thalescpl.com

THALES

SafeNet Data Protection On Demand

SafeNet Data Protection On Demand von Thales ist eine cloud-basierte Plattform, die zahlreiche Services für das Cloud-HSM-Schlüssel-Management und die Verschlüsselung auf einem zentralen Online-Marktplatz bietet. Durch SafeNet Data Protection On Demand wird Sicherheit noch einfacher, kostengünstiger und leichter zu verwalten, denn es gibt keine Hardware, die angeschafft, bereitgestellt und gepflegt werden muss. Stellen Sie den gewünschten Schutz einfach per Mausklick bereit. Fügen Sie Bereitstellungsdienste und Sicherheitsrichtlinien zu, und rufen Sie in nur wenigen Minuten Berichte zur Nutzung ab.

Wählen Sie Ihren gewünschten Security-Service aus einem wachsenden Angebot an Cloud-basierten Sicherheitsanwendungen, darunter Hunderte, die mit dem Industriestandart PKCS11 arbeiten.

SafeNet Data Protection On Demand von Gemalto bietet eine Sicherheit, der Sie vertrauen können:

- Abgrenzung von Schlüsseln und Signaturoperationen von Zertifizierungsstellen, Host-Plattformen und Betriebssystemen
- Automatisierung manueller Schlüssel-Lebenszyklus-Kontrolle und -Prozesse
- Automatische Skalierung auf eine unbegrenzte Anzahl von Diensten
- Bewährte Zuverlässigkeit
- Einrichten eines Sicherheitsdienstes in weniger als fünf Minuten

HSM-On-Demand-Services

HSM-On-Demand
Richten Sie einen zertifizierten Schlüsselspeicher bzw. Key-Vault für Anwendungen oder Integrationsanforderungen mit Ihrem eigenen HSM-on-Demand-Service ein.

Key-Vaults sind eine sichere und vertrauenswürdige Methode zum Schutz kryptografischer Schlüssel und Geheimnisse. Mit Ihrem Key-Vault können Sie kryptografische Schlüssel generieren und/oder speichern und so eine gemeinsame Vertrauensbasis für alle Anwendungen und Dienste schaffen. Sie können Ihren Schlüsselspeicher beispielsweise auch für kryptografische Maßnahmen wie die Ver- und Entschlüsselung von Datenverschlüsselungs-Keys und den Schutz von Geheimnissen (Passwörter, SSH-Schlüssel usw.) verwenden.

HSM-On-Demand für CyberArk

Schützen Sie den Top-Level-Verschlüsselungs-Key von CyberArk in einem HSM.

HSM-On-Demand für CyberArk bietet eine Vertrauensbasis für den Top-Level-Verschlüsselungs-Key von CyberArk in einem HSM. HSM-On-Demand für CyberArk generiert und speichert Serverschlüssel und bietet privaten Schlüsselschutz sowie eine starke Entropie für die Schlüsselgenerierung der Systemschlüssel der Privileged Access Security Solutions von CyberArk.

HSM-On-Demand für den Schutz privater Schlüssel (PKI)

Schützen Sie private Schlüssel von Zertifizierungsstellen, die für den Aufbau der PKI-Vertrauenshierarchie zuständig sind.

PKI-Root-Keys sind die privaten Schlüssel der Zertifizierungsstelle (CA), die für den Aufbau der PKI-Vertrauenshierarchie verantwortlich ist. Root-Zertifizierungsstellen sind der Vertrauensanker in PKI-Implementierungen. Eine Kompromittierung der CA-Schlüssel würde die gesamte PKI-Vertrauenshierarchie gefährden, was Ihre Daten einem Risiko aussetzt. Der Schutz privater Schlüssel (PKI) schafft Vertrauen, indem Ihre privaten Schlüssel geschützt werden.

HSM-On-Demand für Hyperledger

Bringen Sie Vertrauen in Blockchain-Transaktionen, um die erforderlichen Verschlüsselungsmaßnahmen in verteilten Systemen umzusetzen, und schützten Sie kryptografische Schlüssel, das Blockchain-System und digitale Brieftaschen.

