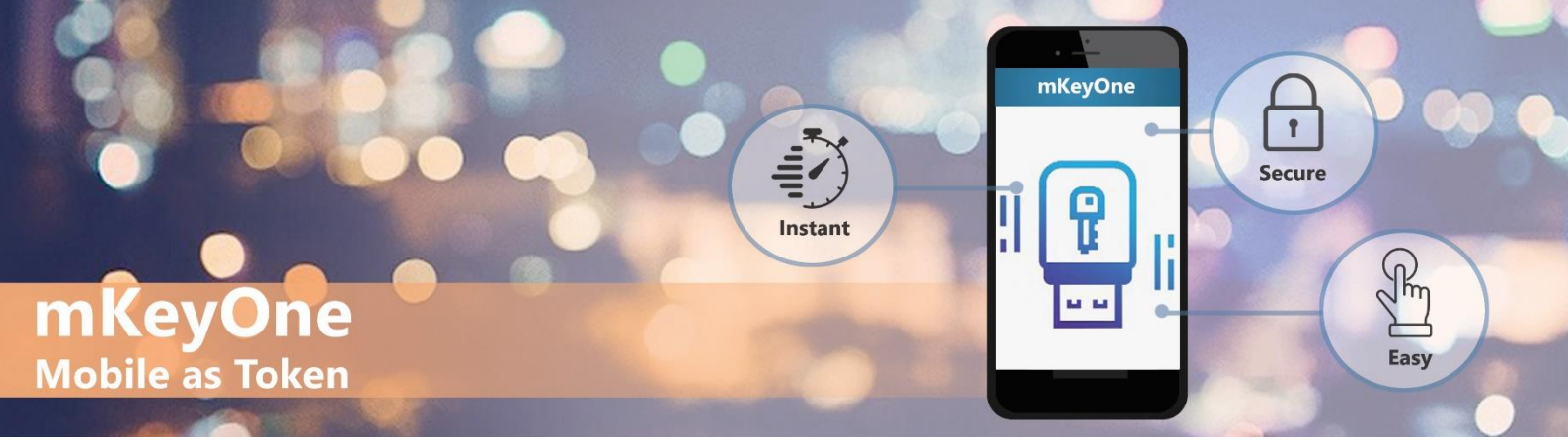


Comprehensive Token

- CCID Compatible
- ISO/IEC 7816
- PC/SC Standard
- Generic Identity Device Specification
- Fully compatible with eCommerce Development Centre of Iran Certificates

Easy Deployment

- Both side Light Installation
- Minimum permissionson portable device
- Integration with all PKI-Enabling Systems
- Auto update
- Cost effective
- USB & WiFi Connectivity

Operating System

- Supported platforms:
  - All Windows (32/64bit)
  - Android
  - iOS (In develop)

Applications

- e-banking
- e- governance
- e- commerce
- e-communication
- e-notarization
- e-insurance
- e-police
- e-health
- e-vote

توکن امضای دیجیتال همراه (mKeyOne)

برای استفاده از زیرساخت کلی عمومی در فرآیندهای انکارناپذیری و استنادپذیری اسناد و عملیات الکترونیک, باید الزامات و اداواتی را مورد بهره برداری قرار داد. یکی از مهمترین این اداوات, مربوط به تجهیزات سمت کاربر نهایی می گردد که مشخصا به توکن و یا کارت هوشمند مرتبط خواهد شد. ابزاری که باید بتواند از کلید خصوصی کاربر حفاظت نموده و کلیه عملیات و محاسبات امضا و رمزگشایی داده را در درون خود صورت دهد. از طرف دیگر باید به راحتی کاربر در نصب و استفاده حتی برای کاربرانی که در حوزه فن آوری اطلاعات دانشی ندارند هرچند در کار خود متخصص و بسیار حرفه ای هستند نیز توجه داشت.

شرکت پندار کوشک ایمن با هسته ای متشکل از مدیران و کارشناسان حوزه اعتماد دیجیتال و زیرساخت کلید عمومی و همچنین با دارا بودن دانش لازمه در حوزه کارتهای هوشمند و تولید اپلت های متنوع نسبت به نیاز جامعه, توانسته است با تکیه بر دانش فنی خود توکن های مبتنی بر گوشی همراه را با موفقیت به بازار معرفی نماید. درحقیقت این توکن ها از امکانات گوشی همراه استفاده نموده و در زمان امضا مشابه یک توکن به سیستم متصل شده و عملیات لازم را با امنیت بالا انجام می دهد.

