Dastine

Public Key Enabling SDK

Complete Cryptography API

- Read Certificate
  - Filter by Subject
  - Filter by Issuer
  - Filter by Key Usage
  - Filter by Hardware/Software
- Digital Signature
- Encryption
- Decryption
- Key Generation
- Certificate Request
- Remove Certificate

Security

- Device Remove Event
- Virtual Random Keypad
- Secure PIN box
- Memory Zeroation
- Buffer overflow control
- Input character control
- Exclusive Lock to Token
- Thread Safe

Multi-Platform

- All Windows Client OS
- 32bit/64bit Architecture
- Popular Web Browsers
- All Programming Platforms

PIN Policy

- PIN Secure Input Method
- PIN Cache Setting (Always/Never)
- PIN Interactive Input/ Fix Input
- PIN Numeric only/ Character only

Easy Deployment

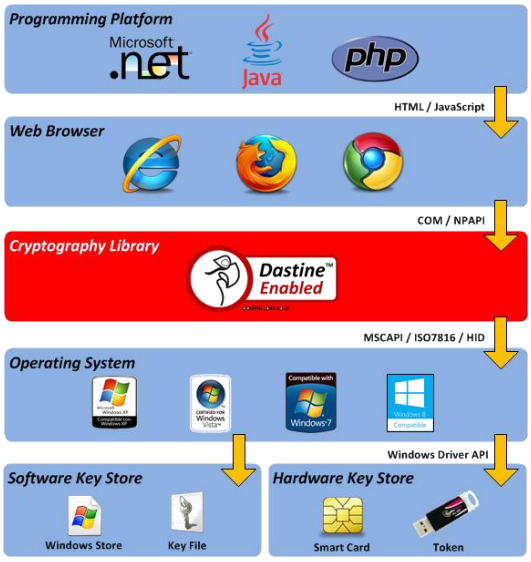
- No requirement to .Net Framework or Java Virtual Machine

میان‌افزار جامع امضای دیجیتال و رمزنگاری

دستینه نام ابزاری نرم‌افزاری است که برای تجهیز سامانه‌ها به خدمات زیرساخت کلید عمومی (PKI-Enabling) از جمله تعامل با گواهینامه الکترونیکی، امضای دیجیتال، رمزنگاری، احراز اصالت و مانند آن طراحی و جهت استفاده عموم برنامه نویسان و تولیدکنندگان نرم‌افزار ارائه شده است. این ابزار قابل استفاده به همراه انواع توکن‌ها و کارت‌های هوشمند در رایانه کاربران بوده و در حال حاضر برای تمامی مرورگر پر استفاده از جمله Microsoft IE، Mozilla Firefox و Google Chrome در دسترس می باشد. طراحی و پیاده سازی این ابزار بگونه ایست که اجرای دستینه وابستگی به نصب بسته‌های نرم افزاری دیگر مانند Net Framework. و یا Java بر روی رایانه کاربران ندارد و بدون نیاز به هیچگونه تنظیم امنیتی اضافه برروی سیستم کاربر قابل نصب و استفاده می‌باشد. دستینه به صورت یک بسته کامل شامل مقاله آموزشی گام به گام، راهنمای جامع توابع برنامه نویسی، نمونه کدهای مختلف رمزنگاری و امضای دیجیتال، صفحه دموی آنلاین جهت تست و ارزیابی توکن و کارت هوشمند، و قابلیت دانلود به صورت رایگان برای کلاینت ها ارائه می شود.

سازگار با انواع سیستم عامل و مرورگر

دستینه با انواع مختلف سیستم‌عامل ویندوز کلاینت تست و آزمون شده است و بدون نیاز به نصب بسته‌های Update، قابل نصب و استفاده برروی تمامی آنها می‌باشد. در نتیجه می‌توان دستینه را بدون نگرانی از مشکلات نگهداری در تعداد زیادی از کلاینت های کاربران، نصب و استفاده نمود. رایانه کاربر می‌تواند هرکدام از نسخه‌های ویندوز اعم از Windows Vista، Windows 7 ، Windows 8 و یا Windows 10 را داشته باشد. همچنین دستینه به شکلی طراحی شده است که می‌تواند برروی انواع معماری 32 و 64 بدون مشکل استفاده شود.



Key Stores

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

Programming Platform

- .Net Framework SDK
- J2EE and J2SE SDK
- PHP
- Others that support JavaScript

Operating System

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

Web Browser

- Microsoft Edge
- Microsoft Internet Explorer (IE) (10 and above)
- Mozilla Firefox (13 and above)
- Google Chrome (4 to 16)

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)

توانایی کار با کارت هوشمند ملی سازمان ثبت احوال کشور

باتوجه به توسعه کاربری کارت ملی هوشمند, محصول دستینه توانسته کیت توسعه نرم افزاری این کارت در خود جای داده و با ساده سازی و حذف پیچیدگی های برنامه نویسی, استفاده از کارت هوشمند ملی را برای تمامی برنامه های تحت وب میسر نماید. از آنجائیکه بسیاری از نرم افزارهای تحت وب با ابزار دستینه به زیرساخت کلید عمومی تجهیز شده اند, عملا با یک ارتقای ساده می توان از ابزار دستینه برای کاربری کارت هوشمند ملی نیز بهره برد.

این اقدام از یک طرف باعث سهولت و افزایش سرعت پیاده سازی شده و از طرف دیگر همزمان می توان با انواع توکن و کارت هوشمند در سامانه تجهیز شده به زیرساخت کلید عمومی استفاده نمود.

قابل استفاده با انواع توکن و کارت هوشمند

دستینه بازه وسیعی از پروتکل‌های ارتباطی را به کار گرفته است تا بتواند با انواع رسانه‌های ذخیره‌سازی کلید تعامل نماید. دستینه می‌تواند با انواع توکن‌های رمزنگاری ارتباط برقرار کند. بدین منظور کافیست توکن مذکور درایور ویندوزی داشته 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 بهره‌برداری شده است. شایان ذکر است که دستینه قادر به تعامل با Windows Store و همچنین فایل‌های حاوی کلید مبتنی بر استاندارد PKCS#12 نیز می‌باشد.

از طرف دیگر دستینه می تواند با کارت هوشمند ایرانی آیدین بدون هیچگونه مشکلی تعامل داشته باشد. بدین ترتیب در صورتی که از ابزار دستینه برای PKI-Enabling نرم‌افزار استفاده شود، کارت هوشمند مذکور، بدون نیاز به نصب هیچگونه درایور و با میان‌افزار، قابل استفاده در طرف کاربر هستند و به عبارت دیگر تنها یک درگاه USB برای کارتخوان کافیست تا کاربر بتواند از کارت هوشمند خود استفاده نماید.

تولید شده در پارک علم و فناوری دانشگاه تهران

دارای گواهی تایید فنی نرم‌افزار از شورای عالی انفورماتیک کشور

برگزیده پنجمین جشنواره نوآوری و فن‌آفرینی جایزه دکتر شهید چمران

پندار کوشک ایمن (PKI Co.)

۸۸۲۲۰۷۱۵ و ۸۸۲۲۰۶۹۰ ۲۱ ۹۸+

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

پندار کوشک ایمن
زیرساخت کلید عمومی و امنیت اطلاعات