PKA CA

فراهم‌کننده کلیه خدمات مرکز صدور گواهینامه الکترونیکی (CA) با امنیت بالا و انعطاف پذیری

قابل توسعه، انعطاف‌پذیر و قابل اعتماد

مرکز صدور گواهینامه (CA) بخش اصلی از یک مجموعه زیرساخت کلید عمومی (PKI) می باشد که مسئولیت صدور، ابطال و مدیریت گواهینامه های الکترونیکی را برعهده دارد. دستگاه PKA-CA برای مدیریت سخت افزاری و نرم افزاری 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) پیش بینی شده است.

امنیت زیاد با ماژول امنیتی سخت‌افزاری (HSM)

این دستگاه در مدل‌های با امنیت بالا، دارای ماژول امنیتی سخت‌افزاری (HSM) می‌باشد. این ماژول، مسئول تولید و نگهداری امن کلیدهای خصوصی مراکز صدور گواهینامه، صدور مهر زمانی و مانند است که نیاز به امنیت بیشتری دارند. در این دستگاه سامانه‌ای تحت عنوان سامانه مدیریت کلید (KMS) تعبیه شده است که مسئول مدیریت کامل چرخه حیات کلید شامل تولید، نگهداری، تهیه پشتیبان، بازیابی و انتقال کلیدها می‌باشد. همچنین جهت امنیت بیشتر، برای نگهداری نسخه پشتیبان کلیدهای خصوصی، از کارت هوشمند ویژه‌ای استفاده می‌گردد.

قابل اتصال به سایر سامانه‌های نرم‌افزاری و سخت‌افزاری

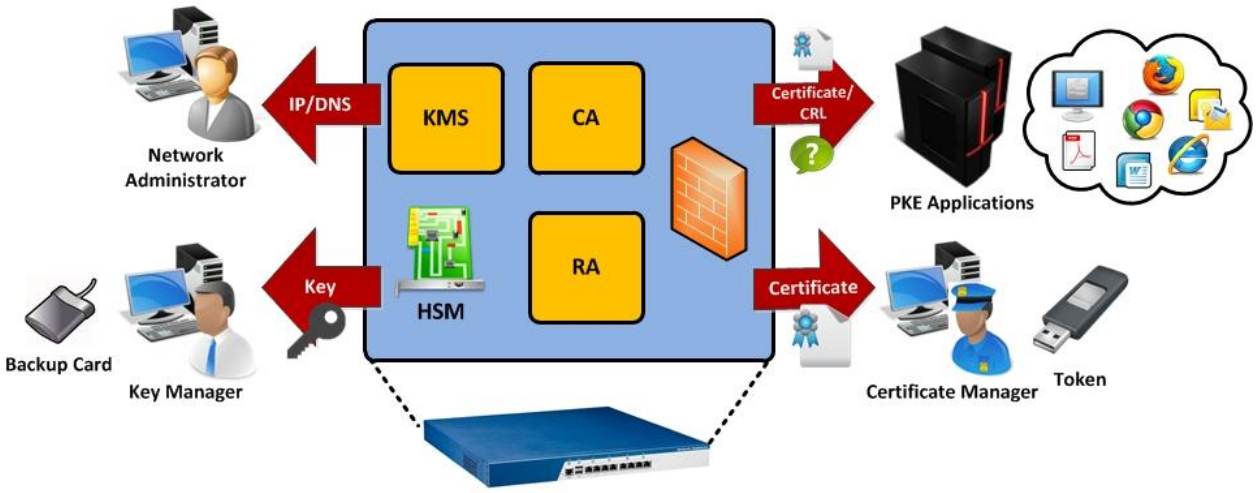
دستگاه PKA به شکلی طراحی شده است که به راحتی قابلیت اتصال به انواع نرم‌افزارهای دیگر را داشته باشد. به کمک این دستگاه می‌توان انواع نرم‌افزارها را به امکانات زیرساخت کلید عمومی مجهز نمود (PKI-Enabling). به این منظور انواع مختلف ارتباطات با این دستگاه جهت توسعه نرم‌افزار، پیش‌بینی شده است. این دستگاه می‌تواند خدمات مختلف خود را در قالب سرویس وب (Web Service) استاندارد ارائه دهد. همچنین برای دو پلتفرم پراستفاده برنامه‌نویسی Net. Framework و Java J2EE/J2SE کتابخانه‌های ویژه توسعه نرم‌افزار ارائه می‌گردد که برنامه‌نویسی در این محیط‌ها را به سهولت امکان‌پذیر می‌گرداند.

