EBOOK

Pourquoi il est temps de revoir votre PKI

Vous voulez migrer vers le cloud ? Voici 5 raisons de moderniser votre PKI

KEYFACTOR

Sommaire

Introduction

Que ce soit pour sécuriser l'infrastructure informatique, la chaîne d'approvisionnement informatique ou pour intégrer des identités dans des produits connectés, les entreprises se tournent vers la PKI (infrastructure de clés publiques) comme technologie éprouvée pour établir la confiance numérique. Cependant, les déploiements de la PKI laissent souvent les équipes aux prises avec une infrastructure coûteuse, une prolifération de certificats et des pannes, ainsi que des solutions matérielles et logicielles fragmentées qui créent davantage de complexité.

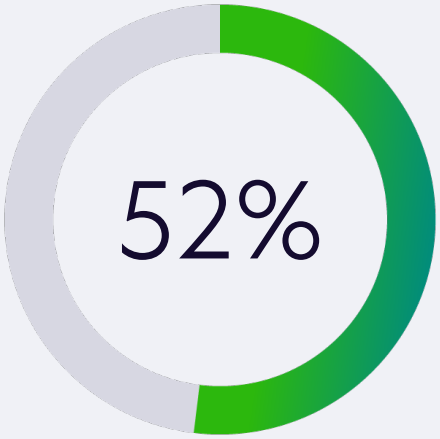
Pour répondre aux exigences des équipes de développement d'applications hybrides et multi-clouds et au rythme effréné, les organisations ont été obligées de repenser leurs systèmes d'information. Pour répondre aux exigences des équipes de développement d'applications hybrides et multi-clouds, les organisations ont été contraintes de repenser leur stratégie de gestion des ICP et des certificats.

PKI traditionnelle vs IT moderne

Microsoft CA, également connu sous le nom de Active Directory Certificate Services (ADCS), a peut-être été un choix facile pour les environnements informatiques traditionnels, mais le chemin vers le cloud et la main-d'œuvre à distance introduit plusieurs nouveaux défis.

Pour commencer, les environnements PKI existants n'ont tout simplement pas été conçus pour le volume élevé et la vitesse d'émission des certificats d'aujourd'hui. De plus, ils ne sont généralement pas intégrés aux outils modernes et, en raison d'erreurs et de négligences, ils peuvent facilement être mal configurés à tout moment au cours de leur longue durée de vie. Sans compter que de nombreuses équipes ne disposent tout simplement pas de l'expertise ou des ressources suffisantes pour se consacrer au déploiement de leur ICP.

Pour ces raisons et bien d'autres encore, de nombreuses organisations ont reconnu la nécessité de moderniser leur ICP ou de la déplacer entièrement vers le cloud. Les solutions PKI as a Service (PKIaaS) ou SaaS PKI offrent tous les avantages d'une PKI de pointe, sans la charge de l'exploiter et de la maintenir en interne. Quel que soit le mode ou l'endroit où vous la déployez, on ne saurait trop insister sur l'importance d'une bonne ICP.



des organisations affirment que les services en nuage sont à l'origine du déploiement de la PKI, des clés et des certificats.

2021 State of Machine Identity Management

L'évolution du rôle de la PKI

Au cours des deux dernières décennies, le monde de la PKI a changé de façon spectaculaire, passant d'une technologie marginale à un élément d'infrastructure omniprésent utilisé par pratiquement toutes les équipes de l'organisation informatique actuelle.

Si la PKI a été adoptée à l'origine pour sécuriser l'Internet, son utilisation a explosé depuis, et elle est désormais utilisée pour tout sécuriser, des réseaux et applications internes aux dispositifs périphériques et à la fabrication intelligente. Elle est essentiellement devenue le fondement de la confiance numérique à une époque où la confiance ne peut être présumée, elle doit être construite.

Web Servers

Certificats SSL/TLS sur les sites web et les applications extérieurs pour assurer la confiance.

Internet of Things (IoT)

Contrôles d'authentification mutuelle, de cryptage et d'intégrité pour les appareils connectés.

Multi-Coud

Certificats éphémères pour authentifier les conteneurs, les microservices et les charges de travail.

