Automatisation de PKI d’entreprise

UN LIVRE BLANC DE SECTIGO

SECTIGO®

Les entreprises ont besoin d'une solution d'authentification qui répondent à des exigences de plus en plus complexes

Les besoins en matière d'authentification dans les entreprises sont de plus en plus complexes. Les applications et les données se trouvent dans des environnements multi-Cloud, le personnel est dispersé et des terminaux innovants doivent être connectés. Tout cela aboutit à la nécessité d'adopter une solide approche de l'identité numérique afin de se protéger de menaces en constante évolution.

Les entreprises se reposent sur les certificats de PKI, qui sont la référence absolue, pour garantir les identités et comme fondement du modèle Zero Trust, une architecture sans mots de passe pour l'identité des utilisateurs, des terminaux, des serveurs et des applications.

Bien qu'il n'y ait pas de solution plus robuste et plus simple pour l'authentification et le chiffrement que l'identité numérique fournie par la PKI, déployer et gérer des certificats représente un défi pour les équipes informatiques qui demande beaucoup de temps et peut engendrer des interruptions de service inutiles. Qu'une entreprise déploie un seul certificat SSL pour un serveur Web ou gère des millions de certificats pour les identités de tous ses terminaux et utilisateurs en réseau, le processus d'émission, de configuration et de déploiement de certificats, de bout en bout, peut prendre des heures par certificat. Pour une entreprise, gérer des certificats manuellement présente aussi le risque d'oublier des certificats jusqu'à leur expiration et de connaître des problèmes de propriété, avec pour résultat l'interruption soudaine de systèmes essentiels à l'activité.

Coût financier de la gestion manuelle des certificats

Les environnements déjà complexes étant en pleine expansion, avec l'inclusion de terminaux mobiles, d'infrastructures de Cloud, de DevOps, de l'Internet des objets, etc., le coût financier d'une gestion efficace des certificats de PKI a fortement augmenté.

L'investissement le plus efficace dans la sécurité est celui qui est à la fois facile à mettre en place et facile à utiliser par les employés. Mais les solutions pour la sécurité telles que les mots de passe demandent aux utilisateurs de se rappeler, de mettre à jour et de gérer leur propre sécurité. Et les équipes informatiques sont submergées de demandes de réinitialisation de mots de passe, qui leur prennent beaucoup de temps, et doivent former les employés à ne pas donner leurs mots de passe face à des tentatives d'hameçonnage sophistiquées. Par exemple, si des employés ne peuvent pas faire de chiffrement/déchiffrement sur leur terminal mobile, ils passent simplement outre le chiffrement des e-mails.

De plus, vos clients et vos utilisateurs internes comptent sur des systèmes professionnels essentiels toujours actifs. L'expiration de certificats a déjà conduit à de nombreuses interruptions de services et d'arrêts de sites Web de grande ampleur, coûtant des millions de dollars en pertes de revenus, en pénalités contractuelles et en procès, sans compter les dommages considérables en matière d'image de marque.

Une gestion déficiente des certificats peut aussi mettre une entreprise en situation de ne plus respecter la réglementation. Afin de se protéger contre le vol d'informations, des règlements tels que l'HIPAA/HITECH, le RGPD et les règles d'acquisition fédérales aux É.-U. (DFARS) exigent le chiffrement des données pour combattre ou limiter les conséquences d'une violation ou d'une divulgation accidentelle. Ne pas respecter les exigences de conformité peut entraîner de fortes amendes. En outre, le RGPD stipule que les amendes se basent non seulement sur l'ampleur de la violation, mais aussi sur le niveau de négligence. Mettre en place une protection robuste sur vos systèmes et terminaux aide donc à réduire le risque de violation, mais cela permet également de limiter le montant de l'amende s'il y a violation.

Addition rapide de coûts d'administration

La gestion de certificats peut être perçue comme une tâche quotidienne simple pour un administrateur Web ou informatique, mais s'assurer que chaque certificat est valide prend beaucoup de temps. Utiliser des processus manuels pour détecter, installer, suivre et renouveler tous les certificats de PKI d'une entreprise demande énormément de travail et est techniquement difficile.

