cpl.thalesgroup.com

THALES

Serviços Thales Data Protection on Demand

Thales Data Protection on Demand é uma plataforma em nuvem que oferece uma ampla gama de serviços de segurança de hardware e gerenciamento de chaves em nuvem através de um simples mercado online. Com Luna Cloud HSM e serviços de gerenciamento de chave Data Protection on Demand (DPoD), a segurança fica mais simples, mais rentável e mais fácil de gerenciar porque não é preciso comprar hardware, instalá-lo e fazer sua manutenção. Basta clicar e instalar a proteção que você precisa, provisionar serviços, adicionar políticas de segurança e obter relatórios de uso em minutos.

Com uma crescente variedade de aplicativos de segurança em nuvem ao seu alcance, incluindo centenas que usam a interface PKCS11 padrão do setor, selecione o serviço de segurança que você precisa a partir de uma gama crescente de opções e integrações.

Data Protection on Demand oferece segurança que você pode confiar:

- Dados seguros na nuvem
- Isola chaves e operações de assinatura das autoridades certificadoras, plataformas de hospedagem e sistemas operacionais
- Automatiza controle e processos do ciclo de vida das chaves
- Escalabilidade automática com o clique de um botão
- Segurança comprovada com 99,95% de garantia de nível de serviço (SLA)
- Configure um serviço de segurança em menos de 5 minutos

Serviços Luna Cloud HSM

HSM on Demand

Configure e acesse um serviço de HSM em nuvem para as operações criptográficas da sua empresa.

HSMs são mecanismos seguros e confiáveis utilizados para proteger chaves criptográficas e segredos. Utilize seu HSM para gerar e/ou armazenar chaves criptográficas, estabelecendo um ponto comum de confiança para todas os aplicativos e serviços. Você também pode utilizar seu HSM para realizar operações criptográficas como criptografia/decriptação de chaves de criptografia de dados, proteção de segredos (senhas, chaves SSH etc.), e muito mais.

HSM on Demand para CyberArk

Chave de criptografia da Solução de Segurança de Acesso Privilegiado CyberArk de alto nível em um HSM.

O HSM On Demand para CyberArk oferece um ponto comum de confiança em um HSM para a chave de criptografia da solução de segurança de acesso privilegiado CyberArk . O HSM on Demand para CyberArk gera e armazena as chaves do servidor, fornecendo proteção de chave privada e forte entropia para a geração de chaves para o sistema de chaves da solução de segurança de acesso privilegiado CyberArk.

HSM on Demand para assinatura digital

Assinatura digital do autor de pacotes de software e firmware ou documentos eletrônicos para assegurar a integridade do remetente.

As assinaturas digitais são utilizadas para estabelecer a identidade do editor de pacotes de documentos, software e firmware, e para comprovar a integridade dos dados assinados. O comprometimento de chaves de assinatura digital permite a invasores se passar pelo autor original e criar suas próprias atualizações mal-intencionadas (malware). Os serviços de assinatura digital da solução Data Protection on Demand protegem as chaves privadas associadas à assinatura de aplicativos em um serviço HSM e previnem que as chaves sejam atacadas ou roubadas.

HSM on Demand para Hyperledger

Proteção segura das transações em blockchain para executar as operações de criptografia necessárias em sistemas distribuídos.

O HSM on Demand para Hyperledger armazena as chaves privadas utilizadas pelos membros do blockchain Hyperledger para assinar todas as transações, e assegura que as chaves criptográficas não possam ser utilizadas por dispositivos ou pessoas não autorizadas para algumas dos aplicativos do blockchain Hyperledger. O HSM on Demand para Hyperledger oferece alta segurança nos data centers e em nuvem, permitindo vários usuários de identidades blockchain por partição como prova de transação e para requisitos de auditoria.

HSM on Demand para Java Code Signer

Gera e protege as chaves privadas associadas com seu aplicativo Code Signer em um HSM.