Secure Email

Signer numériquement et crypter les e-mails sur les appareils d'entreprise et les appareils BYOD.

Appareils de réseau

Authentication between routers, firewalls, load balancers and SSL inspectors.

DevOps

Signature des conteneurs et des constructions de logiciels, et la sécurisation des charges de travail éphémères.

MFA / SSO

Authentification multifactorielle pour les applications d'authentification unique telles que Windows Hello ou Office 365.

Accès WiFi

Authentification des connexions Wi-Fi pour garantir que seuls les utilisateurs de confiance accèdent au réseau.

Accès VPN

Remplacement des solutions d'authentification VPN coûteuses par une authentification par certificat sans mot de passe.

Mobile Devices

Accès sécurisé pour les applications mobiles, les navigateurs mobiles, l'authentification Wi-Fi, le cryptage des e-mails S/MIME, etc.

Le bon choix : Principaux points à prendre en compte

Concevoir, déployer et maintenir les systèmes nécessaires pour soutenir une PKI d'entreprise moderne peut être une mission complexe sans une bonne approche. C'est pourquoi il est essentiel d'évaluer si votre organisation dispose de la solution, de l'expertise et de l'infrastructure adéquates pour gérer une ICP capable de soutenir votre entreprise à mesure qu'elle se développe.

Cas d'usage

Le nombre d'outils et d'applications dépendant de la PKI pour l'identité et l'authentification a considérablement augmenté. Les certificats sont désormais utilisés pour tout, de la signature de logiciels à l'authentification dans les déploiements de microservices. Pour réussir un déploiement, il est essentiel d'identifier les différents types de certificats, les modèles, les prototypes et les capacités d'automatisation nécessaires pour prendre en charge ces différents cas d'utilisation.

Expertise

Un petit nombre d'entreprises disposent d'un expert interne (ou d'une équipe) dédié à la PKI, mais pour la plupart d'entre elles, il s'agit plutôt d'une "patate chaude" que l'on refile à tout administrateur désireux de s'en charger. Il est important de se demander si vous disposez de l'expertise et de la largeur de bande nécessaires au sein de votre équipe pour mettre en place et gérer une ICP robuste pendant toute sa durée de vie de 15 à 20 ans. Si ce n'est pas le cas, vous pouvez envisager un service PKI hébergé ou géré.

Migration vers le cloud

Chaque déploiement de la PKI est différent. Certaines organisations sont plus avancées dans leur voyage dans le nuage, d'autres en sont encore à déterminer ce qui doit rester derrière leur pare-feu. La bonne nouvelle est que la technologie de l'ICP a progressé de façon spectaculaire et qu'il existe aujourd'hui beaucoup plus d'options de déploiement qu'auparavant, notamment la PKI en tant que service (PKIaaS).

Évolutivité et disponibilité

Un autre élément clé à prendre en compte est l'accord de niveau de service (SLA) prévu pour le temps de fonctionnement et la disponibilité, en particulier lorsque vous passez à l'échelle avec de nouveaux cas d'utilisation. La haute disponibilité (HA), la sauvegarde et la reprise après sinistre (BU/DR), ainsi que la capacité à gérer les certificats émis par votre PKI à l'échelle sont autant de facteurs importants pour la prise en charge d'environnements comptant des milliers, voire des millions de certificats.

Niveaux de sécurité et d'assurance

La PKI ne se résume pas aux logiciels et aux certificats de l'autorité de certification. Vous devrez également prendre en compte les mesures de protection et les politiques nécessaires autour de votre infrastructure PKI pour atteindre les niveaux d'assurance attendus et protéger les clés privées derrière votre racine de confiance. Certaines réglementations sectorielles ou politiques de sécurité internes peuvent également dicter les paramètres spécifiques requis pour votre déploiement PKI.

Les défis commerciaux

Il est clair que la PKI est une composante essentielle de la sécurité et de la confiance digitale, mais il existe un certain nombre de défis qui peuvent faire obstacle au succès.

Absence de propriété claire

La PKI a toujours été une sorte de "patate chaude" technique. Elle passe d'une équipe à l'autre ou d'une personne à l'autre sans qu'il y ait de propriété claire, et lorsqu'un incident tel qu'une panne de certificat se produit, il est difficile de réagir efficacement.

