yubico

Protection des clés cryptographiques avec le plus petit module de sécurité matériel du monde

Le YubiHSM 2 est disponible en tant que solution de niveau 3 validée par la norme FIPS 140-2 ou en tant que solution non FIPS, avec les mêmes capacités, et assure une sécurité cryptographique matérielle sans compromis pour les applications, les serveurs et les dispositifs informatiques à une fraction du coût et de la taille des HSM traditionnels.

Sécuriser le cycle de vie de la clé de chiffrement

Les clés de chiffrement stockées dans les logiciels sont vulnérables aux menaces

Le coût de la cybercriminalité mondiale devrait atteindre 6 000 milliards de dollars en 2021, soit une augmentation par rapport aux 3 000 milliards de dollars de 2015.[1] Le stockage logiciel des clés de chiffrement pour les serveurs est de plus en plus vulnérable à mesure que les attaques deviennent plus sophistiquées. Le vol des clés de chiffrement d'un serveur peut entraîner une brèche de sécurité catastrophique. Par exemple, si la clé privée d'une autorité de certification est compromise, un attaquant peut prétendre être votre site Web.

Le YubiHSM 2 et le YubiHSM 2 FIPS changent la donne pour une sécurité efficace des clés

Assurez le stockage et l'exploitation sécurisés des clés cryptographiques matérielles pour les applications, les serveurs et les dispositifs informatiques, tout en éliminant le coût et la complexité des modules de sécurité matériels (HSM) traditionnels. Les solutions HSM de Yubico, résistantes à la falsification, offrent un retour sur investissement à faible coût et de haute sécurité dans un format "nano" portable qui permet une utilisation flexible sur divers appareils et emplacements. Avec le YubiHSM 2 et le YubiHSM 2 FIPS, les organisations peuvent empêcher les clés cryptographiques d'être copiées par des pirates, des logiciels malveillants et des personnes internes ayant de mauvaises intentions. Elles peuvent s'intégrer rapidement au HSM en utilisant le SDK 2.0 open source.

Protection matérielle sécurisée des clés cryptographiques

Les clés cryptographiques stockées dans un logiciel peuvent être copiées et sont vulnérables à la distribution accidentelle et au vol à distance. En l'absence de procédures strictes, il est facile pour les administrateurs ou les initiés malveillants de sauvegarder les clés sur des clés USB, de les transférer par FTP ou de les partager avec d'autres via un service de stockage sur le cloud. En outre, des attaquants sophistiqués peuvent obtenir un accès administrateur ou déployer un cheval de Troie malveillant qui s'installe sur les serveurs, recherche les clés cryptographiques, puis les copie pour les vendre sur des sites Web sombres comme Alphabay.

Les solutions HSM, basées sur du matériel, permettent un stockage et des opérations de clés sécurisés en empêchant la copie et la distribution accidentelles des clés, et en empêchant le vol à distance des clés stockées.

- Stockage et opérations sécurisés des clés sur du matériel inviolable, avec journalisation des audits.
- Capacités cryptographiques étendues, notamment le hachage, l'enveloppement de clés, la signature asymétrique, le décryptage, l'attestation, etc.

Une conception innovante pour une utilisation flexible

Les HSM traditionnels montés en rack et basés sur des cartes ne sont pas pratiques pour de nombreuses organisations en raison des problèmes d'adaptation à la taille du HSM et de la complexité de son déploiement. De plus, l'espace en rack dans les centres de données partagés comprend souvent des boîtiers de serveurs physiques avec des portes métalliques pour sécuriser l'accès, ce qui limite l'espace disponible.

Avec les solutions HSM de Yubico, les organisations peuvent facilement sécuriser les serveurs, les applications, les bases de données, les chaînes de montage, les dispositifs IoT, les échanges de crypto-monnaies et plus encore avec un facteur de forme " nano " portable qui permet un déploiement rapide et flexible dans divers environnements. Le HSM s'insère facilement dans un emplacement USB et s'adapte aux boîtiers de sécurité physique.

[1]Cybersecurity Ventures

- Le facteur de forme “ nano “ permet un déploiement et une utilisation flexibles sur différents appareils et emplacements.
- Port USB-A entièrement dissimulé
- Partageable en réseau pour être utilisé par des applications sur d’autres serveurs.

Faible coût, retour sur investissement élevé en matière de sécurité

Les clés cryptographiques stockées dans un logiciel sont exposées aux pirates et aux attaques de logiciels malveillants. Par ailleurs, les HSM traditionnels peuvent être coûteux à déployer.