HSM-On-Demand für Hyperledger speichert die privaten Schlüssel, mit denen die Blockchain-Hyperledger-Mitglieder alle Transaktionen signieren, und sorgt dafür, dass kryptografische Keys nicht von unbefugten Geräten oder Personen für eine Reihe von Blockchain-Hyperledger-Anwendungen verwendet werden. HSM-On-Demand für Hyperledger bietet eine hohe Sicherheit für Rechenzentren und die Cloud und unterstützt die partitionsbasierte Mandantenfähigkeit von Blockchain-Identitäten als Transaktionsnachweis und für Audit-Anforderungen.

HSM-On-Demand für digitale Signaturen

Autoren können Software- und Firmware-Pakete und elektronische Dokumente digital signieren, um die Integrität des Absenders zu gewährleisten.

Digitale Signaturen werden verwendet, um die Identität des Herausgebers von Dokumenten, Software- und Firmware-Paketen festzustellen und um die Integrität der signierten Daten nachzuweisen. Die Kompromittierung digitaler Signaturschlüssel ermöglicht es Angreifern, sich als der ursprüngliche Autor auszugeben und eigene bösartige Updates (Malware) zu erstellen. Mit einem Service für digitale Signaturen von SafeNet Data Protection On Demand können Sie die privaten Keys schützen, die mit Ihrer Signaturanwendung in einem HSM-Dienst verbunden sind, und so verhindern, dass die privaten Schlüssel gestohlen oder kompromittiert werden.

HSM-On-Demand für Oracle TDE

Stellen Sie sicher, dass Oracle-TDE-Datenbank-Datenverschlüsselungs-Keys mit einem Master-Key des HSM-On-Demand-Service verschlüsselt werden, um eine optimale Leistung und Skalierbarkeit zu gewährleisten.

Aus Leistungs- und Skalierbarkeitsgründen werden Verschlüsselungs-Keys normalerweise lokal in der Datenbank vorgehalten. Hier stellt sich allerdings die Frage, wie die zur Verschlüsselung von Daten verwendeten Keys geschützt werden können. Die Lösung: Alle lokalen Verschlüsselungs-Keys einschließlich Data Encryption Keys (DEK) werden mit einem Key Encryption Key (KEK) bzw. Master-Key verschlüsselt, der im HSM-On-Demand-Serviceschlüsselspeicher hinterlegt ist. Damit wird sichergestellt, dass nur entsprechend autorisierte Dienste berechtigt sind, den DEK zu entschlüsseln.

HSM-On-Demand für Java-Code-Signaturen

Signieren Sie Java-Artefakte mit einem Verschlüsselungs-Key, der auf einem HSM generiert wurde.

Mit HSM-On-Demand für Java-Code-Signaturen können Sie verhindern, dass private Schlüssel gestohlen oder kompromittiert werden, indem Sie kryptografische Operationen des Java-Anwendungsservers auf ein HSM auslagern. Die Sicherheit wird durch die Erstellung von Signaturschlüsseln und Zertifikaten unter Verwendung der HSM-Entropie deutlich erhöht, und kryptografische Java-Code-Signaturvorgänge werden innerhalb des HSM-on-Demand-Service durchgeführt. Darüber hinaus wird die Leistung verbessert, da kryptografische Operationen von Signaturservern ausgelagert werden.

HSM-On-Demand für Microsoft Active Directory Certificate Services

Schützen Sie die Schlüssel Ihrer Microsoft Root Certificate Authority (CA) in einem HSM.

