پارسا

ماژول امنیت سخت‌افزاری (HSM) پرداخت صدف هنگام

مشخصات فنی

شناسه سند..... TS-HSM-01-01

شماره نگارش..... ۱/۱

تاریخ نگارش..... ۱۴۰۵/۰۶/۱۸

سازنده..... پارسا

طبقه‌بندی سند..... **عادی**

تهران، طرشت، تقاطع بلوار شهید صالحی و بلوار شهید اکبری، پلاک ۲۸، برج فناوری شریف، طبقه اول، واحد ۱۰۸

(۰۲۱) ۶۵۰۱۳۰۳۲

www.parsasharif.ir

مشخصات فنی ماژول امنیت سخت‌افزاری پرداخت هنگام	
سطح امنیتی	FIPS 140-2 Level 3
مرز حفاظت سخت‌افزاری	پیاده‌سازی و اجرای کلیه عملیات حساس امنیتی در داخل سخت‌افزار
عملیات مورد پشتیبانی	عملیات رمزنگاری مورد استفاده در شبکه پرداخت ایران • قابلیت استفاده در بانک‌ها (صادرکنندگان و پذیرندگان کارت بانکی)، PSP ها (پذیرندگان کارت بانکی) • تولید MAC پیام‌های شبکه پرداخت (ISO 8583) مطابق با شبکه شتاب (نسخه ۷ و ۸) • عملیات PIN (پشتیبانی از PIN Blockهای مورد استفاده در شبکه شتاب ISO 0-4) • رمزنگاری / رمزگشایی داده‌های حساس (CSD) شبکه پرداخت • قابلیت استفاده از چندین LMK (Local Master Key) • قابلیت پشتیبان‌گیری و بازیابی LMK • پشتیبانی از ورود و خروج امن کلیدهای انتقال (Transport Key/ Zone Master Key)
حفاظت فیزیکی	• تشخیص دستکاری فیزیکی (Tamper Evidence) و پاسخ به آن (Tamper Response) با استفاده از سنسورهای حفاظت فیزیکی • اعمال حفاظت فیزیکی بر اساس استاندارد FIPS 140-2 Level 3/4 • مجهز به باتری قابل تعویض از بیرون (توسط کاربر)
مطابقت با استانداردها	• FIPS 140-2 Level 3/4 • PCI-PTS HSM • استانداردهای فنی شتاب و شاپرک
رمزنگاری نامتقارن	RSA (1024, 2048, 4096) • PKCS#1v1.5, PKCS#1v2.2 (OAEP, PSS) ECDSA • SECP256R1, SEC256K1, SECP384R1 • BrainpoolP256R1, BrainpoolP384R1, BrainpoolP512R1, BrainpoolP512T1
رمزنگاری متقارن	AES (128, 192, 256) • Modes: ECB, CBC, GCM DES (56), TDES (112, 168) • Modes: ECB, CBC
Hash Functions	SHA-1 SHA-2 (224, 256, 384, 512)
MAC Algorithms	MAC [ANSI X9.19] (AES, TDES) Complient with ISO 9797-1 (AES, TDES): • 6 types of MAC • 4 types of padding • 2 types of key derivation مطابقت با نسخه‌های ۷ و ۸ استاندارد شبکه شتاب ایران
Supported PIN Blocks	ISO 9564 (ISO 0, ISO 1, ISO 2, ISO 3, ISO 4) مطابقت با نسخه‌های ۷ و ۸ استاندارد شبکه شتاب ایران
Wrap/Unwrap Algorithms	Symmetric Wrap/Unwrap (AES/DES/TDES)

Backup/Restore HSM Domain key (LMK) M_of_N Secret Sharing (HSM to Multiple USB Tokens)	**پشتیبان‌گیری/بازیابی امن**
Hardware-based True Noise Source NIST SP 800-90A compliant CTR-DRBG	**تولید عدد تصادفی**
+ Multiple Administrators per HSM Device + Separate Administrator account for Audit Operations + Security Administartor (SA) for general adminisratrion + Multiple Security Oficers (SOs) for Multiple LMK mamgmnent	**کاربران/نقش‌ها**
Syslog, SIEM	**Logging/Audit**
مدیریت HSM مبتنی بر SSH	**واسط مدیریت HSM**
TCP/IP	**واسط ارتباطی**

Mechanism	**Performance of Hengam HSM**
MAC calculation	8000 cps
PIN block translation	4000 cps
PIN Generation / Verification	4000 cps
AES/TDES Enc/Dec	4000 cps

پشتیبانی می‌شود.	**High Availability (HA) Active-Active Failover Loadbalancing**
پشتیبانی می‌شود.	**Network Time Protocol (NTP)**
• Network Access Control Rules • SNMP	**Network Management**
+ 1U Rack Mount + Hot-Swap dual Power Supply + Ethernet port (1 Gbps) + USB and Serial ports (for HSM Management) + LED (Power, Tamper) + LCD + KLD (Key Loading Device)	**مشخصات فیزیکی، واسط‌ها و پورت‌های ارتباطی**