sectigo

Moderniser la gestion de vos certificats numériques pour atteindre l'agilité cryptographique

Par où commencer et comment procéder

Table des matières

Introduction

De 398 jours à 47 jours : la nouvelle ère des certificats numériques.

La fin du cycle de renouvellement annuel des certificats publics est proche. En avril 2025, le CA/Browser Forum a voté en faveur d'une proposition d'Apple qui réduira, à terme, la durée de validité des certificats à seulement 47 jours. Ce bouleversement majeur de l'industrie est un signal d'alarme : non seulement les équipes devront désormais renouveler les certificats tous les mois, mais elles devront aussi adopter de nouveaux systèmes et de nouvelles méthodes de gestion pour y parvenir.

L'une des principales raisons de ce raccourcissement des cycles est liée à la sécurité future. Avec l'arrivée de l'informatique quantique, le framework de cybersécurité du NIST (National Institute of Standards and Technology) a évolué pour intégrer ce risque imminent. Il exige désormais des organisations qu'elles adaptent leurs pratiques afin de respecter les normes de cryptographie post-quantique.

En résumé, des durées de validité plus courtes permettent de neutraliser rapidement les certificats compromis, de déployer sans attendre de nouveaux algorithmes cryptographiques et de protéger les entreprises à mesure que l'informatique quantique se démocratise.

Définition : Qu'est-ce que l'informatique quantique ?

L'informatique quantique est un domaine de l'informatique qui exploite les principes de la mécanique quantique — tels que la superposition, l'intrication et l'interférence quantique — pour traiter l'information d'une manière impossible pour les ordinateurs classiques.

Au lieu d'utiliser des bits traditionnels (qui ne peuvent représenter qu'un 0 ou un 1), les ordinateurs quantiques utilisent des bits quantiques, ou qubits. Un qubit peut exister simultanément dans une combinaison des états 0 et 1 (grâce à la superposition). Lorsque les qubits sont intriqués, l'état d'un qubit est directement lié à celui d'un autre, quelle que soit la distance qui les sépare. Cela permet aux ordinateurs quantiques d'effectuer certains types de calculs en parallèle, augmentant ainsi leur puissance potentielle de manière exponentielle.

Pourquoi cela concerne votre sécurité numérique

L'informatique quantique permettra, par nature, de casser les algorithmes traditionnels.

Plus précisément, l'algorithme quantique de Shor représente une menace directe pour les systèmes de cryptographie à clé publique les plus répandus, à savoir RSA et ECC (Elliptic Curve Cryptography). Ces algorithmes garantissent la sécurité de la plupart des communications numériques, y compris les certificats à courte durée de vie.

Conscient de ce risque existentiel, le NIST prévoit de supprimer progressivement les algorithmes RSA et ECC entre 2030 et 2035. Cette transition accélérée vers les normes de cryptographie post-quantique (PQC), combinée à l'obligation sectorielle des certificats de 47 jours, impose une action immédiate.

Pour s'engager sur la voie de l'agilité cryptographique, la recommandation essentielle est d'automatiser la gestion du cycle de vie des certificats (CLM - Certificate Lifecycle Management). L'automatisation garantit que les entreprises peuvent basculer rapidement vers les nouveaux algorithmes PQC dès qu'ils sont finalisés et déployés. C'est précisément là que Sectigo intervient.

Le défi

Le compte à rebours commence aujourd'hui.

Le CA/Browser Forum a validé la proposition de réduction de la durée de vie des certificats début 2025, lançant le compte à rebours d'une diminution exponentielle des périodes de validité.

À quoi ressemblera l'avenir ?

Mars 2026 — 398 jours > 200 jours

Mars 2027 — 200 jours > 100 jours

Mars 2029 — 100 jours > 47 jours

L'impact

Les renouvellements, qui s'effectuent actuellement sur un rythme annuel, passeront bientôt à une cadence mensuelle. Cela signifie que les certificats risquent davantage d'être compromis lorsque les ordinateurs quantiques seront capables de casser les algorithmes actuels.