HSM-On-Demand für Microsoft AD CS (Active Directory Certificate Services) bietet eine Vertrauensbasis für den Signaturschlüssel der Microsoft Root Certificate Authority (CA) in einem HSM. HSM-On-Demand für Microsoft AD CS setzt gehärtete Grenzen für den kryptografischen Root-Signatur-Key der Microsoft Root Certificate Authority, mit dem die öffentlichen Schlüssel der Zertifikatsinhaber signiert werden. Durch die Bereitstellung der Vertrauensbasis für den öffentlichen Schlüssel der CA wird die Sicherheit von Microsoft gestärkt, z. B. bei der Konfiguration von Anwendungsservern, die Microsoft AD CS in verteilten Rechenzentren hosten.

HSM-On-Demand für Microsoft Authenticode

Generieren und schützen Sie Ihre Microsoft-Authenticode-Zertifikate auf einem HSM.

HSM-On-Demand für Microsoft Authenticode bietet gehärtete Grenzen für digitale Microsoft-Authenticode-Zertifikate. Der HSMoD-Service lässt sich in Microsoft Authenticode integrieren und schafft so ein vertrauenswürdiges System zum Schutz der organisatorischen Anmeldeinformationen des Softwareanbieters. Die von der Singaturanwendung innerhalb des HSM-Service verwendeten Keys werden geschützt. Durch die Verwendung von HSM-On-Demand für Microsoft Authenticode können Benutzer sicherstellen, dass relevante Microsoft-Systeme sowie Soft- und Hardwareprodukte den anerkannten Standards entsprechen und verhindern, dass Signaturschlüssel von unbefugten Personen genutzt werden.

HSM-On-Demand für Microsoft SQL Server

Aktivieren Sie die Verschlüsselung von Microsoft SQL Server auf einem HSM.

Der HSM-On-Demand-Service bietet eine Vertrauensbasis für die Speicherung von Schlüsseln, die in Microsoft SQL verwendet werden. Verschlüsselungs-Keys werden nicht zusammen mit Verschlüsselungsdaten gespeichert. Daten können mit Verschlüsselungs-Keys verwendet werden, auf die nur der Datenbankbenutzer im HSM-On-Demand-Dienst Zugriff hat. Kryptografische Vorgänge wie die Schlüsselerstellung, Verschlüsselung, Entschlüsselung usw. lassen sich an das HSM übertragen.

On-Demand-Services für das Schlüssel-Management

Key Broker On Demand für Salesforce

Erstellen Sie Schlüsselmaterial (Mandantengeheimnisse) für Salesforce, und verwalten Sie Ihre Schlüssel und Sicherheitsrichtlinien zusammen mit Salesforce Shield über den gesamten Lebenszyklus hinweg.

Mit Key Broker On Demand können Sie Richtlinien erstellen und durchsetzen und so die Compliance sicherstellen. Um die Sicherheit und Vertraulichkeit Ihrer Daten zu gewährleisten, können Sie Ihren eigenen Schlüssel (Bring Your Own Key, BYOK) innerhalb des SafeNet Data Protection On Demand Service in der Cloud nutzen. Key Broker On Demand bietet eine Service-Ebene (GUI/API) und ermöglicht es Ihnen, Schlüsselmaterial (Salesforce-Mandantengeheimnis) für Salesforce zu erstellen und Ihre Schlüssel mit Salesforce Shield über den gesamten Lebenszyklus hinweg zu verwalten.

Sie haben die gewünschten Informationen nicht gefunden? Kontaktieren Sie uns, um alles über künftige Services zu erfahren: dpondemand@gemalto.com

Über Thales

Die Menschen, denen Sie für den Schutz ihrer Privatsphäre vertrauen, vertrauen Thales, um ihre Daten zu schützen. Wenn es um Datensicherheit geht, werden Organisationen mit einer steigenden Zahl von entscheidenden Momenten konfrontiert. Egal ob der Moment das Erstellen einer Verschlüsselungsstrategie, der Wechsel in die Cloud, oder die Durchsetzung von Compliance ist - Sie können Thales vertrauen, um Ihre digitale Transformation zu sichern.

Entscheidende Technologie für entscheidende Momente.

> thalescpl.com <

Americas – Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100, Austin, TX 78759 USA • Tel: +1 888 343 5773 or +1 512 257 3900 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com