Avec les solutions HSM de Yubico, les organisations bénéficient d’une sécurité et d’opérations cryptographiques élevées de niveau entreprise sans le prix des HSM traditionnels.

- Réduction significative des dépenses d’investissement : jusqu’à 90 % moins cher que les HSM traditionnels.
- Réduction de la consommation d’énergie de l’entreprise

Intégration rapide, gestion facile

Avec le SDK de YubiHSM 2, les développeurs peuvent rapidement intégrer le HSM dans les produits et applications d’entreprise avec des capacités telles que la génération et l’importation de clés, la signature et la vérification, ainsi que le cryptage et le décryptage de données. Les développeurs peuvent également rendre ces fonctionnalités accessibles via la norme industrielle PKCS#11.

- Prise en charge d’applications personnalisées à l’aide de bibliothèques open source. Interfaces via YubiHSM KSP, PKCS#11 et bibliothèques natives.
- La gestion à distance réduit la complexité et les coûts de gestion

Traitez les cas d’utilisation existants et émergents

Sécurisez les échanges de cryptomonnaies : Le marché des cryptomonnaies connaît une croissance rapide et sa valeur devrait atteindre mille milliards de dollars en 2018. Cette évolution exponentielle s’accompagne également d’un volume élevé d’actifs qui doivent être protégés pour atténuer les nouveaux risques de sécurité. On recense un nombre croissant de brèches touchant à des échanges. Cela aurait pu être évité grâce à une stratégie de sécurité fondée sur les bonnes pratiques et impliquant un module de sécurité matériel. Avec YubiHSM 2 SDK, les développeurs qui créent des solutions pour les échanges de cryptomonnaies peuvent rapidement intégrer le HSM afin de protéger les clés de chiffrement et d’assurer la sécurité des informations financières confidentielles.

Sécuriser l’Internet des objets (IoT) : L’Internet des objets (IoT) est un domaine en pleine émergence où les systèmes fonctionnent souvent dans des environnements hostiles.[2] La sécurisation des clés de chiffrement est dans ce cas d’autant plus importante que les entreprises doivent protéger les informations confidentielles. De nombreuses applications de l’IdO utilisent des clés de chiffrement, mais le niveau de sécurité actuel est insuffisant. Cela est dû en partie au fait qu’il est compliqué de protéger les clés de chiffrement et d’enregistrer les certificats sur les passerelles ou les proxys de l’IdO, et que les HSM traditionnels sont trop volumineux et trop lourds pour certains environnements IdO, tels que les voitures connectées. Avec le SDK open source, les développeurs qui créent des applications IoT peuvent rapidement intégrer le YubiHSM 2 ou le YubiHSM 2 FIPS ultra portable pour protéger les clés de chiffrement et empêcher les environnements IoT critiques d’être victimes de piratages hostiles.

Sécuriser les services du cloud : Une sécurité forte pour les environnements dans le cloud est essentielle, car les entreprises doivent garantir que leurs données y sont en sécurité. Le HSM peut être déployé dans un centre de données et fonctionner comme un composant d’une infrastructure de cloud. Les organisations ont ainsi l’esprit tranquille, car elles savent que le service d’hébergement sur le cloud de leur choix utilise le HSM dans le cadre de leur offre.

Sécuriser les services de certificats Microsoft Active Directory : Le HSM peut fournir des clés matérielles pour l’implémentation d’une PKI basée sur Microsoft. Le déploiement du HSM pour les services de certificats Microsoft Active Directory protège non seulement les clés privées de l’autorité de certification, mais aussi tous les services de signature et de vérification utilisant la clé privée.[3]

Résumé

Le YubiHSM 2 et le YubiHSM 2 FIPS permettent aux organisations de toutes tailles d’améliorer la sécurité des clés de chiffrement tout au long de leur cycle de vie, de réduire les risques et de garantir le respect des réglementations de conformité. Avec le module YubiHSM SDK 2.0 disponible en open source, les organisations peuvent facilement et rapidement intégrer la prise en charge du HSM dans une large gamme de plateformes et de systèmes pour les cas d’utilisation existants et émergents où une sécurité forte est plus nécessaire que jamais.

[2] https://www.smartcard-hsm.com/2017/02/14/IoT_Devices_with_SmartCard-HSM.html

[3] Remarque : Tous les aspects du YubiHSM 2 SDK 2.0 sont disponibles en open source sauf le Key Storage Provider (KSP) pour une utilisation avec les services de certificats Microsoft Active Directory

Yubico AB
Kungsgatan 44
2nd floor
SE-111 35 Stockholm
Sweden

Yubico Inc.
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301 États-Unis
844-205-6787 (numéro vert)
650-285-0088