# PKA-SA

## Public Key Infrastructure

All PKI Services In One Device


### Comprehensive PKI Services

- 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

### Flexibility, Scalability and Reliability

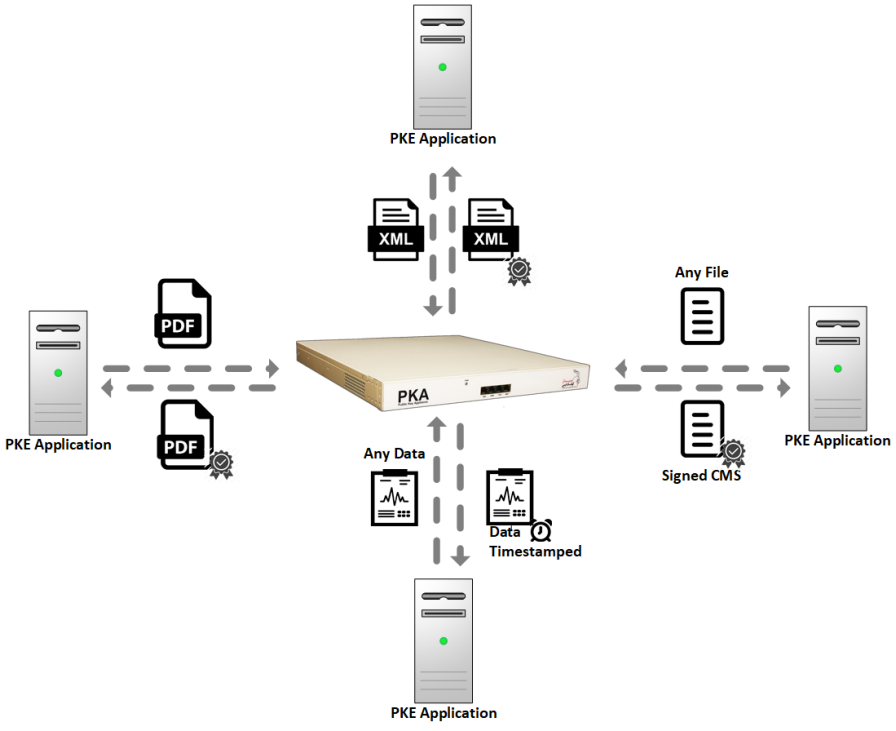
- Integration with other systems for PKI-Enabling
- Integration by Web-Service and SDK
- High Performance
- High Available with redundancy and fault tolerance

## سامانه یکپارچه و کامل صدور امضای دیجیتال

دستگاه PKA مدل SA کلیه خدمات امضای دیجیتال متمرکز را در یک دستگاه مجتمع ارائه می‌نماید. این دستگاه خدمات مختلف اعم از مرکز صدور مهر زمانی مطمئن (TSA)، مرکز صدور امضای دیجیتال اسناد PDF، مرکز صدور امضای دیجیتال پیغام‌های XML و مرکز صدور امضای دیجیتال با قالب CMS را در یک دستگاه فراهم کرده است. این دستگاه می‌تواند به عنوان مرکز امن و یکپارچه برای صدور امضای دیجیتال و مهر زمانی مطمئن در سازمان مورد استفاده قرار گرفته و به سایر سرورها و سامانه‌ها خدمات خود را در قالب سرویس وب ارائه نماید. بدین ترتیب می‌توان کلیه اسناد و داده‌های سازمان را در قالب استاندارد PDF توسط این دستگاه، امضای دیجیتال نمود. همچنین می‌توان امضای دیجیتال را برروی داده‌های با قالب XML موجود در پایگاه داده و یا بین دو سرور اضافه کرده و یا هر نوع داده را با قالب استاندارد پایه CMS امضای دیجیتال نمود.

## پشتیبانی از ماژول امنیتی سخت‌افزاری (HSM)

این دستگاه دارای ماژول امنیتی سخت‌افزاری (HSM) درونی جهت تولید و نگهداری امن کلیدهای خصوصی مراکز صدور مهر زمانی، امضاکننده PDF، امضاکننده XML و امضاکننده CMS 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
- Timestamp Service: 600 tps
- PDF Singing: 150 tps
- XML Signing: 150 tps
- CMS Signing: 150 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 3161
  (Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP))
- RFC 3778
  (The application/pdf Media Type)
- RFC 4330
  (Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI)
- FIPS 180-4
  (Secure Hash Standard (SHS))
- FIPS 140-2
  (Security Requirements for Cryptographic Modules)
- PKCS#1
  (RSA Cryptography Standard)
- PKCS#7
  (Cryptographic Message Syntax Standard)
- PKCS#10
  (Certification Request Standard)
- PKCS#11
  (Cryptographic Token Interface)
- XML-Sig
  (XML Signature Syntax and Processing)

## Physical Characteristics

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

## مرکز صدور مهر زمانی مطمئن (TSA)

دستگاه PKA مدل SA قادر است تا به عنوان مرکز صدور مهر زمانی مطمئن (TSA) در سازمان مورد استفاده گیرد. این دستگاه می‌تواند با دریافت بسته داده، مهر زمانی را به آن اضافه نموده و مجموعه نهایی را امضای دیجیتال نماید. این فرآیند مطابق پروتکل TSP و استاندارد RFC3161 صورت می‌پذیرد. از طرف دیگر این دستگاه می تواند توسط پروتکل NTP زمان همگام‌سازی شده را از مرجع معرفی شده دریافت نماید.

## مرکز صدور امضای دیجیتال در قالب PDF

دستگاه PKA مدل SA می‌تواند نقش سروری متمرکز برای تولید امضای دیجیتال برروی اسناد با قالب PDF را برعهده داشته باشد. در این شرایط، دستگاه می‌تواند انواع تنظیمات استاندارد فایل PDF مانند متن هشدار و یا لوگوی امضای سازمان را دریافت کرده و در مختصات مورد نظر قرار دهد. امضای دیجیتال تولیدشده برروی فایل‌های PDF به صورت استاندارد می‌باشد و قبل بازخوانی و اعتبارسنجی در کلیه نرم‌افزارها و ابزارهای PDF مانند Adobe Acrobat Reader و یا Foxit Reader هستند.

## 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.

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