

Introduction à la gestion des certificats



La gestion des certificats est le processus de surveillance et de gestion des cycles de vie -de l'acquisition et du déploiement au suivi du renouvellement, de l'utilisation et de l'expiration- de tous les certificats SSL/TLS déployés dans un réseau. Ce processus offre aux administrateurs informatiques une visibilité et un contrôle complets de leurs environnements SSL/TLS et les aide à anticiper les violations de sécurité, les pannes et les problèmes de conformité.

Avant de comprendre pourquoi la gestion des certificats SSL/TLS doit faire partie intégrante de la stratégie de sécurité informatique de votre organisation et comment mettre en place un programme de gestion des certificats à l'échelle de l'entreprise, voyons comment les certificats contribuent à la sécurité des communications en ligne.

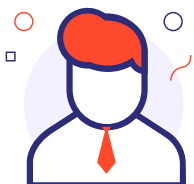
Les certificats SSL et leur rôle dans la sécurisation des communications en ligne.

Vous pouvez consulter le certificat SSL de tout site Web fonctionnant en HTTPS et vous y trouverez les informations suivantes:

Les certificats SSL sont généralement signés et émis par des entités appelées autorités de certification (CA). Il s'agit d'organisations tierces qui jouent un rôle essentiel dans la sécurité de l'internet en agissant en tant qu'incarnation de la confiance pour les deux parties - les propriétaires de sites Web achètent des certificats SSL pour gagner la confiance de leurs clients et les visiteurs du site comptent sur le SSL pour la confidentialité de leurs données. Les sociétés de navigation ne font confiance qu'aux certificats SSL émis par des autorités de certification reconnues au niveau international et affichent des messages d'erreur lorsqu'ils se connectent à des sites Web qui utilisent des certificats SSL générés localement.



Clé publique: Indique les détails de la clé publique et l’algorithme cryptographique utilisés pour signer le certificat



Identité du propriétaire du site : Identifie le propriétaire du site qui a installé le certificat sur son site web