Par exemple, la simple installation manuelle d'un certificat SSL avec un seul domaine Web implique plusieurs étapes et peut coûter facilement plus de $50 par serveur Web. La figure 1 détaille les étapes qu'un administrateur Web doit effectuer pour correctement installer un seul certificat SSL. Pour une entreprise possédant 2 000 serveurs Web, cela exigerait d'avoir une personne à temps plein pour simplement renouveler les certificats avant leur expiration.

Figure 1 – Étapes nécessaires à l'installation manuelle de certificats SSL

Étapes	Durée
Choix/Achat de certificats SSL	De quelques minutes à plusieurs heures
Connexion SSH au serveur Web	< 2 minutes. Recherche de l'adresse et des informations d'authentification du serveur.
Saisie de commandes pour valider le contrôle de domaine (pour un nouveau domaine)	De quelques minutes à plusieurs heures. Lecture de la documentation, saisie des commandes adéquates. Les forums d'administrateurs Web sont remplis de questions/réponses et de solutions de dépannage, ce qui indique qu'ils sont nombreux à rencontrer des problèmes lors de cette étape.
Demande d'émission du certificat et téléchargement	Jusqu'à 5 à 10 minutes. Lecture de la documentation, saisie des commandes adéquates.
Copie des fichiers de certificat à l'emplacement prévu sur le serveur (varie selon le serveur Web)	< 2 minutes. Recherche de l'emplacement pour le fichier serveur, saisie des commandes adéquates.
Modification du fichier de configuration du serveur Web pour que ce dernier puisse utiliser le certificat SSL et publier le https	De quelques minutes à plusieurs heures. Lecture de la documentation, saisie des commandes adéquates, sauvegarde du fichier. Les forums d'administrateurs Web sont remplis de questions/réponses et de solutions de dépannage, ce qui indique qu'ils sont nombreux à rencontrer des problèmes lors de cette étape.
Mise à jour/Redémarrage du serveur Web afin d'appliquer la configuration	< 1 minute
Test Toutes les étapes ci-dessus doivent être réalisées scrupuleusement. Sinon, le temps passé et le travail effectué seront vains et des systèmes essentiels à l'activité se trouveront hors service.	De quelques minutes à plusieurs heures. En l'absence de messages d'erreur, le test est rapide. Prendre des mesures liées à des messages d'erreur nécessite de modifier le fichier de configuration du serveur Web.

L'évolution de la cryptographie crée de nouveaux défis en matière de sécurité

Aujourd'hui, les entreprises sont confrontées à une nouvelle menace pour la sécurité en raison de l'évolution de la cryptographie. D'ici quelques années, l'informatique quantique aura rendu inefficaces les algorithmes de chiffrement RSA et ECC actuels que nos systèmes numériques utilisent. Alors que le NIST et des autorités de certification telles que Sectigo Quantum Labs développent des certificats X.509 reposant sur des algorithmes de chiffrement qui résistent à l'informatique quantique, il est évident que les entreprises vont devoir adopter de nouveaux types de cryptographie, à une vitesse sans précédent.

Pour une entreprise qui a installé manuellement 10 000 certificats pour différents utilisateurs, serveurs, terminaux et applications, cela prendrait jusqu'à un an à cinq personnes pour retrouver et remplacer tous les certificats. Avant que cela soit fait, un individu malveillant aura exploiter la cryptographie exposée pour usurper l'identité du propriétaire légal ou déchiffrer des informations sensibles.

L'entreprise moderne a besoin de solutions automatisées

Avec les écueils et les ramifications financières inhérents à la gestion manuelle des certificats de PKI, le retour sur investissement de la gestion automatisée du cycle de vie des certificats est évident. Les professionnels de l'informatique doivent repenser leur stratégie de gestion du cycle de vie des certificats. En particulier du fait que les entreprises vont sur le marché plus rapidement avec de nouveaux services basés sur le DevOps, les entreprises ont besoin d'une solution automatisée garantissant que les certificats sont bien configurés et mis en place, sans intervention humaine. Non seulement cette automatisation élimine les interruptions de service, mais elle permet aussi aux départements informatiques de contrôler les coûts opérationnels et de lancer plus rapidement des services sur le marché.

