Gestion des certificats : le guide ultime

Bonnes pratiques d'administration de centaines, voire de milliers de certificats SSL/TLS

digicert®

Sommaire

Introduction

Gérer un portfolio de certificats demande une vigilance de tous les instants : un certificat oublié ou expiré, et c'est tout un enchaînement de coûts et d'ennuis qui guette votre entreprise. Pour les grandes structures, une panne liée à un problème de certificat se solde par une perte sèche de 15 millions de dollars en moyenne.[1] Sans compter les répercussions en termes de sécurité et de réputation, avec dans leur sillage une perte de confiance des clients et une chute des ventes.

En tant qu'administrateur du portfolio de certificats, vous êtes probablement chargé de piloter toutes les variables de l'infrastructure PKI de votre entreprise (gestion des certificats, approbations rapides, respect des bonnes pratiques SSL/TLS, etc.).

L'une des hantises de votre métier, c'est de se dire que quelque part sur votre réseau, un certificat échappe à la vigilance de vos systèmes de contrôle. Si bien qu'un jour ou l'autre, un serveur tombera en panne et vous devrez recoller les morceaux.

Imaginez maintenant une sorte de checklist géante, capable de vous indiquer sur quelles phases du cycle de vie de vos certificats vous concentrer pour préserver la sécurité de votre réseau.

Comme chaque environnement a ses spécificités, il n'existe évidemment pas de checklist universelle, sorte de modèle passe-partout. Certaines responsabilités sont toutefois communes à tous les gestionnaires de certificats pour assurer la sécurité des données, des salariés et de leur entreprise en général.

De la maîtrise du cycle de vie de vos certificats à l'optimisation de la performance de vos équipes, en passant par l'utilisation des API, ce guide vous livre toutes les clés d'une gestion efficace et sans faille de vos certificats.

Cap sur une gestion PKI parfaitement maîtrisée

Autorité de Certification, autorité d'enregistrement, politiques de certificats, système de gestion des certificats... jongler entre les différentes composantes d'une infrastructure PKI n'est pas de tout repos. Certes, déployer un certificat n'a rien de compliqué a priori, mais ce déploiement doit s'accompagner d'une bonne gestion pour maintenir la sécurité de votre entreprise.

Dans les grandes structures, les administrateurs SSL/TLS gèrent des milliers, voire des millions de certificats. Dans ce type d'environnement, comment s'assurer que chaque certificat est déployé et géré comme il se doit, jour après jour, semaine après semaine ?

Le problème : garder le contrôle. La solution : implémenter de bonnes pratiques pour améliorer votre visibilité, économiser du temps et simplifier votre quotidien.

En appliquant ces préceptes, vous troquez un souci permanent contre la sérénité que procure un réseau sécurisé.

Bonne pratique n°1 : utilisez une plateforme de gestion MPKI

Les solutions Managed PKI (MPKI) permettent aux entreprises de gérer et commander leurs certificats, sans les coûts associés à la gestion d'une Autorité de Certification en interne. Parmi les Autorités de Certification les plus réputées, nombreuses sont celles qui offrent des solutions MPKI. La majorité des grandes entreprises optent pour ce choix en raison des avantages financiers notamment.

Avec une solution MPKI, une grande partie des efforts liés au maintien d'une infrastructure PKI interne sont délégués à une Autorité de Certification externe, sans aucune concession sur votre sécurité.

[1] 2015 Cost of Failed Trust Report: When Trust Online Breaks, Businesses Lose Customers. Consulté le 26 juin 2017. https://www.venafi.com/assets/pdf/wp/Ponemon-When-Trust-Online-Breaks-Businesses-Lose-Customers-white-paper.pdf

Mieux encore, vous simplifiez tous les aspects de la gestion du cycle de vie de vos certificats (émission, inspection, résolution de problèmes et renouvellement).

