digicert®

Guide d'évaluation de la sécurité de vos certificats

Votre chemin vers la réduction des coûts et l'élimination des indisponibilités grâce à une infrastructure à clé publique (PKI) dynamique

GUIDE

Introduction

Le monde connecté exige une gestion efficace des certificats

Les certificats PKI constituent le fondement de la confiance numérique pour le monde connecté. Les réseaux actuels reposent sur des infrastructures de plus en plus complexes qui s'adaptent et évoluent au rythme des besoins des entreprises. Ces réseaux ne fonctionnent pas indépendamment les uns des autres. Les systèmes actuels interagissent avec de nombreux autres réseaux, internes et externes. À un tel niveau de complexité, la confiance passe par une gestion des certificats évolutive et modulable.

Méthodologie

En quoi consiste la maîtrise de la gestion du cycle de vie des certificats (CLM) ?

La gestion du cycle de vie des certificats (CLM) est un processus par lequel les pratiques manuelles et ponctuelles sont remplacées par des opérations automatisées et basées sur des politiques de sécurité. À mesure que la maîtrise des processus s'améliore, les coûts et les risques associés diminuent considérablement. L'implémentation d'outils de gestion, de politiques et de processus d'automatisation intégrée plus solides sont autant d'éléments importants dans votre transition vers l'agilité cryptographique, ou crypto-agilité.

La crypto-agilité est la capacité à mettre à jour ou à remplacer rapidement les algorithmes, les clés et les protocoles cryptographiques de manière automatisée, avec une interruption minimale des opérations. Si le CLM est un élément important de la crypto-agilité, il est important de comprendre que son champ d'application englobe également d'autres actifs cryptographiques, tels que les clés de chiffrement pour les bases de données, les disques durs d'ordinateurs, les clés d'authentification multifacteur (MFA), etc.

La révolution de la PKI

La PKI connaît une résurgence plus ou moins forcée. Ce renouveau est le fruit d'une série d'événements qui exigent de réagir face à différents impératifs : menaces de sécurité, réglementations, scalabilité et difficultés liées à la gestion du cycle de vie. La bonne nouvelle est que cette transformation débouchera sur une nouvelle génération de PKI plus sûre, plus résiliente et plus agile.

Facteurs à l'origine de la révolution PKI

- **Réduction de la durée de validité des certificats**
  D'ici à 2029, les organisations devront utiliser des certificats d'une durée de validité de 47 jours pour tous les cas d'usage de certificats publiquement approuvés. Cette décision du CA/Browser Forum rendra les processus manuels pratiquement impossibles à conserver.

- **Explosion des identités machines**
  Des API et aux appareils IoT, en passant par les conteneurs et les environnements multicloud, les machines représentent aujourd'hui des milliards de connexions. Bientôt, il y aura trois fois plus d'appareils que d'êtres humains, sans compter la vague annoncée d'agents IA qui auront eux aussi besoin d'identités de confiance.

- **Échelle et complexité opérationnelles**
  Les environnements cloud et hybrides traditionnels brouillent les frontières entre les PKI externes, internes et fédérées. Ces systèmes requièrent de grands volumes et une grande diversité de types de certificats, ce qui nécessite un CLM flexible capable de connecter les PKI de manière transparente.

- **La menace quantique**
  Le fondement même de la PKI, à savoir des algorithmes cryptographiques qui ne peuvent être devinés ou cassés par force brute par la puissance de calcul actuelle, est désormais menacé. Les calculateurs quantiques seront bientôt capables de casser les algorithmes cryptographiques existants. De nouveaux algorithmes résistant à l'informatique quantique existent, mais ils doivent être testés et déployés partout d'ici 2029, selon Gartner et d'autres experts du secteur.

L'échelle de maîtrise du CLM

L'échelle ci-dessous présente trois niveaux de maturité concernant l'outil CLM : Débutant, élémentaire et maîtrise. Chaque niveau fournit un aperçu du profil type de votre environnement de gestion à date. Dans les sections suivantes, cette échelle est appliquée à des pratiques de référence dans six domaines clés de la gestion du cycle de vie (CLM), avec des descriptions adaptées à chaque niveau de maîtrise correspondant à chaque discipline.

- Débutant
  Cette gestion s'opère principalement par des processus manuels de manière réactive suite à un évènement, avec très peu de visibilité sur l'intégralité des certificats ou concernant des risques existants. Les processus sont difficiles à contrôler et les politiques sont soit sous-développées, soit déployées en silos, ce qui rend leur application difficile. L'inventaire des certificats est souvent géré dans des fichiers Excel.

