digicert®

Certificats TLS d'une durée de 47 jours : Foire aux questions

GUIDE

Certificats TLS d'une durée de 47 jours : Foire aux questions

Q : Quelles sont les nouvelles règles concernant la durée de validité des certificats ?

Trois changements majeurs dans les nouvelles règles TLS du CA/B Forum entreront en vigueur en mars 2026 :

1. La durée de validité maximale d'un certificat TLS public passera de 398 jours à 47 jours.

2. La période maximale pendant laquelle les informations de validation sur les domaines et les adresses IP peuvent être réutilisées passera de 398 jours à 10 jours.

3. La période maximale pendant laquelle les informations sur l'identité du demandeur (SII, les détails d'identification de l'entité juridique à laquelle le certificat est délivré) peuvent être réutilisées passera de 825 jours à 398 jours.

L'automatisation de certains certificats publics peut nécessiter des outils ou des compétences spécifiques, mais pour la plupart d'entre eux, le processus devrait être relativement simple. Il existe une documentation détaillée et le service est souvent gratuit (comme c'est le cas avec DigiCert).

Q : Quel est le calendrier d'entrée en vigueur des changements ?

La durée de validité maximale d'un certificat TLS public diminuera au cours des prochaines années :

- Jusqu'au 15 mars 2026, la durée de validité maximale d'un certificat TLS sera de 398 jours.
- À partir du 15 mars 2026, la durée de validité maximale d'un certificat TLS passera à 200 jours.
- À partir du 15 mars 2027, la durée de validité maximale d'un certificat TLS passera à 100 jours.
- À partir du 15 mars 2029, la durée de validité maximale d'un certificat TLS passera à 47 jours.

La période maximale pendant laquelle les informations de validation des domaines et des adresses IP peuvent être réutilisées diminuera également :

- Jusqu'au 15 mars 2026, la période maximale pendant laquelle les informations de validation d'un domaine peuvent être réutilisées sera de 398 jours.
- À partir du 15 mars 2026, la période maximale pendant laquelle les informations de validation d'un domaine peuvent être réutilisées passera à 200 jours.
- À partir du 15 mars 2027, la période maximale pendant laquelle les informations de validation d'un domaine peuvent être réutilisées passera à 100 jours.
- À partir du 15 mars 2029, la période maximale pendant laquelle les informations de validation d'un domaine peuvent être réutilisées passera à 10 jours.

Q : Quelle est la différence entre la durée de validité maximale d'un certificat (ramenée à 47 jours) et la période maximale de réutilisation des informations de validation d'un domaine (ramenée à 10 jours) ?

La durée de validité maximale d'un certificat est le nombre maximal de jours pendant lesquels un certificat est considéré comme valide. Pour délivrer un certificat, une autorité de certification (AC) doit vérifier et valider que le demandeur contrôle bien le nom de domaine ou l'adresse IP identifié(e) dans le certificat. Si vous avez un certificat et que vous le renouvelez une fois par an (selon les règles actuelles), vous ferez procéder à cette vérification chaque année lors de la commande de renouvellement.

Mais que se passe-t-il si vous devez remplacer le certificat avant de le renouveler, par exemple si la clé privée est compromise ? Dans ce cas de figure, l'autorité de certification peut réutiliser la validation effectuée lors du dernier renouvellement, ce qui vous évite de devoir procéder à une nouvelle validation. Cela s'explique par le fait que la période maximale de réutilisation de la validation du domaine est encore en cours.

Les exigences de base (c'est-à-dire les règles du CA/B Forum pour la délivrance des certificats) ont toujours spécifié les deux délais séparément, mais elles les ont généralement fixés au même nombre. Le changement dans la phase finale des nouvelles règles, selon laquelle la durée de validité maximale d'un certificat sera (in fine) de 47 jours, alors que les informations de validation d'un domaine ne pourront être réutilisées que pendant 10 jours, vise à garantir que la validation est effectuée fréquemment, sachant qu'elle devient rapidement périmée. Ce changement souligne également la conviction du CA/B Forum selon laquelle la validation des domaines doit être automatisée. Avec des délais aussi courts, la vérification manuelle devient en effet une charge importante. Une fois automatisés, les délais courts ne posent aucun problème.

