

Procrypt KM-X HSM — Datasheet

Genel Bakış

Procrypt KM-X, Procenne Teknoloji A.Ş. tarafından geliştirilen, PCI HSM v3 sertifikalı, 19" rack mount Hardware Security Module'dür. Anahtar üretimi, saklama ve kriptografik işlemleri tamper protection korumalı donanım içinde gerçekleştirir; çoklu izole partition yapısıyla birden fazla uygulamaya aynı anda hizmet verir.

Öne Çıkan Özellik	Değer
Sertifikasyon	PCI HSM v3 veya üzeri
Performans	≥ 1.000 RSA-2048 RAW Sign/sn
İzole partition (slot)	10 (lisansla artırılabilir)
Bağlantılı uygulama sunucusu	10 (lisansla artırılabilir)
API	PKCS#11 (Windows / Linux)
Yüksek erişilebilirlik	HA ve Round Robin load balancing

Donanım Özellikleri

Parametre	Değer
Form faktör	19" rack mount
Güç girişi	100–240 V AC, 50–60 Hz
Güç kaynağı	2 adet dahili redundant PSU
Network	2 × 1 GbE Ethernet
Dahili depolama	≥ 3 GB
Fiziksel güvenlik	Tamper protection; manuel Emergency Erase (acil silme) mekanizması
Etiketleme	Silinmeyen malzemedan seri numarası etiketi
Yaşam döngüsü	Üretimi devam eden ürün (EoL değil)

PROCENNE TEKNOLOJİ ANONİM ŞİRKETİ
Üniversite Mah. Sarıgül Sk. B Blok No:37/1
İç Kapı No:72 Avcılar/İstanbul
Avcılar V.D.No.: 1331009988
İTO Sicil No: 390792-0

Kriptografik Özellikler

Kategori	Desteklenen
Asimetrik	RSA 1024–4096 bit; ECC (P-192, P-224, P-256, P-384, P-521); ECDH (P-192, P-224, P-256, P-384, P-521)
ECC şifreleme	Desteklenir
Simetrik	AES, DES, 3DES
Simetrik modlar	ECB, CBC, OFB64, CFB-8
Hash	SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
MAC	HMAC (SHA ailesi), TDES CMAC, AES CMAC
RNG	NIST SP 800-90 uyumlu; simetrik ve asimetrik anahtar üretimi
Anahtar üretimi	On-board key generation ve cihaz içinde güvenli saklama
Performans	≥ 1.000 RSA-2048 RAW Sign/sn

Partition ve Uygulama Desteği

Parametre	Değer
İzole partition (slot)	10 adet, lisansı dahil; ek lisansla artırılabilir
Partition izolasyonu	Tam izolasyon; her partition'ın bağımsız administrator'ı
Erişim kimlik doğrulaması	Partition başına ayrı parola
Eşzamanlı uygulama sunucusu	10 adet; ek lisansla artırılabilir
İşlem modeli	Network üzerinden gelen isteklerde multi-threaded işleme
API	PKCS#11
Client OS	Windows, Linux (PKCS#11 kütüphaneleri dahil)

PROCENNE TEKNOLOJİ ANONİM ŞİRKETİ
Üniversite Mah. Sarıgül Sk. B Blok No: 37/1
İç Kapı No: 72 Avcılar / İstanbul
Avukat V.D. No: 7331009983
İTO Sicil No: 890792-8

Yönetim, Yedekleme ve Loglama

Parametre	Değer
Yönetim arayüzü	GUI; cihazla güvenli (şifreli) iletişim
Uzaktan yönetim	Desteklenir
Rol tabanlı erişim	Administrator, Operator vb. Pkcs11 rol ve yetki seviyeleri
Key backup / restore	Tanımlı prosedürlerle güvenli yedekleme ve geri dönüş
Cihazlar arası klonlama	Mevcut HSM'lerdeki tüm objelerin güvenli kanal üzerinden eksiksiz klonlanması
Yerel loglar	Usage, audit ve error logları cihaz üzerinde tutulur
Merkezi loglama	Audit ve system loglarının Syslog ile merkezi log sunucusuna iletimi

Yazılım Çözümü ve Kullanım Alanları

Parametre	Değer
High Availability	HA modu desteklenir
Load balancing	HSM'ler arası yük dağıtımı; Round Robin
Uygulama	Pkcs11 ile EMV, 3D Secure, e-cüzdan, online bankacılık uygulamaları
İmzalama	Pkcs11 ile E-İmza, E-Fatura, güvenli e-posta
Diğer kullanım alanları	Pkcs11 ile Database encryption, authentication, SSL termination
Kayıt yönetimi	Audit, event ve system loglarının oluşturulması ve yönetimi

Sertifikasyon ve Teslimat Kapsamı

Parametre	Değer
Sertifika	PCI HSM v3 veya üzeri
Kutu içeriği	HSM cihazı, tüm bağlantı ve güç kabloları, driver ve yönetim yazılımları

Parametre	Değer
Lisans	10 partition ve 10 uygulama sunucusu lisansı dahil
Teslimat durumu	Orijinal ambalajında, yeni ve kullanılmamış

PROCENNE TEKNOLOJİ ANONİM ŞİRKETİ
Üniversite Mah. Sarıgül Sk. 3 Blok No: 37/1
İç Kapı No: 72 Avcılar / İstanbul
Avcılar V.D. No.: 7331009900
İTO Sicil No: 890792-0