Dernièrement, la PKI a évolué pour devenir encore plus polyvalente. L'interopérabilité, des temps de disponibilités élevés et la gouvernance restent des avantages clés. Mais, aujourd'hui, les solutions PKI offrent également la possibilité d'améliorer l'administration et la gestion du cycle de vie des certificats grâce aux fonctionnalités suivantes :

Automatisation

Accélération du déploiement des certificats tout en éliminant les coûts et les erreurs

Évolutivité

Gestion de certificats par centaines, par milliers ou même par millions

Agilité cryptographique

Mise à jour de l'efficacité de la cryptographie, révocation et remplacement rapides des certificats à risque par des certificats résistants à l'informatique quantique en réponse aux menaces nouvelles ou changeantes

Visibilité

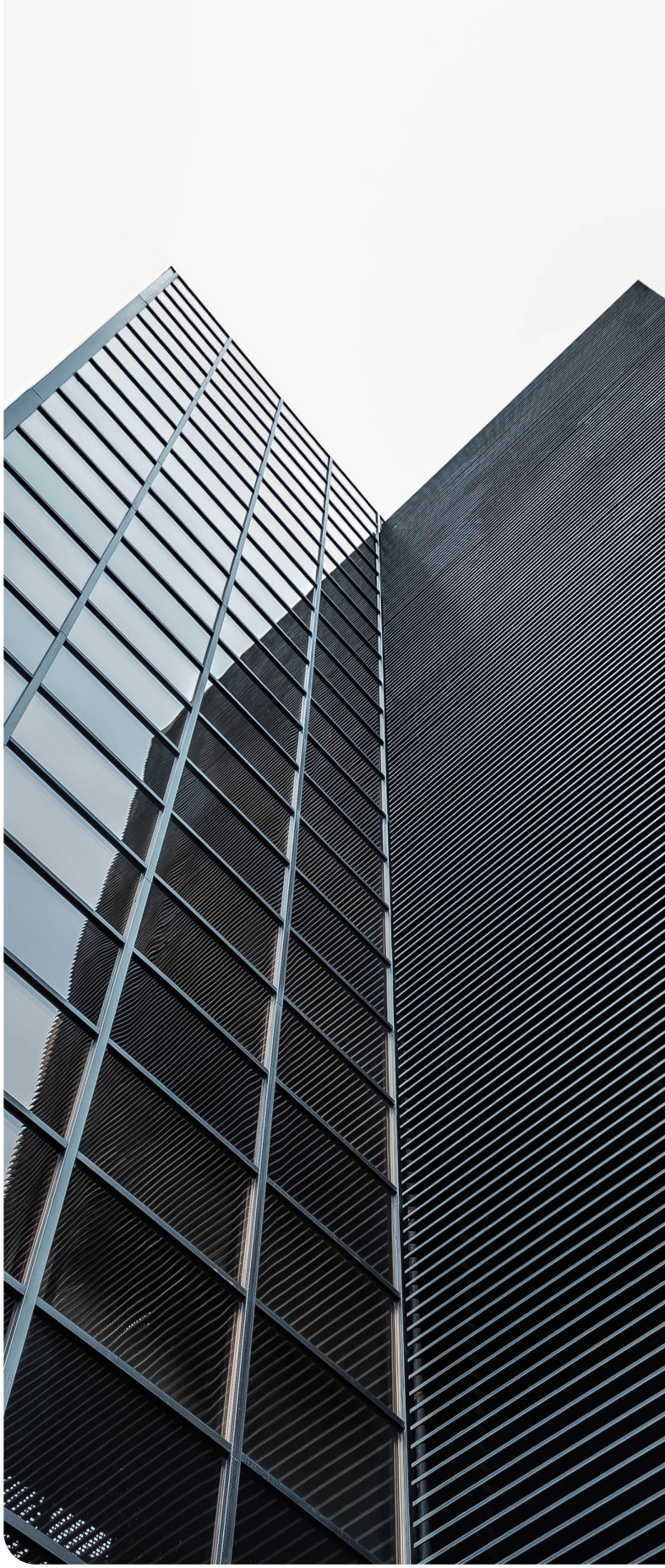
Visualisation de l'état des certificats via une interface unique pour tous les utilisateurs, terminaux, serveurs et applications

Gagner du temps et garder le contrôle avec l'automatisation de PKI de Sectigo

Avec les systèmes, applications et terminaux disparates qui utilisent des certificats numériques, les équipes informatiques gèrent souvent des services d'automatisation différents, venant de prestataires différents, proposant des interfaces et une qualité d'assistance différentes. Un tableau de bord unique pour la gestion des certificats, qui automatise la détection, le déploiement et la gestion du cycle de vie pour tous les cas d'utilisation et toutes les plateformes de prestataires, offre l'efficacité que promet l'automatisation. Et les équipes informatiques gardent en permanence le contrôle des définitions et règles de configuration, de sorte que les étapes d'automatisation sont correctement effectuées.