Le risque

Un renouvellement mensuel multiplie par 12 le risque d'oublis ou de révocations manquées. Votre entreprise s'expose ainsi à un risque 12 fois plus élevé d'interruptions de service, de failles de conformité et d'atteinte à sa réputation.

Il n'y a pas que la durée de vie des certificats qui diminue.

Les périodes de validation du contrôle du domaine (DCV) sont également revues à la baisse. La DCV est utilisée par les autorités de certification avant d'émettre un certificat SSL pour vérifier que l'auteur de la demande est bien autorisé à utiliser le domaine concerné. Sans cette validation, aucun certificat ne peut être émis ou déployé. Même les certificats à courte durée de vie doivent passer par cette étape avant leur émission.

Mars 2026 — 398 jours > 200 jours

Mars 2027 — 200 jours > 100 jours

Mars 2029 — 100 jours > 10 jours

L'impact

La réduction des périodes de DCV renforce la sécurité en réduisant la fenêtre de tir des attaquants pour exploiter des clés compromises, et en garantissant que tous les domaines sont bien utilisés par des tiers autorisés.

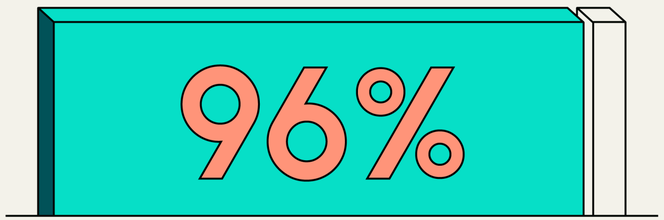
Le risque

La charge de travail manuelle va devenir intenable sur un rythme mensuel, d'autant plus que tous les certificats n'auront pas les mêmes échéances. Cela entraînera des failles de validation, des interruptions de service et des perturbations pour l'activité de l'entreprise.

Pourquoi c'est important

Anticiper est la clé, mais peu d'entreprises sont prêtes.

Le calendrier étant fixé, les entreprises sont instamment priées d'agir dès maintenant. Pourtant, les rapports montrent que beaucoup ne sont pas prêtes et n'ont pas anticipé les étapes concrètes pour atteindre l'agilité cryptographique à temps. Face à ce problème bien réel mais ignoré ou sous-estimé, c'est l'avenir même de la cybersécurité qui est menacé.



des entreprises s'inquiètent de l'impact des certificats de 47 jours sur leur activité.

Moins de 1 sur 5 (19 %) se sent prête pour des renouvellements mensuels.

Seulement 28 % des entreprises disposent d'une visibilité complète sur leurs certificats.

L'impératif stratégique de l'agilité cryptographique

Atteindre l'agilité cryptographique est plus simple que vous ne le pensez.

L'automatisation est la seule voie possible pour gérer les certificats dans un monde post-quantique. Une fois l'informatique quantique standardisée, les algorithmes cryptographiques seront modifiés et émis à une fréquence inédite, exigeant des entreprises une réactivité instantanée pour maintenir la sécurité de leurs systèmes. Sans automatisation, les organisations dépendent d'une gestion manuelle qui mobilise les équipes informatiques au détriment de projets critiques, tout en s'exposant aux risques d'erreurs humaines.

Visibilité

Pour savoir où en sont vos processus, vous devez d'abord cartographier vos certificats.

Utilisez un outil d'inventaire, tel que Discovery de Sectigo Certificate Manager, pour scanner tous vos environnements et recenser l'ensemble des certificats de votre entreprise.

Identifiez ensuite les technologies de votre infrastructure qui participent à leur gestion.

Automatisation

La gestion automatisée du cycle de vie des certificats (CLM) est indispensable pour atteindre l'agilité cryptographique.

Grâce à l'automatisation, les équipes IT peuvent programmer les certificats pour qu'ils se renouvellent tout seuls et s'adaptent automatiquement aux nouvelles normes de conformité.

