EVERTRUST

Le chemin vers 47 jours de validité des certificats SSL/TLS

Un guide pratique pour les organisations face aux certificats numériques à durée de vie courte

Introduction

Si vous lisez ces lignes, vous êtes sans doute déjà informé de la récente décision du CA/Browser Forum : la durée de validité maximale des certificats SSL/TLS publics sera progressivement réduite à 47 jours.

Cette évolution s'inscrit dans une tendance amorcée il y a plus de 13 ans, au cours desquels la durée de vie des certificats n'a cessé de diminuer. De même, cette réduction progressive, planifiée jusqu'en 2029, s'appuie sur des calendriers clairement définis par les instances de régulation et les principaux acteurs du secteur.

L'objectif est double : renforcer la sécurité globale de l'écosystème numérique et accélérer l'agilité cryptographique, tout en limitant les risques liés à la compromission des identités numériques.

Pour les organisations, il ne s'agit pas d'une simple évolution technique, mais d'un véritable changement de paradigme.

La gestion des certificats devient désormais un processus continu et à haute fréquence, impactant l'ensemble des opérations IT, la conformité réglementaire et la gestion des risques stratégiques.

Le passage aux certificats à courte durée de vie remet en question des pratiques longtemps ancrées et nécessite l'adoption de nouvelles méthodes, car les processus manuels et les outils hérités ne seront plus adaptés à cette nouvelle réalité.

Cependant, au cœur de cette transformation se dessine une véritable opportunité. Les organisations qui sauront s'adapter rapidement ne se contenteront pas de réduire leur exposition aux risques ; elles gagneront également en agilité pour anticiper et se conformer efficacement aux nouvelles normes et exigences réglementaires, au fur et à mesure de leur évolution.

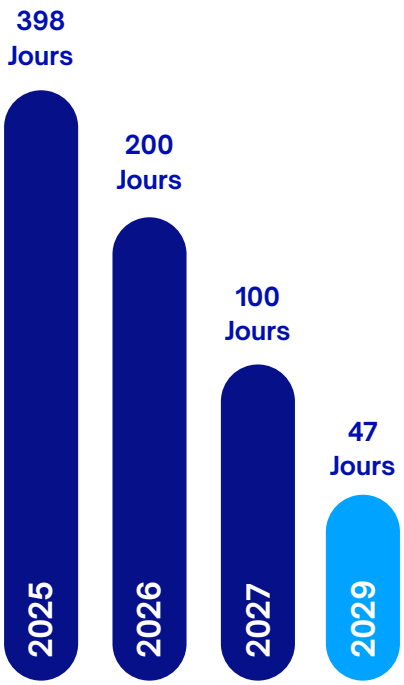
Ce livre blanc se veut votre guide stratégique pour aborder sereinement cette transition. Nous y analyserons les facteurs qui motivent la réduction de la durée de vie des certificats, les répercussions sur l'ensemble de l'écosystème numérique, ainsi que les actions concrètes que votre organisation peut mettre en œuvre pour renforcer sa résilience et préserver la confiance, aujourd'hui comme demain.

L'évolution des durées de vie des certificats SSL/TLS

Comprendre la poussée vers des périodes de validité plus courtes

Les certificats numériques constituent depuis longtemps le socle de la sécurisation des échanges en ligne, garantissant l'authentification des identités et le chiffrement des données sur Internet. Historiquement, les certificats SSL/TLS étaient délivrés pour plusieurs années, offrant une certaine commodité opérationnelle, mais exposant également les organisations à des risques accrus.

En effet, la persistance de clés compromises ou l'utilisation prolongée de standards cryptographiques obsolètes pouvaient fragiliser durablement la sécurité des systèmes. Aujourd'hui, l'une des menaces majeures réside dans la nécessité de migrer vers la cryptographie post-quantique: dans ce contexte, la réduction de la durée de vie des certificats devient un enjeu critique pour limiter l'exposition et renforcer la résilience face aux nouvelles vulnérabilités.



Qui décide de ces changements ?

La réduction de la durée de vie des certificats SSL/TLS n'est pas le fruit d'une décision unilatérale d'un régulateur, mais résulte d'un processus de consensus industriel complexe. Le principal acteur à l'origine de ces évolutions est le CA/Browser Forum, un consortium volontaire créé en 2005.