Une solution MPKI vous permet donc de gagner du temps pour mieux vous concentrer sur le suivi des détails importants de vos certificats. À savoir :

- Dates d'expiration
- Erreurs sur les terminaux SSL/TLS
- Demandes de certificats émises par vos collègues
- Révocations éventuelles
- Autorités de Certification émettrices

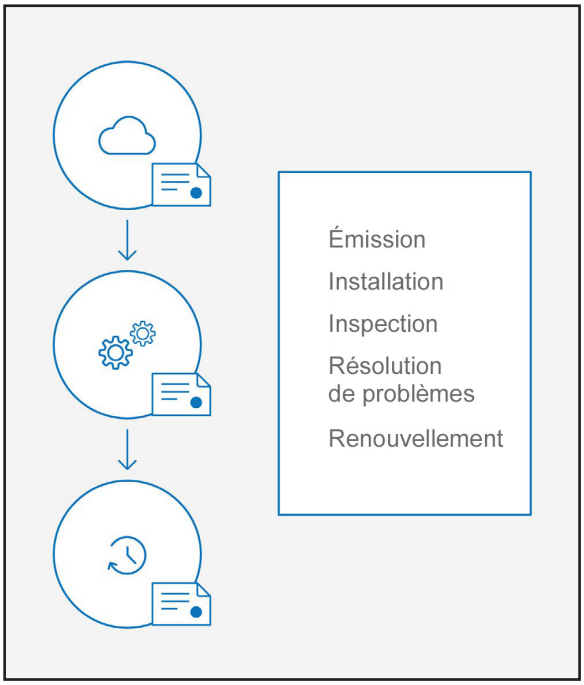
Il y a quelques années encore, nombre d'entreprises géraient leurs certificats à l'aide de simples tableurs. Selon TechTarget (et vous le savez probablement par expérience), « c'est là le meilleur moyen de commettre des erreurs, comme des omissions, de mauvaises assignations ou des libellés de certificats erronés. »[2]

Avec une plateforme MPKI, fini les tableurs et les requêtes par e-mail. Le suivi des détails et la gestion des demandes de certificats sont largement automatisés, réduisant du même coup le risque d'erreur humaine. Résultat : une gestion des certificats plus simple et moins chronophage.

Bonne pratique n°2 : misez sur les API pour automatiser

En donnant aux développeurs un accès à une multitude de technologies, les API gomment les frontières entre entreprises. En matière de gestion des certificats, une API facilite l'automatisation et la personnalisation des opérations pour les équipes IT.

UNE PLATEFORME MPKI SIMPLIFIE LA GESTION DU CYCLE DE VIE DES CERTIFICATS



Si l'interface utilisateur d'un outil de gestion SSL/TLS peut convenir aux petites entreprises, les grandes structures ont pour leur part besoin d'une solution plus personnalisée. En ce sens, certains outils de gestion PKI vous donnent accès à une API permettant de personnaliser vos workflows et fonctionnalités, mais aussi d'automatiser vos processus pour réduire le nombre d'interventions manuelles. Une API peut donc se révéler extrêmement utile pour adapter votre administration SSL/TLS à vos besoins.

[2] Shapland, R., SSL Certificate Management: Avoiding Costly Mistakes. Consulté le 26 juin 2017. http://searchsecurity.techtarget.com/tip/SSL-certificate-management-Common-mistakes-and-how-to-avoid-them

Vous êtes ainsi équipé pour gérer des milliers, voire des millions de certificats selon votre secteur. En plus de vous simplifier la vie, l'automatisation vous permet de réduire le risque d'erreur humaine et de pannes liées à des problèmes de certificats, avec à la clé un niveau de sécurité renforcé.

L'automatisation vous fait aussi économiser du temps sous bien des aspects du cycle de vie de vos certificats SSL/TLS. Par exemple :

- Demandes de certificats
- Approbation de demandes de certificats
- Refus de demandes de certificats
- Téléchargement de certificats
- Renouvellement de certificats
- Révocation de certificats
- Réémission de certificats

Avec l'évolution des standards et le raccourcissement des périodes de validité des certificats SSL/TLS, l'automatisation ne sera bientôt plus une option, mais une nécessité absolue.

Enfin, le recours à une API réduit la complexité inhérente à la gestion de certificats émis par diverses Autorités de Certification. En écartant les demandeurs de l'équation, vous améliorez votre maîtrise du processus de renouvellement : lorsque vous automatisez le renouvellement de vos certificats dont l'expiration est prévue dans 90, 60 ou 30 jours, vous ne vous souciez plus de savoir si l'un de vos collaborateurs passera ou non la commande auprès de l'Autorité de Certification en question, car la tâche est déjà programmée.