- Elémentaire
  Cette gestion comprend une visibilité centralisée avec un contrôle partiel sur les notifications et la réduction des risques. Une gouvernance axée sur des politiques est en cours d'introduction et les renouvellements de certificats sont automatisés sur plus de 30 % des systèmes, tandis que le déploiement automatisé des certificats est déjà en place pour un petit nombre de systèmes et d'applications critiques. Les pannes dues à des défaillances des processus manuels de gestion des certificats sont fréquentes.

- Maîtrise
  Cette gestion inclut une visibilité centralisée avec un contrôle quasi complet sur les notifications et l'atténuation des risques. La gouvernance axée sur des politiques est désormais la norme plutôt que l'exception. Le renouvellement des certificats est automatisé sur plus de 50 % des systèmes, tandis que leur déploiement est automatisé sur les systèmes les plus critiques. Les efforts en cours se concentrent sur l'intégration des systèmes de niveau 2 et 3 dans le cadre d'une stratégie de crypto-agilité plus large.

Appliquer le modèle à votre organisation

Parce que votre organisation a des besoins propres, l'application d'outils et de processus de crypto-agilité à votre portfolio de certificats nécessite de comprendre où vous vous situez dans l'échelle de la connaissance.
Ce guide vous aide à évaluer six domaines clés de la gestion du cycle de vie des certificats afin de déterminer la position de votre organisation à mesure que vous progressez vers la crypto-agilité.

Évaluation

Évaluez votre niveau de connaissance CLM dans votre organisation

Ces bonnes pratiques décrivent l'état optimal des solutions, des workflows et de la gouvernance liés à la crypto-agilité. Utilisez ces descriptions pour dresser le bilan de votre situation actuelle et tracer la voie vers une plus grande maturité.

Catégorie 1

Découverte et inventaire

La capacité à localiser tous vos certificats, à connaître leur configuration, leur date d'expiration, leur propriétaire et leur utilité pour l'organisation. L'établissement de cet inventaire nécessite des données provenant de sources multiples afin d'obtenir une visibilité totale sur vos PKI externes, internes et non visibles.

- **Débutant :** suivi manuel, généralement à l'aide de fichiers excel. La visibilité est fragmentée et limitée, avec peu d'informations sur l'ensemble du portfolio de certificats et des risques associés.

- **Elémentaire :** découverte programmée avec une automatisation limitée. Les propriétaires sont identifiés et les notifications de base pour les renouvellements et les expirations sont en place, ce qui améliore la visibilité et la responsabilité.

- **Maîtrise :** découverte continue et en temps réel des sources PKI internes, externes et tierces. Un registre centralisé des propriétaires de certificats est documenté et exploité pour les alertes proactives, les workflows d'approbation et la gouvernance à grande échelle. Le système fournit également des analyses pour le suivi des coûts et les prévisions.

Explication

La découverte sous-tend l'inventaire, lequel permet d'élaborer des politiques et, *in fine*, d'automatiser. Lorsque vous disposez de capacités de découverte et d'inventaire, vous pouvez localiser tous vos certificats et connaître leurs configurations, leurs dates d'expiration, leurs propriétaires et leur utilité pour l'entreprise – y compris pour les certificats relevant du Shadow IT.

Catégorie 2

Politique et gouvernance

Il s'agit de l'implémentation et de l'application de politiques bien définies pour soumettre la délivrance, le renouvellement et la révocation des certificats à des règles. Ces politiques permettent d'éviter les abus, de minimiser le risque de panne et d'accès non autorisé à un certificat, et de s'assurer que l'organisation reste en conformité avec les normes et les réglementations.

- **Débutant :** un contrôle est certes en place, mais la gouvernance est occasionnelle et généralement réactive. Il n'existe aucun moyen efficace d'appliquer ou d'auditer les politiques dans l'ensemble de l'environnement. Il est donc quasiment impossible d'en assurer une application cohérente et de responsabiliser les différentes parties prenantes.
- **Elémentaire :** bien qu'il existe une communication constante et une certaine gouvernance, l'application des politiques est encore largement manuelle. Il reste difficile d'en assurer la cohérence entre les différentes unités opérationnelles ou régions.
- **Maîtrise :** la gouvernance est intégrée dans les processus CLM par le biais d'une automatisation pilotée par les politiques. Les règles sont appliquées de manière dynamique, ce qui garantit une délivrance, un renouvellement et une révocation cohérentes des certificats. Les équipes peuvent rapidement rendre compte de l'état des actifs PKI.

Explication

Une politique et une gouvernance solides réduisent les erreurs humaines, accélèrent la remédiation et renforcent la responsabilisation au sein des équipes et des environnements. De tâche laborieuse et réactive, la gestion des certificats se transforment en un atout stratégique proactif.