Parties prenantes clés du CA/Browser Forum

Autorités de certification (CA)

digicert · Let's Encrypt · ENTRUST · SSL.com

Fournisseurs de navigateurs

Google · Edge

Autres parties prenantes

Depuis sa création, ce Forum élabore les Exigences de Base qui encadrent l'émission, la validation et la gestion des certificats publics, constituant ainsi la pierre angulaire des standards de sécurité sur Internet.

Proposition	Débat	Révision	Vote
Soumises au vote	Mois de discussions	Intégration des retours	Adoption formelle

La récente décision de limiter la validité maximale des certificats à 47 jours a été initialement portée par Apple, puis rapidement soutenue par Google. Cette mesure a été adoptée à la suite de débats approfondis réunissant à la fois les autorités de certification (CA) et leurs clients, illustrant la dynamique collaborative et l'importance du dialogue au sein de l'écosystème.

Pourquoi des durées de vie plus courtes ?

L'impératif de sécurité derrière la rotation accélérée des certificats

Réduire la période de validité des certificats SSL/TLS introduit de nouvelles demandes de gestion, mais c'est une étape nécessaire pour renforcer la sécurité numérique.

4 raisons majeures pour des durées de vie plus courtes

1

Minimiser les compromissions

Les durées de vie plus courtes réduisent drastiquement la fenêtre d'opportunité lorsque les certificats sont compromis ou mal gérés.

- Le temps moyen de détection d'intrusion est de 277 jours, plus long que les nouvelles durées de vie des certificats
- Les attaques de détournement de domaine persistent jusqu'à l'expiration du certificat
- La validation faible au moment de l'émission devient obsolète en quelques semaines

2

Pallier les défaillances de révocation

Certains navigateurs contournent ou échouent lors des vérifications de révocation, laissant des certificats révoqués actifs trop longtemps

- L'implémentation OCSP varie selon les navigateurs, créant une protection utilisateur inégale
- Les problèmes de connectivité réseau peuvent empêcher la vérification de révocation en temps réel
- La validation initiale faible devient caduque rapidement

3

Favoriser l'agilité cryptographique

La rotation rapide des certificats permet une adoption plus rapide de nouveaux standards cryptographiques et d'algorithmes résistants aux ordinateurs quantiques.

- Le NIST estime que les ordinateurs quantiques casseront RSA-2048 d'ici 2030
- Les durées de vie actuelles des certificats retardent la migration cryptographique de 1 à 2 ans
- Les cycles de 47 jours permettent des mises à jour d'algorithmes à l'échelle de l'organisation en moins de 3 mois

4

Stimuler l'adoption de l'automatisation

Les renouvellements fréquents rendent la gestion manuelle des certificats impossible, poussant à l'adoption de la gestion automatisée du cycle de vie.

- Les processus manuels causent la majorité des pannes liées aux certificats
- Les cycles de 47 jours nécessitent 8 fois plus d'opérations de renouvellement par an
- L'automatisation gère les changements rapidement et avec un minimum de perturbations

Que se passe-t-il si aucune action n'est entreprise ?

La réduction à 47 jours de la durée de validité des certificats SSL/TLS impose une nouvelle cadence de gestion. Sans adaptation, plusieurs risques majeurs menacent la continuité et la sécurité de votre organisation :

Interruptions de service accrues

L'augmentation du nombre de renouvellements multiplie les risques d'expiration non détectée.
Un certificat expiré peut rendre un site ou une application indisponible, impactant directement l'activité.

Dégradation de la confiance et de l'image

Un avertissement de sécurité ou une interruption de service nuit à la réputation de l'organisation et peut entraîner une perte durable de confiance de la part des clients et partenaires.

Charge opérationnelle excessive

La gestion manuelle devient rapidement chronophage et source d'erreurs, mobilisant les équipes IT sur des tâches répétitives au détriment de projets à plus forte valeur ajoutée.

Non-conformité réglementaire

Le non-respect des exigences de sécurité et de disponibilité peut entraîner des sanctions, des audits défavorables ou des ruptures contractuelles.

Quelle solution?

