PKA-VA

Public Key Infrastructure

All PKI Services In One Device

Comprehensive PKI Services

- Verification Authority (VA)
  CRL and OCSP services
- Public Key Directory (PKD)
  Certificate repository
- Key Management System (KMS)
  Secure Key life-cycle management

Security

- Includes embedded HSM with FIPS 140-2 Level 3 Certificate
- Secure key generation and key storage by HSM
- Secure customized Linux in core
- Internal Firewall and Proxy

Flexibility, Scalability and Reliability

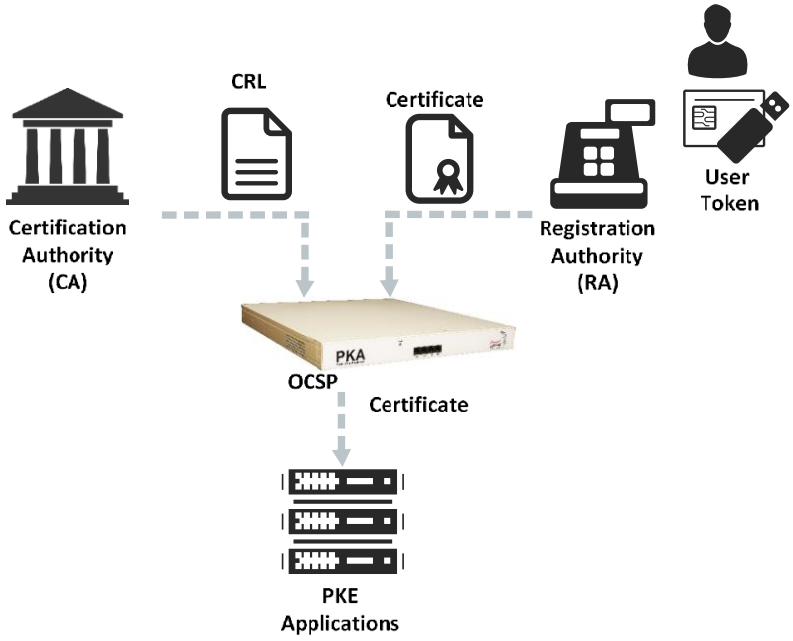
- Integration with other systems for PKI-Enabling
- Integration by Web-Service and SDK
- High Performance
- High Available with redundancy and fault tolerance

سامانه‌ای یکپارچه برای اعتبارسنجی گواهینامه الکترونیکی

دستگاه PKA مدل VA کلیه خدمات زیرساخت کلید عمومی (PKI) مرتبط با اعتبارسنجی گواهینامه‌های کاربران را در یک دستگاه مجتمع ارائه می‌نماید. این دستگاه خدمات مختلف شامل مرکز اعتبارسنجی گواهینامه (VA) و مخزن یا دایرکتوری کلید عمومی (PKD) را در یک دستگاه فراهم کرده است. این دستگاه قادر است تا فایل‌های لیست گواهینامه-های باطله (CRL) را از آدرس‌های نقطه انتشار تنظیم شده (CDP) منطبق بر زمانبندی‌های ذکر شده در سند دستورالعمل اجرایی گواهینامه (CPS) دریافت نموده و در خود ذخیره نماید. سپس این دستگاه می‌تواند سرویس استعلام برخط گواهینامه (OCSP) را به سرورها و سامانه‌های نرم‌افزاری داخلی سازمان ارائه کند. بدین ترتیب نیازی به اتصال مستقیم سرورهای مختلف سازمان به مرکز صدور گواهینامه (CA) نیست. همچنین این دستگاه قادر است پایگاه داده استاندارد گواهینامه‌های کاربران یا دایرکتوری کلید عمومی (PKD) را مبتنی بر پروتکل LDAP فراهم نماید. در نتیجه هر توکن یا گواهینامه‌ای از کاربر که در سیستم ثبت شود، یک نسخه از گواهینامه وی در دستگاه PKA ذخیره می‌گردد و در صورت نیاز در آینده با پروتکل استاندارد LDAP قابل بازیابی در هر کدام از سرورها و سامانه‌های سازمان می‌باشد.

پشتیبانی از ماژول امنیتی سخت‌افزاری (HSM)

این دستگاه دارای ماژول امنیتی سخت‌افزاری (HSM) درونی جهت تولید و نگهداری امن کلیدهای خصوصی امضای پاسخ استعلام برخط وضعیت گواهینامه (OCSP Signer) است که سطح بالاتری از امنیت را فراهم می‌کند. در این دستگاه سامانه‌ای تحت عنوان سامانه مدیریت کلید (KMS) تعبیه شده است که مسئول مدیریت کامل چرخه حیات کلیدها شامل تولید، نگهداری، تهیه پشتیبان، بازیابی و انتقال می‌باشد. همچنین جهت امنیت بیشتر، برای نگهداری نسخه پشتیبان کلیدهای خصوصی، از کارت هوشمند ویژه‌ای استفاده می‌گردد. از طرف دیگر، این دستگاه می‌تواند به انواع دستگاه‌های HSM تحت شبکه مبتنی بر استاندارد PKCS#11 متصل شود.



