cpl.thalesgroup.com

THALES

Thales Data-Protection-on-Demand-Dienste

Thales Data Protection on Demand ist eine Cloud-basierte Plattform, auf der eine breite Auswahl von Cloud-HSM und Schlüsselverwaltungsdiensten über einen einfachen Online-Marktplatz angeboten wird. Die Luna Cloud-HSM- und Schlüsselverwaltungsdienste auf Data Protection on Demand (DPoD) sorgen einfach, kostengünstig und ohne großen Verwaltungsaufwand für Sicherheit, da keine Hardware angeschafft, installiert und gewartet werden muss. Mit nur einem Klick können Sie den erforderlichen Schutz sowie Dienste bereitstellen, Sicherheitsrichtlinien hinzufügen und in Minutenschnelle auf Nutzungsberichte zugreifen.

Sie haben jederzeit schnellen Zugriff auf eine stetig wachsende Zahl an Cloud-basierten Sicherheitsanwendungen, darunter hunderte, die mit der branchenüblichen PKCS11-Schnittstelle arbeiten. Wählen Sie einfach aus einer sich erweiternden Zahl von Optionen und Integrationen die Sicherheitsdienste aus, die Sie benötigen.

Data Protection on Demand bietet Ihnen Sicherheit, auf die Sie vertrauen können:

- Sichert Cloud-Daten
- Isoliert Schlüssel und Signierprozesse von Zertifizierungsstellen, Hostplattformen und Betriebssystemen
- Automatisiert das Lifecyle-Management und die Verwaltungsprozesse für Ihre Schlüssel
- Skaliert Dienste automatisch mit nur einem Knopfdruck
- Bewährte Zuverlässigkeit mit 99,95 % SLA
- Richtet einen Security-Service in weniger als 5 Minuten ein

Luna Cloud-HSM-Dienste

HSM on Demand

Richten Sie einen Cloud-HSM-Dienst für die kryptographischen Prozesse Ihres Unternehmens ein.

HSM sind sichere und vertrauenswürdige Mechanismen zum Schutz kryptographischer Schlüssel und Geheimnisse. Mit Ihrem HSM können Sie kryptographische Schlüssel erstellen und/oder speichern und so einen allgemeinen Root of Trust für alle Anwendungen und Dienste einrichten. Darüber hinaus können Sie Ihr HSM für kryptographische Operationen wie z. B. die Verschlüsselung/Entschlüsselung von kryptographischen Datenschlüsseln, den Schutz von vertraulichen Daten (Passwörtern, SSH-Schlüssel usw.) und vieles mehr nutzen.

CYBERARK

HSM on Demand für CyberArk

Top-Level-Crypto-Schlüssel der Privileged Access Security Solution von CyberArk in einem HSM sichern.

HSM on Demand für CyberArk bietet einen Root of Trust für die kryptographischen Top-Level-Schlüssel der Privileged Access Security Solution von CyberArk in einem HSM. HSM on Demand für CyberArk erstellt und speichert die Serverschlüssel und bietet so Schutz für private Schlüssel und starke Entropie für die Erstellung von Systemschlüsseln für die Privileged Access Security Solution von CyberArk.

HSM on Demand für digitale Unterschriften

Signiert den Autor von Software- und Firmware-Paketen oder elektronischen Dokumenten digital, um die Integrität des Senders zu garantieren

Digitale Signaturen legen die Identität des Herausgebers von Dokumenten sowie Software- und Firmware-Paketen fest und sind ein Nachweis für die Integrität der signierten Daten. Indem Sie digitale Signaturen kompromittieren, können Angreifer sich als ursprünglicher Autor ausgeben und eigene bösartige Aktualisierungen erstellen (Malware). Die digitalen Signierdienste in Data Protection on Demand schützen die mit den Signieranwendungen in einem HSM-Dienst verbundenen privaten Schlüssel und verhindern, dass diese kompromittiert oder gestohlen werden.

HSM on Demand für Hyperledger

Gewährleistet vertrauenswürdige Blockchain-Transaktionen, um in dezentralen Systemen die erforderlichen kryptographischen Operationen auszuführen.

HSM on Demand für Hyperledger speichert die von den Mitgliedern der Blockchain Hyperledger zum Signieren aller Transaktionen verwendeten privaten Schlüssel und gewährleistet, dass kryptographische Schlüssel nicht von nicht autorisierten Geräten oder Personen für eine Auswahl an Blockchain-Anwendungen von Hyperledger verwendet werden können. HSM on Demand für Hyperledger bietet höchste Sicherheit in Rechenzentren und in der Cloud. Es ermöglicht mehrere Blockchain-Identitäten pro Partition als Transaktionsnachweis und zu Prüfzwecken zu verwenden.