Manque d'expertise

La PKI ne fait pas partie des compétences de base de nombreuses équipes informatiques et de sécurité. L'expertise peut être difficile à trouver et à conserver, alors à moins que vous ne disposiez des compétences et des heures d'équivalent temps plein (ETP) nécessaires au sein de votre personnel, vous devrez peut-être renforcer votre équipe avec un partenaire de confiance.

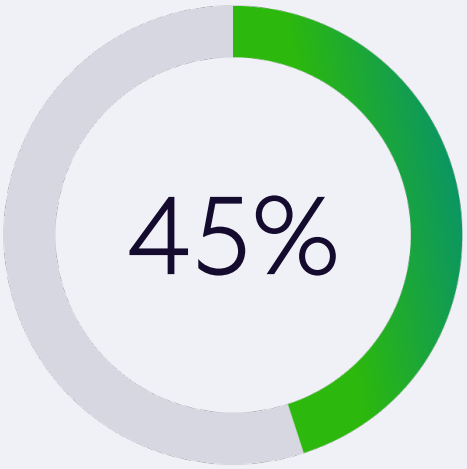
Outils et processus disparates

Les équipes de sécurité s'appuient trop souvent sur un patchwork inefficace de PKI internes et d'autorités de certification (CA), d'outils de surveillance et d'interfaces de gestion qui ne parviennent pas à fournir une visibilité et un contrôle cohérents.

Infrastructure CA obsolète

Les déploiements de PKI initialement construits pour une ou deux applications sont maintenant étirés pour couvrir plus d'utilisateurs et d'appareils que jamais. Les anciens systèmes PKI qui n'ont pas été conçus à l'origine pour des choses comme le cloud computing et les appareils IoT peuvent devenir un obstacle opérationnel.

Seulement



des entreprises ont suffisamment personnel dédié à leur PKI.

2021 State of Machine Identity Management

PKI à l'ombre

Différentes équipes déploient souvent leurs propres autorités de certification (CA) pour des cas d'utilisation spécifiques sans tenir compte des politiques informatiques de l'entreprise. Les autorités de certification peuvent être mal configurées et les certificats non suivis, ce qui entraîne des résultats d'audit inattendus et des pannes.

5 raisons pour moderniser votre PKI

Alors, pourquoi est-il temps de repenser votre PKI ?

Voici les principales raisons pour lesquelles les organisations migrent des anciens systèmes PKI vers une solution PKI moderne.

1. Déployez à votre manière

En matière de PKI, il n'y a pas de taille unique. La manière et l'endroit où vous déployez votre PKI est une décision critique, la flexibilité est donc importante. Par exemple, une solution basée sur le cloud, telle que Keyfactor EJBCA SaaS ou PKI as a Service, offre une évolutivité et une facilité de déploiement en mode cloud. En revanche, une solution sur site, telle qu'une appliance matérielle ou logicielle EJBCA, peut s'avérer plus judicieuse si vous disposez de ressources disponibles ou si vous êtes soumis à des exigences réglementaires strictes pour déployer et gérer la PKI en interne.

Dans un cas comme dans l'autre, les déploiements PKI existants ne peuvent généralement pas répondre au besoin de flexibilité des opérations hybrides et multi-cloud. Pour tenir compte des défis uniques de votre organisation, notamment en matière de sécurité, de budget et de disponibilité des ressources, votre équipe a besoin d'options de déploiement qui répondent à ses besoins actuels et lui permettent de se développer avec souplesse au fil du temps, notamment dans le cadre de scénarios tels que la migration de la PKI, les activités de fusion et d'acquisition et la PKI hybride.

2. Répondre à tous les cas d'utilisation

Tout comme vous avez besoin de la flexibilité nécessaire pour vous déployer n'importe où, vous devez également être en mesure de vous intégrer facilement à vos outils et applications existants. L'auto-enregistrement fonctionne bien pour l'infrastructure Microsoft, mais les paysages informatiques d'aujourd'hui sont beaucoup plus complexes, impliquant de multiples systèmes d'exploitation, services et plateformes en nuage.