Face à cette nouvelle réalité, **l'automatisation intelligente s'impose comme la seule réponse viable** à la gestion des certificats SSL/TLS à durée de vie réduite

Le CLM : une approche globale et automatisée

Le Certificate Lifecycle Management offre une vision complète de la gestion des certificats, couvrant l'ensemble de leur cycle de vie : de la découverte initiale à la révocation finale, en passant par l'émission, le déploiement, le renouvellement et la surveillance continue.

Une approche en trois piliers

1 Automatisation du cycle de vie

Éliminer les interventions manuelles chronophages en automatisant l'émission, le renouvellement et la révocation des certificats. Cette automatisation doit être capable de gérer des milliers de certificats simultanément, sans intervention humaine.

2 Visibilité et gouvernance

Disposer d'une vue d'ensemble en temps réel de tous les certificats de l'organisation, qu'ils soient déployés sur des serveurs physiques, dans le cloud, ou sur des conteneurs. Cette centralisation permet un pilotage proactif et une réaction immédiate aux incidents.

3 Expertise humaine

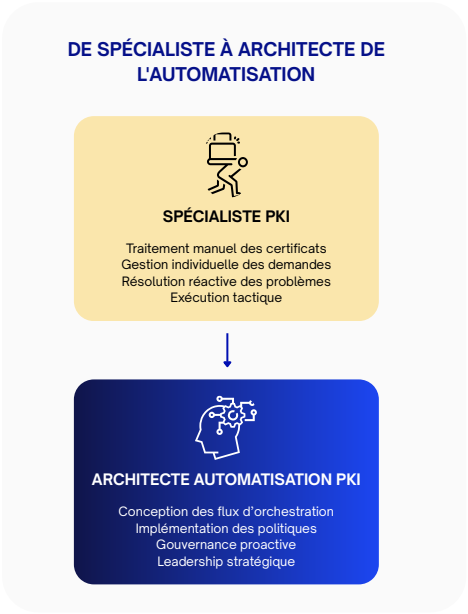
Transformer le rôle des équipes PKI : d'opérateurs tactiques, elles deviennent architectes stratégiques de la sécurité, concevant les politiques et orchestrant l'automatisation plutôt que d'exécuter des tâches répétitives.

L'Humain au cœur de la transformation

À l'ère de l'automatisation, la gestion moderne des certificats connaît une évolution majeure, redéfinissant en profondeur le rôle de l'expert PKI.

Loin de se limiter au traitement manuel des demandes individuelles, ces experts deviennent architectes de la sécurité numérique: ils conçoivent, déploient et optimisent des flux de travail automatisés à l'échelle de l'entreprise, en s'appuyant sur des solutions avancées de gestion du cycle de vie des certificats.

Dans ce contexte, la technologie n'efface pas la valeur humaine : elle la repositionne au cœur de la transformation. L'expertise PKI reste indispensable pour piloter l'automatisation, garantir la conformité, anticiper les risques et accompagner l'organisation dans la transition vers des processus plus agiles et résilients.



Concevoir et piloter l'automatisation

Les experts PKI définissent les stratégies, sélectionnent les outils adaptés (comme ACME), et orchestrent l'intégration des solutions d'automatisation dans l'écosystème existant. Ils s'assurent que les processus automatisés répondent réellement aux besoins métiers et respectent les exigences de sécurité.

Garantir la conformité et la gouvernance

L'humain veille à l'application des politiques internes et réglementaires, attribue les responsabilités et valide les circuits d'approbation. Il adapte en continu les pratiques pour rester conforme aux évolutions des normes et des attentes du secteur.

Anticiper et gérer les risques

Les spécialistes PKI identifient les nouveaux risques liés à la réduction de la durée de vie des certificats, mettent en place des plans de gestion d'incidents, et réagissent rapidement en cas de compromission ou de défaillance technique.

Accompagner le changement et former les équipes

Ils jouent un rôle clé dans la sensibilisation, la formation et l'accompagnement des équipes métiers et IT, afin d'assurer une adoption fluide des nouveaux processus et renforcer la culture de la sécurité.

Si l'expertise humaine reste le moteur de la transformation, elle doit aujourd'hui s'appuyer sur des outils capables de répondre à la complexité et à la fréquence accrue des opérations.

En effet, la multiplication des certificats publics ou privés, et la nécessité d'éviter toute interruption de service rendent la gestion manuelle impossible à grande échelle.

