بررسی اجمالی iKey :

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

- نصب بسیار ساده بصورت Plug & Play در دوسطح برای کاربران و مدیران. ضمنا قابلیت نصب دلخواه را با استفاده از پارامترهای نصب را نیز فراهم می سازد.

- دارای حافظه های PKI و non-PKI

  - از حافظه PKI برای انجام عملیات رمز نگاری و رمزگشایی اطلاعات و همچنین نگهداری گواهینامه های دیجیتال استفاده می شود. که حافظه توسط رمز عبور خاص خود حفاظت می گردد.

  - توسط حافظه non-PKI شما میتوانید اطلاعات شخصی ویا محرمانه خود را (همانند شماره تلفن های خاص وشماره حساب بانکی و...) ذخیره نمایید. همچنین در این قسمت بجز فایل های اطلاعاتی می توانید شمارنده و یا فایل های مربوط به احراز هویت از طریق روش های مختلف همانند Challenge and Secret را نیز قرار دهید.

- iKey دارای سطوح مختلف دسترسی بر اساس رمزعبور است که بشکل زیر تقسیم بندی می گردد:

  - دسترسی به حافظه PKI توسط رمزعبور خاص خود که به آن PIN گفته می شود.

  - دسترسی به حافظه non-PKI بطرق زیر:

    - Guest :در این وضعیت بدون وارد نمودن رمزعبور به اطلاعاتی که برای این گروه تعریف شده است دسترسی خواهیم داشت.
    - User : در این وضعیت با وارد نمودن این رمزعبور، می توانیم به اطلاعات این سطح و همچنین به اطلاعات کاربر Guest دسترسی پیدا کنیم.
    - Administrator : با استفاده از این رمزعبور، بالاترین سطح دسترسی به حافظه و امکانات iKey فراهم می گردد. به این رمز عبور SOPIN نیز گفته می شود.

لازم به ذکر است که اختصاص و تنظیم حافظه های فوق، فقط و فقط توسط SOPIN میسر می گردد . ضمنا حجم کلی حافظه درمدلهای مختلف متفاوت می باشد.

- برای جلوگیری از دسترسی به حافظه داخلی iKey از طریق روش های سعی و خطا، امکانی وجود دارد که باعث محدودیت در تعداد دفعات وارد نمودن رمز عبور میگردد. درصورت بوجود آمدن این وضعیت، iKey بطور کامل قفل شده و تا زمانیکه SOPIN برای باز نمودن آن وارد نشود، iKey دروضعیت قفل شده باقی خواهد ماند. ضمنا رمزعبور SOPIN را نیز دارای چنین خصوصیتی است.

بنابراین درصورت سعی در بدست آوردن رمزعبور SOPIN و قفل شدن iKey ، لازمه باز شدن فقط و فقط پاک نمودن کلیه محتویات توسط کارخانه و یا توزیع کننده این محصول خواهد بود.

- بطور کلی دسترسی به امکانات iKey با استفاده از روش های زیر میسر می باشد :
  - بدون استفاده از ابزارهای برنامه نویسی
  - بااستفاده از امکانات برنامه نویسی

موارد کاربری iKey بدون استفاده از ابزارهای برنامه نویسی

درصورتیکه درسازمان خود امکانات برنامه نویسی فراهم نباشد می توان از iKey برای موارد زیر بهره برداری نمود:

- امکان ورود به شبکه با استفاده از گواهینامه دیجیتالی

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. این روش به مدیران شبکه اطمنیان عدم ورود فرد یا افرادغیرمجاز را می دهد.

- بدلیل استفاده iKey از یک پورت USB و وجود آن برروی بیشتر کامپیوترهای امروزی و همچنین عدم نیاز به دستگاههای جانبی (همانند کارت خوان) می توان iKey را جایگزینی مناسب برای کارتهای هوشمند درنظر گرفت.

- با توجه به اینکه iKey محصولی است کاملا استاندارد می توان از آن برای امضای دیجیتالی و رمزنگاری Email با استفاده از گواهینامه های دیجیتال نیز استفاده نمود. برای استفاده از این قابلیت تنها کافیست که تنظیمات امنیتی لازم جهت استفاده از گواهینامه در برنامه های استاندارد ارسال و دریافت Email (همانند MS Outlook ویا Outlook Express) اعمال شود تا از این پس داده های ارسالی توسط iKey امضا و به رمز درآید. این امکان می تواند از یک مجموعه کوچک تا حد ارسال و دریافت نامه درسطح بین المللی و از طریق اینترنت با توجه به تنظیمات کامپیوتر میزبان صورت پذیرد.

