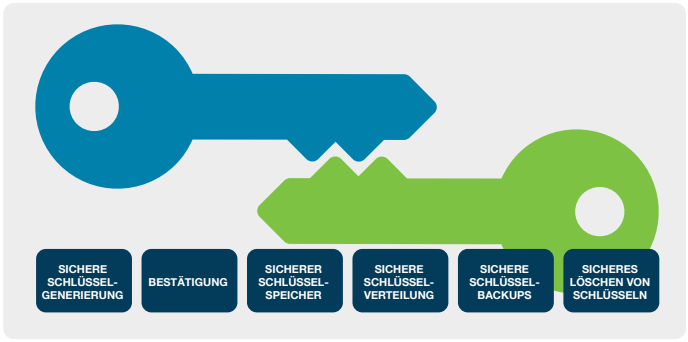
yubico

Schutz für kryptografische Schlüssel mit dem kleinsten Hardware-Sicherheitsmodul (HSM) der Welt

Das YubiHSM 2 ist erhältlich als FIPS 140-2 Level-3 validierte / zertifizierte Lösung sowie als Nicht-FIPS zertifizierte Lösung. Beide Produktlinien haben aber die gleichen Funktionen. Beide Lösungen gewährleisten kompromisslose kryptografische Hardware-Sicherheit für Anwendungen, Server und und Computergeräte YubiHSM 2 YubiHSM 2 FIPS zu einem Bruchteil der Kosten und Größe von traditionellen HSMs.

YubiHSM 2

YubiHSM 2 FIPS



Schutz kryptografischer Schlüssel über den gesamten Lebenszyklus der Schlüssel

In Software gespeicherte kryptografische Schlüssel sind gegenüber Bedrohungen anfällig

Die Kosten der weltweiten Cyberkriminalität werden sich im Jahr 2021 voraussichtlich auf 6 Billionen US-Dollar belaufen, ein Anstieg von 3 Billionen US-Dollar im Jahr 2015[1]. Die Speicherung kryptografischer Schlüssel für Server in Software wird immer anfälliger für immer ausgefeiltere Angriffe. Der Diebstahl kryptografischer Schlüssel von einem Server kann ein katastrophales Datenleck zur Folge haben. Wenn beispielsweise ein privater Schlüssel von einer Zertifizierungsstelle kompromittiert wurde, kann ein Angreifer eine Phishing Site online nehmen, die sich als Ihre Website ausgibt.

Das YubiHSM 2 und das YubiHSM 2 FIPS setzen einen neuen Maßstab für effektive Schlüsselsicherheit

Sichern Sie die Speicherung von kryptografischen Schlüsseln und Operationen für Anwendungen, Server und Computer in Hardware und eliminieren Sie gleichzeitig die Kosten und die Komplexität traditioneller Hardware-Sicherheitsmodule (HSMs). Die HSM-Lösungen von Yubico sind manipulationssicher und bieten einen kostengünstigen, hochsicheren ROI in tragbaren ‘Nano’-Formfaktor, der einen flexiblen Einsatz auf verschiedenen Geräten und Standorten möglich macht. Mit dem YubiHSM 2 und YubiHSM 2 FIPS können Unternehmen verhindern, dass kryptografische Schlüssel von Angreifern, Malware und böswilligen Insidern kopiert werden. Unternehmen können mit Hilfe des Open Source SDKs schnell eigene Lösungen entwickeln oder vorhandende Systeme einfach integrieren.

Sicherer Hardware-Schutz für Kryptografische Schlüssel

In Software gespeicherte kryptografische Schlüssel können kopiert werden und sind anfällig für versehentliche Weitergabe und den Diebstahl aus der Ferne. Ohne strenge Kontrolle ist es für Administratoren oder böswillige Insider ein Leichtes Schlüssel auf USB-Sticks zu sichern, sie per FTP zu übertragen oder sie mit anderen über einen Cloud-Speicherdienst zu teilen. Außerdem können raffinierte Angreifer so Admin-Zugriff erlangen oder Trojaner-Malware einsetzen die sich auf Servern installiert, nach kryptografischen Schlüsseln sucht und diese dann zum Verkauf auf Dark-Web-Seiten wie Alphabay kopiert.

YubiHSM2 und YubiHSM2 FIPS ermöglichen eine sichere Schlüsselspeicherung und Betrieb, indem sie das versehentliche Kopieren und Verteilen von von Schlüsseln und verhindern den Diebstahl von gespeicherten Schlüsseln aus der Ferne.

- Sichere Schlüsselspeicherung und -operationen auf manipulationssicherer Hardware, mit Audit-Protokollierung.
- Umfangreiche kryptografische Funktionen einschließlich Hashing, Key Wrapping, asymmetrisches Signieren, Entschlüsselung, Attestierung und mehr.

Innovatives Design für flexiblen Einsatz

Herkömmliche rackmontierte und kartenbasierte HSMs sind für viele Organisationen nicht praktikabel für viele Unternehmen nicht praktikabel, da die Größe und Komplexität der HSMs. Hinzu kommt, Serverschränke mit Metallgittertüren, um den Zugang zu sichern. Serverschränke mit Metallgittertüren zur Sicherung des Zugangs was den verfügbaren Platz einschränkt.

Mit den HSM-Lösungen von Yubico können Unternehmen problemlos Server, Anwendungen, Datenbanken, Fließbänder, IoT-Geräte Kryptowährungsbörsen und mehr mit einem tragbaren ‘Nano Formfaktor, der einen schnellen und flexiblen Einsatz in verschiedenen Umgebungen

Der YubiHSM 2 oder YubiHSM 2 FIPS passt problemlos in einen USB Steckplatz und liegt fast bündig, um physikalische Sicherheits Gehäusen.