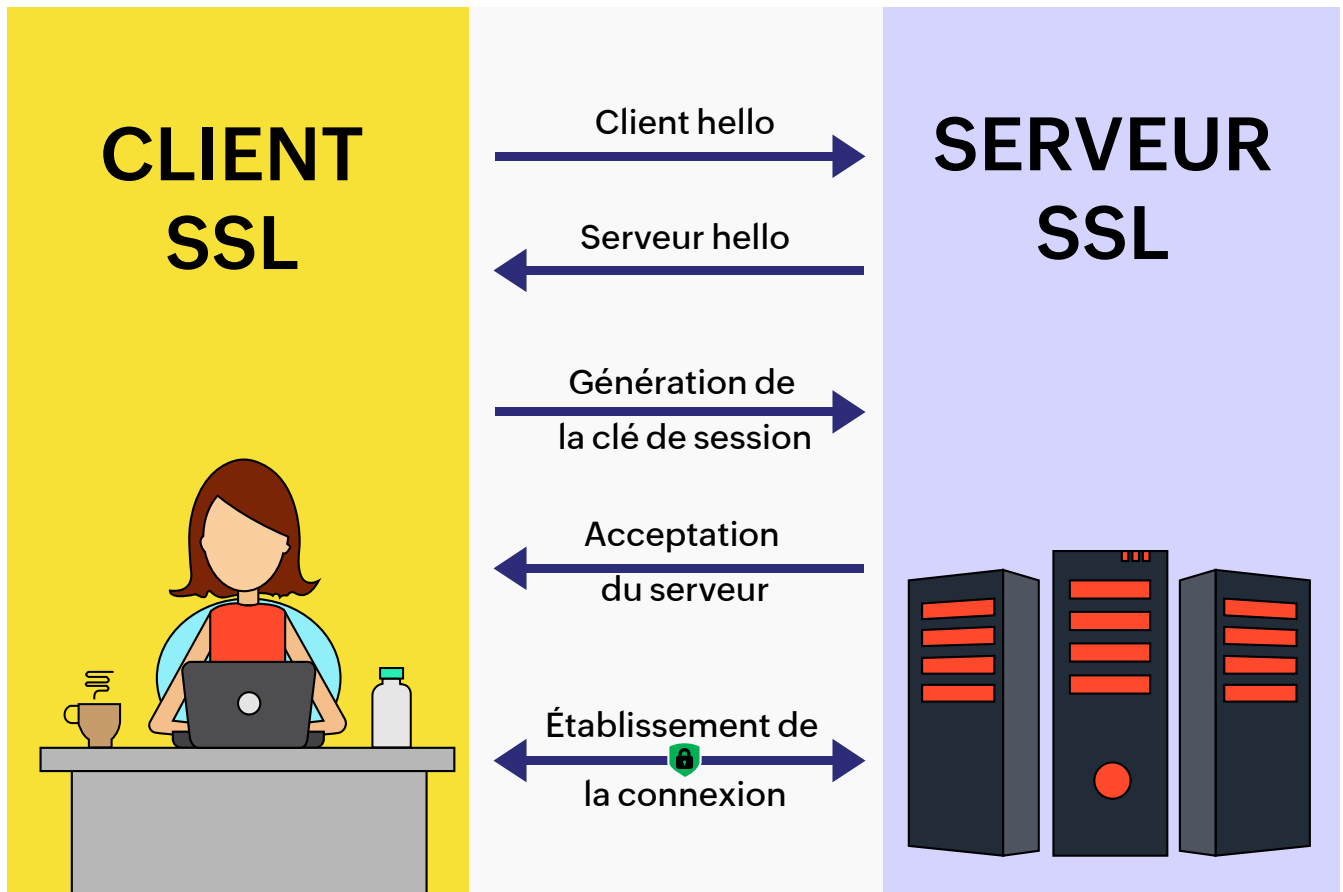
Signature numérique : Indique la signature d’un tierce partie de confiance qui autorise la légitimité de l’identité du propriétaire du site et de son site web.

Les certificats SSL sont généralement signés et émis par des entités appelées autorités de certification (CA). Il s’agit d’organisations tierces qui jouent un rôle essentiel dans la sécurité de l’internet en agissant comme l’incarnation de la confiance pour les deux parties - les propriétaires de sites achètent des certificats SSL pour gagner la confiance de leurs clients et les visiteurs des sites comptent sur le SSL pour la confidentialité de leurs données. Les sociétés de navigation ne font confiance qu’aux certificats SSL émis par des autorités de certification reconnues au niveau international et affichent des messages d’erreur lorsqu’ils se connectent à des sites web qui utilisent des certificats SSL générés localement.

Comment fonctionnent les certificats SSL?

Lorsque les navigateurs tentent d'établir une session cryptée avec un site Web sécurisé par SSL, la séquence d'opérations suivante se déroule en arrière-plan :

1. Le navigateur se connecte à un serveur Web sécurisé par SSL et demande au serveur de prouver son identité.
2. Le serveur web reçoit la demande et renvoie une copie de son certificat SSL ainsi que sa clé publique.
3. Le navigateur reçoit le certificat et vérifie sa légitimité en le comparant à une liste prédéfinie de CA de confiance. Si le navigateur fait confiance au certificat, il crée une clé symétrique appelée clé de session, la chiffre à l'aide de la clé publique du serveur et la renvoie au serveur.
4. Le serveur Web décrypte le message à l'aide de sa clé privée, envoie un accusé de réception (chiffré à l'aide de la clé de session) au navigateur pour lancer la session.
5. Le navigateur et le serveur commencent ensuite la session, dans laquelle toutes les informations échangées sont cryptées à l'aide de la clé de session.