Une API est donc le meilleur moyen d'économiser du temps en automatisant et en personnalisant votre gestion des certificats.

Bonne pratique n°3 : décelez les certificats oubliés

Les certificats inconnus ou non autorisés sont la bête noire des administrateurs SSL/TLS. Leur présence s'explique par un triple phénomène : l'augmentation générale du nombre de certificats en circulation, la multiplication des personnes habilitées à commander et installer des certificats, et la rotation des effectifs au sein des entreprises. Ces certificats « sauvages » sont problématiques dans la mesure où ils passent inaperçus. Or, comment gérer quelque chose dont on ignore l'existence ?

Avec un outil d'inspection, vous bénéficiez à la fois d'une visibilité générale et d'une analyse granulaire de votre portfolio de certificats. De nombreuses Autorités de Certification offrent des outils d'inspection conçus pour la recherche de certificats et l'agrégation d'informations issues des analyses de votre environnement. Dans le meilleur des scénarios, ces outils recensent tous les certificats déployés sur votre réseau, quelle que soit l'Autorité de Certification émettrice. Ils vous permettent ainsi d'éviter toute erreur due à un suivi manuel, sans compter qu'ils accélèrent aussi considérablement la tenue de vos inventaires.

Dès lors qu'elles sont effectuées au moins une fois par semaine, ces analyses vous offrent une visibilité complète sur vos certificats actifs et facilitent la détection précoce d'éventuels problèmes, y compris des certificats sauvages qui menaceraient l'intégrité de votre marque. Une fois ces certificats découverts, la résolution du problème n'est plus qu'une formalité.

Bonne pratique n°4 : organisez votre équipe

Une bonne gestion de vos certificats passe par une bonne gestion des collaborateurs en charge de votre infrastructure PKI.

Donnez à vos salariés les moyens d'accomplir leurs missions : répartissez-les en équipes ou départements, attribuez-leur des droits d'accès adaptés, assurez-vous qu'ils comprennent bien leurs responsabilités et informez-les au moindre changement des processus en place.

SEGMENTEZ VOTRE ENTREPRISE

Pour simplifier la demande de certificats affluant du monde entier, il est important de structurer vos équipes en pôles, unités ou départements distincts. Les demandes sont ainsi réparties en fonction de leur provenance, leur adresse IP ou tout autre critère de classement.

Ce type d'organisation se révèle particulièrement utile lors de la réception de demandes incomplètes : vous savez alors à qui vous adresser pour obtenir les données manquantes. Et en cas d'expiration inopinée d'un certificat, vous êtes en mesure de remonter jusqu'à la personne concernée.

ASSIGNEZ DES RÔLES

Pour maintenir le contrôle de votre infrastructure PKI, il est essentiel d'assigner un rôle précis à chacun de vos collaborateurs. En attribuant les bons droits d'accès aux bonnes personnes, vous créez les conditions d'un suivi plus rationnel et de renouvellements plus sereins.

Commencez par examiner où et comment vos collaborateurs interviennent dans les processus. Quel que soit leur rôle (utilisateur régulier, administrateur avec droit d'approbation des demandes, etc.), vos utilisateurs doivent accéder à votre plateforme de gestion des certificats dans le cadre des pouvoirs qui leur sont conférés. De plus, en donnant aux utilisateurs la possibilité de formuler eux-mêmes leurs demandes, vous vous libérez d'une tâche facilement délégable à des collaborateurs compétents.

Concernant les demandeurs ponctuels, vous pouvez leur accorder un accès limité et temporaire à titre d'invités. Vous préservez ainsi la sécurité de vos certificats en n'octroyant un accès qu'aux personnes qui en ont réellement besoin.

SENSIBILISEZ VOS ÉQUIPES

Informer vos effectifs sur vos processus et les former à de nouveaux outils est un effort permanent.

Pour déployer et gérer vos certificats, vos développeurs et vos administrateurs système ont besoin de connaissances techniques spécifiques. Vous partagez les mêmes objectifs, alors n'hésitez pas à les consulter lors de vos prises de décisions.