L'automatisation permet également de s'intégrer aux différents systèmes de l'écosystème de l'entreprise pour s'assurer que rien ne passe entre les mailles du filet.

Agilité cryptographique

L'agilité cryptographique ne peut être atteinte que si l'entreprise a automatisé ses processus. Par définition, l'agilité est la capacité d'agir vite et de manière fluide — face à l'informatique quantique, c'est une question de survie.

Lorsque les algorithmes changeront, les entreprises auront la certitude d'éviter les pannes coûteuses, les violations de données ou les attaques, car l'automatisation se chargera du plus gros du travail.

La menace quantique

Le temps presse : les attaques HNDL et TNFL

	Harvest Now, Decrypt Later (HNDL)	Trust Now, Forge Later (TNFL)
Principe	Les attaquants collectent aujourd'hui des données chiffrées (flux réseau interceptés, fichiers stockés, e-mails, etc.) dans l'espoir de les décrypter plus tard, lorsque les ordinateurs quantiques seront assez puissants (via l'algorithme de Shor qui cassera RSA/ECC).	Plutôt que les données chiffrées, ce risque vise les signatures numériques et l'authentification. Aujourd'hui, les entreprises font confiance aux signatures pour les mises à jour logicielles, les e-mails signés, les certificats ou les transactions blockchain. Demain, les ordinateurs quantiques permettront aux attaquants de falsifier ces signatures « de confiance ».
Exemple	• Un cybercriminel enregistre aujourd'hui tout le trafic VPN ou les sessions TLS. • Ces données sont inutilisables pour le moment (car chiffrées en RSA ou ECC). • Dans 5 à 10 ans, il utilisera un ordinateur quantique pour casser le chiffrement et lire les données en clair (informations historiques sensibles, données médicales, secrets de fabrication).	• Un gouvernement archive des documents signés numériquement avec RSA. • Dans 15 ans, un ordinateur quantique pourrait générer une fausse signature identique à l'authentique. • Des archives historiques, des chaînes d'approvisionnement logicielles ou des documents juridiques pourraient ainsi être falsifiés rétroactivement.
Conséquence	Même si vos données ne semblent pas « importantes » aujourd'hui, elles pourraient être sensibles demain. La confidentialité à long terme est donc menacée.	Même si nous cessons d'utiliser RSA/ECC à l'avenir, les anciennes signatures resteront vérifiables. L'authenticité des preuves numériques passées pourra donc être contestée.

Le "Quantum-Day" approche

Les normes de cryptographie post-quantique du NIST sont prêtes

Un ordinateur quantique suffisamment puissant, utilisant l'algorithme de Shor, sera capable de casser les algorithmes RSA et ECC à une vitesse exponentielle, rendant instantanément vulnérables toutes les données qu'ils protégeaient. Face aux attaques HNDL et TNFL déjà en cours, il est crucial de comprendre les mesures prises par le NIST pour assurer notre sécurité future. Voici les trois principaux algorithmes FIPS (Federal Information Processing Standard) publiés par le NIST pour protéger les identités numériques à l'ère post-quantique.

FIPS 203

C'est la norme principale pour le chiffrement général. Ses points forts résident dans la taille comparativement réduite de ses clés de chiffrement (faciles à échanger entre deux parties) et sa vitesse d'exécution. Elle s'appuie sur l'algorithme CRYSTALS-Kyber, rebaptisé ML-KEM (Module-Lattice-Based Key Encapsulation Mechanism).

FIPS 204

C'est la norme principale pour la protection des signatures numériques. Elle utilise l'algorithme CRYSTALS-Dilithium, rebaptisé ML-DSA (Module Lattice-Based Digital Signature Algorithm).

FIPS 205

Également conçue pour les signatures numériques, cette norme emploie l'algorithme Sphincs+, rebaptisé SLH-DSA (Stateless Hash-Based Digital Signature Algorithm). Elle repose sur une approche mathématique différente de celle de ML-DSA et sert de méthode de secours au cas où ML-DSA s'avérerait vulnérable.