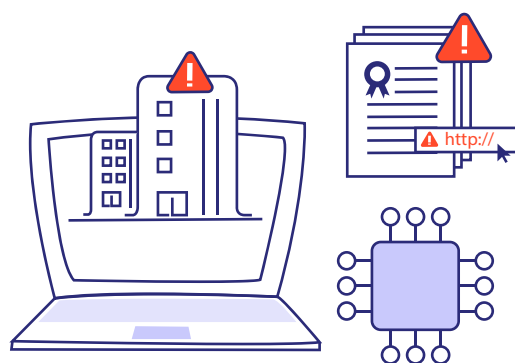
Toutefois, la mise en œuvre du cryptage SSL pour les sites web n'est pas un processus ponctuel. Les certificats SSL expirent après une durée prédéfinie et doivent être constamment renouvelés. S'ils ne sont pas renouvelés, les navigateurs perdent confiance dans la légitimité du site, ce qui se traduit par des messages d'erreur. Dans le pire des cas, les certificats expirés peuvent également ouvrir la voie à des violations de la sécurité. Par conséquent, les organisations doivent surveiller les cycles de vie de tous les certificats déployés sur leur réseau et contrôler constamment leur utilisation pour éviter tout risque de violation de données ou de panne de site Web.

État actuel de la gestion des certificats dans l'informatique d'entreprise

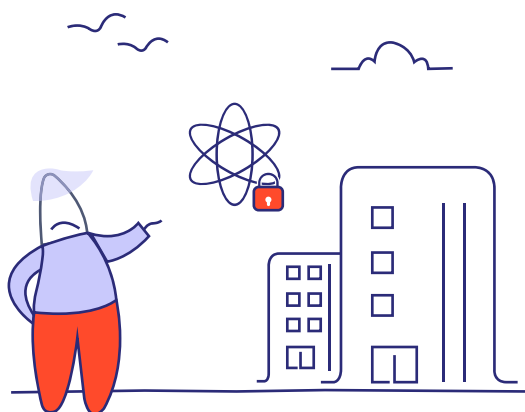


61% des entreprises déploient davantage de clés et de certificats en raison de la réduction de la durée de vie des certificats.

60% des entreprises n'ont pas de stratégie cryptographique à l'échelle de l'entreprise pour le déploiement des clés et des certificats.

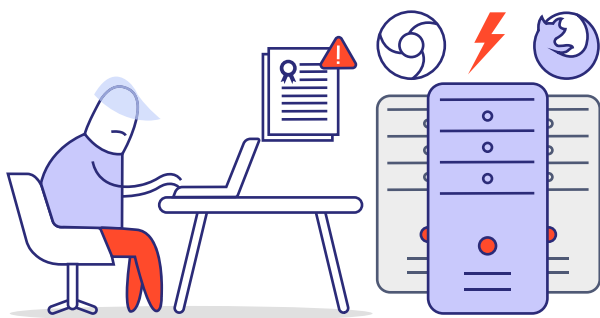
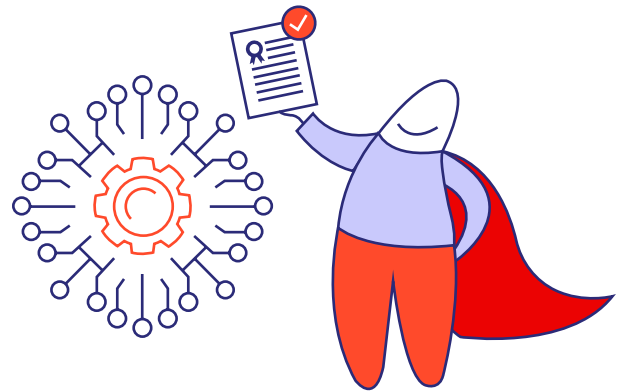


51% des entreprises considèrent l'agilité cryptographique comme une priorité stratégique majeure pour la sécurité informatique.



* State of Machine Identity Management, Ponemon Institute, 2021

82% des entreprises estiment que les certificats SSL/TLS sont les plus importants pour l'identité des machines.



41% des entreprises ont connu 4 interruptions de service ou plus en raison de l'expiration des certificats au cours des 24 derniers mois.

