PKA-FA

Public Key Infrastructure

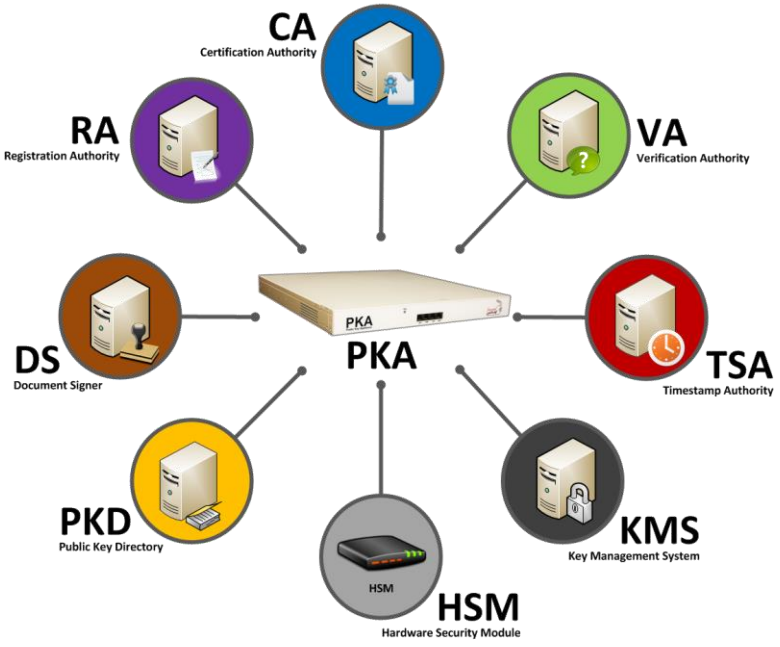
All PKI Services In One Device

سامانه‌ای یکپارچه برای امضای دیجیتال و رمزنگاری

دستگاه PKA مدل FA کلیه خدمات زیرساخت کلید عمومی (PKI) را در یک دستگاه مجتمع ارائه می‌نماید. این دستگاه خدمات مختلف اعم از مرکز صدور گواهینامه الکترونیکی (CA)، مرکز ثبت نام (RA)، مرکز اعتبارسنجی گواهینامه (VA)، مخزن یا دایرکتوری کلید عمومی (PKD)، مرکز صدور مهر زمانی مطمئن (TSA) و مرکز صدور امضای دیجیتال (DS) را در یک دستگاه فراهم کرده و سازمان را از خرید تجهیزات گوناگون، صرف هزینه‌های مالی زیاد و زمان طولانی برای اجرای پروژه بی‌نیاز می‌گرداند. این دستگاه از ماژول‌های سخت‌افزاری و نرم‌افزاری استانداردی بهـــره می‌برد که مدیریتی یکپارچه را در اختیار سازمان قرار می‌دهد. در این دستگاه راه حل جامعی ارائه می‌شود که مدیریت کامل چرخه حیات گواهینامه الکترونیکی از لحظه صدور تا ابطال و پس از آنرا تحت مدیریت متمرکز و یکپارچه ایجاد می‌کند.

پشتیبانی از ماژول امنیتی سخت‌افزاری (HSM)

این دستگاه دارای ماژول امنیتی سخت‌افزاری (HSM) درونی جهت تولید و نگهداری امن کلیدهای خصوصی مراکز صدور گواهینامه، صدور مهر زمانی و مانند 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.



Comprehensive PKI Services

- Certification Authority (CA)
  Certificate issuing and revoking
- Registration Authority (RA)
  Registering and certificate request
- Verification Authority (VA)
  CRL and OCSP services
- Public Key Directory (PKD)
  Certificate repository
- Timestamp Authority (TSA)
  Trusted timestamp with digital signature
- PDF Signer (DS)
  Central PDF digital signing
- XML Signer (DS)
  Central XML digital signing
- CMS Signer (DS)
  Central CMS digital signing
- 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
- Three separated Security Zones

Flexibility, Scalability and Reliability

- Integration with other systems for PKI-Enabling
- Integration by Web-Service and SDK
- Separation of various services for Scalability
- High Performance
- High Available with redundancy and fault tolerance

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/ RFC 4387/ RFC 5019/ RFC 2253/ RFC 2396/ RFC 3161/ RFC 2818/ RFC 3778
- FIPS 180-4/ FIPS 140-2
- PKCS#1/ PKCS#7/ PKCS#10/ PKCS#11/ PKCS#12
- XML-Sig

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).

قابل توسعه، انعطاف پذیر و قابل اعتماد

این دستگاه به شکل مولفه‌ای (ماژولار) طراحی شده است و قابلیت انعطاف بالایی دارد، به شکلی که در صورت نیاز خدمات مختلف آن قابل تفکیک از یکدیگر است. 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 امنـــیتی، تست‌های گوناگونی را پشت سر گذاشته و تمهیدات مختلف امنیتی در آن گنجانده شده است و دارای فایروال و پراکسی داخلی می‌باشد. 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 اعتماد متقابل (Cross-Certification) را پشتیبانی نماید.

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