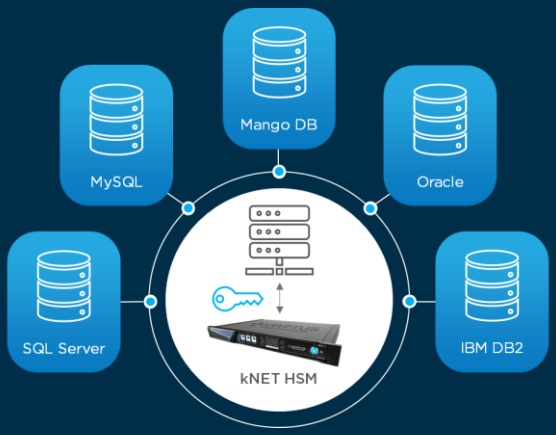
KRYPTUS
shaping trusted bonds

KEY MANAGEMENT SOLUTION

GESTÃO CENTRALIZADA E SEGURA DAS CHAVES CRIPTOGRÁFICAS

A solução **Kryptus KMS** combina a orquestração do ciclo de vida das chaves criptográficas e a aplicação automática de criptografia com a segurança baseada em hardware de alta performance para a guarda segura e processamento das chaves.

Realizando a gestão e a distribuição das chaves criptográficas, a solução **Kryptus KMS** controla o uso de chaves para aplicativos, banco de dados e comunicações.



CRIPTOGRAFIA DE BANCO DE DADOS

- Integração nativa ou TDE transparente, para vários tipos de base de dados.
- Conectores especiais Oracle e SQL Server.
- Totalmente compatível com o protocolo KMIP, permitindo compatibilidade com a criptografia nativa para dados estruturados ou não estruturados.
- TDE é a opção nativa para vários sistemas.
- Implementa a adequação aos privilégios para dar acesso às chaves usadas no TDE, criptografando e controlando seu uso.

CRIPTOGRAFIA DE BANCO DE DADOS NÃO ESTRUTURADOS

Realiza a orquestração de chaves nos modelos HYOK e BYOK em um ambiente multicloud.

- Integração via KMIP para controlar privilégios de criptografia em VM, VSAN e NSX.
- Gerenciamento das chaves mestras de clientes da AWS e outros requisitos de gerenciamento de chaves.
- APIs de orquestração para registrar as chaves no Gerenciamento de Chaves do Azure.
- Integrável ao Google Cloud.
- Storages: Via KMIP em produtos como Dell, HPE 3PAR, NetApp, Racktop, Cray.

CENTRALIZE O GERENCIAMENTO DE CHAVES COM KRYPTUS KMS.

ESCALABILIDADE

Proteção contínua com capacidade para armazenar milhões de chaves.

AUTOMATIZAÇÃO

Agenda e executa operações criptográficas em milhões de chaves de uma só vez.

COMPATIBILIDADE

Integra-se perfeitamente com tecnologias legadas, atuais e futuras.

CONFORMIDADE

Oferece relatórios completos e suporte para auditorias de conformidade.

PROTEÇÃO DE CHAVES COM KNET HSM

A proteção de chaves é feita através da integração do Kryptus KMS a módulos de segurança de hardware kNET HSM que promovem o armazenamento seguro de chaves em configurações independentes e de alta disponibilidade.
kNET HSM da Kryptus é um dispositivo multiuso de máxima segurança, projetado para oferecer um ambiente escalável e de alto desempenho para armazenamento, gerenciamento e operações de chaves criptográficas.

- FIPS 140-2 nível 3 (EFP/EFT)
- ICP-Brasil NSH3
- Separação em HSM virtuais (multitenant)
- Criptografia simétrica e assimétrica
- APIS: KMIP, PKCS#11, Microsoft CSP, Java JCA/JCE
- Duplo fator de autenticação (TOTP, HOTP)
- Proteções físicas e lógicas contra abertura, boot seguro, sensores de temperatura e tensão.

FIPS Level 3 Certified 140-2

ICP Brasil

PRINCIPAIS CARACTERÍSTICAS

INTEROPERABILIDADE

- Interface totalmente compatível com KMIP 1.0–1.4.
- Suporte de agentes para diversos sistemas, banco de dados, file server e aplicação.
- Serviços KMIP através de TTLV, HTTPS, JSON e XML.
- Registro CEF para integração rápida do SIEM.
- Capacidade de encaminhar operações KMIP para outras administradores de chaves compatíveis com KMIP.
- Suporte a Microsoft EKM.
- Interface PKCS # 11 e KMIP para integração com KNET HSM.
- Criptografa e gerencia máquinas virtuais por meio de interoperabilidade com VMware vSphere e vSAN.

EXTENSIBILIDADE

- Serviços RESTful para integrar o Kryptus KMS com serviços corporativos existentes.
- Script personalizado Kryptus KMS para automatizar operações complexas de criptografia e gerenciamento de chaves.
- Capacidade de cifrar sistemas de arquivos, máquinas virtuais, políticas e segredos.
- Conectores de pseudonimização e anonimização para atender à LGPD, com agentes de criptografia para preservação de formato, tokenização e mascaramento em padrão FIPS.
- Gestão de certificados com busca e varredura de chaves.
- Orquestradores Windows e Linux para tradução de protocolos baseados em serviços Microsoft KMIP, autoridades de certificação, NETCONF, entre outros.

ESCALABILIDADE

- Kryptus KMS Data Store foi projetado para manter um repositório de centenas de milhões de chaves.
- Alta disponibilidade e backups completos usando replicação criptografada com dispositivos Kryptus KMS Geo-Separated para garantir a guarda das chaves.
- Programação Kryptus KMS para executar scripts de automação.

SEGURANÇA

- Os dispositivos Kryptus KMS são executados com SELinux no modo obrigatório para proteger os processos em execução e manter protocolos rígidos.
- Funções de usuário para gerenciamento do sistema e política de chaves que permitem a separação de controles.
- A função Policy Engine permite definir serviços de pontos de decisão criptográfica para a integridade de pessoas em escala IoT.
- Política Kryptus KMS para definir regras de autorização nas operações de gerenciamento de chaves externas.
- Conexões TLS mútuas para distribuição de chaves, objetos de segurança, gerenciamento, políticas eficazes e instruções de orquestração.
- A segurança posicional impõe controles de acesso obrigatórios dependendo de onde uma determinada conexão de cliente está associada na hierarquia do Kryptus KMS.
- Todos os dispositivos Kryptus KMS usam unidades de autocriptografia com certificação FIPS para garantir a segurança de dados caso uma unidade seja removida fisicamente.

KRYPTUS
shaping trusted bonds

HQ

+55 (19) **3112-5000**

faleconosco@kryptus.com

Rua Maria Teresa Dias da Silva, 270
Campinas –SP, Brazil

www.kryptus.com

EMEA

+41 **79 932 19 23**

kryptus.emea@kryptus.com

Rue Galilée 7,1400, Yverdon
Switzerland