Sectigo fournit des solutions d'automatisation de certificats permettant aux entreprises d'être agiles et efficaces, et de maintenir le contrôle sur tous les certificats de leur environnement. Sectigo prend en charge l'installation, la révocation et le renouvellement automatisés des certificat SSL/TLS et non SSL via des protocoles standard, des API et l'intégration de prestataires tiers.

De plus, avec Sectigo, vous n'êtes jamais limité à un certain volume de certificats comme cela peut être le cas avec des solutions open source. Les solutions d'automatisation de Sectigo permettent à votre équipe de sécurité de facilement mettre en place une politique de sécurité, de protéger les communications, prévenir de toute perte de données via un accès non autorisé, et de mettre à l'épreuve du temps les systèmes, applications et terminaux dans votre entreprise.



SECTIGO®

Automatisation de la gestion des certificats SSL/TLS

Pour les certificats SSL/TLS, Sectigo propose la gestion automatique des certificats via les composants suivants :

- **Prise en charge du protocole pour l'environnement de gestion automatisée des certificats (ACME) :** le gestionnaire de certificats de Sectigo prend en charge le protocole ACME, vous permettant d'automatiser l'émission de certificats, leur installation et leur révocation, pour une large gamme de serveurs Web et d'équilibreurs de charge. Le protocole ACME demande aux équipes informatiques peu de temps pour configurer et exécuter l'automatisation de la gestion de leurs certificats, faisant de ce protocole un composant de plus en plus adopté pour la sécurité de l'entreprise.

Sectigo prend en charge les types de certificats DV, OV, EV et SSL privés via ACME et offre un contrôle total pour les administrateurs informatiques. Sectigo fournit le serveur ACME et travaille avec des clients compatibles ACME, y compris Certbot de l'Electronic Frontier Foundation (dont Sectigo est un soutien). Voir la figure 2 pour savoir comment l'authentification de certificats avec ACME fonctionne.

Fonctionnement du protocole ACME pour la gestion automatique des certificats de PKI