Le même calendrier de vérification des domaines s'applique aux certificats OV et EV. À terme, la validation de ces domaines devra être effectuée selon le même calendrier que les certificats DV, c'est-à-dire tous les 200/100/10 jours. Toutefois, les autres informations contenues dans ces certificats (c'est-à-dire le nom et l'adresse de l'organisation titulaire) ne devront être renouvelées que tous les 398 jours. La vérification du domaine peut et doit être automatisée, comme pour les certificats DV, même si les autres informations ne peuvent pas être entièrement automatisées.

Q : Aux dates d'entrée en vigueur des changements successifs, les navigateurs n'accepteront-ils plus les certificats dont la durée de validité est supérieure à 200/100/47 jours ?

Non, pas exactement. La restriction porte sur les types de certificats que les autorités de certification peuvent délivrer, et non sur ceux que les navigateurs peuvent accepter. Le navigateur vérifie si la date actuelle est comprise dans la période de validité du certificat.

Lorsque les changements entreront en vigueur, les autorités de certification ne pourront plus émettre de certificats TLS d'une durée de validité supérieure à 200/100/47 jours. Toutefois, un certificat d'une durée de validité de 398 jours, délivré avant l'entrée en vigueur du changement de règles, restera valable jusqu'à son expiration. Il en va de même pour les certificats de 200 jours lorsque la règle passera à 100 et les certificats de 100 jours lorsque la règle passera à 47.

Q : Qu'est-ce que le CA/B Forum ?

Le CA/Browser Forum (CA/B Forum ou CABF, en abrégé) est un organisme sectoriel de standardisation composé d'autorités de certification comme DigiCert (appelées émetteurs de certificats dans les normes du CABF) et d'éditeurs d'applications (généralement des navigateurs web, appelés consommateurs de certificats dans les normes du CABF) qui utilisent des certificats pour authentifier une ressource. D'autres parties intéressées sont également membres, mais le vote est limité aux émetteurs de certificats qualifiés et aux consommateurs.

Les premières exigences TLS de base pour les certificats TLS sont entrées en vigueur en 2012. D'autres groupes de travail planchent également sur des normes relatives à la signature de code et aux certificats S/MIME.

Q : Quelles sont mes options ?

Il n'y a qu'une solution valable : automatisez la gestion du cycle de vie de vos certificats (CLM). Depuis de nombreuses années, le CA/B Forum et les acteurs du secteur (y compris DigiCert) préviennent leurs clients que la durée de validité des certificats se raccourcirait et que la gestion manuelle des certificats ne serait plus une solution viable.

La grande majorité des cas d'usage des certificats de vérification de domaine (DV) peuvent être automatisés assez facilement à l'aide des normes ACME (Automated Certificate Management Environment) et ARI (ACME Renewal Information). Cette fonctionnalité est incluse sans frais supplémentaires dans DigiCert CertCentral. Pour les cas plus complexes, Trust Lifecycle Manager (TLM) de DigiCert fournit un accompagnement à l'automatisation pour une grande variété de configurations d'entreprise.

Une PKI interne, également connue sous le nom de PKI privée, est une autre option pour certaines applications. De nombreux certificats publiquement approuvés sont utilisés pour protéger des ressources qui ne nécessitent pas d'accès public et qui, selon les bonnes pratiques, ne devraient pas être accessibles depuis Internet. Les administrateurs utilisent parfois des certificats publics pour ces ressources parce que c'est la solution la plus simple, mais la bonne approche consiste à utiliser une PKI interne.

Une PKI interne émet des certificats qui ne sont « valides » ou approuvés qu'au sein de votre entreprise pour la communication entre des ressources privées. En ce sens, vous pouvez définir vos propres règles pour les durées de vie des certificats et de nombreux autres paramètres.

Vous pourriez gérer vous-même tous les logiciels d'une PKI interne, mais il s'agit d'une tâche complexe et sujette aux erreurs. DigiCert propose différentes solutions PKI internes pour des cas d'usage particuliers : entreprises, cloud et industrie.