Catégorie 3

Automatisation CLM intégrée

Il s'agit de la capacité à automatiser le renouvellement et le déploiement des certificats de différentes autorités de certification, ainsi que le déploiement de certificats sur les serveurs, applications, appareils et autres matériels spécifiques, sur une base reproductible et avec une intervention humaine minimale. Cette capacité dépend d'un inventaire solide et centralisé, avec des politiques définies et un recensement des propriétaires de certificats, ainsi que de méthodes et de protocoles d'intégration adaptés aux exigences de chaque système.

Remarque : bien que le protocole ACME (Automated Certificate Management Environment) soit souvent considéré comme synonyme de l'automatisation de la gestion des certificats, l'ACME ne représente qu'une petite partie de cette automatisation.

- **Débutant:** pas de gestion ou de renouvellement automatisé. Les administrateurs renouvellent et installent les certificats manuellement, à l'aide d'alertes ou d'autres rappels dans leur calendrier. À mesure que les volumes de certificats augmentent et que leurs durées de validité diminuent, la charge de travail explose, de même que le nombre de pannes.
- **Élémentaire :** les machines individuelles sont configurées pour vérifier l'état des certificats, les renouveler et les installer automatiquement, selon un calendrier régulier. L'automatisation est morcelée et il n'existe aucun moyen de contrôler le statut des certificats, de résoudre les erreurs ou d'appliquer les politiques de manière centralisée.
- **Maîtrise :** automatisation centralisée des renouvellements, des remplacements et de l'installation des certificats, sur la base d'un inventaire central et d'une attribution de la propriété des certificats définie par des politiques globales. Cette automatisation facilite l'adoption planifiée des changements cryptographiques à venir, y compris la cryptographie post-quantique (PQC).

Explication

Étant donné que le protocole ACME doit être configuré sur chaque terminal, il ne s'adapte pas facilement à des environnements complexes. Même lorsque la propriété des certificats est répartie entre plusieurs équipes ou systèmes, une approche centralisée de la gestion est essentielle. Cela garantit visibilité, cohérence et contrôle, ce que l'ACME ne peut pas assurer à lui seul. Vous avez besoin d'autres protocoles et intégrations pour centraliser la gestion de toutes les tâches dans l'ensemble de votre écosystème.

Catégorie 4

Préparation aux audits

Ceci décrit la capacité à suivre et journaliser de manière proactive tous les certificats grâce à l'automatisation, avec les fonctionnalités d'analyse et de reporting nécessaires pour produire rapidement des preuves de conformité. Le but est d'unifier les données des certificats et les journaux de modification connexes dans les systèmes d'entreprise, y compris Active Directory, et les plateformes d'Asset Management telles que SAP EAM et les outils ITSM.

- **Débutant :** pratiquement aucune preuve de conformité ni de capacité à produire ces preuves en temps utile. Faute de contrôle des actifs, des risques et des besoins existants, l'organisation ne peut pas répondre aux exigences d'audit ou prévenir les pannes.
- **Elémentaire :** les inventaires et les preuves du respect des politiques sont disponibles mais ne sont pas centralisés. Le suivi des politiques et des procédures n'est pas homogène pour l'ensemble des certificats et des applications. Il est possible d'obtenir de la visibilité et de mener des audits, mais cela mobilise des ressources importantes.
- **Maîtrise :** comptabilisation complète des certificats, des politiques et des procédures pour la majorité des applications de votre entreprise. Cela permet de répondre rapidement aux audits et de prouver que les politiques sont bien appliquées.

Explication

Pour éviter toute infraction aux politiques et réglementations, vous devez savoir où se trouvent vos certificats et être en mesure de les gérer activement. L'élément clé est l'audit complet de toutes les autorités de certification et de tous les systèmes, avec la possibilité d'établir des rapports conformes aux normes du secteur.

Catégorie 5

PKI publique, interne et fédérée

Cette catégorie concerne la visibilité et le contrôle convergés sur toutes les PKI (publiques, internes ou fédérées), quel que soit le cas d'usage. Il s'agit de pouvoir utiliser le bon type de modèle de confiance pour le bon cas d'usage.

- **Débutant :** des PKI internes existent probablement au sein de l'organisation, mais il n'existe en revanche aucun moyen de trouver et de gérer ces certificats d'AC privées de manière centralisée.
- **Elémentaire :** l'organisation a mappé ses différentes PKI et s'est attaquée aux problèmes critiques de sécurité ou de conformité. Toutefois, ces PKI restent isolées et gérées séparément.
- **Maîtrise :** l'organisation dispose d'une visibilité totale et de capacités de gestion des PKI publiques, internes et fédérées par le biais d'un système consolidé. Les PKI internes peuvent être gérées par une solution centralisée plutôt que par des outils applicatifs. Un système CLM efficace peut remplacer en toute transparence l'AC Microsoft pour la gestion des certificats issus de l'Active Directory. Il peut gérer les certificats de n'importe quelle autorité de certification publique, ce qui facilite le transfert des certificats d'une autorité à l'autre.

