امضای دیجیتال و رمزنگاری داده برای همه

یکی از مهمترین چالش های حوزه اسناد الکترونیک مبحث استنادپذیری سند و امنیت مبادلات الکترونیکی می باشد. این موضوع عمدتا بدلیل پیچیدگی های پیاده سازی و بعضا هزینه های بالای پرسنلی و زمانی در مقیاس سازمان های بزرگ و متوسط پیاده سازی می گردد و از اینرو عموم جامعه امکان بهره برداری از این خدمت را نداشته و ندارند.

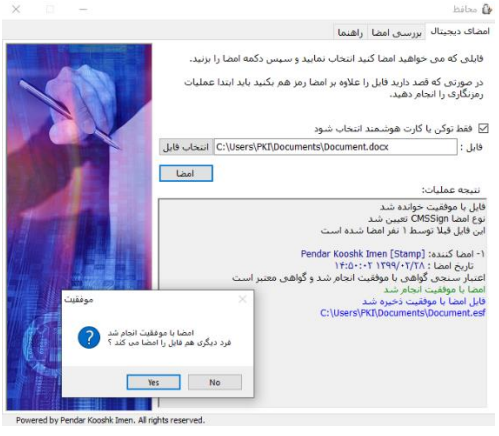
محافظ (Sign & Seal) نام ابزاری نرم‌افزاری است که برای جامعیت بخشی به این هدف توسط متخصصین شرکت پندار کوشک ایمن طراحی و به بازار ارائه شده است. توسط این برنامه و تنها با داشتن گواهی الکترونیک می توان از بحث استنادپذیری و محرمانگی اسناد بدون کوچکترین دانشی از حوزه زیرساخت کلید عمومی بهره برد.

این ابزار با تعامل با گواهینامه الکترونیکی قادر به امضای دیجیتال چند باره سند و رمزنگاری آن برای گیرنده می باشد. طراحی و پیاده سازی این ابزار بگونه ایست که اجرای آن هیچگونه وابستگی به نصب بسته‌های خاص نرم افزاری بر روی رایانه کاربران ندارد و بدون نیاز به هیچگونه تنظیم امنیتی اضافه برروی سیستم کاربر قابل نصب و استفاده می باشد. محافظ به همراه یک ویدیو آموزشی گام به گام رایگان ارائه می شود.

قابل استفاده با انواع توکن و کارت هوشمند

محافظ بازه وسیعی از پروتکل‌های ارتباطی را به کار گرفته است تا بتواند با انواع رسانه‌های ذخیره‌سازی کلید تعامل نماید. محافظ می‌تواند با انواع توکن‌های رمزنگاری بصورت نرم افزار یا سخت افزاری ارتباط برقرار کند. در حالت نرم افزاری تنها داشتن کلید خصوصی برای امضا کفایت می کند. بدین معنی که محافظ قادر است با Windows Store و همچنین فایل‌های حاوی کلید مبتنی بر استاندارد PKCS#12 ارتباط برقرار نماید. جهت استفاده از توکن سخت افزاری نیز باید درایور ویندوزی آن نصب شده باشد. همچنین دستینه می‌تواند با بهره‌گیری از استاندارد ISO/IEC 7816 با انواع کارت هوشمند ارتباط برقرار نماید. جهت ارتباط با کارتخوان‌های کارت هوشمند نیز از استاندارد ارتباطی PC/SC بهره-برداری شده است.

از طرف دیگر محافظ می تواند با کارت هوشمند ایرانی آیدین بدون هیچگونه مشکلی تعامل داشته باشد. بدین ترتیب که کارت هوشمند مذکور، بدون نیاز به نصب هیچگونه درایور و یا میان‌افزار، قابل استفاده در طرف کاربر خواهد بود و به عبارت دیگر تنها یک درگاه USB برای کارتخوان کافیست تا کاربر بتواند از کارت هوشمند خود استفاده نماید.