Q : Ces changements de normes ont-ils une incidence sur les PKI internes (privées) ?

Non, les exigences de base ne sont contraignantes que pour les autorités de certification publique.

Une PKI interne fonctionne à l'intérieur de votre réseau ou de vos environnements cloud. Il inclut les autorités de certification, mais les règles appliquées par les AC internes, y compris les dates d'expiration des certificats, sont laissées à votre discrétion. Il peut être préférable de choisir des dates d'expiration courtes, même pour les PKI internes, mais ce n'est pas obligatoire.

Il est possible de gérer soi-même tous les logiciels d'une PKI interne, sachant qu'il s'agit cependant d'une tâche complexe et sujette aux erreurs. DigiCert propose différentes solutions PKI internes pour des cas d'usage particuliers : entreprises, cloud et industrie.

Q : Devrai-je payer plus cher pour remplacer mes certificats plus souvent ?

Non, du moins pas avec DigiCert CertCentral. Vous payez vos certificats sous la forme d'un abonnement annuel. Pendant la durée de votre abonnement, vous pouvez renouveler ou remplacer vos certificats gratuitement aussi souvent que nécessaire, et les abonnements incluent l'automatisation ACME/ARI sans frais supplémentaires. C'est notamment parce que nous anticipons ce type d'évolution que nous avons opté pour un modèle d'abonnement.

Nous constatons qu'une fois les renouvellements de certificats automatisés, les clients passent volontairement à des cycles de remplacement plus courts, car c'est facile et il n'y a aucune raison de ne pas le faire. Vous pouvez, par exemple, passer directement à un renouvellement tous les 30 jours et obtenir ainsi l'assurance d'être déjà prêt pour 2029.

Q : Les nouvelles règles affecteront-elles les certificats intermédiaires et les certificats racine ?

Non, elles n'affectent que les certificats Leaf émis par une autorité de certification intermédiaire.

Le CA/B Forum ou d'autres organismes de standardisation n'imposent aucune règle limitant la durée de validité des certificats racine et intermédiaires, mais il existe des bonnes pratiques généralement reconnues. De leur côté, les éditeurs de logiciels consommateurs de certificats fixent leurs propres règles pour leurs programmes de racine de confiance, lesquels peuvent varier considérablement.

La politique du Root Store de Mozilla indique en section 7.4 que Mozilla invalidera les certificats racine 15 ans après que la clé a été générée.

Les règles relatives à la durée de validité dans la politique du programme Chrome Root, version 1.6 (15 février 2025), sont plus complexes. Il n'y a pas de limite de durée de validité, mais « [t]out certificat d'une AC racine, dont le matériel de clé correspondant a été généré il y a plus de 15 ans, sera supprimé du Chrome Root Store sur une base continue ». Les racines contenant des clés créées avant le 16 avril 2014 seront donc supprimées selon un calendrier annuel fixe défini dans la politique du programme racine.

Le programme Trusted Root de Microsoft indique que « [l]es AC racine nouvellement créées doivent être valides pour un minimum de 8 ans et un maximum de 25 ans, à compter de la date de soumission ». Les différences de règles entre la politique de Microsoft et les autres politiques s'expliquent par la variété des applications prises en charge par Microsoft dans sa PKI, laquelle est beaucoup plus large que celle des autres navigateurs.

Une pratique de bon sens veut que le certificat de l'AC racine n'expire pas avant les certificats des AC intermédiaires qui lui sont rattachés.

Une mauvaise gestion des cycles de vie des certificats d'AC racine et intermédiaire peut avoir de graves conséquences, comme cela s'est produit récemment lorsqu'un certificat d'AC intermédiaire de Google, apparemment oublié, a expiré, mettant de nombreux appareils Google Chromecast hors service.

Q : Comment automatiser la gestion du cycle de vie des certificats ?

Pour les cas courants et simples, tels que les serveurs web et les certificats TLS publics, l'automatisation est gratuite pour les clients de CertCentral qui utilisent des normes largement répandues comme ACME (Automated Certificate Management Environment) et ARI (ACME Renewal Information).