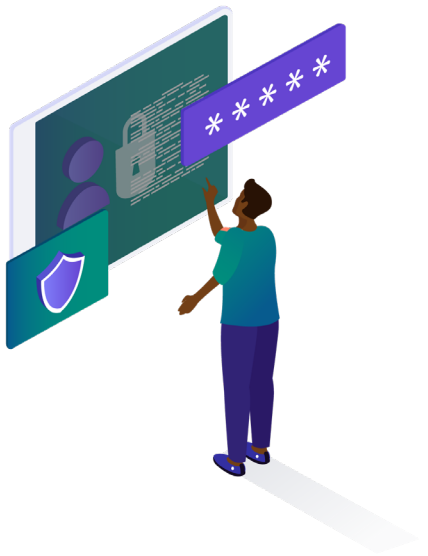
Les développeurs attendent des certificats qu'ils soient facilement utilisables via une API. Les fabricants ont besoin d'intégrer les certificats dans les produits directement sur le lieu de fabrication.

Pour répondre à une variété de cas d'utilisation, la PKI doit être adaptable et extensible. Les solutions PKI modernes prennent en charge des milliers d'opérations de certificat par seconde et offrent une prise en charge intégrée de protocoles tels que SCEP, ACME, EST et CMP, ainsi qu'une solide API REST sous-jacente. Ce niveau de flexibilité est inestimable lorsque vous avez affaire à différents appareils, systèmes d'exploitation et zones géographiques.

Qu'en est-il de Microsoft CA ?

Vous êtes donc à la recherche d'une nouvelle solution PKI moderne pour prendre en charge de nouveaux cas d'utilisation tels que la migration vers le cloud et DevOps, mais vous avez toujours des cas d'utilisation traditionnels déjà pris en charge par Microsoft CA. Devriez-vous migrer ? Ou devriez-vous conserver votre PKI actuelle ?

La réponse est simple : les deux sont possibles. Trouver la bonne solution PKI vous permettra de prendre en charge des cas d'utilisation modernes avec des outils natifs de Microsoft comme Auto-enrollment, Intune et Azure Key Vault. Elle vous permettra également de fonctionner en tandem avec Microsoft CA ou de migrer au fil du temps vers votre nouvelle PKI avec un minimum de perturbations.



3. Échelle sans limites

Parce que votre PKI prend en charge des applications critiques, l'évolutivité et les performances sont une préoccupation majeure. Le problème de nombreux déploiements de PKI hérités, tels que Microsoft CA, est que vous ne pouvez installer qu'une seule CA par serveur. Sans la prise en charge intégrée de la multi-location et de la haute disponibilité (HA), l'empreinte de votre PKI peut devenir très complexe, très rapidement. Sans parler du coût croissant de la maintenance.

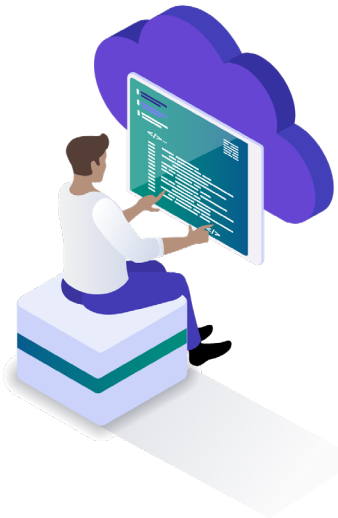
Que vous optiez pour un déploiement entièrement géré, un SaaS clé en main ou un déploiement sur site, les solutions PKI modernes facilitent un déploiement rapide et évolutif sans limitations telles que des frais par certificat ou des serveurs CA supplémentaires. Sur le plan technique, tous les composants de l'infrastructure à clé publique, tels que les autorités de certification (CA), les autorités d'enregistrement (RA) et les autorités de validation (VA), peuvent être mis en œuvre beaucoup plus rapidement pour répondre à la demande.

L'adoption d'une PKI fournie par SaaS ou entièrement gérée peut vous faire gagner beaucoup de temps et de ressources à mesure que vous évoluez, avec des accords de niveau de service intégrés pour garantir le temps de fonctionnement et une surveillance 24/7 pour s'assurer que votre PKI reste saine et opérationnelle.

Pourquoi la PKI en tant que service ?

