بسم الله الرحمن الرحیم

معرفی محصول

توکن امنیتی سخت افزاری

شرکت مهندسی ارتباطی

پیام پرداز

پیشران اطلاعات و ارتباطات امن

به نام او

توکن امنیتی کیا۳

دایره حملات رایانه‌ای هر روز وسیع‌تر می‌شود. امروزه علیرغم استفاده از مکانیزم‌های متنوع رمزنگاری، حمله کنندگان با نفوذ به رایانه‌ها، کلیدهای رمزنگاری را از حافظه رایانه دزدیده و امنیت سامانه‌ها را مورد تهدید قرار می‌دهند. در این میان تنها راهی که همچنان از سطح امنیت فوق‌العاده بالایی برخوردار است استفاده از ماژول‌های رمزنگاری سخت‌افزاری است. در این راهکار کلیدهای رمزنگاری به صورت غیرقابل استخراج در داخل ماژول ذخیره شده و عملیات رمزنگاری به صورت سخت‌افزاری در درون ماژول انجام می‌گیرد. بنابراین کلید رمزنگاری از ماژول خارج نشده و نفوذگران امکان دسترسی به کلید را نخواهند داشت.

توکن امنیتی کیا۳ یک ماژول رمزنگاری سخت‌افزاری بومی است که خدمات تولید و ذخیره امن کلیدهای رمزنگاری و همچنین اجرای عملیات رمزنگاری متقارن و نامتقارن را در اختیار قرار می‌دهد. توکن کیا۳ مبتنی بر تکنولوژی کارت هوشمند طراحی شده و با استفاده از رابط *USB* به رایانه متصل می‌گردد. پشتیبانی از استانداردهای روز دنیا این امکان را فراهم می‌سازد تا بتوان از توکن کیا۳ در کلیه کاربردهای امن مبتنی بر زیرساخت کلید عمومی (*PKI*) که در حال حاضر به صورت آماده در اکثر سیستم عامل‌ها، تجهیزات و برنامه‌های کاربردی مشهور ارائه می‌شوند استفاده نمود و کارهای خود را در محیطی کاملا امن انجام داد.

ویژگی‌ها

- ✓ الگوریتم رمز نامتقارن *RSA(512-4096)* به صورت سخت‌افزاری (*On-board*)
- ✓ تولید زوج کلید *RSA* در داخل ماژول به صورت سخت‌افزاری
- ✓ تولید فوق‌العاده سریع زوج کلید در کسری از ثانیه
- ✓ الگوریتم‌های رمز متقارن استاندارد *AES(128-256)*، *DES*، *3DES* و الگوریتم اختصاصی پیام‌پرداز (*PAYA2*) به صورت سخت‌افزاری
- ✓ الگوریتم‌های چکیده‌ساز *SHA1*، *SHA256*، *MD5* و صحت *HMAC* به صورت سخت‌افزاری
- ✓ قابلیت استفاده از الگوریتم‌های رمز سفارشی

- ✓ مولد اعداد تصادفی سخت‌افزاری
- ✓ حافظه امن داخلی و سیستم فایل قدرتمند
- ✓ اطمینان کامل از عدم خروج کلیدهای خصوصی از توکن در هر شرایط
- ✓ شناسایی خودکار توسط کامپیوتر (بدون نیاز به نصب درایور)
- ✓ واسط *USB* استاندارد
- ✓ محافظت کانال *USB* با روش‌های رمزنگاری
- ✓ دارای حافظه جانبی به صورت *CD* مجازی جهت نگهداری ابزارهای مورد نیاز کاربران
- ✓ قابلیت *Write* محتویات *CD* مجازی با استفاده از ابزار اختصاصی توکن توسط سازمان‌های مشتری
- ✓ امکان استفاده در محیط‌های ویندوز و لینوکس
- ✓ بسته برنامه‌نویسی قدرتمند شامل:
  - رابط کارت هوشمند
  - رابط استاندارد *PKCS#11*
  - رابط استاندارد *Microsoft CAPI*
  - رابط اختصاصی ساده

کاربردها

- ✓ قابلیت به‌کارگیری در کلیه کاربردهای مبتنی بر *PKI* سازگار با استانداردهای *CSP* و *PKCS#11* از قبیل:
  - امضای دیجیتال و مبادله محرمانه *Email* در محیط‌های *Microsoft Outlook*، *Mozilla Thunderbird* و *Netscape*
  - امضای دیجیتال اسناد در *Microsoft Office* و *Adobe Acrobat*
  - ورود دوعاملی به *Domain* در سیستم عامل ویندوز (یا اصطلاحا *Smart Card Logon*) و سیستم عامل لینوکس
  - ارتباطات امن راه دور از طریق *VPN* در راه‌کارهای مبتنی بر ویندوز، لینوکس، سیسکو و ... مبتنی بر پروتکل‌های *PPTP*، *L2TP*، *SSTP*، *IPSec*، *SSL Over VPN* و ...

- ذخیره امن اطلاعات در سرویس‌های *EFS* و *BitLocker* ویندوز و برنامه *TrueCrypt*
- برقراری *SSL* دوسویه در مرورگرهای *IE* و *Firefox*
- احراز اصالت دوعاملی در بستر شبکه با سوییچ‌های مبتنی بر پروتکل *IEEE 802.1x*

✓ قابل استفاده در کاربردهای دولت الکترونیک از قبیل:

- سامانه‌های اظهارنامه الکترونیکی و مالیات بر ارزش افزوده
- سامانه تدارکات الکترونیکی دولت (ستاد)
- سامانه مدیریت و ثبت سفارشات دولت
- سامانه ثبت معاملات املاک و مستغلات کشور
- سامانه راهنامه بین المللی الکترونیک ایران

✓ قابلیت بکارگیری جهت احراز اصالت دوعاملی و امضای دیجیتال در نرم‌افزارهای اتوماسیون اداری از قبیل برید، همکاران سیستم، چارگون، رایورز، تورین‌تن و ....

✓ توسعه برنامه‌های کاربردی امن به وسیله برنامه‌نویسان و پیاده‌سازی سرویس‌های امنیتی از قبیل:

- احراز اصالت دوعاملی کاربر
- امضای دیجیتال
- ذخیره‌سازی امن داده‌های حساس
- محرمانه‌سازی و صحت‌سنجی داده‌ها
- قفل سخت‌افزاری جهت جلوگیری از تکثیر غیرمجاز

سازگاری

✓ استانداردهای کارت هوشمند *ISO 7816-4,8,9*

✓ *PKCS#1, 11, 12*

✓ *Microsoft CAPI (CSP)*

✓ مدیریت گواهی دیجیتال *X.509 V3 Certificate Storage*

✓ درایور کارتخوان *PC/SC*

✓ سازگار با میان‌افزار *PKE* دستینه (*Dastine-Enabled*)