ProCrypt

prOLenne DIGITAL SECURITY

Simple, Stable, Secure:

ProCrypt HSM

Single Platform for Payment Systems and General Purpose

Meet the needs for both payment systems and general purpose in a single platform with ProCrypt HSM, which is the Turkey's first and among the firsts in the world that received PCI HSM 4.x certificate.

ProCrypt HSM offers a high level of security and performance in banking transactions, digital transformation projects and general data protection with its scalable architecture and platform-independent 24/7 operating principle.

COMMON CRITERIA CERTIFIED EAL4+

PCI Security Standards Council®

9001 ISO CERTIFIED · 27001 ISO CERTIFIED · 15504 ISO CERTIFIED · ENVIRONMENTAL MANAGEMENT SYSTEM ISO 14001 · RoHS · CE

Türkiye Discover the potential

General Purpose – Payment Systems

PKI Certificate Signing and Verification	Payment Systems	SSL/TLS	Database Security	e-Signature and e-Invoice
Web and Mobile App Security	IOT/5G	Blokchain Security	Personal Data Protection Law	Cloud Security

ProCrypt HSM

ProCrypt HSM's protected, hardened and innovative design enables it to perform **cryptographic operations** and protect encryption keys at the hardware security level.

Being both internationally certified **(PCI HSM, CC EAL 4+, RoHs, CE, Made in Türkiye)** and local and national production ProCrypt HSM can be used in different areas with only one hardware and the appliance can run all the functions about HSM simultaneously.

High-tech product ProCrypt HSM is designed with **uninterruptable spec (24/7)** and **high performance (up to 10.000 TPS).**

ProCrypt HSM can be scaled horizontally with the compact and scalable architecture and is **platform independent** for usage to different scenarios.

With PCAM (ProCrypt Admin Management) ProCrypt HSM provides **ease to key configuration** and importing and allow the user to manage these operations with an easy and secure GUI.

ProCrypt HSM provides strong authentication, **hierarchical and independent role-based user management with a high-security point of view.**

ProCrypt HSM stores strong integration specs with **a simple, stable, and high-tech infrastructure.**

Technical Specifications

KM-X

Physical Characteristics	**Size**	1 U - 482.6mm x 738mm x 44.1mm (19" x 29" x 1.74")
	Weight	12kg (26,45 lbs)
	Input Voltage	100 - 240V, 50 - 60Hz, 40w Dual Hot Swappable Power Supply
	Operating Temperature	0°C - 40°C (32°F - 104°F)
	Humidity	%10 - %90 (relative, non condensing)
	Connection Interface	2 x 10/100/1000 Mbps
	Resilience	Mean Time Between Failures (MTBF) 100,536 hrs
Cryptographic Algorithms	**HASH/Message Digest/HMAC**	MD5, MD5-HMAC, SHA-1, SHA-2, SHA-1 HMAC, SHA-2 HMAC, RIPEMD, RIPEMD160, RIPEMD160_HMAC, RIPEMD160_RSA_PKCS,BLAKE2B, BLACK2s, MD4, SM3, SipHash
	Symmetric	AES, DES, DES3 (TripleDES), ARIA, BLOWFISH, CAMELLIA , RC2, RC4, SEED, DES-X, SM4
	Asymmetric	RSA (up to 4096 bits), DHE, ECDH, DSA, ECDSA, X9.42 DH, ED25519, ED448, Poly1305, SM2, CMAC
	RNG	NIST SP 800-90 Compatible TRNG
	5G	MILENAGE, TUAK, SNOW 3G, ZUC, SNOW V
	Post Quantum	KYBER, DILITHUM, FALCON
Performance	**RSA 2048**	5.000 TPS - 10.000 TPS*
	ECDSA 256-bit Prime Signing	30.000 TPS
	RSA Key Generation 2048 bit	15 per second (with key pooling features 100+)
	AES_GCM 256-bit	30.000 TPS
	Partition/Slot	5.000

***5.000 TPS is provided by ProCrypt KM-X Performance, 10.000 TPS is provided by ProCrypt Km-X Premium**

API (Application Programming Interface)

PKCS#11, OpenSSL Engine, PKM Interface

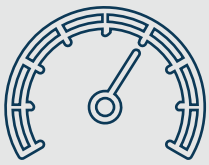
OS (Operating Systems)

Windows, Linux (E.g. Ubuntu, Debian,CentOS...)

Certification & Compliance

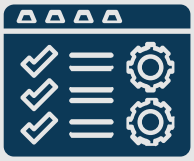
Common Criteria EAL4+ (*ADV_IMP.2, ALC_CMC5, ALC_DVS.2, AVA_VAN.5, ALC_FLR.2*)
PCI HSM v3.0
PCI HSM v4.0
CE
RoHS

Performance & Scalability



Scalable up to 5.000 cryptographically isolated partitions/slot, Performance options up to 12.000 TPS, provided by hardware based, encryption, Multi-Threading to optimize performance, Various performance optionsfor diffrent requirements, Upgradable performance levels, Linear increased performance with additional hardware security modules, Load-Balancing

Functions & Applications



Payment Systems, e-Signature, e-Correspondence, e-Invoice Infrastructures, e-Correspondence 2.0 Support, Digital Transformation Projects, Mobile App Security, File/Disk Encryption, Database Encryption, SSL Offloading, Electronic Authentication Systems, Cloud HSM, EMV, NFC and Contactless Payments, IoT and 5G Security, Blockchain Infrastructure


ProCrypt