[Source: National Institute of Standards and Technology]

La solution

N'attendez pas pour automatiser.

Les menaces HNDL et TNFL seront les plus redoutables une fois l'informatique quantique démocratisée. Que pouvez-vous faire dès aujourd'hui pour protéger proactivement votre entreprise ? **Automatiser**.

La gestion manuelle est déjà chronophage, source d'erreurs et hautement risquée ; la situation va encore s'aggraver. Sans les rapports d'un système automatisé, vous n'avez aucune visibilité sur votre parc de certificats, aucun contrôle de la conformité, et vous dépendez d'humains pour réagir rapidement, 24 heures sur 24, lorsque les ordinateurs quantiques briseront les algorithmes. La gestion manuelle revient à attendre que la crise éclate.

Un CLM automatisé est rapide et s'adapte à la taille de votre entreprise, vous maintenant en conformité avec les dernières mises à jour et garantissant votre résilience à l'ère quantique. Grâce à votre capacité à pivoter rapidement et à suivre l'ensemble de vos certificats, la probabilité que votre entreprise subisse une interruption de service devient quasi nulle.

L'automatisation est aussi synonyme d'économies.

Il est évident que la trajectoire vers l'agilité cryptographique passe par l'automatisation. Non seulement elle offre un système clair, conforme et évolutif pour l'informatique post-quantique, mais elle permettra également à votre entreprise de réaliser des économies à long terme. Si elle représente un investissement aujourd'hui, elle fera demain la différence entre une journée de travail ordinaire et une panne qui coûterait des millions à votre entreprise.

Sectigo propose une plateforme CLM centralisée : Sectigo Certificate Manager (SCM). Vos certificats publics et internes sont regroupés sur un seul tableau de bord, doté d'une interface universelle (indépendante de l'autorité de certification) qui vous permet de découvrir, d'émettre, de déployer et de renouveler vos certificats, quel que soit l'organisme émetteur.

"L'automatisation a rendu le déploiement rapide et facile pour les centaines de certificats que Medecision gère actuellement."

David Lundy, Vice-président, Succès Client chez Medecision

À l'ère de l'informatique post-quantique, il est essentiel de s'assurer que votre plateforme automatisée est prête pour l'avenir. Nos experts sectoriels président le CA/Browser Forum, sont membres de l'organisation de sécurité ETSI et travaillent sans relâche à perfectionner nos solutions pour faire de Sectigo le fournisseur de CA et de CLM le plus fiable du marché.

"SCM vous transmet des mises à jour proactives concernant toutes les évolutions de l'écosystème SSL, y compris les alertes et les problèmes de sécurité, et garantit qu'aucun certificat n'expire de manière imprévue. Toutes ces fonctionnalités permettent à votre entreprise de s'appuyer sur une infrastructure IT qui reste totalement sécurisée."