- در صورت عدم حضورکاربر در محل شرکت و تمایل جهت برقراری ارتباط با سرور از طریق VPN و یا با استفاده از امکانات Terminal Services ، iKey امکان تایید هویت کاربر را برای ایجاد ارتباط امن میسر میسازد.

- از دیگر امکانات iKey ثبت گواهینامه کاربر بر روی کامپیوتر در زمان اتصال و حذف گواهینامه به محض جدا کردن آن است . این عمل تضمین حفظ اطلاعات را در زمان عدم اتصال iKey فراهم می سازد.

- همانطور که قبلا نیز درخصوص استاندارد بودن iKey اشاره شد ، اعمال سیاست هایForce logoff , Lock System در صورت بیرون آوردن 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 .

موارد کاربری iKey با استفاده از ابزارهای برنامه نویسی

- استفاده از الگوریتم های نامتقارن (RSA 1024 به صورت سخت افزاری) و متقارن
iKey با استفاده از حافظه PKI مربوط به خود و توسط الگوریتم های رمزنگاری متقارن و نامتقارن امکان ایجاد ارتباطی امن و ارسال و دریافت اطلاعات بصورت رمز شده را فراهم میسازد.

- iKey امکان درهم سازی اطلاعات را توسط الگوریتم های یکطرفه همانند MD5 و با استفاده از روش های XOR,HMAC CHAP را به صورت سخت افزاری فراهم میسازد . توسط الگوریتم های فوق امکان ورود به وب سایتها و یا محلهای خاص در سطح شبکه اینترنت و یا اینترانت مقدور خواهد بود. ضمنا قابلیت تایید هویت کاربر با داشتن iKey و رمزعبور مربوطه (Two-Factor Authentication) ، فراهم می گردد.

- iKey SDK
توسط این SDK قابلیت تولید فایل های اطلاعاتی و شمارنده ها وهمچنین نحوه ذخیره اطلاعات محرمانهٔ مورد نیاز الگوریتم MD5 را برای برنامه نویس میسر و امکان نوشتن و خواندن اطلاعات مجاز را به وی خواهد داد.

- استفاده از توابع رمز استاندارد باتوجه به سیستم عامل
iKey از طریق توابع PKCS#11,12,15 (برای ارتباط با سیستم عامل های غیر ویندوز همانند Unix) و MSCAPI (برای سیستم عامل های ویندوز) امکانات زیر را فراهم میکند :

- **تولید کلید :** این حالت امکان تولید کلید های عمومی و خصوصی و همچنین تولید کلید متقارن را برای برنامه نویسان فراهم می نماید.
- **رمزنگاری و رمزگشایی اطلاعات :** کاربر میتواند اطلاعات ارسالی خود را با استفاده از کلید عمومی گیرنده رمز کند و برای وی ارسال نماید تا گیرنده ، اطلاعات دریافتی را با استفاده از کلید خصوصی خود رمزگشایی و به محتوای آن دسترسی پیدا نماید .
- **امضای دیجیتالی و تایید هویت:** کاربر میتواند اطلاعات ارسالی خود را با استفاده از کلید خصوصی خود امضا و برای گیرنده ارسال نماید تا گیرنده با استفاده از کلید عمومی وی از هویت فرستنده اطلاعات اطمینان حاصل نماید .
- **Import & Export:** این حالت امکان Export کلید عمومی جهت توزیع بین دیگر کاربران و Import کلید عمومی، جهت به رمز درآوردن اطلاعات برای گیرنده مشخص را میسر میسازد.

- در هنگام استفاده از روش Challenge and Secret نیاز به تولید مقادیر تصادفی می باشد . iKey امکان تولید رشته های عددی و کاراکتری تصادفی را بصورت سخت افزاری جهت تسریع سرعت را فراهم می سازد. بدیهی است که امکان یاد شده لزوما برای استفاده در روش فوق نخواهد بود و برنامه نویسان می توانند از آن برای کاربردهای دیگر نیز بهره ببرند.