Com o HSM on Demand para Java Code Signer é possível impedir que chaves privadas sejam roubadas ou atacadas através da transferência de operações criptográficas do servidor de aplicativos Java para um HSM. A segurança é significativamente fortalecida através da geração de chaves de assinatura e certificados que utilizam entropia de HSM e as operações de criptografia de assinatura de código Java são executadas no Serviço HSM on Demand. Além disso, isso melhora o desempenho, pois as operações criptográficas são transferidas dos servidores de assinaturas.

HSM on Demand para Microsoft Active Directory Certificate Services

Protege as chaves de seu Microsoft Root Certificate Authority (CA) em um HSM.

O HSM on Demand para Microsoft ADCS (Active Directory Certificate Services) fornece um ponto de confiança para o Microsoft Root Certificate Authority (CA) assinar a chave em um HSM. Isso impõe limites fortalecidos para a chave raiz de assinatura criptográfica da CA, usada para assinar as chaves públicas dos detentores de certificados. Ao fornecer o ponto de confiança para a chave pública da CA, a segurança da Microsoft é fortalecida, como ao configurar servidores de aplicativos que hospedam o Microsoft ADCS em data centers dispersos.

HSM on Demand para Microsoft Authenticode

Gera e protege seus certificados Microsoft Authenticode em um HSM.

O HSM on Demand para Microsoft Authenticode fornece limites fortalecidos para certificados digitais Microsoft Authenticode. O serviço HSM on Demand integra-se com o Microsoft Authenticode para fornecer um sistema confiável para proteger as credenciais empresariais do editor do software, e protege as chaves utilizadas pelo aplicativo de assinatura de código dentro do serviço HSM. O HSM on Demand para Microsoft Authenticode assegura que os sistemas, software e produtos de hardware relevantes da Microsoft sigam os padrões aprovados, e impedem o acesso às chaves de assinatura por entidades não autorizadas.

HSM on Demand para Microsoft SQL Server

Transfere as operações criptográficas do Microsoft SQL Server para um HSM.

O serviço HSM on Demand fornece o ponto de confiança para armazenamento de chaves utilizadas no Microsoft SQL, a fim de que as chaves de criptografia não residam com dados de criptografia. Os dados podem ser criptografados utilizando chaves de criptografia que apenas o utilizador da base de dados tem acesso no serviço HSM on Demand e operações criptográficas como criação de chaves, criptografia, decriptação etc. podem ser transferidas para o HSM.

HSM on Demand para Oracle TDE

Assegura que as chaves de criptografia TDE Oracle sejam protegidas por uma chave mestra que reside no HSM.

As chaves de criptografia são geralmente armazenadas localmente na base de dados por razões de desempenho e escalabilidade, mas isso gera um problema de como proteger as chaves de criptografia que foram utilizadas para criptografar dados. A solução é proteger as chaves de criptografia locais, geralmente chamadas de chaves de criptografia de dados (Data Encryption Keys, DEK) com uma chave principal de criptografia de dados (Key Encryption Key, KEK) ou chave principal que reside no cofre de chaves do serviço HSM on Demand. Isso garante que apenas os serviços autorizados tenham permissão para descriptografar as DEK.

HSM on Demand para proteção de chave provada de PKI

Chaves privadas seguras pertencentes às autoridades de certificação responsáveis pelo estabelecimento da hierarquia de confiança da PKI.

As chaves raiz da PKI são as chaves privadas pertencentes à Autoridade Certificadora (CA) responsável por estabelecer a hierarquia de confiança da PKI. As Autoridades Certificadoras Raiz são a âncora de confiança para instalações de PKI e o comprometimento destas chaves comprometeria toda a hierarquia de confiança da PKI, deixando seus dados em risco. A solução PKI Private Key Protection gera confiança ao proteger suas chaves privadas.

Luna HSM Backup

Faz backup e restaura os HSMs Luna locais da sua empresa.