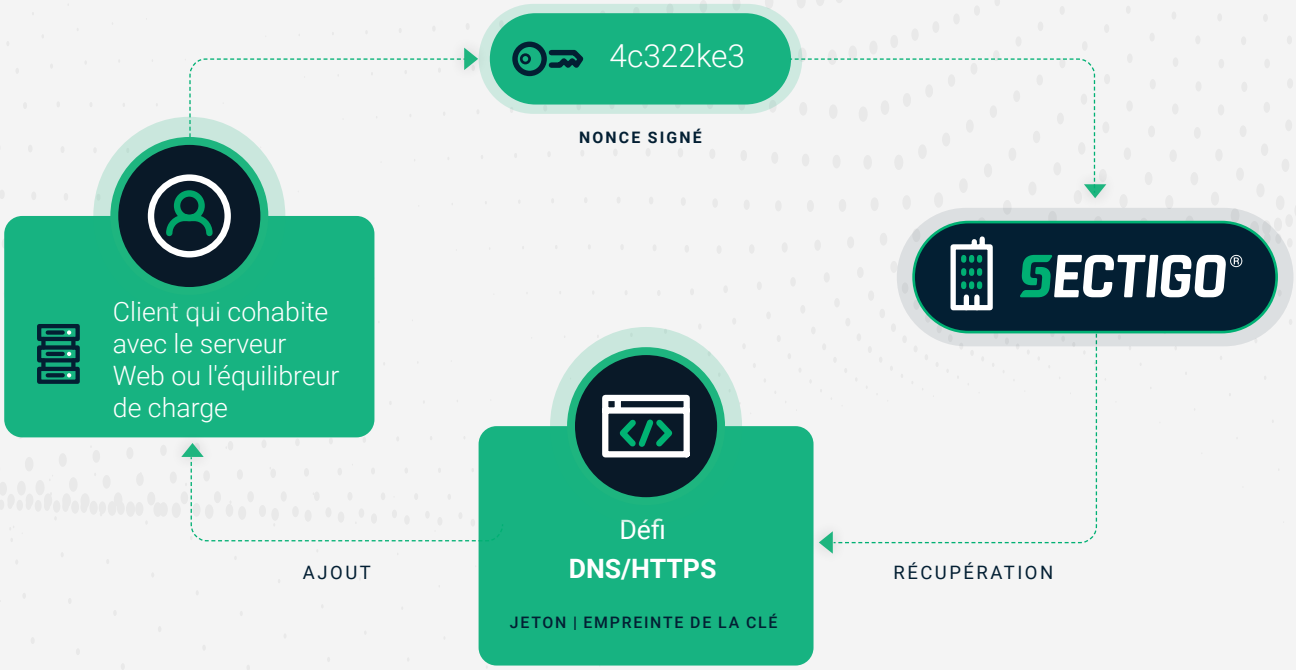


Figure 2 – Processus d'authentification par protocole ACME

Automatisation de la gestion des certificats SSL/TLS

- **API REST :** dans certains cas, les entreprises préfèrent intégrer des applications de Sectigo avec l'API REST de Sectigo. Si cela nécessite plus de développement au niveau de l'application, cela permet de faire évoluer la gestion des certificats et de personnaliser le flux de travail.

  En outre, grâce à l'API REST, Sectigo intègre directement tous les environnements de mise en conteneur et d'outils d'automatisation les plus courants, tels que Docker, Chef, Ansible, Salt Stack, Terraform, Puppet et Jenkins. Nous incluons également des mécanismes pour incorporer la PKI dans le pipeline d'intégration continue et de déploiement continu (CI/CD), des structures d'orchestration telles que Kubernetes et des coffres-forts de tiers tels que HashiCorp Vault.

- **Agent d'installation automatisé pour les locaux des clients :** avec l'agent réseau de Sectigo, vous pouvez automatiser la gestion des certificats dans de nombreux systèmes, tels que les serveurs Web Apache, Tomcat, IIS et F5. L'agent réseau des locaux des clients est intégré au gestionnaire de certificats de Sectigo pour planifier l'émission, l'installation et le renouvellement des certificats.
- **Intégration avec des prestataires tiers :** Sectigo intègre directement les prestataires tiers les plus courants pour aider les clients à réaliser l'automatisation complète de leurs certificats à l'aide de technologies populaires déjà en place dans les environnements informatiques, tels que l'équilibreur de charge Big-IP de F5, le contrôle de diffusion d'application (ADC) de Citrix, et la plateforme de flux de travail informatique de ServiceNow.

  Voir la figure 3 qui présente une liste des plateformes et technologies actuellement prises en charge.

Figure 3 – Solutions d'automatisation actuellement prises en charge pour les certificats SSL/TLS

Serveur Web/Équipement réseau/Outils de DevOps		Choix du client			
Type	**Plateforme**	**Agent d'installation de Sectigo**	**ACME**	**API REST de Sectigo**	**Intégration personnalisée**
Serveur Web	Serveur HTTP Apache	Oui	Oui	Disponible	
	Apache Tomcat	Oui	Oui	Disponible	
	IIS	Oui	Oui	Disponible	
	NGINX		Oui	Disponible	
	Autres serveurs Web pris en charge par Certbot		Oui	Disponible	
Équilibreur de charge	F5	Oui	Oui	Disponible	Oui
	Citrix ADC (auparavant NetScaler)		Oui	Disponible	Oui
Gestion de service informatique	ServiceNow			Disponible	Oui
Outils de DevOps	Ansible			Disponible	
	AWS ELB		Oui	Disponible	
	Chef			Disponible	
	Docker			Disponible	
	HashiCorp Vault			Disponible	
	Jenkins			Disponible	
	Kubernetes		Oui	Disponible	
	Puppet			Disponible	
	SaltStack			Disponible	
	Terraform			Disponible	

Automatisation de l'installation de certificats non SSL

De nombreux systèmes, applications et terminaux utilisent des certificats non SSL, par exemple les certificats d'identité pour les terminaux mobiles. Pour l'installation de certificats non SSL, Sectigo fournit les composants suivants :