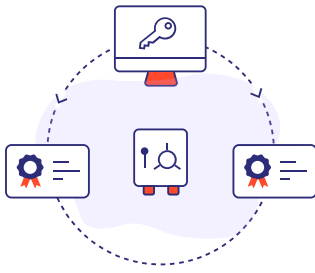
Simplifier la gestion des certificats SSL/TLS

Avec la transformation numérique et l'adoption du cloud qui s'emparent de presque tous les secteurs, les organisations assistent à un déferlement de certificats dispersés sur leurs réseaux. En outre, les communautés de navigateurs s'orientent de plus en plus vers des certificats à courte durée de vie dans le but d'améliorer la sécurité de base des services en ligne. Ces facteurs ont laissé aux administrateurs informatiques l'énorme responsabilité de suivre le cycle de vie de chaque certificat de sécurité déployé dans leur réseau, de surveiller ces certificats pour détecter toute activité inhabituelle et de les renouveler avant leur expiration. Cette tâche est très difficile, surtout pour les grandes organisations qui disposent d'un grand nombre de certificats. Une plateforme centralisée capable d'automatiser les opérations de gestion des certificats et de fournir des informations sur l'environnement SSL d'une organisation est exactement ce dont les administrateurs informatiques ont besoin. Voici quelques-uns des nombreux avantages liés au déploiement d'une solution de gestion centralisée de gestion des certificats :



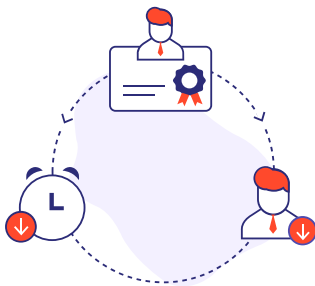
1. Des alertes en temps opportun pour éviter les pannes et protéger la réputation de la marque.

Il n'est pas rare que les entreprises laissent un ou deux certificats expirer par erreur. Mais il suffit d'un seul certificat SSL expiré pour que les visiteurs perdent confiance dans la crédibilité de votre marque. La mise en œuvre d'une solution de gestion centralisée des certificats permet d'alerter les administrateurs lorsque les certificats sont sur le point d'expirer et de réduire le risque de pannes du site Web dues à l'expiration inattendue d'un certificat.



2. Inventaire centralisé et transparence accrue.

Très souvent, les certificats SSL sont demandés et déployés par les équipes localement, selon les besoins, mais leur existence est vite oubliée. La gestion centralisée permet de consolider tous les certificats d'une organisation dans un référentiel unique et de rationaliser les processus d'acquisition, de déploiement et de renouvellement. Les administrateurs bénéficient ainsi d'une transparence et d'un contrôle complets sur leurs environnements SSL.