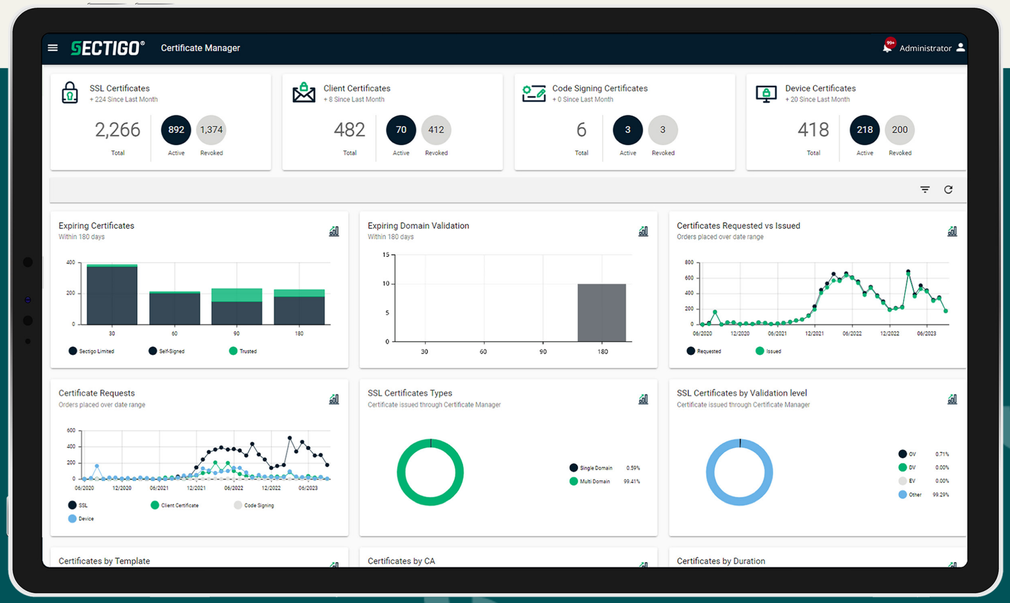
Andrew Rust, Responsable technique chez Aviva

Le ROI de Sectigo Certificate Manager

243% de ROI

Amortissement en < 6 mois

Valeur actuelle net de 3,9 M$



Conclusion

Le plan d'action.

Agir maintenant pour assurer l'avenir.

Nos experts ont élaboré un plan d'action pour mettre en œuvre l'automatisation et se préparer à la première réduction de la durée de vie des certificats (qui passera à 200 jours en mars 2026), et au-delà.

Le monde des certificats numériques est resté relativement stable pendant de nombreuses années. Tout cela est sur le point de changer. L'adoption de la validité de 47 jours n'est que le début d'une transformation rapide du secteur et de l'avenir du CLM. Face à une menace d'attaque qui pourrait devenir un problème massif demain, agir le plus tôt possible pour renforcer la sécurité de votre entreprise constitue une police d'assurance indispensable.

À mesure que l'échéance quantique se rapproche du "Jour Q", vos systèmes manuels ne feront que devenir un fardeau. Sans transition vers l'automatisation dès aujourd'hui, votre entreprise devra réagir dans l'urgence aux changements d'algorithmes. L'automatisation n'est plus un confort, c'est un outil de mission critique. N'attendez pas : automatisez dès aujourd'hui pour économiser du temps, de l'argent et réduire les risques dans un avenir post-quantique.

Les étapes clés à franchir :

À court terme (0-6 mois)