- **Protocole d'inscription par transport sécurisé (EST) :** Sectigo prend en charge le protocole EST qui est utilisé pour gérer l'équipement réseau de nombreux fournisseurs. En fait, de nombreux fournisseurs prennent déjà en charge EST. Ce protocole est également répandu dans les environnements IoT en raison de son efficacité et de sa prise en charge des clés à cryptographie sur courbes elliptiques (ECC). Sectigo propose un client EST commercial et prend aussi en charge les divers clients EST open source disponibles.
- **Protocole d'inscription de certificat simple (SCEP) :** le SCEP est utilisé depuis près de vingt ans et de nombreuses entreprises l'ont adopté. Comme le protocole SCEP ne requiert pas de payer une licence et qu'il demande aux équipes informatiques très peu de temps pour le configurer et l'exécuter, il est devenu quasiment omniprésent dans la sécurité des entreprises. Les systèmes de gestion de terminaux mobiles (MDM), tels que Microsoft Intune et AirWatch, utilisent le SCEP pour l'inscription des certificats de PKI. Les terminaux mobiles peuvent ainsi remplacer les mots de passe Wi-Fi et permettre de s'identifier sur un VPN. La plupart des équipements réseau, y compris les routeurs, les équilibreurs de charge, les concentrateurs Wi-Fi, les dispositifs VPN et les pare-feu, prennent aussi en charge le protocole SCEP pour l'inscription des certificats.

Figure 4 – SCM utilise SCEP pour transmettre les certificats au MDM, qui les installe sur le terminal mobile

Dans l'environnement Sectigo, SCEP peut être utilisé pour inscrire des certificats dans les systèmes d'exploitation Linux, MacOS et autres.

- **Agent Microsoft :** un serveur proxy Sectigo peut se situer entre le Bureau Microsoft et le service de certificats Active Directory. Il intercepte les demandes de certificats passant par le protocole d'inscription de certificats clients Windows (WCCE) et fournit automatiquement le certificat au Bureau sans intervention d'un employé.
- **Gestionnaire de certificats mobiles de Sectigo (MCM) :** Sectigo MCM délivre et gère les certificats et les clés sur les terminaux iOS, Chrome OS et Android sans intervention ou presque de l'utilisateur. Il prend en charge tous les types de certificats et peut fonctionner avec tous les terminaux, systèmes d'exploitation et protocoles d'inscription courants. Sectigo utilise un MDM intégré à notre gestionnaire de certificats ou une approche avec portail en libre-service, selon les exigences des clients.

Automatisation de l'installation de certificats délivrés par ADCS

Grâce au service de certificats Active Directory de Microsoft (ADCS), les administrateurs informatiques peuvent ordonner à tous les serveurs et à tous les terminaux d'inscrire et de renouveler automatiquement les certificats émis par Active Directory. Mais cette automatisation ne vaut que pour les applications fonctionnant sous Windows. Les entreprises d'aujourd'hui disposent de terminaux qui n'utilisent pas le système d'exploitation de Microsoft, ce qui signifie que les administrateurs et les employés partagent la charge de devoir renouveler et installer les certificats pour tous les terminaux et applications non Microsoft. Pour ces certificats, les administrateurs utilisent souvent une méthode, source d'erreurs, reposant sur des tableaux afin de suivre manuellement la date d'émission des certificats, leur emplacement d'installation, leur robustesse cryptographique, leur date d'expiration et la personne qui en est responsable.

Sectigo propose les possibilités suivantes :

- Continuer d'utiliser ADCS comme autorité de certification (AC) racine, définir Sectigo comme l'AC qui émet les certificats et les installe automatiquement sur les terminaux ou applications. L'entreprise n'a pas besoin de réincorporer l'AC racine.
- Continuer d'utiliser ADCS comme l'AC qui émet les certificats. Le gestionnaire de certificats Sectigo détecte les certificats émis par ADCS, génère un rapport sur leurs attributs/leur propriété, et il envoie des notifications avant leur expiration.
- Remplacer à la fois ADCS, en tant qu'AC racine, et l'AC qui émet les certificats par l'AC de Sectigo. Cela élimine les coûts d'exploitation d'ADCS tout en automatisant entièrement l'émission et l'installation des certificats.