L'installation et la maintenance d'une PKI complète nécessitent des ressources et une expertise. Tout logiciel de CA s'appuie sur une pile technologique robuste, qui nécessite une surveillance, une maintenance et des mises à jour constantes.

En optant pour une PKI fournie par SaaS ou entièrement gérée, vous réduisez les besoins internes de gestion d'un autre composant d'infrastructure critique. Un partenaire de confiance garantit que votre PKI est gérée selon les meilleures pratiques et avec la plus grande assurance, tandis que vos équipes peuvent se concentrer sur les objectifs commerciaux essentiels.



4. Simplifier et consolider la PKI

Une PKI d'entreprise typique se développe au fil du temps, avec l'évolution des besoins commerciaux et l'ajout de nouveaux cas d'utilisation. Si l'on ne planifie que pour le court terme ou pour des cas d'utilisation spécialisés, on se retrouve souvent avec un environnement PKI hypertrophié, des politiques de sécurité incohérentes et des coûts croissants. En outre, les anciens systèmes PKI présentent des limitations fonctionnelles qui les rendent inaptes à répondre aux besoins actuels et aux exigences réglementaires.

Face à l'augmentation de la demande de certificats numériques, de nombreux responsables de la sécurité cherchent à simplifier et à consolider leur infrastructure d'autorité de certification et à appliquer une meilleure gouvernance et un meilleur contrôle. Une solution d'AC flexible et évolutive vous permet de couvrir tous vos cas d'utilisation de l'ICP avec une seule plateforme. Au lieu de s'appuyer sur un ensemble disparate d'outils CA et crypto, les organisations peuvent commencer à consolider leurs cas d'utilisation PKI dans une plateforme centralisée, réduire le coût total de possession et établir un centre d'excellence Crypto (CCoE).

5. Permettre l'automatisation et l'agilité

Au-delà des rouages de votre infrastructure PKI, vous avez besoin de visibilité et de contrôle sur les certificats émis dans votre environnement, qu'ils proviennent d'AC publiques ou privées. De nombreuses équipes s'appuient sur des feuilles de calcul inefficaces, des rappels de calendrier et des scripts maison pour assurer le suivi, mais les cycles de vie plus courts et les volumes plus importants de certificats rendent le suivi presque impossible.

Le choix de la bonne solution PKI peut vous permettre non seulement d'émettre, mais aussi de gérer et d'automatiser le cycle de vie des clés et des certificats. En combinant une PKI hautement évolutive avec l'automatisation du cycle de vie des certificats, les organisations peuvent relever ces deux défis avec une seule solution. Plus important encore, elle vous donne la flexibilité de gérer et d'automatiser le renouvellement et le provisionnement des certificats à travers toutes les autorités de certification de votre environnement, ce qui pourrait inclure d'autres fournisseurs d'autorités de certification natives du cloud ou de confiance publique.

Pourquoi l'agilité des AC est essentielle

Il est important de simplifier et de consolider les fournisseurs lorsque cela est possible, mais la réalité est que des exigences et des environnements de confiance différents peuvent rendre nécessaire l'utilisation de plusieurs PKI et AC.

Il est essentiel d'avoir une visibilité sur l'ensemble de votre paysage de certificats, y compris les émetteurs publics, privés et basés sur le cloud, pour éviter les pannes et les risques de sécurité résultant de l'utilisation de plusieurs interfaces et outils pour gérer les certificats. Cela signifie également que vous pouvez rester crypto-agile et ajouter ou changer facilement de fournisseur d'AC en fonction de vos besoins et de l'évolution inévitable des normes cryptographiques.

La PKI propulsée par Keyfactor

Chez Keyfactor, nous pensons que les équipes devraient avoir la flexibilité de déployer la PKI de la manière et à l'endroit où elles en ont besoin - dans le cloud ou sur site, entièrement gérée ou auto-hébergée. Cette approche aide les organisations à simplifier leur PKI et à permettre la confiance numérique à travers leur paysage connecté, quel qu'il soit aujourd'hui et quelle que soit son évolution dans le futur.