O Luna HSM Backup é uma oferta de serviço HSM on Demand que realiza backup dedicado e reabilita um local para os HSMs Luna locais da sua empresa. Com os HSMs Luna, é possível fazer backup de segurança e restaurar as chaves do HSM. As chaves são diretamente clonadas e podem passar de uma unidade local para a nuvem e da nuvem para uma unidade local. A replicação automática de chaves é ativada para backup para HSM Cloud Luna, HSMs Luna locais (incluindo Luna Backup HSM) e também para HSMs Luna dedicados Azure, IBM e AWS (suporte PED no 3º trimestre de 2020). Garantimos que o backup realizado dos serviços HSM Cloud Luna é para um serviço HSM Cloud Luna resiliente (99,95% SLA), e suas chaves são armazenadas seguramente em um hardware com certificação NIST FIPS 140-2 Nível 3.

Serviços associados

Keyfactor Code Assure

A assinatura de código à velocidade do DevOps, assina com segurança qualquer código em qualquer lugar.

O Keyfactor Code Assure centraliza as operações de assinatura de código em única plataforma intuitiva. Os programadores podem ter a liberdade de assinar rapidamente qualquer código, de qualquer lugar, enquanto as chaves permanecem fechadas em um cofre seguro.

Keyfactor Control

A plataforma de identidade com segurança ponta-a-ponta para dispositivos conectados.

O serviço Keyfactor Control torna fácil e acessível a incorporação de uma identidade segura de alta segurança em cada passo do ciclo de vida de um dispositivo IoT. Através da concepção, produção, instalação e gestão contínua, o Keyfactor Control fornece a base de identidade necessária para produzir e manter os dispositivos mais seguros do mercado - oferecendo a liberdade de conceber grandes produtos e a confiança de que esses serão instalados e permanecerão seguros durante todo o tempo que estiverem em uso.

Keyfactor Command

Identidade digital segura para toda a empresa.

O Keyfactor Command é a plataforma de gestão de certificados baseada em nuvem mais completa e escalável do mundo, oferecendo liberdade para proteger todas as identidades da empresa. Obtenha todos as vantagens de possuir PKI sem ter riscos. É mesmo necessário que você tenha que fazer o serviço de gestão? O Keyfactor Command também está disponível para ambientes hospedados por clientes

Key Management on Demand Services

Key Broker on Demand para Salesforce

Cria materiais importantes (segredos do tenant) para o Salesforce e gerencia suas chaves e políticas de segurança em conjunto com o Salesforce Shield em todo o seu ciclo de vida.

Utilizando o Key Broker on Demand é possível criar e aplicar políticas, ajudando a garantir a conformidade. Para garantir ainda mais a segurança e privacidade dos seus dados, é possível trazer a sua própria chave (BYOK) para o serviço Data Protection on Demand na nuvem. Através de uma camada de serviço (GUI/API), o Key Broker on Demand possibilita que você crie materiais de chaves (Salesforce tenant secret) para o Salesforce e gerencia suas chaves do Salesforce Shield em todo o ciclo de vida.

Se você não encontrar o que procura aqui, contacte-nos para saber sobre novos serviços: dpondemand@gemalto.com

Sobre a Thales

As pessoas em quem você confia para proteger sua privacidade confiam na Thales para proteger seus dados. Em termos de segurança de dados, as organizações enfrentam cada vez mais momentos decisivos. Seja na criação de uma estratégia de criptografia, migração para a nuvem ou cumprimento de normas de conformidade, você pode confiar na Thales para proteger sua transformação digital.

Tecnologia decisiva para momentos decisivos.

> cpl.thalesgroup.com <

Américas – Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100, Austin, TX 78759 USA • Tel.:+1 888 343 5773 ou +1 512 257 3900 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Ásia- Pacífico – 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: apacsales.cpl@thalesgroup.com
Europa, Oriente Médio e África – 350 Longwater Ave, Green Park, Reading, Berkshire, UK RG2 6GF • Tel.:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com