Comprehensive Response to Cryptographic Requirements

- Read Certificate
- Digital Signature
- Verify/Validate Signature
- Encryption
- Decryption
- Multiple Signature
- Fully supported PAdES (PDF Advanced Electronic Signatures)

Easy Deployment

- Protable Application
- No dependency
- No Installation Required
- Context Menu operations

Specifications

- Ease of use with user friendly interface
- Supported Soft-Tokens (P12, Pfx)
- Supported Hard-Tokens (MSCAPI)
- Supported IDin Smartcard
- PDF Standard Signing
- CMS Standard Signing
- Recovering original signed/encrypted data
- Container base (.esf files)

Key Stores

- Secure Token by MS-CAPI
- Smart Card by MS-CAPI
- Windows Key Store
- File Key Store (PKCS#12)
- IDin without Driver

Operating System

- Windows Vista (SP1/SP2) (32/64)
- Windows 7 (SP1) (32/64)
- Windows 8/8.1 (32/64)
- Windows 10 (32/64)

Standards

- FIPS 180-4
  (Secure Hash Standard (SHS))
- RFC 2396
  (Uniform Resource Identifiers (URI): Generic Syntax)
- PKCS#1
  (RSA Cryptography Standard)
- PKCS#7
  (Cryptographic Message Syntax Standard)
- PKCS#10
  (Certification Request Standard)
- PKCS#12
  (Personal Information Exchange Syntax Standard)
- PC/SC
  (Personal Computer/Smart Card)
- ISO/IEC 7816
  (Identification cards - Integrated circuit(s) cards)
- NIST SP 800-73-3
  (Interfaces for Personal Identity Verification (PIV))
- MS-CAPI
  (Microsoft Cryptography API)

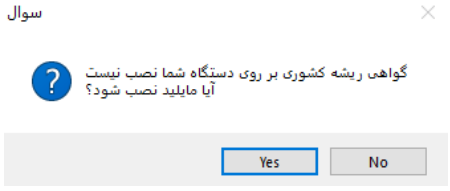
Download link:
http://pki.co.ir/download/signandseal.exe

قابلیت امضای چندگانه و اعتبار سنجی اسناد

برنامه محافظ این قابلیت را دارد تا بتواند یک فایل را چندین بار و توسط گواهینامه های مختلف امضا نماید. این کاربری همانند عقد قراردادهای تجاری در سطوح مختلف می باشد که چندین نفر امضای خود را روی برگه به تحریر می آورند. همچنین این برنامه می تواند فایل های امضا شده را اعتبارسنجی نموده تا قبل از امضای بعدی, اطمینان لازم از صحت داده وجود داشته باشد.

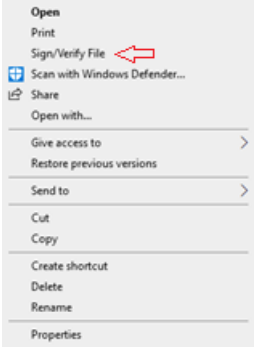
نصب خودکار گواهینامه های ریشه کشور

جهت تسهیل بیشتر فرآیند کار و آسودگی خاطر کاربران از صحت گواهی نامه مورد استفاده, نرم افزار محافظ در اولین بار اجرا قادر به نصب خودکار گواهینامه های ریشه کشور می باشد. این اقدام از یک طرف در راستای توسعه بیشتر و استفاده موثرتر از این سرمایه ملی صورت پذیرفته و از طرف دیگر این اطمینان را به کاربر استفاده کننده از ابزار می دهد که گواهی دریافتی نیز از مرکز معتبری دریافت شده است.



سهولت در استفاده

محافظ به شکلی طراحی شده است که نیاز به نصب از طریق برنامه های نصبی نداشته و پس از اولین اجرا به explorer ویندوز متصل شده تا فرآیند امضا و اعتبارسنجی را با سهولت بیشتری صورت دهد.



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