ADCS ne peut pas automatiquement installer des certificats dans de nombreux cas d'utilisation des entreprises, notamment :

- Serveurs Web
- Terminaux mobiles Apple, Android ou Chromebook sans système de gestion mobile
- Coffre-fort Azure
- Identités de personnes ou de terminaux hors Microsoft Active Directory
- Équilibreurs de charge
- Équipement réseau
- Signature de code
- Conteneurs DevOps
- Authentification d'administrateurs de serveurs par SSH
- Extensions d'e-mails multi-usage sécurisées (S/MIME) reconnues publiquement
- Signature de documents reconnues par Adobe Reader, Adobe Sign
- Terminaux de l'IoT
- Capacité de fournir le même historique de clé de chiffrement pour tous les terminaux que possèdent le même utilisateur

Le gestionnaire de certificats de Sectigo complète ADCS en automatisant l'installation des certificats et en supprimant une gestion manuelle à la fois coûteuse et source d'erreurs. Il garantit à l'entreprise que les certificats sont bien gérés et qu'ils n'arrivent pas à expiration inopinément.

Conclusion : gagnez en sérénité en automatisant votre PKI avec Sectigo

La PKI est la meilleure technologie pour supprimer les mots de passe et s'assurer que seuls des utilisateurs et des terminaux autorisés accèdent aux systèmes d'une entreprise.

Pionnière dans le domaine du SSL et des technologies associées, la société Sectigo est aujourd'hui l'un des leaders mondiaux de la PKI. Sectigo continue d'investir dans des technologies, des normes et des solutions nouvelles pour rester à la pointe de la sécurité et protéger votre activité des menaces numériques.

Avec Sectigo, vous avez plus de :

Choix

Avec la philosophie de Sectigo tournant autour de l'interopérabilité et de l'utilisation de normes ouvertes telles qu'ACME, SCEP et EST comme bases, vous pouvez être sûrs que vous aurez toujours une grande liberté de choix et de contrôle sur votre solution PKI. Et si quelque chose devait mal se passer, vous disposez d'un contact disponible en permanence.

Facilité d'utilisation

Contrairement à d'autres entreprises, Sectigo se concentre sur l'identité numérique, à la fois comme autorité de certification publique et comme l'un des plus grands fournisseurs de PKI privées. En tirant avantage de notre automatisation des déploiements de certificats et de nos technologies de gestion/génération de rapports via une interface unique, permettant de centraliser et de simplifier les tâches fastidieuses liées à la gestion du cycle de vie des certificats, vous permettez à votre équipe de se concentrer sur des tâches à plus forte valeur ajoutée.

Valeur

Le modèle de licence de Sectigo n'induit pas un paiement à l'émission, mais plutôt à l'utilisation. Les certificats qui ne sont plus utilisés (p. ex. quand quelqu'un quitte votre entreprise) peuvent être transférés.

Visibilité sur l'avenir

Sectigo est l'une des plus grandes autorités de certification au monde et nous investissons en permanence dans des technologies et des solutions nouvelles. En devenant notre partenaire, vous êtes sûr que votre entreprise restera en pointe en matière de cryptographie à mesure que vos besoins évolueront et s'étendront. Nos technologies automatiques garantissent l'agilité cryptographique permettant de s'adapter aux avancées des techniques de calcul et de cryptographie qui nécessitent des mises à jour de vos algorithmes de hachage et de chiffrement.

Sérénité

Tout cela vous apporte plus de sérénité. Sectigo est conforme WebTrust et SOC 3, et nos liens avec le CA/Browser Forum ainsi qu'avec certains organismes gouvernementaux aident à assurer que nous recevons des alertes précoces concernant les problèmes de sécurité des PKI. En outre, notre approche open source permet de limiter les vulnérabilités de sécurité. Par sa taille, son évolutivité, sa position parmi les leaders et ses investissements continus dans la PKI, Sectigo est votre partenaire idéal pour sécuriser les bases de votre infrastructure numérique.

Sectigo est l'un des plus grands acteurs en matière de technologie de cybersécurité, fournissant des solutions d'identité numérique, incluant les certificats TLS/SSL, la sécurité sur le Web, le DevOps, l'IoT et la gestion de PKI professionnelle. Étant l'une des plus grandes autorités commerciales de certification du monde, avec plus de 700 000 clients et 20 ans d'expérience dans le domaine des solutions de confiance en ligne, Sectigo fournit des solutions de confiance publiques et privées éprouvées pour sécuriser les serveurs Web, les identités numériques, les terminaux connectés et les applications. Reconnue pour ses innovations primées et son assistance client du meilleur niveau, Sectigo fournit les technologies nécessaires pour sécuriser les environnements numériques d'aujourd'hui comme de demain.

Pour en savoir plus, visitez notre site www.sectigo.com et suivez @SectigoHQ