ماژول امن سخت افزاری

دستگاه ماژول امنیتی سخت‌افزاری (HSM) یا Hardware Security Module، سخت‌افزاری است که مسئولیت تولید، نگهداری، سرویس دهی و ارائه خدمات مرتبط با کلیدهای رمزنگاری را در سامانه‌های مختلف فناوری اطلاعات برعهده دارد. این دستگاه که عموما قلب امنیتی سیستم‌ها محسوب می‌شود، دارای فناوری‌های خاص رمزنگاری است که مانند گاوصندوق کلید دیجیتال و همچنین شتاب دهنده عملیات رمزنگاری عمل نموده و درخواست‌های رمزنگاری بدون اثر گذاری و یا اختصاص هرگونه منابع سیستمی برای آن ارسال می‌شود.

این دستگاه در بسیاری از پروژه های ملی کشور مورد استفاده قرار گرفته و امنیت یا اعتماد سیستم براساس آن بنا می‌شود. پروژه های بزرگی چون کارت سوخت، گذرنامه الکترونیکی، کارت هوشمند ملی و ... نیازمند استفاده از HSM برای نگهداری کلیدهای اصلی و ریشه هستند. پروژه های بانکی مختلفی نیز مبتنی بر این دستگاه راه اندازی و اجرا می شوند، از جمله پروژه های مرتبط با کارت هوشمند، زیرساخت کلید عمومی (PKI)، رمزنگاری، امنیت شبکه و بسیاری دیگر.

Cryptographic Processing

- Asymmetric:
  - RSA (1024 to 4096 bit) Padding: PKCS#1 v1.5, PKCS#1 v2.2 (OAEP, PSS)
  - Diffie-Hellman
- Symmetric:
  - AES (128 to 256)
  - DES, 3DES (112, 168) Modes: ECB, CBC, OFB, CTR,GCM
- Hash/Message Digest:
  - MD5, SHA1, SHA2 (224, 256, 384, 512)
  - HMAC, CMAC, MAC (ANSI X9.9, X9.19)
- Random Number Generation:
  - Hardware-based True Noise Source
  - NIST SP 800-90A compliant CTR-DRBG

Performance

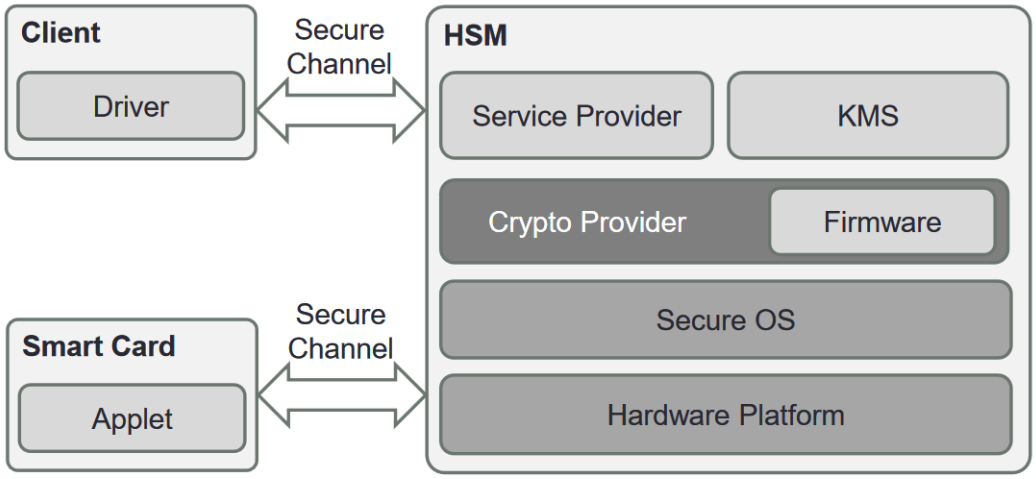
- Up to 4500 RSA-1024 signings/sec
- Up to 800 RSA-2048 signings/sec
- Up to 8000 AES-ECB Enc/Dec
- Dual LAN
- Multi-threaded APIs
- Multi-processed APIs

Programming Interfaces

- PKCS#11
- Java JCA/JCE
- OpenSSL Engine
- Microsoft .Net

Security

- FIPS 140-2 Level 2, Level 3 compliances
- Physical tamper protection
- True Random Number Generation
- Backup of key material (M of N)
- Cloning (HSM to HSM)



Operating Systems

- Linux/Unix
- Windows

Connectivity

- Ethernet 10/100/1000 mbps
- USB (Management)
- LED (Power, Tamper)
- LCD
- PED (PIN Entry Device)

Physical Characteristics

- Standard 2U rack mount chassis
- Dimensions:
- 53 mm x 42mm x 8.5 mm
- Dual swappable AC power supplies
- Weight: 12.7kg
- Input Voltage: 100-240V, 50-60Hz
- Power Consumption: 180W maximum
- Temperature: operating 0°C – 35°C, storage -20°C – 60°C
- Relative Humidity: 5% to 95% (38°C) non-condensing