Bien entendu, tous les certificats ne sont pas des certificats TLS publics et toutes les technologies ne prennent pas en charge l'ACME. Pour ces cas, DigiCert Trust Lifecycle Manager offre des capacités d'automatisation et des intégrations avancées.

Automatiser avec ACME n'est pas une simple formalité. Vous devez apporter des modifications à l'appareil ou à l'application (généralement un serveur web) pour lequel le certificat est demandé. Mais pour la plupart des administrateurs, le processus est simple et bien documenté.

Q : Que sont l'ACME et l'ARI ?

ACME est l'Automated Certificate Management Environment (environnement de gestion automatisée des certificats). ARI est l'ACME Renewal Information (information sur le renouvellement de l'ACME).

L'ACME est une norme reconnue par toutes les grandes autorités de certification, selon laquelle un logiciel client (généralement un serveur web) demande un certificat à l'AC et l'installe sur le client. Le serveur web est le client dans ce scénario.

Le logiciel client doit également prendre en charge l'ACME. La compatibilité ACME est largement répandue mais pas universelle. Le programme client ACME s'exécute généralement sur le système client, selon un calendrier utilisant le cron de Linux ou les tâches planifiées de Windows, mais il existe d'autres solutions qui intègrent le calendrier dans des produits de plus grande taille.

L'ARI est une norme connexe qui permet au serveur de proposer un calendrier rappelant au client qu'il doit renouveler le certificat avant qu'il n'expire. Correctement configuré, l'ARI peut demander au client de renouveler le certificat si celui-ci a été révoqué, ce qui permet d'éviter une panne.

Q : Quel sera l'impact sur mes certificats de validation d'organisation (OV) et de validation étendue (EV) ?

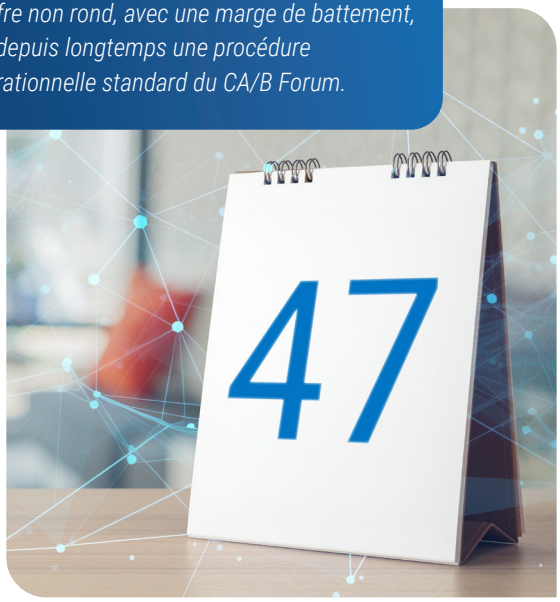
Selon les nouvelles règles applicables aux certificats TLS, à compter du 15 mars 2026, les informations validées sur l'identité du sujet (SII) ne pourront être réutilisées que pendant 398 jours, contre 825 auparavant.

Cela signifie en substance que pour vos certificats OV et EV, vous devrez faire revérifier les informations SII – à savoir les informations du certificat qui identifient votre organisation – tous les ans au lieu de tous les deux ans.

Dans le cadre des exigences TLS de base, cette vérification doit s'opérer chaque année par téléphone avec un représentant de DigiCert et ne peut donc pas être entièrement automatisée.

Notez que les certificats OV et EV protègent également les noms de domaine, ce qui signifie que la durée de validité des certificats OV et EV changera au même rythme que celle des certificats DV : elle passera à 200 jours en 2026, à 100 jours en 2027 et à 47 jours en 2029. L'automatisation la gestion de ces certificats est donc tout aussi impérative que celle des certificats DV.

Ce modèle de fixation d'une période sur un chiffre non rond, avec une marge de battement, est depuis longtemps une procédure opérationnelle standard du CA/B Forum.



Q : Pourquoi 47 jours ?