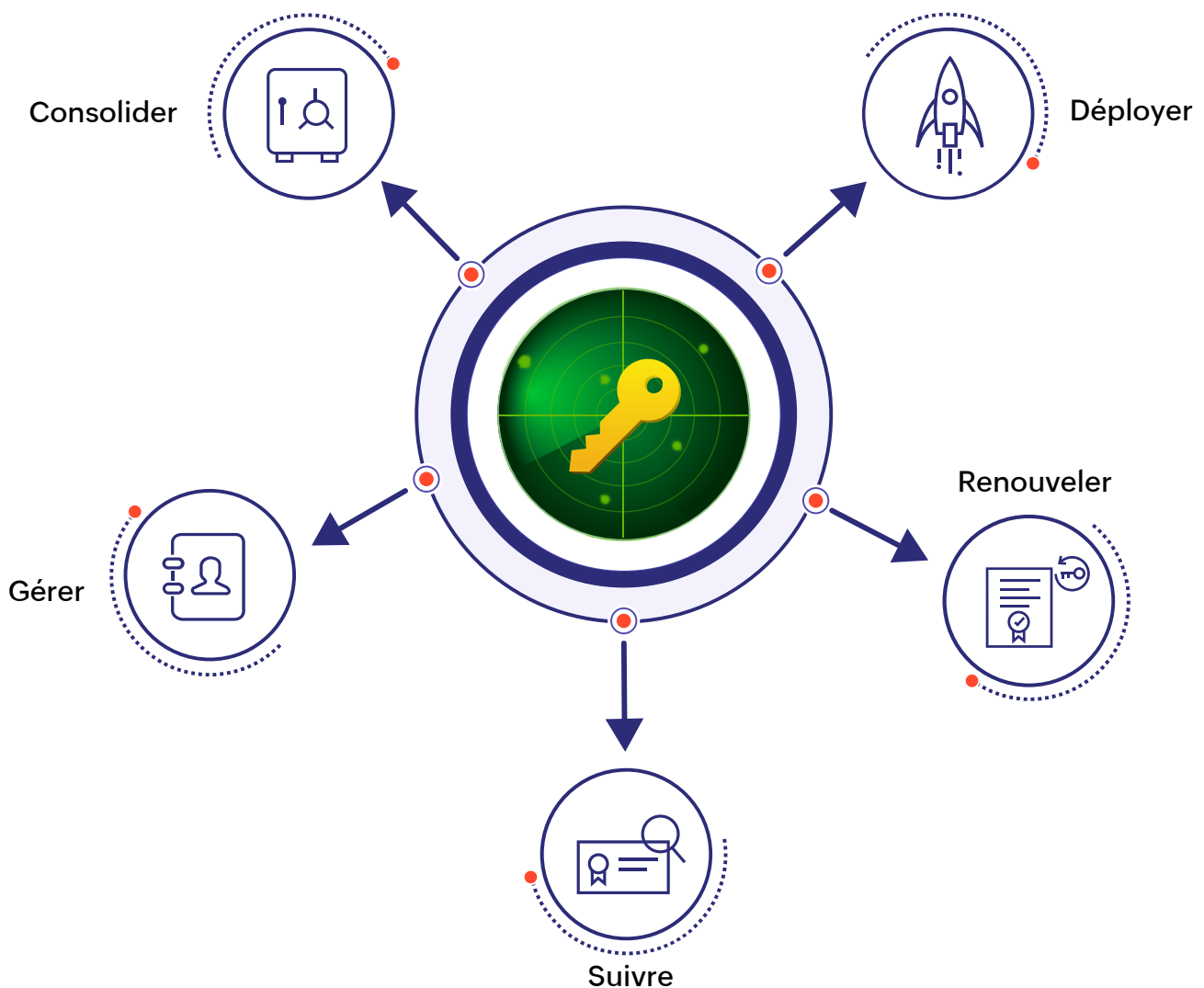


3. Réduction du temps et des efforts.

Par-dessus tout, la centralisation et l'automatisation de la gestion des certificats réduisent considérablement les coûts opérationnels et le temps du personnel associés à la gestion des certificats individuels.

Éliminez la dépendance aux certificats en centralisant la gestion du cycle de vie avec Key Manager Plus.

Key Manager Plus, notre solution Web de gestion des clés et des certificats, offre aux administrateurs une visibilité et un contrôle indispensables sur leur environnement SSL. Elle centralise et automatise les opérations liées à la gestion des cycles de vie des certificats et permet d'anticiper les attaques de sécurité, les problèmes de conformité et les pannes de site dues à l'expiration inattendue des certificats. Voici un résumé rapide des fonctionnalités de Key Manager Plus :



- Découverte et inventaire centralisés des certificats SSL
- Outil de génération de CSR intégré
- Flux de travail simplifié pour les demandes de certificats
- Gestion du cycle de vie complet grâce à des intégrations d'autorités de certification tierces.
- Intégrations Active Directory et MS Store
- Rapports instantanés et complets sur toutes les opérations de gestion des certificats
- Tableau de bord intuitif

Obtenez une visibilité et un contrôle complets de votre environnement SSL/TLS.

Planifiez une démo personnalisée