Usage

- Public Key Infrastructure (PKI)
- Payment and Bank's Switches (PIN Translation, Mac Validation, PIN Generation, ..)
- Web/Application Server (HTTPS/SSL/TLS)
- Encryption and Decryption
- Database Security, Transparent Data Encryption
- Smart Card/SIM Issuance

Ease of Management

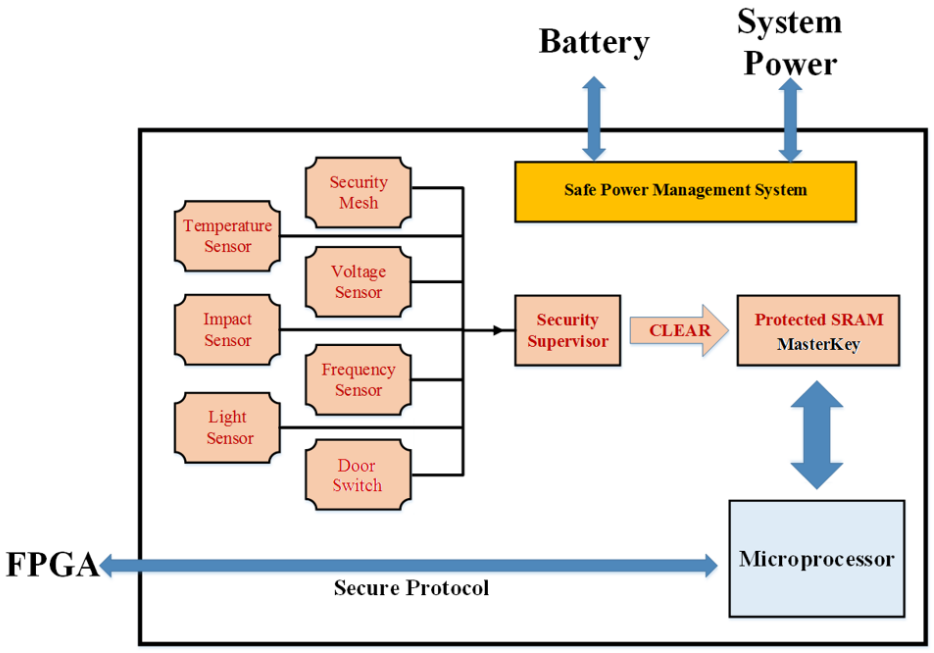
- Multiple Administrators per HSM Device
- Two distinct Users per HSM Partition:
    - Security Officer
    - Normal User

معماری استاندارد و کاملا بومی

باتوجه به کاربردهای حیاتی و زیرساخت‌هایی که در آنها HSM بعنوان نقطه اعتماد مورد استفاده قرار می گیرد, پروژه HSM با همکاری شرکت پندار کوشک ایمن و پژوهشکده پارساشریف برنامه ریزی و زمانبندی گردید. در ابتدا برای تولید محصول HSM، چند محصول خارجی مورد بررسی دقیق قرار گرفت و چند پروژه تحقیقاتی روی آنها انجام شده است. سپس با مهندسی معکوس، معماری محصول بومی براساس آنها طراحی گردید. البته معماری نهایی طراحی شده عملا ترکیبی از مدل معماری چند محصول مختلف می باشد که ایرادات آنها را نیز برطرف کرده و مدل بهتری در آن ارائه شده است.

از طرف دیگر، با انجام پروژه های تحقیقاتی در همکاری با دانشگاه های معتبر کشور، کلیه استانداردهای این حوزه مورد مطالعه قرار گرفته است که در قالب گزارشی مفصلی در آرشیو شرکت موجود می باشد. این مطالعات جهت شناخت و مهندسی معکوس و برنامه ریزی پیاده سازی محصول HSM استفاده شده است.

در تولید محصول HSM، از راهبرد اصولی شرکت پندار کوشک ایمن و پژوهشکده پارساشریف تبعیت شد. در این راهبرد، معماری محصول با دقت و صرف زمان زیاد طراحی شده و سپس تست صورت می پذیرد. این دستگاه قادر است تا خدمات مدیریت کلید را مبتنی بر استاندارد PKCS#11 برروی بستر شبکه فراهم نماید و استانداردهای امنیتی لازم مانند FIPS 140-2 را رعایت کرده است. این دستگاه آماده است تا سرویس های مورد نیاز سامانه های اطلاعاتی و امنیتی مانند مرکز صدور گواهی (CA) و یا رمزنگاری و تولید PIN برای کارت های بانکی را انجام داده و به صورت استاندارد به ابزارهای مختلفی که هم اکنون وجود دارند، متصل شود.



پندار کوشک ایمن (PKI Co.)

۸۸۲۲۰۷۱۵ و ۸۸۲۲۰۶۹۰ ۲۱ ۹۸+

info@pki.co.ir www.pki.co.ir