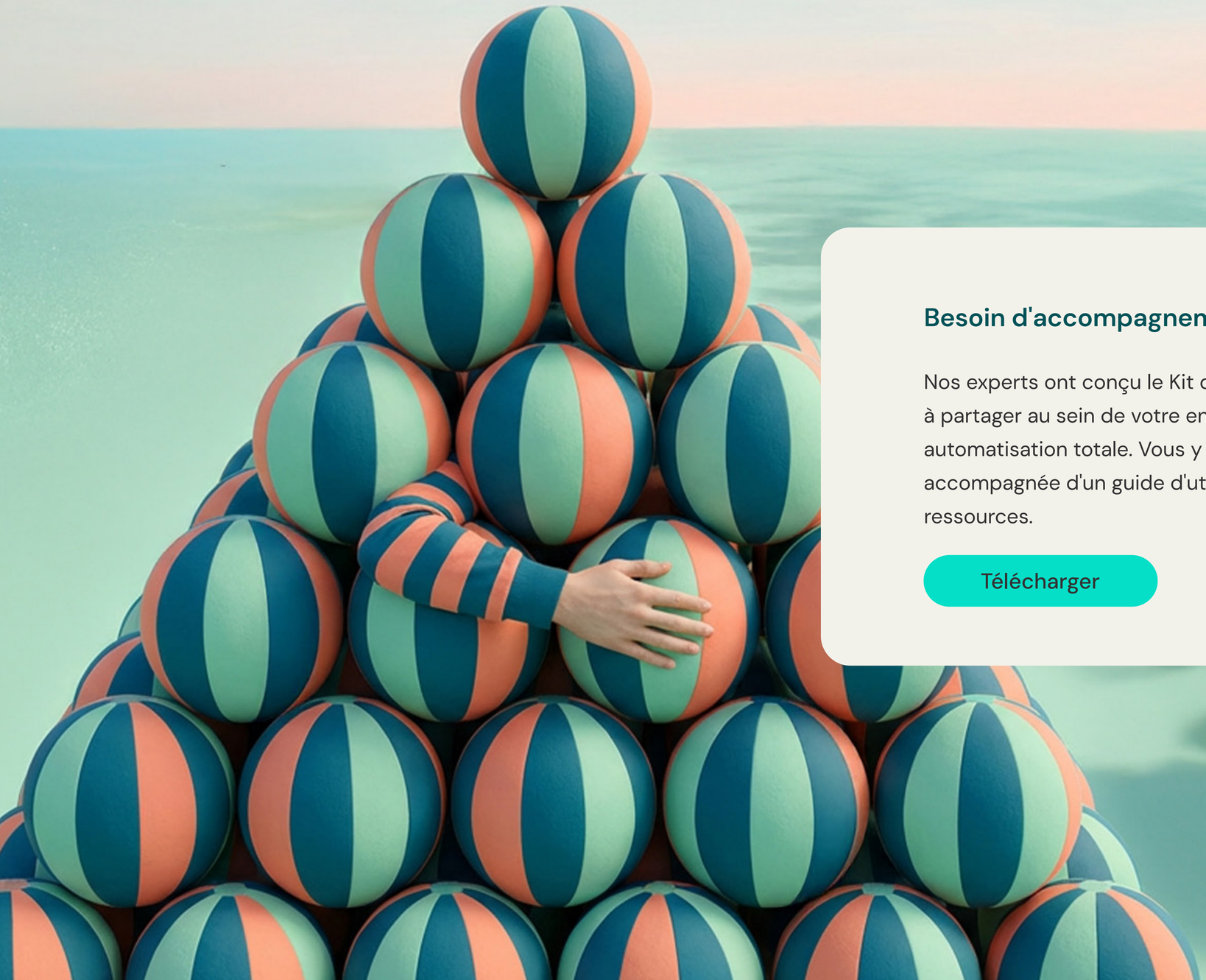
Faîtes l'inventaire de vos certificats et de votre infrastructure technologique, et commencez à intégrer au moins une automatisation

À moyen terme (6-18 mois)

Déployez un CLM complet, intégrez-le à vos outils DevOps et alignez-vous avec votre fournisseur.

À long terme (18 mois et +)

Créez un Centre d'Excellence Cryptographique et adoptez la migration vers la cryptographie post-quantique (PQC).



Besoin d'accompagnement ?

Nos experts ont conçu le Kit de ressources 47 jours, un guide complet d'outils à partager au sein de votre entreprise pour amorcer la transition vers une automatisation totale. Vous y trouverez notre méthode exclusive en 5 étapes accompagnée d'un guide d'utilisation pour tirer le meilleur parti de nos ressources.

Télécharger

sectigo

À propos de Sectigo

Sectigo est le fournisseur le plus innovant en matière de gestion du cycle de vie des certificats (CLM), offrant des solutions complètes qui sécurisent les identités humaines et machines pour les plus grandes marques mondiales. La plateforme CLM automatisée et cloud-native de Sectigo émet et gère les certificats numériques à travers toutes les autorités de certification (CA) afin de simplifier et d'optimiser les protocoles de sécurité au sein des entreprises. Sectigo est l'une des autorités de certification les plus importantes, les plus anciennes et les plus reconnues, comptant plus de 700 000 clients et deux décennies d'expertise au service de la confiance numérique.

Contactez-nous

© 2026 Sectigo. Tous droits réservés.