PKA-CA

Public Key Infrastructure

All PKI Services In One Device

Comprehensive PKI Services

- Certification Authority (CA)
  Certificate issuing and revoking
- Registration Authority (RA)
  Registering and certificate request
- Verification Authority (VA)
  CRL services
- 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

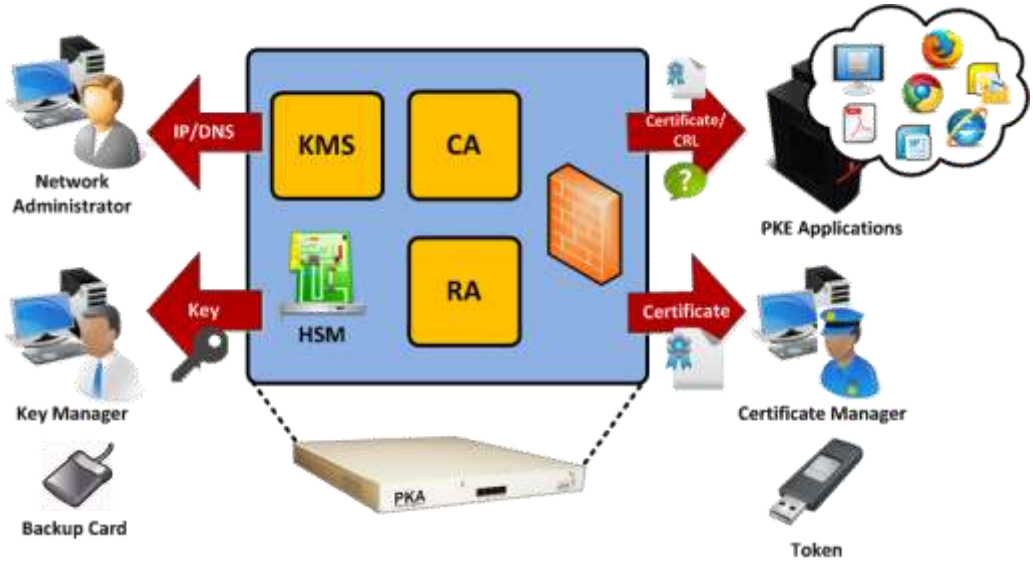
- Integration with other systems for PKI-Enabling
- Integration by Web-Service and SDK
- High Performance
- High Available with redundancy and fault tolerance

سامانه‌ای یکپارچه برای صدور و مدیریت گواهینامه الکترونیکی

مرکز صدور گواهینامه (CA) بخش اصلی از یک مجموعه زیرساخت کلید عمومی (PKI) می باشد که مسئولیت صدور، ابطال و مدیریت گواهینامه‌های الکترونیکی را برعهده دارد. دستگاه PKA-CA برای مدیریت سخت‌افزاری و نرم‌افزاری سامانه CA طراحی شده است. این دستگاه می‌تواند همزمان چند مرکز صدور گواهینامه (CA) را در خود جای دهد و خدمات مختلف را برای هر یک از آن‌ها ارائه نماید. همچنین می‌تواند انواع مدل‌های اعتماد (Trust Model) و سلسله مراتب مراکز صدور گواهینامه (CA Hierarchy) اعم از ریشه خارجی، ریشه داخلی، میانی خارجی، میانی داخلی و همچنین اعتماد متقابل (Cross-Certification) را پشتیبانی نماید و به صورت برخط یا برون خط مورد استفاده قرار گیرد. در داخل این دستگاه امکان انتشار خودکار لیست گواهینامه های باطل شده (CRL) نیز پیش بینی شده است.

پشتیبانی از ماژول امنیتی سخت‌افزاری (HSM)

این دستگاه دارای ماژول امنیتی سخت‌افزاری (HSM) درونی جهت تولید و نگهداری امن کلیدهای خصوصی مراکز صدور گواهینامه 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
- Certificate Issuing: 10 tps
- CRL Downloading: 250 tps

Software Development Kit

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

Token and Smart Card

- Certificate Issuing on all types of Token and Smart Card based on MS-CAPI
- Certificate Issuing on Iranian Tokens including ParsKey and KeyA3 without any driver

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 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)
- PKCS#12 (Personal Information Exchange Syntax Standard)
- MS-CAPI (Microsoft Cryptography API)

Physical Characteristics

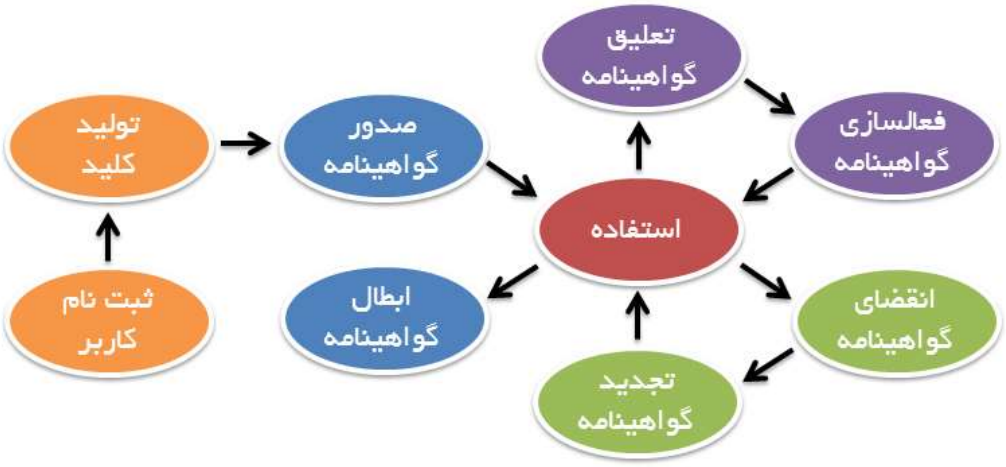
- Connectivity: 1 Gbps Ethernet
- Dimensions: 426 x 450 x 44 mm
- ۱□ □□□□□□□□□

سامانه ثبت نام و مدیریت توکن

این دستگاه مجهز به سامانه ثبت نام (RA) داخلی می باشد که امکان تعریف کاربران و صدور گواهینامه برای توکن و کارت هوشمند را فراهم می آورد. از طریق همین سامانه می توان در صورت مفقود شدن و سرقت توکن کاربر، درخواست ابطال گواهینامه وی را ارسال کرد. همچنین قابلیت انواع جستجو در گواهینامه های صادر شده و باطل شده از طریق این سامانه فراهم می باشد. در کنار این سامانه، کیت توسعه نرم افزاری (SDK) پیش بینی شده است که از طریق آن می توان امکان صدور گواهینامه و توکن را به سامانه های نرم افزاری دیگر اضافه نمود. از این طریق نرم افزار اتوماسیون مشتری می تواند به کمک یک کتابخانه نرم افزاری، سرویس وب دستگاه PKA را فراخوانی کرده و اقدام به دریافت گواهینامه الکترونیکی نماید.

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).



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

+۹۸ ۲۱ ۸۸۲۲۰۶۹۰ و ۸۸۲۲۰۷۱۵

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