HSM on Demand für Java Code Signer

Erstellt und schützt die mit ihrer Java-Code-Signer-Anwendung assoziierten privaten Schlüssel in einem HSM.

HSM on Demand für Java Code Signer verhindert den Diebstahl oder das Kompromittieren privater Schlüssel, indem es die kryptographischen Operationen eines Java-Anwendungsservers auf ein HSM auslagert. Durch das Erstellen von Signierschlüsseln und Zertifikaten, die HSM-Entropie verwenden, wird die Sicherheit deutlich verbessert und die kryptographischen Operationen für das Code Signing für Java werden innerhalb des HSM-on Demand-Dienstes ausgeführt. Dies führt zudem zu besserer Leistung, da die kryptographischen Operationen aus den Signierservern ausgelagert werden.

HSM on Demand für Active-Directory-Zertifizierungsdienste von Microsoft

Sichert die Schlüssel Ihrer Microsoft-Root-Zertifizierungsstellen (Root-CA) in einem HSM

HSM on Demand für Microsoft ADCS (Active Directory Certificate Services – Active-Directory-Zertifizierungsdienste) stellt einen Root of Trust für den Signierschlüssel einer Microsoft-Root-CA in einem HSM bereit. Dadurch werden die Begrenzungen des kryptographischen Root-Signierschlüssels der CA verstärkt, die dazu dienen, die öffentlichen Schlüssel der Zertifikatsinhaber zu signieren. Die Bereitstellung des Root of Trust für den öffentlichen Schlüssel des CA verstärkt die Sicherheit von Microsoft-Diensten, unter anderem bei der Konfiguration von Anwendungsservern, die Microsoft ADCS in dezentralen Rechenzentren hosten.

HSM on Demand für Microsoft Authenticode

Erstellt und sichert Ihre Microsoft Authenticode-Zertifikate auf einem HSM

HSM on Demand für Microsoft Authenticode verstärkt die Grenzen digitaler Zertifikate von Microsoft Authenticode. Der HSM-on-Demand-Dienst kann in Microsoft Authenticode integriert werden und stellt so ein vertrauenswürdiges System zum Schutz der Unternehmensanmeldedaten des Software-Herausgebers bereit. Außerdem sichert er die von der Code-Signing-Anwendung im HSM-Dienst verwendeten Schlüssel. HSM on Demand für Microsoft Authenticode gewährleistet, dass wichtige Systeme sowie Soft- und Hardwareprodukte von Microsoft anerkannte Standards einhalten und verhindert, dass Unbefugte auf die Signierschlüssel zugreifen.

HSM on Demand für Microsoft SQL Server

Lagert die kryptographischen Operationen von Microsoft SQL-Servern auf ein HSM aus

Der HSM-on-Demand-Dienst stellt einen Root of Trust für die Speicherung der von Microsoft SQL verwendeten Schlüssel bereit, sodass kryptographische Schlüssel nicht am selben Ort wie Verschlüsselungsdaten gespeichert werden. Die Daten können mit kryptographischen Schlüsseln verschlüsselt werden, auf die im HSM-on-Demand-Dienst nur der Datenbanknutzer Zugriff hat. Kryptographische Operationen wie Schlüsselerstellung, Verschlüsselung, Entschlüsselung usw. können auf das HSM ausgelagert werden.

HSM on Demand für Oracle TDE

Gewährleistet, dass die kryptographischen Schlüssel von Oracle TDE mit einem Masterschlüssel geschützt sind, der im HSM gespeichert wird.

Kryptographische Schlüssel werden aus Gründen der Leistung und Skalierbarkeit in der Regel lokal in der Datenbank gespeichert. Das macht allerdings den Schutz der kryptographischen Schlüssel, mit denen die Daten verschlüsselt wurden, zu einem Problem. Dieses kann gelöst werden, indem man die lokalen kryptographischen Schlüssel, häufig als DEK (Data Encryption Keys) bezeichnet, mit einem so genannten Key Encryption Key (KEK) oder Masterschlüssel schützt, der im Key Vault des HSM on Demand gespeichert ist. Dadurch ist gewährleistet, dass ausschließlich autorisierte Dienste eine Verschlüsselung des DEK anweisen dürfen.

HSM on Demand für PKI Private Key Protection

Sichert die privaten Schlüssel von Zertifizierungsstellen, die für die Vertrauenshierarchie einer PKI verantwortlich sind.