Performance

- Up to 32 Concurrent Connections
- OCSP Service: 500 tps
- PKD Download: 3000 tps

Software Development Kit

- J2EE and J2SE SDK
- .Net Framework SDK
- Web-Service API (SOAP)

Hardware Security Module (HSM)

- Includes embedded HSM with FIPS 140-2 Level 3 Certificate
- Embedded HSM 25/220/600 tps (1024 bit RSA signature/second)
- Supporting various Network HSMs by PKCS#11 Interface (SafeNet, nCipher, Utimaco, Boll, etc.)

PKI Standards

- RFC 5280 (X.509 Certificate and Certificate Revocation List (CRL) Profile)
- RFC 4387 (X.509 Operational Protocols: Certificate Store Access via HTTP)
- RFC 5019 (The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments)
- RFC 2253 (Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names)
- RFC 2396 (Uniform Resource Identifiers (URI): Generic Syntax)
- FIPS 180-4 (Secure Hash Standard (SHS))
- FIPS 140-2 (Security Requirements for Cryptographic Modules)
- PKCS#1 (RSA Cryptography Standard)
- PKCS#10 (Certification Request Standard)
- PKCS#11 (Cryptographic Token Interface)

Physical Characteristics

- Connectivity: 1 Gbps Ethernet
- Dimensions: 426 x 450 x 44 mm
- 1U Rackmount

قابل اتصال به سایر سامانه‌های نرم‌افزاری

دستگاه PKA به شکلی طراحی شده است که به راحتی قابلیت اتصال به انواع دیگر نرم‌افزارهای سازمان را داشته باشد. به کمک این دستگاه می‌توان تمامی سامانه‌های نرم‌افزاری را به زیرساخت کلید عمومی مجهز نمود (PKI-Enabling). بدین منظور انواع مختلف ارتباطات با این دستگاه جهت توسعه نرم‌افزار، پیش‌بینی شده است. این دستگاه می‌تواند خدمات مختلف خود را در قالب سرویس تحت وب (Web-Service) ارائه کرده و دارای کتابخانه برنامه‌نویسی (SDK) برای دو پلتفرم تولید نرم‌افزار Net Framework. و Java J2EE/J2SE می‌باشد. بوسیله این ابزارها می‌توان به راحتی و در زمانی کوتاه، سامانه‌های نرم‌افزاری دیگر را به خدمات زیرساخت کلید عمومی مجهز نمود (PKI-Enabling).

ارائه سرویس پایدار و قابل اعتماد

این دستگاه به شکلی طراحی شده است که می‌تواند چند عدد از آن با دستگاهی بنام PKA-HAC به صورت ترکیبی استفاده شود. در این معماری، دو یا چند دستگاه PKA به صورت Active-Active به یکدیگر متصل می‌شوند تا تعداد تراکنش بالاتری را پشتیبانی نموده و در عین حال مقاومت بیشتری در برابر خرابی‌های احتمالی داشته باشند. بدینوسیله می‌توان توان پردازشی مجموعه را افزایش داد و همچنین به ضریب اطمینان بیشتری از نظر مقابله با خرابی (Fault Tolerance) دست یافت. این دستگاه از نظر امنیتی، تست‌های گوناگونی را پشت سر گذاشته و تمهیدات مختلف امنیتی در آن گنجانده شده است و دارای فایروال و پراکسی داخلی می‌باشد.

تولید شده در پارک علم و فناوری دانشگاه تهران

دارای گواهی ثبت اختراع از اداره کل مالکیت های صنعتی

دارای تاییدیه از آزمایشگاه امنیت مرکز تحقیقات صنایع انفورماتیک
زیر نظر مرکز توسعه تجارت الکترونیکی

برگزیده دهمین جشنواره ملی فن آفرینی شیخ بهایی

مجهز به دستگاه HSM دارای استاندارد FIPS 140-2 Level 3

پندار کوشک ایمن (PKI Co.)

ایران، تهران، خیابان کارگر شمالی، پردیس شمالی دانشگاه تهران، پارک علم و فناوری،
ساختمان شماره ۲، واحد ۲۰۵
۸۸۲۲۰۷۱۵ و ۸۸۲۲۰۶۹۰ ۲۱ ۹۸+
info@pki.co.ir www.pki.co.ir