Pensez également à les maintenir informés de tout changement de politique ou règlement. De votre côté, n'oubliez pas de suivre régulièrement les communications du CA/Browser Forum ou le blog de votre fournisseur SSL/TLS privilégié pour rester en prise permanente avec les tendances et l'évolution des standards.

Bonne pratique n°5 : accélérez votre processus d'approbation

L'émission d'un large volume de certificats impose une parfaite maîtrise de votre infrastructure PKI pour accélérer et simplifier le processus d'approbation. Dès lors que vous collaborez avec une Autorité de Certification très prompte à valider vos demandes, le seul point de blocage se situe généralement au niveau de l'administrateur chargé de l'approbation en interne.

Comment y remédier ? Si vous avez bien organisé vos utilisateurs et vos départements, envoyez les e-mails de vérification directement à l'administrateur concerné. Il n'aura alors qu'à vérifier les données et donner son feu vert. Plus besoin de tourner en rond à la recherche de la bonne personne : vos certificats sont déployés dans la foulée de leur validation.

Bonne pratique n°6 : soyez attentifs aux notifications

L'absence de notifications est un vrai problème pour les administrateurs SSL/TLS. Sans elles, certains certificats risquent de ne pas être renouvelés, avec les problèmes de sécurité que cela entraîne. Si vous ne deviez recevoir qu'un type de notification, ce devrait être pour vos certificats sur le point d'expirer. Mais le reste du cycle de vie n'est pas à négliger pour autant. D'autres notifications pourront notamment vous être très utiles pour les demandes de certificats en attentes, les révocations récentes ou encore les certificats à réémettre.

C'est là que les tableurs montrent leurs limites : ils ne peuvent ni évoluer, ni envoyer de notifications. Certains administrateurs programment des rappels dans leur calendrier Outlook aux dates de renouvellement. Cette méthode est néanmoins risquée : l'administrateur peut en effet oublier d'activer une alarme ou quitter l'entreprise sans transmettre l'information à ses collègues, sans compter les autres imprévus d'ordre technique ou humain. Conclusion : les tableurs ne sont pas une solution.

De plus, lorsqu'un certificat doit être renouvelé et que son responsable omet de le faire, il vous revient d'identifier cette personne au plus vite, de déterminer si le certificat est utilisé ou non, et sur quel serveur il est installé. Inutile de dire que plus vite vous en serez notifié, plus vite vous interviendrez.

Il est également important d'établir des procédures en cas de problèmes spécifiques. Imaginez qu'un certificat expire dans 7 jours. Il est impératif que vous en soyez immédiatement alerté. Si la notification vous arrive à temps, vous pourrez agir avant qu'il ne soit trop tard. Grâce à ce genre de précautions, vous éviterez les expirations de certificats inopinées pouvant entraîner la paralysie d'un serveur.

Bonne pratique n°7 : surveillez votre réseau et générez des rapports

Moins de visibilité sur votre réseau, c'est aussi plus de soucis pour vous. Avec une plateforme MPKI, vous pouvez restituer sur un seul et même tableau de bord les détails de tous vos certificats captés lors de vos analyses réseau. Cette console centralisée vous permet d'effectuer des inspections plus poussées.

Vous bénéficiez ainsi d'éclairages concis sur votre portfolio de certificats pour évaluer l'état général de votre réseau en un coup d'œil. Vous profitez également d'une visibilité sur les expirations à venir, les terminaux vulnérables et les demandes de certificats en attentes, pour ne citer que ces quelques exemples.

Cette surveillance de tous les instants est sans doute la meilleure garante d'une visibilité totale sur votre environnement.

En effet, la combinaison des fonctions de recherche et de reporting peut considérablement améliorer votre compréhension et votre maîtrise de votre portfolio de certificats.

Voici quelques conseils pour en exploiter le plein potentiel :

- Déployez un agent pour l'analyse de votre réseau et la création d'un rapport au moins une fois par mois
- Si possible, automatisez vos analyses à l'aide d'un script
- Intervenez sur les terminaux vulnérables après chaque analyse
- Approuvez les demandes de certificats aussi vite que possible
- Optez pour des renouvellements automatiques pour éviter les pannes

En surveillant ainsi votre réseau, de près comme de loin, vous effectuez une inspection continue, indispensable à la gestion du cycle de vie de vos certificats.