Explication

Dans le monde réel, le nombre de certificats dans les PKI privées ou internes dépasse de très loin celui des PKI publiques, mais la différence devrait probablement être plus importante. Les administrateurs système utilisent parfois des certificats publics, en particulier des certificats gratuits, alors que l'application serait plus sûre et le risque moins grand avec une PKI interne ou fédérée. Vous devez choisir la PKI adaptée au cas d'usage et conserver une capacité de surveillance et de contrôle de chaque certificat, quel qu'en soit le type.

Catégorie 6

Évolutivité et extensibilité

Les solutions et les processus crypto-agiles favorisent la croissance et le changement au sein de l'organisation au fil du temps, notamment en préparation à la cryptographie post-quantique (PQC).

- **Débutant :** la gestion des certificats est fragmentée et non évolutive, ce qui nécessite une intervention manuelle à chaque étape. Il en résulte un système fragile et réactif dont l'évolutivité est limitée.
- **Elémentaire :** la délivrance de certificats est partiellement standardisée, combinant des AC anciennes, des services cloud et des AC publiques. Cependant, la gestion est encore fragmentée, de même que le développement et la maintenance des intégrations.
- **Maîtrise :** le contrôle central permet à la PKI d'entreprise de fonctionner on-prem et dans un ou plusieurs clouds. Ce niveau de PKI s'adapte à la croissance du nombre d'utilisateurs et de machines, tout en s'intégrant à de nombreuses technologies au fur et à mesure de l'évolution de l'infrastructure de l'entreprise.

Explication

Les intégrations complexes provoquent souvent des pannes, nécessitent des corrections fréquentes et peinent à s'adapter aux nouvelles exigences et aux nouveaux workflows. Les processus CLM matures permettent à votre organisation de répondre de manière dynamique aux besoins métiers et de sécurité, grâce notamment au provisionnement automatisé, à l'application flexible des politiques et à des intégrations transparentes dans les environnements on-prem, cloud et hybrides.

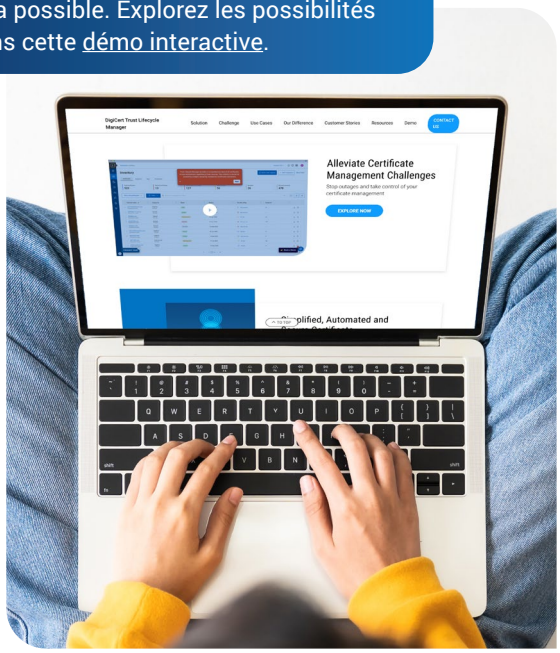
Comment utiliser ce guide ?

Prochaines étapes

Maintenant que vous avez une meilleure idée du niveau de maturité de votre organisation, il est important de garder à l'esprit le fait que l'automatisation n'est pas une fin en soi. N'essayez pas non plus d'atteindre le stade de maturité ultime. En se concentrant sur des solutions, des processus et des politiques crypto-agiles, votre organisation continuera à s'adapter à la croissance de vos systèmes, à l'évolution des normes et à l'apparition de nouvelles menaces.

Avec la bonne solution CLM en place, vous pouvez assurer la pérennité de votre infrastructure, garantir la conformité et maintenir la confiance dans un écosystème digital en rapide évolution.

Découvrez comment DigiCert rend tout cela possible. Explorez les possibilités dans cette démo interactive.



À propos de DigiCert

Chez DigiCert, nous sommes toujours restés fidèles à ce mot d'ordre : A better way. Plus qu'un simple slogan, cette quête perpétuelle d'un meilleur moyen de sécuriser Internet est profondément ancrée dans notre ADN. C'est pourquoi nos solutions PQC, TLS, PKI et IoT sont utilisées partout, des millions de fois par jour, par des entreprises et des particuliers du monde entier. C'est aussi pour cela que notre support et nos services atteignent les taux de satisfaction client les plus élevés du marché. Et c'est enfin pourquoi nous continuerons à concevoir des solutions garantes d'un avenir sûr à l'ère de l'informatique quantique.