLS ist hierfür ein jährliches Telefongespräch mit einem DigiCert-Vertreter erforderlich; der Prozess kann daher nicht vollständig automatisiert werden.

Beachten Sie, dass OV- und EV-Zertifikate auch Domainnamen schützen, so dass sich die Gültigkeitsdauer der OV- und EV-Zertifikate nach demselben Zeitplan wie die der DV-Zertifikate ändert: auf 200 Tage im Jahr 2026, auf 100 Tage im Jahr 2027 und auf 47 Tage im Jahr 2029. Die Notwendigkeit, die Verwaltung dieser Zertifikate zu automatisieren, ist ebenso groß wie für DV-Zertifikate.

Diese Art der Festlegung eines Zeitraums mit zusätzlichem Spielraum ist seit langem das Standardverfahren des CA/B-Forums.

Frage: Warum 47 Tage?

47 Tage mögen wie eine willkürliche Zahl erscheinen, aber es handelt sich um eine einfache Berechnung:

- 200 Tage = maximale Tageszahl für 6 Monate (184 Tage) + 1/2 30-Tage-Monat (15 Tage) + 1 Tag Spielraum
- 100 Tage = maximale Tageszahl für 3 Monate (92 Tage) + ~1/4 30-Tage-Monat (7 Tage) + 1 Tag Spielraum
- 47 Tage = maximale Tageszahl für 1 Monat (31 Tage) + 1/2 30-Tage-Monat (15 Tage) + 1 Tag Spielraum

Diese Art der Festlegung eines Zeitraums mit zusätzlichem Spielraum ist seit langem das Standardverfahren des CA/B-Forums. Die derzeitige maximale Gültigkeitsdauer von 398 Tagen wurde als maximale Tageszahl für 1 Jahr (366 Tage) + maximale Tageszahl für 1 Monat (31 Tage) + 1 Tag Spielraum gewählt.

Frage: Stehen diese Veränderungen in irgendeiner Weise im Zusammenhang mit der Bedrohung der Kryptographie durch das Quantencomputing?

Nicht direkt, aber wir gehen davon aus, dass sie zur Vorbereitung auf die Post-Quanten-Kryptographie (PQC) beitragen, indem sie Unternehmen dazu zwingen, automatisierte Lösungen für die Zertifikatsverwaltung einzusetzen.

In den kommenden Jahren wird der Übergang zu PQC viele Änderungen an den kryptografischen Systemen in der Infrastruktur (z. B. Zertifizierungsstellen), an den Kundenstandorten (Webserver und andere Anwendungen, die digitale Zertifikate verwenden) und an der Software selbst (Webbrowser, Netzwerkgeräte usw.) mit sich bringen. Um mit diesen Veränderungen Schritt halten zu können, müssen die Unternehmen in der Lage sein, ihre Software schnell und ohne Unterbrechung des Betriebs zu ändern. Die automatisierte Verwaltung des Lebenszyklus von Zertifikaten leistet einen wichtigen Beitrag dazu.

Zertifikate sind nur ein – wenn auch wichtiger – Teil von PQC. Viele andere Software- und Hardwareprodukte, die Sie verwenden, von vielen verschiedenen Anbietern, müssen ebenfalls aktualisiert werden, um PQC zu unterstützen. Es ist erwähnenswert, dass 2029, das Jahr, in dem diese Veränderungen in vollem Umfang in Kraft treten, auch das Jahr ist, in dem Unternehmen laut Gartner auf die Quanten-Technologie vorbereitet sein müssen.

Frage: Wie sind Clients, die keine Browser sind (z. B. Netzwerkgeräte) betroffen?

Der Markt für öffentliche TLS-Zertifikate unterstützt überwiegend browserorientierte Zertifikate, die auf einem Webserver der einen oder anderen Art installiert sind, aber es gibt auch andere. VPN-Gateways und einige IoT-Geräte sind gute Beispiele dafür.

Auch auf diesen Geräten wird der Rhythmus der Zertifikatslebensyklen beschleunigt werden müssen. Viele von ihnen unterstützen ACME oder ein anderes Automatisierungsprotokoll direkt, so dass das Ändern von Parametern keine besonders aufwendige Aufgabe darstellt. In anderen Fällen gibt es vielleicht Unterstützung für einen alternativen Automatisierungsmechanismus oder gar keinen, so dass der Benutzer etwas programmieren muss, um zu automatisieren.

Die Anpassung dieser Geräte an den neuen Zeitplan wird ein gängiges Problem sein. Es ist wichtig, ein vollständiges Inventar der betroffenen Ressourcen zu erstellen, wobei DigiCert Sie unterstützen kann.

Kann ich meine Zertifikate vor dem Termin 2026 erneuern und dann noch 398 Tage lang nutzen?

Ja, die Regeln gestatten es, ein 398 Tage lang gültiges Zertifikat zu erhalten, indem Sie vor dem 15. März 2026 erneuern. Dies ist eine einmalige Verlängerung – bei der nächsten Erneuerung Ihrer Zertifikate wird die maximale Laufzeit auf 100 Tage reduziert. Stellen Sie sicher, dass Sie die Automatisierung mit CertCentral oder Trust Lifecycle Manager vor deren Ablauf einrichten, um darauf vorbereitet zu sein.

Wenn Sie ein Zertifikat am oder nach dem 15. März 2026 neu ausstellen müssen, muss DigiCert (wie jede andere öffentliche Zertifizierungsstelle) die zu diesem Zeitpunkt geltenden Regeln einhalten, so dass Sie bestenfalls ein 200-Tage-Zertifikat erhalten.

Der beste Zeitpunkt für die Automatisierung der Zertifikatsverwaltung ist so früh wie möglich, um sicherzustellen, dass Sie auf alle anstehenden Aufgaben vorbereitet sind und keine Ausfälle riskieren – sei es wegen Ablaufs der Gültigkeit oder aus anderen Gründen.

Erfahren Sie mehr darüber, wie DigiCert Ihnen helfen kann, die Zertifikatsverwaltung zu automatisieren und sich auf eine kürzere Lebensdauer der Zertifikate vorzubereiten.