Bonne pratique n°8 : utilisez un outil de détection des vulnérabilités

Une nouvelle vulnérabilité peut se déclarer à tout moment. D'où l'importance de pouvoir résoudre les problèmes rapidement.

Selon un rapport Bay Dynamics publié en 2017, 74 % des équipes de sécurité se disent débordées par la gestion des vulnérabilités dans les très grandes entreprises. Et pour cause : elles se retrouvent parfois face à plus d'un million de failles sur leurs systèmes.

« La gestion et la neutralisation de toutes les vulnérabilités fait peser une énorme pression. »[3]

Au moment où vous lisez ces lignes, certaines de ces vulnérabilités pourraient bien menacer votre portfolio SSL/TLS. Or, un certificat ne vous protégera que partiellement si vous utilisez un chiffrement obsolète ou des versions SSL/TLS vulnérables.

[3] Monahan, D., A Day in the Life of a Cyber Security Pro. Consulté le 26 juin 2017. https:// baydynamics.com/content/uploads/2017/05/4-19-17-FINAL-EMA-A-Day-in-the-Life-of-a-Security-Pro.pdf

Pour gérer les vulnérabilités sur vos terminaux SSL/TLS plus sereinement, optez pour un outil qui pourra analyser votre réseau, rechercher les vulnérabilités et fournir des informations sur vos points faibles..

Ces outils se révèlent particulièrement utiles quand ils repèrent une vulnérabilité et établissent le lien avec les terminaux affectés. Vous pouvez alors intervenir sûrement et rapidement.

Bonne pratique n°9 : choisissez une plateforme tout-en-un

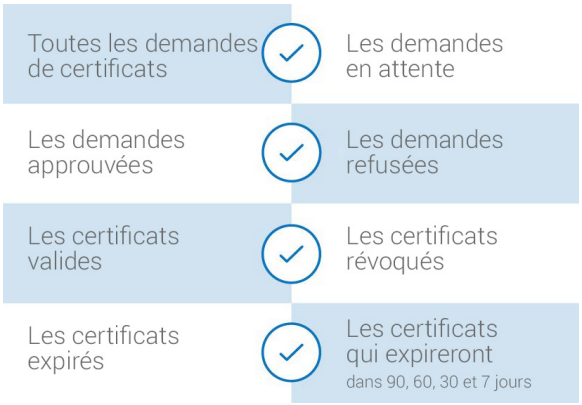
Simplifiez-vous la vie, optez pour une plateforme de gestion des certificats qui réponde à tous vos besoins :

- Solution MPKI
- Tableau de bord complet
- Automatisation à l'aide d'API
- Recherche de certificats
- Segmentation et attribution de rôles utilisateur
- Configuration de notifications et procédures d'escalade en cas de problèmes
- Détection des vulnérabilités

Votre plateforme est l'instrument qui vous permet de garder le contrôle sur votre infrastructure PKI et de gérer le cycle de vie de vos certificats (émission, installation, inspection, résolution de problèmes et renouvellement).

La plateforme CertCentral® de DigiCert est une suite logicielle de gestion des certificats taillée pour les besoins des grandes entreprises. Sa mission : simplifier vos opérations de gestion, personnaliser vos workflows et automatiser l'émission de vos certificats.

SURVEILLEZ VOTRE RÉSEAU DANS SES MOINDRES RECOINS. POUR CE QUI EST DE VOS CERTIFICATS, GÉNÉREZ DES RAPPORTS POUR :



Grâce à l'API DigiCert Services, les administrateurs SSL/TLS peuvent automatiser tous les processus ou presque. L'API peut en effet s'intégrer à des applications tierces et s'adapter à d'autres outils.

Avec une plateforme tout-en-un conçue pour surveiller, gérer, rechercher vos certificats et détecter d'éventuelles vulnérabilités, vous bénéficiez de la visibilité indispensable sur votre réseau. Ajoutez à cela une organisation rigoureuse de vos équipes, une segmentation précise et une répartition claire des rôles de chacun, et vous parviendrez à une maîtrise totale de votre portfolio de certificats.

Choisir CertCentral, c'est opter pour la sérénité.

Pour plus d'infos sur CertCentral® ou nos API,contactez notre service commercial au 1 855 800 3444 ou écrivez-nous à sales@digicert.com.

digicert®