قابلیت ثبت نام گواهی

محصول mKeyOne دارای یک مرکز ثبت نام گواهی داخلی می باشد که قادر است مطابق با استانداردهای ریشه کشوری، کاربر را احرازهویت و گواهینامه دیجیتال وی را از مرکز گواهی سطح برنز اخذ نماید. همچنین برای کاربرانی که درخواست گواهی سطح نقره نیز داشته باشند این امکان فراهم شده تا تنها با ثبت اطلاعات معتبر از خود بتوانند کد رهگیری را دریافت نموده و با حضور در یکی از مراکز ثبت نام و پس از احرازهویت حضوری؛ گواهی خود را در گوشی همراه خود داشته باشند.

نکته قابل توجه اینکه محصول mKeyOne می تواند از طریق NFC گوشی, محتوای کارت هوشمند صادره توسط هریک از مراکز میانی گواهی را خوانده و درصورتیکه گواهی کارت هوشمند معتبر باشد, گواهی جدید را با همان کاربرد و برای همان هویت در گوشی همراه صادر نماید. این عملیات بدون نیاز به احرازهویت صورت خواهد پذیرفت.

Security

- Architecture based on Mobile Trusted Execution Environment (TEE)
- Highly protected Private Keys
- Multiple Certificates Supported
- PIN Based Protection
- Encrypted Channel
- Phone Lock Type is needed to Token Initialization
- Two Security Levels: Security Officer (SO) & Personal Identification Number (PIN)

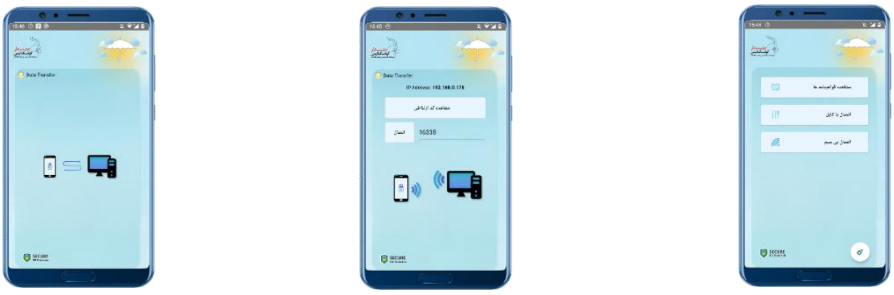
Benefits

- mKeyOne is using a MS-CAPI that is commonly available to multiple applications.
- Smartcard Based Architecture so would provide better interoperability in some situations without requiring a translation mechanism that could be costly in terms of overhead, security, and performance
- All functions is using hardware specification to further improve performance
- Embedded face recognition for certificate registration

اتصال چندگانه

محصول mKeyOne بگونه ای طراحی شده است که می تواند از دو روش برای اتصال به رایانه استفاده نماید. یکی روش اتصال با کابل و دیگری از طریق شبکه بیسیم. این موضوع از آنجایی اهمیت وِیژه ای پیدا می کند که زمان تایید یک فرآیند بواسطه امضای دیجیتال محتوا می تواند باعث از دست دادن فرصت ها در بسترهای متفاوتی همانند بازرگانی, مالی و بانکی, .. و حتی قراردادهای شخصی گردد, و از اینرو نبود عاملی مثل کابل ارتباط USB نباید مخل این موضوع گردد.

در هر دو شکل ارتباط(USB,WiFi) سیستم عامل ویندوز مشابه اتصال یک توکن به پورت USB خود عمل نموده و بدون درخواست هرگونه درایور مجزا, توکن را شناسایی می نماید. از این نقطه به بعد, فرآیند امضا دقیقا مشابه توکن بوده و همه برنامه‌های کاربردی استاندار جهان براحتی با آن برخورد خواهد نمود.



امنیت بالا

در هر محصولی سادگی کاربری اهمیت ویژه ای دارد ولی این موضوع نباید مانع از کاهش سطوح امنیتی گردد. این موضوع نیز از دید کارشناسان شرکت پندار کوشک ایمن پوشیده نبوده و بگونه ای تمامی ارتباطات حفاظت شده اند.

کلید خصوصی که بیشترین نگرانی از بابت افشای آن می باشد در بخش TEE گوشی همراه بعنوان یک المان امن تولید و نگهداری می گردد. برای دسترسی به آن نیز رمز کاربر الزامی می‌باشد. در مورد کانال ارتباطی چه ارتباط سیمی و چه نوع بیسیم آن نیز تماما اطلاعات با پروتکلی مشابه SSL توسط کلید جلسه به رمز درآمده و لذا با خواندن مسیر نیز اطلاعات افشا نخواهند شد.

تولید شده در پارک علم و فناوری دانشگاه تهران

پندار کوشک ایمن (PKI Co.)

۸۸۲۲۰۷۱۵ و ۸۸۲۲۰۶۹۰ ۲۱ ۹۸+

info@pki.co.ir www.pki.co.ir

زیرساخت کلید عمومی و امنیت اطلاعات