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.

مبتنی بر استانداردهای روز دنیا

کلیه خدمات این دستگاه به صورت استاندارد پیاده‌سازی شده‌اند و به راحتی قابلیت اتصال به انواع سامانه‌های استاندارد دیگر مانند MS IIS (Internet Information Service)، MS IE (Internet Explorer)، FireFox، Chrome، مجموعه MS Office و سیستم‌عامل‌های MS Windows و Linux وجود دارد.



امتیازات

امنیت زیاد

- حاوی ماژول امنیتی سخت‌افزاری (HSM) دارای استاندارد امنیتی FIPS 140-2 Level 3
- تولید، نگهداری و استفاده امن از کلیدها به روش مطمئن در سخت‌افزار امنیتی
- استفاده از سیستم‌عامل سفارشی و امن‌سازی‌شده در هسته دستگاه
- دارای تمهیدات مختلف امنیتی اعم از فایروال، پراکسی و مناطق امنیتی (Security Zones) در داخل دستگاه
- دارای تاییدیه امنیتی از آزمایشگاه امنیت مرکز صدور گواهی ریشه کشور

انواع خدمات مرکز صدور گواهینامه

- ارائه کلیه خدمات مرکز صدور گواهینامه (CA) شامل چرخه حیات کامل گواهینامه الکترونیکی از صدور تا ابطال
- ارائه کلیه خدمات مرکز ثبت نام (RA) شامل ثبت اطلاعات کاربر و صدور توکن
- انتشار خودکار و منظم وضعیت گواهینامه های باطل شده به صورت لیست گواهینامه های باطله (CRL)
- انتشار گواهینامه‌های مراکز صدور گواهینامه
- ارائه کلیه خدمات سامانه مدیریت کلید (KMS) شامل چرخه حیات کامل کلید از تولید تا امحاء

انعطاف و توسعه پذیری

- میزبانی همزمان چند مرکز صدور گواهینامه به صورت یکجا و در قالب یک دستگاه واحد
- قابلیت ایجا انواع مدل اعتماد (Trust Model) و سلسله مراتب مرکز صدور گواهینامه (CA Hierarchy)
- قابلیت اتصال از طرق مختلف شامل سرویس وب (Web Service) و یا کتابخانه برنامه‌نویسی (SDK)
- منطبق بر استانداردهای مختلف رمزنگاری و زیرساخت کلید عمومی ازجمله مجموعه PKCS و X.509
- قابلیت تفکیک خدمات مختلف براساس نیاز در آینده
- ارائه خدمات با سرعت زیاد و کارایی بالا در کنار قابلیت اطمینان

مشخصات فنی

سیستم عامل استفاده کننده

- MS Windows XP/7/Vista/2003/2008
- Linux (Redhat/Suse/Ubuntu)
- VMWare (Player/Workstation/ESX/ESXi)

ماژول پشتیبان کلید

- کارت هوشمند مطابق با استاندارد ISO 7816

رابط‌های برنامه نویسی

- سرویس وب مطابق با استاندارد SOAP
- کتابخانه برنامه نویسی به زبان جاوا
- کتابخانه برنامه نویسی به زبان .Net

مشخصات فیزیکی

- ارتباط از طریق شبکه 10/100/1000 Ethernet, CAT5, UTP
- اندازه 426mm x 450mm x 44mm

- قابلیت نصب در رک (1U Rackmount)

الگوریتم‌های رمزنگاری

- RSA 1024/2048/4096
- PKCS#1 v2.1

استاندارد های زیرساخت کلید عمومی (PKI)

- PKCS#1/7/10/11/12/15
- X.509 Certificate: RFC 5280
- SHA-1/SHA-256/SHA-384/SHA-512
- SSL/TLS v3.0
- PEM/JKS/P12
- CRL/CDP: RFC5280/RFC4387

استانداردهای امنیتی

- FIPS 140-2 Level 3 برای ماژول امنیتی سخت‌افزاری (HSM)
- تاییدیه امنیتی از آزمایشگاه امنیت مرکز صدور گواهی ریشه کشور

تلفن: ۸۸۲۲۰۶۹۰ ۲۱ ۹۸+

رایانامه: info@pki.co.ir

وبسایت: www.pki.co.ir