بررسی اجمالی iKey :

- کوچکی iKey درحد یک کلید باعث حمل آسان و نصب فقط یک درایور ، سهولت در راه اندازی آن را میسر نموده است.

- iKey یک رسانه رمزنگاری پیشرفته است که با داشتن حافظه امن PKI و بهره بردن از یک پردازشگر رمز داخلی، قابلیت و اطمینان بسیار بالایی را برای کاربران خود در مباحث مختلف رمزنگاری همانند احرازهویت، امضای دیجیتال، مخفی سازی و درهم اطلاعات فراهم ساخته است
- توکن iKey دارای حافظه ای با ظرفیت 64 KB ، قابلیت نگهداری ۱۵ گواهینامه دیجیتال با طـول ۲۰۴۸ را امکـان پـذیر میسـازد. دسترسی به حافظه این توکن تنها با وارد نمودن رمز عبور خاص خود میسر میباشد.
- پشتیبانی از سیستم‌عامل‌های

  - Microsoft Windows 2000
  - MicrosoftWindows 2003
  - Microsoft Windows XP
  - Microsoft Windows Vista
  - Microsoft Windows 7
  - Apple MacOS 10.4.6 and above

- بطور کلی دسترسی به امکانات iKey با استفاده از روش های زیر میسر می باشد :

  - موارد مورد استفاده برای مدیران شبکه با استفاده از امکانات موجود در شبکه
  - موارد مورد استفاده برای برنامه نویسان رمز

موارد مورد استفاده برای مدیران شبکه

❖ امکان ورود به شبکه محلی با استفاده از گواهینامه دیجیتال

در این حالت کاربر برای ورود به شبکه نیاز به گواهینامه ای داردکه توسط مدیر شبکه از CA Server (Certificate Authority) دریافت و در حافظه PKI موجود در iKey ذخیره میشود . این روش جایگزینی بسیار مناسب برای نام کاربر و رمزعبور در هنگام ورود به شبکه می باشد و کاربر در هنگام ورود پس از اتصال iKey به سیستم، تنها کافیست PIN مربوطه را وارد نماید.
تعیین سیاست هایForce logoff , Lock System در صورت خارج نمودن iKey از کامپیوتر ، توسط مدیران شبکه امکان پذیر است.
لازم به ذکر است که سیاست های یاد شده، قسمتی از تنظیمات (DC(Domain Controller میباشد .

مزایای استفاده از این روش در:

- بالا بردن امنیت شبکه
- اطمنیان به مدیران شبکه در عدم ورود فرد یا افرادغیرمجاز به شبکه داخلی سازمان
- عدم وجود رمزهای عبور ساده با عمر بالا برای کاربران
- عدم ورود پرسنل بجای یکدیگر به شبکه
- غیرفعال نمودن برنامه های همانند Key Logger
- امکان تغییر طول رمزهای عبور کاربران نسبت به شرایط کاری آنان

❖ امکان ورود به شبکه خصوصی با استفاده از گواهینامه دیجیتال

جهت برقراری ارتباط با شبکه داخلی هنگام عدم حضورکاربر درمحل سازمان از طریق VPN و یا در هنگام حضور با استفاده از امکانات Terminal Services ، iKey امکان تایید هویت کاربر را برای شروع یک ارتباط امن میسر میسازد.

❖ امکان امضا و رمزگشایی نامه های الکترونیک شخصی با استفاده از گواهینامه دیجیتال

با توجه استاندارد بودن iKey و شناخت آن برای بسیاری از برنامه های موجود، می توان از آن برای امضای دیجیتالی و رمزنگاری پست الکترونیک نیز استفاده نمود. برای استفاده از این قابلیت تنها کافیست که تنظیمات امنیتی لازم جهت استفاده از گواهینامه دیجیتالی ذخیره شده در iKey در برنامه های استاندارد ارسال و دریافت پست الکترونیک (همانند MS Outlook ، Outlook Express و یا Thunderbird و ...) اعمال شود تا از این پس داده های ارسالی توسط iKey امضا و یا داده های دریافتی از رمز خارج شوند. این امکان می تواند از یک مجموعه کوچک تا حد ارسال و دریافت نامه درسطح بین المللی و از طریق شبکه اینترنت با توجه به تنظیمات رایانه کاربر نهایی صورت پذیرد.

امکانات برنامه نویسی برای برنامه نویسان رمز:

❖ استفاده از توابع برنامه نویسی رمز استاندارد

بمنظور برقراری ارتباط با انواع ادوات رمزکننده، استانداردهای مشخصی در دنیا تهیه و توزیع شده است. برای استفاده و دسترسی به یک ابزار استاندارد باید تولید کننده این استانداردها را در ابزار تولید شده قرار داده باشد تا برقرای ارتباط به شکلی راحت و کاملا ایمن امکان پذیر گردد.

مدیای رمزنگاری iKey نیز از این قاعده مستثنی نبوده و از طریق توابع رمز PKCS#11 v2.01 و MSCAPI v2.0 و Microsoft PC/SC برای برنامه نویس امکان برقراری ارتباط را مسیر ساخته است.

با برقرای این ارتباط می توان به حداقل توانمندی های زیر دست یافت:

- تولید کلیدهای رمز با استفاده از پردازشگر داخلی با توانمندی تولید کلیدهای رمز RSA با طول ۲۰۴۸ و ۱۰۲۴ بیت بصورت کاملا سخت افزاری
- رمزنگاری و رمزگشایی اطلاعات بصورت کاملا امن و در داخل حافظه داخلی
- امضای دیجیتالی و تایید هویت با استفاده از گواهینامه ها و یا کلید های تولید شده توسط کاربر

❖ استفاده از الگوریتم های رمز متقارن و نامتقارن و توابع درهم سازی استاندارد

با توجه به تعریف الگوریتم های زیر در iKey امکان ایجاد ارتباطی امن و ارسال و دریافت اطلاعات بصورت رمز شده براحتی میسر خواهد بود:

- کلید نامتقارن
  - RSA 1024-bit, RSA 2048-bit, DSA 1024-bit
- کلید متقارن
  - 3DES, RC4, RC2, AES 256-bit,AES 128-bit
- امضای دیجیتال
  - RSA 1024-bit, RSA 2048-bit
- درهم سازی اطلاعات
  - MD5 , MD2 , SHA-1, SHA-256

❖ دارای استاندارد امنیتی FIPS 140-2 level 3

این استاندارد از بارزترین استانداردهای امنیتی برای انواع ادوات رمزنگاری می باشد که کسب آن برای تولید کننده نیاز به گذر از انواع آزمایش های سخت و پیچیده را لازم می نماید.

خوشبختانه رسانه رمزنگاری iKey موفق به دریافت این گواهی در سطح ۳ آن شده است.

از دیگر گواهی های کسب شده توسط این محصول می توان به موارد زیر اشاره داشت:

Common Criteria EAL 2
RoHS
China RoHS
FCC Part 15 - Class B
CE