47 jours peut sembler un chiffre arbitraire, mais il s'agit d'un simple effet cascade :

- 200 jours = 6 mois maximum (184 jours) + 1/2 mois de 30 jours (15 jours) + 1 jour de battement
- 100 jours = 3 mois maximum (92 jours) + ~1/4 mois de 30 jours (7 jours) + 1 jour de battement
- 47 jours = 1 mois maximal (31 jours) + 1/2 mois de 30 jours (15 jours) + 1 jour de battement

Ce modèle de fixation d'une période sur un chiffre non rond, avec une marge de battement, est depuis longtemps une procédure opérationnelle standard du CA/B Forum. La limite actuelle de 398 jours a été fixée à 1 année maximale (366 jours) + 1 mois maximal (31 jours) + 1 jour de battement.

Q : Ces changements sont-ils liés d'une manière ou d'une autre aux menaces que l'informatique quantique fait peser sur la cryptographie ?

Pas directement, mais nous pensons qu'elles auront pour effet d'améliorer le niveau de préparation à la cryptographie post-quantique (PQC) en obligeant les organisations à adopter des solutions automatisées de gestion des certificats.

Dans les années à venir, le passage à la PQC impliquera de nombreux changements dans les systèmes cryptographiques de l'infrastructure (les autorités de certification, par exemple), sur les sites des clients (serveurs web et autres applications qui utilisent des certificats numériques) et dans les logiciels eux-mêmes (navigateurs web, équipements réseau, etc.). Pour rester en phase avec ces changements, les organisations devront être en mesure d'apporter des modifications à leurs logiciels rapidement et sans perturber leurs activités. La gestion automatisée du cycle de vie des certificats constitue un élément important à cet égard.

Les certificats ne sont qu'une partie, certes importante, de la PQC. Vos nombreux autres logiciels et matériels, provenant de différents fournisseurs, devront également être mis à jour pour prendre en charge la PQC. Il est intéressant de noter que 2029, l'année où ces changements prendront pleinement effet, est également l'année où, selon Gartner, les organisations devront être prêtes pour l'arrivée de l'informatique quantique.

Q : Comment les clients hors navigateurs (comme les équipements réseau) sont-ils affectés ?

Dans son immense majorité, le marché des certificats TLS publics s'adresse à des certificats installés sur des serveurs web communiquant avec des navigateurs, mais il en existe d'autres. Les passerelles VPN et certains appareils IoT en sont de bons exemples.

Ces dispositifs devront également augmenter la cadence de leur CLM. Nombre d'entre eux prennent déjà directement en charge l'ACME ou d'autres protocoles d'automatisation répandus, de sorte que la modification des paramètres ne constitue pas une tâche majeure. Dans d'autres cas, la prise en charge peut être inexistante ou se limiter à un mécanisme d'automatisation alternatif, auquel cas l'utilisateur doit programmer lui-même un script d'automatisation.

Sur ces appareils, l'adaptation au nouveau calendrier deviendra un problème courant. Il est important de dresser un inventaire complet de vos actifs concernés, un processus dans lequel DigiCert peut vous aider.

Puis-je renouveler mes certificats avant la date limite de 2026 tout en bénéficiant d'une durée de validité de 398 jours ?

Oui, il est possible d'obtenir à nouveau 398 jours de durée de validité en renouvelant avant le 15 mars 2026. Il s'agit d'une extension unique – la prochaine fois que vous renouvellerez vos certificats, la durée de validité maximale sera ramenée à 100 jours. Veillez à automatiser le processus à l'avance à l'aide de CertCentral ou de Trust Lifecycle Manager pour bien vous préparer.

Si vous devez renouveler la clé du certificat à partir du 15 mars 2026, DigiCert (ou toute autre autorité de certification publique) devra se conformer aux règles en vigueur à cette date, ce qui vous donnera, au mieux, un certificat d'une durée de 200 jours.

Le mieux est d'automatiser la gestion de vos certificats le plus tôt possible pour éviter les pannes dues à une expiration ou à toute autre cause.

Découvrez comment DigiCert peut vous aider à automatiser la gestion des certificats pour vous préparer à des durées de vie plus courtes.