C'est dans ce contexte que le Certificate Lifecycle Management (CLM) s'impose comme une solution incontournable offrant une approche globale et automatisée pour gérer l'ensemble du cycle de vie des certificats : de la découverte à l'émission, du renouvellement à la révocation, en passant par le déploiement et la surveillance continue

› SOLUTION EVERTRUST

Certificate Lifecycle Manager

La gestion orchestrée, de bout en bout

Visibilité totale sur votre parc de certificats

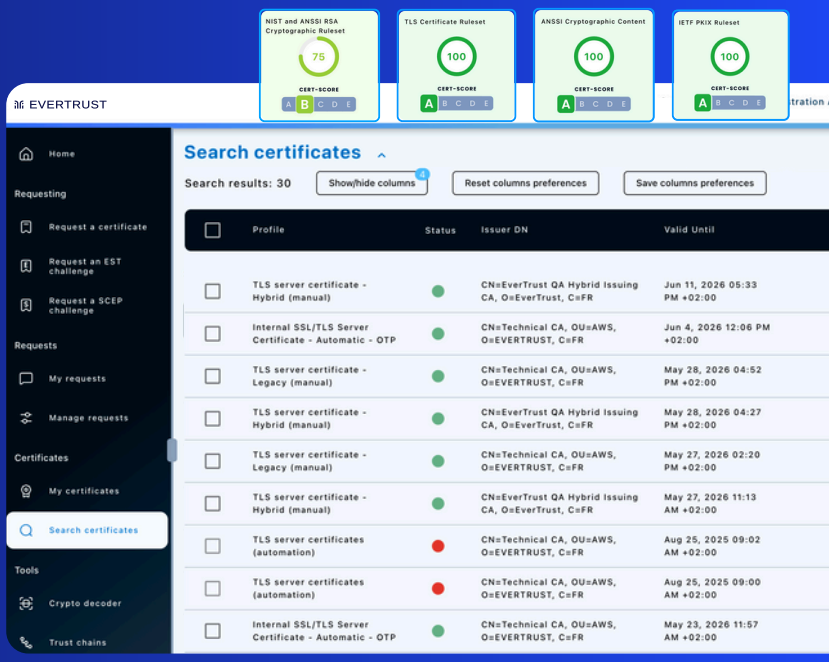
Centralisez et cartographiez instantanée tous vos certificats dispersés : réseau, conteneurs, clouds, workloads, load balancers...

Automatisation complète du cycle de vie

Gérez l'émission, le renouvellement, la révocation et le déploiement de tous vos certificats via des workflows automatisés, en intégrant aussi bien vos PKI internes que les autorités publiques

Alertes intelligentes et prévention des incidents

Recevez des notifications proactives en cas de certificats proches de l'expiration, de non-conformité ou d'incident, avec des tableaux de bord dynamiques pour piloter la sécurité de vos certificats en temps réel et réduire le risque d'interruption



Gestion unifiée des politiques et conformité

Appliquez automatiquement vos politiques de sécurité (algorithmes, longueurs de clé, restrictions CA) sur l'ensemble des certificats et bénéficiez d'une traçabilité complète pour simplifier audits et conformité réglementaire (NIS2, PCI DSS, ISO 27001...)

EVERTRUST

À propos

EVERTRUST est une société Européenne qui développe des solutions de gestion des certificats numériques et d'infrastructure à clés publiques (PKI) pour les entreprises et organisations mondiales.

Fondée en 2017, l'entreprise propose une gamme d'outils couvrant l'ensemble du cycle de vie des certificats numériques : gestion automatisée des certificats publics et privés, autorité de certification privée haute performance, autorité de validation (OCSP) et autorité d'horodatage (TSA).

Basée en France, EVERTRUST est certifiée ISO 27001 et membre d'Hexatrust, du PKI Consortium et de la Microsoft Intelligent Security Association (MISA).

EVERTRUST se positionne aujourd'hui comme un acteur européen indépendant répondant aux enjeux croissants de souveraineté numérique.

+20%

des grands groupes français accompagnés

+30M

certificats gérés via nos solutions

+500K

identités machines gérées via nos solutions

Passez à l'automatisation intelligente et sécurisée

Je contacte EVERTRUST