Mieux encore, nous combinons nos solutions PKI avec une automatisation du cycle de vie de bout en bout pour les clés et les certificats dans l'informatique d'entreprise, les DevOps, et même les environnements de fabrication IoT et IIoT. Il s'agit d'une plateforme unique pour l'automatisation de la PKI et de l'identité des machines.

Pourquoi Keyfactor

✓ Une profonde expertise en PKI

La PKI est plus qu'un simple logiciel. Nous avons plus de 20 ans d'expérience dans l'ingénierie, l'architecture et la conception de la PKI.

✓ Une seule plateforme

Our customers benefit from a single platform for PKI and certificate lifecycle automation. Less complexity, more agility.

✓ Simplicité

La Securité fonctionne seulement si elle est adoptée par tous. Nos solutions sont dediées pour les experts PKI et les utilisateurs de tous les jours afin de simplifier la PKI et les certificats.

✓ Flexibilité

Vous avez la possibilité d'exécuter la PKI comme et où vous le souhaitez, que ce soit dans le nuage, dans une architecture hybride ou sur place.

✓ Scalabilité

Nos solutions ont été testées et prouvées pour fonctionner sans effort dans des environnements comptant des millions, voire des milliards, de certificats.

✓ Confiance et conformité

Keyfactor travaille sans relâche pour se conformer aux normes de sécurité de l'industrie telles que ISO 27001, ISO 9001, Critères communs, SOC 2 Type II, et plus encore.

© 2023 Keyfactor, Inc. All Rights Reserved

Déployez votre PKI, à votre façon

GÉRÉ
PKI comme service
Disponible en tant que service

PKI zéro-touch gérée 24/7 avec une racine hors ligne et protégée par air.

SAAS
EJBCA SaaS
Disponible en AWS

PKI SaaS clé en main, déployée et gérée par Keyfactor.

CLOUD
EJBCA Cloud
Disponible en AWS & Azure

PKI autogérée déployée dans votre environnement en cloud.

SOFTWARE
EJBCA Software
Disponible comme appliance virtuelle

Déployer dans votre propre centre de données et intégrer avec votre fournisseur de HSM.

HARDWARE
EJBCA Hardware
Disponible sous forme de hardware clé en main

Déployer une PKI clé en main avec une pile matérielle et logicielle complète et un HSM.

Gérer l'identité de chaque machine

SÉCURITÉ DES ENTREPRISES
Keyfactor Command
Disponible on-prem, hybrid or SaaS

Évitez les pannes et favorisez la crypto-agilité grâce à une visibilité visibilité, le contrôle et l'automatisation des clés et des certificats.

SÉCURITÉ DES PRODUITS
Keyfactor Control
Disponible on-prem, hybrid or SaaS

Sécuriser les produits IoT dès leur conception grâce à une gestion de pour les appareils et les chaînes d'approvisionnement de fabrication.

© 2023 Keyfactor, Inc. All Rights Reserved

Prêt à repenser votre PKI?

Il arrive un moment où chaque organisation dépasse son ancien déploiement PKI, que ce soit en raison d'une migration vers le cloud, de l'expiration de l'AC ou de la nécessité de prendre en charge de nouveaux cas d'utilisation. Que vous en soyez là aujourd'hui ou que vous planifiez l'avenir, nous sommes prêts quand vous l'êtes à entamer la conversation.

CONTACTEZ-NOUS

Commencez à moderniser votre PKI, demandez une démonstration à un expert de Keyfactor.

DEMANDEZ UNE DÉMONSTRATION

KEYFACTOR

Keyfactor est la plateforme d'identité machine et IoT pour les entreprises modernes. L'entreprise aide les équipes de sécurité à gérer la cryptographie comme une infrastructure critique en simplifiant la PKI, en automatisant la gestion du cycle de vie des certificats et en permettant la crypto-agilité à l'échelle.

Pour plus d'informations, visitez le site www.keyfactor.com ou suivez-nous sur LinkedIn, Twitter, et Facebook.

Construit sur une base de confiance et de sécurité, Keyfactor est fier d'être un employeur qui respecte l'égalité des chances, qui soutient et défend le développement d'un lieu de travail fiable, sécurisé, diversifié et inclusif.

CONTACTEZ-NOUS

- www.keyfactor.com
- +1.216.785.2946