- Der ‘Nano’-Formfaktor ermöglicht eine flexible Bereitstellung und Nutzung über Geräte und Standorte hinweg
- Vollständig verdeckter Einsatz des USB-A-Ports
- Netzwerkfreigabe zur Nutzung durch Anwendungen auf anderen Servern

[1]Cybersecurity Ventures

Niedrige Kosten, hoher Sicherheits-ROI

In Software gespeicherte kryptografische Schlüssel sind anfällig für Hacker und Malware-Angriffe. Alternativ können herkömmliche HSMs kostspielig in der Bereitstellung sein.

Mit den HSM-Lösungen von Yubico erhalten Unternehmen eine hohe kryptografische Sicherheit und einen Betrieb ohne dem traditionellen HSM-Preisschild.

- Signifikante Capex-Reduktion: bis zu 90% günstiger als traditionelle HSMs
- Gerät mit geringem Stromverbrauch reduziert den Energieverbrauch

Schnelle Integration, einfache Verwaltung

Mit dem YubiHSM 2 SDK können Entwickler schnell die Unterstützung für die FIPS- oder Nicht-FIPS-Version des HSM in Unternehmensprodukte und -anwendungen integrieren, mit Funktionen wie Generieren und Importieren von Schlüsseln, Signieren und Verifizieren sowie Verschlüsselung und Entschlüsselung. Entwickler können diese Funktionen auch Funktionen über den Industriestandard PKCS#11 zugänglich machen.

- Unterstützung benutzerdefinierter Anwendungen durch Open-Source Bibliotheken. Schnittstellen über YubiHSM KSP, PKCS#11 und native Bibliotheken
- Fernverwaltung reduziert die Komplexität der Verwaltung und Kosten

Abdeckung aktueller und zukünftiger Anwendungsfälle

Sicherer Umtausch von Kryptowährungen: Der Kryptowährungsmarkt verzeichnet ein rasantes Wachstum und erreicht 2018 voraussichtlich einen Marktwert in Höhe von 1 Milliarde US-Dollar. Dieses enorme Wachstum ist auch mit zahlreichen Assets verbunden, die vor Sicherheitsrisiken geschützt werden müssen. Bei mehreren Kryptowährungsbörsen ist es zu Datenlecks gekommen.Diese Datenlecks nehmen stets zu und hätten allesamt möglicherweise mit einem Best Practice-Sicherheitsansatz unter Beteiligung eines Hardwaresicherheitsmoduls verhindert werden können. Mit dem YubiHSM 2-SDK können Entwickler von Lösungen für Kryptowährungsbörsen das HSM schnell integrieren, um kryptografische Schlüssel und sensible Finanzdaten zu schützen.

Sichere Internet of Things-(IoT-)Umgebungen: Das Internet der Dinge (Internet of Things, IoT) ist ebenfalls ein schnell wachsender Markt, in dem Systeme oft in gefährdeten Umgebungen betrieben werden. Dabei ist die Sicherung kryptografischer Schlüssel noch wichtiger, da Unternehmen sensible Informationen schützen müssen. Kryptografische Schlüssel werden in zahlreichen IoT-Anwendungen mit nur unzureichenden Sicherheitsmaßnahmen verwendet. Das ist teilweise darauf zurückzuführen, dass der Schutz kryptografischer Schlüssel und die Registrierung von Zertifikaten bei IoT-Gateways oder -Proxys bisher kompliziert waren und traditionelle HSMs zu groß und sperrig für bestimmte IoT-Umgebungen wie vernetzte Autos sind. Mit dem Open-Source-SDK können Entwickler von IoT-Anwendungen das tragbare YubiHSM 2 oder YubiHSM 2 FIPS schnell integrieren, um kryptografische Schlüssel zu schützen und die feindliche Übernahme kritischer IoT-Umgebungen zu verhindern.

Sichere Cloud-Services: Hohe Sicherheit für Cloud-Umgebungen ist unerlässlich, da Organisationen sicherstellen müssen, dass ihre Daten in der Cloud geschützt werden. Das HSM kann in einem Rechenzentrum bereitgestellt und als Komponente einer Cloud-Infrastruktur eingesetzt werden. Unternehmen können sich entspannt zurücklehnen, wenn ihr Cloud-Serviceanbieter das YubiHSM 2 im Rahmen seines Angebots verwendet.

Sichere Microsoft Active Directory-Zertifikatdienste: Das HSM kann kryptografische Schlüssel für die Microsoft-basierte PKI-Implementierung eines Unternehmens sicher bereitstellen. Das HSM für Microsoft Active Directory Zertifikatsservices schützt dabei nicht nur die privaten Schlüssel der Zertifizierungsstelle, sondern auch alle Signatur- und Verifizierungvorgänge die den privaten Schlüssel nutzen.

Zusammenfassung

Mit dem YubiHSM 2 und YubiHSM 2 FIPS können Unternehmen aller Größenordnungen die Sicherheit kryptografischer Schlüssel im gesamten Lebenszyklus verbessern, Risiken mindern und die Einhaltung gesetzlicher Vorschriften sicherstellen. Mit dem als Open-Source-SDK verfügbaren YubiHSM SDK 2.0 können Unternehmen Unterstützung für das YubiHSM 2 einfach und schnell in zahlreiche Plattformen und Systeme integrieren, und zwar für aktuelle und zukünftige Anwendungsfälle mit höchsten Sicherheitsanforderungen.

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

[3] Hinweis: Alle Aspekte des YubiHSM 2 SDK 2.0 sind als Open-Source-Elemente verfügbar, mit Ausnahme des Key Storage Provider (KSP) für Microsoft Active Directory-Zertifikatdienste

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

Yubico Inc.
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301 USA
844-205-6787 (gebührenfrei)
650-285-0088