PKI-Root-Schlüssel sind die privaten Schlüssel von Zertifizierungsstellen (CA), die für die Vertrauenshierarchie einer PKI verantwortlich sind. Root-CA sind der Vertrauensanker in PKI-Bereitstellungen. Eine Kompromittierung der CA-Schlüssel würde die gesamte Vertrauenshierarchie der PKI und damit auch Ihre Daten gefährden. PKI Private Key Protection schafft Vertrauen durch den Schutz Ihrer privaten Schlüssel

Luna HSM-Backup

Backup und Wiederherstellung für die vor Ort bereitgestellten-Luna-HSM Ihres Unternehmens

Luna HSM Backup ist ein HSM-on-Demand-Dienst, der ein spezielles Backup und einen Wiederherstellungsort für die vor Ort bereitgestellten Luna HSM Ihres Unternehmens bietet. Mit Luna HSM können Sie HSM-Schlüsselmaterial sichern und wiederherstellen. Die Schlüssel werden direkt geklont und können von On-Premises in die Cloud und von der Cloud On-Premises verschoben werden. Für das Backup auf Luna Cloud-HSM, vor Ort befindliche Luna HSM (einschließlich Luna Backup HSM) sowie auf Luna HSM speziell für Azure, IBM und AWS ist automatische Schlüsselreplikation aktiviert (PED-Support ab dem dritten Quartal 2020). Sie haben die Gewissheit, dass das Backup auf einen Luna-Cloud-HSM-Dienst mit hoher Ausfallsicherheit (SLA mit 99,95 % Verfügbarkeit) erfolgt und dass Ihre Schlüssel sicher in nach NIST FIPS 140-2 Level 3 zertifizierter Hardware gespeichert werden.

Partner-Dienste

Keyfactor Code Assure

Code Signing mit der Geschwindigkeit von DevOps – signiert Code sicher und überall

Keyfactor Code Assure zentralisiert die Code-Signing-Operationen auf einer einzelnen intuitiven Plattform. Entwickler haben die Freiheit, einen beliebigen Code schnell und von überall zu signieren, während dieser in einer sicheren Vault verschlossen bleibt.

Keyfactor Control

Die sichere End-to-End-Identitätsplattform für verbundene Geräte

Mit Keyfactor Control können hochgesicherte Identitäten in jede Phase des Lebenszyklus von IoT-Geräten eingebettet werden. Während der Entwicklung, Herstellung, Bereitstellung und der laufenden Verwaltung der sichersten Geräte auf dem Markt bietet Keyfactor Control die entsprechende Identitätsgrundlage. Dadurch haben Sie die Freiheit, großartige Produkte zu entwickeln sowie die Gewissheit, dass deren sichere Bereitstellung über den gesamten Nutzungszeitraum gewährleistet ist.

Keyfactor Command

Sichert die digitalen Identitäten des gesamten Unternehmens.

Keyfactor Command ist die weltweit kompletteste Cloud-basierte Plattform mit der höchsten Skalierbarkeit zur Verwaltung von Zertifikaten. Sie bietet Ihnen die Freiheit, alle Identitäten im gesamten Unternehmen zu sichern. Nutzen Sie alle Vorteile einer PKI, ohne sich um die Risiken kümmern zu müssen. Müssen Sie es unbedingt selbst hosten? Keyfactor Command gibt es auch für beim Kunden gehostete Umgebungen.

Schlüsselverwaltungsdienste on Demand

Key Broker on Demand für Salesforce

Erstellt Schlüsselmaterial (Nutzergeheimnisse) für Salesforce und verwaltet Ihre Schlüssel und Sicherheitsrichtlinien gemeinsam mit Salesforce Shield über deren gesamten Lebenszyklus.

Mit Key Broker on Demand können Sie Richtlinien entwickeln und durchsetzen, um die Einhaltung gesetzlicher Vorschriften zu gewährleisten. Um Ihre Daten aus weiterhin zu sichern und zu schützen, können Sie im Data-Protection-on-Demand-Dienst in der Cloud BYOK (Bring your own key, Bereitstellung eines eigenen Schlüssels) nutzen. Key Broker on Demand stellt eine Dienstebene (GUI/API) bereit. Damit sind Sie in der Lage, Schlüsselmaterial (Salesforce Nutzergeheimnisse) für Salesforce zu erstellen und Ihre Schlüssel gemeinsam mit Salesforce Shield über den gesamten Lebenszyklus zu verwalten.

Wenn Sie das Gesuchte hier nicht finden können, wenden Sie sich bitte an uns unter dpondemand@gemalto.com, um sich über kommende Dienste zu informieren.

Über Thales

Die Menschen, denen Sie den Schutz Ihrer Daten anvertrauen, vertrauen beim Datenschutz auf Thales. Beim Thema Datensicherheit stehen Unternehmen immer häufiger vor entscheidenden Momenten. Egal, ob es darum geht, eine Verschlüsselungsstrategie zu entwickeln, Ihre Daten in die Cloud zu übertragen oder Compliance-Anforderungen zu erfüllen – Sie können sich bei der Sicherung Ihrer digitalen Transformation auf Thales verlassen.

Entscheidende Technologie für entscheidende Momente.