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

- CodeSigned by VeriSign CA
- Timestamped by VeriSign TSA
- Device Insert and 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

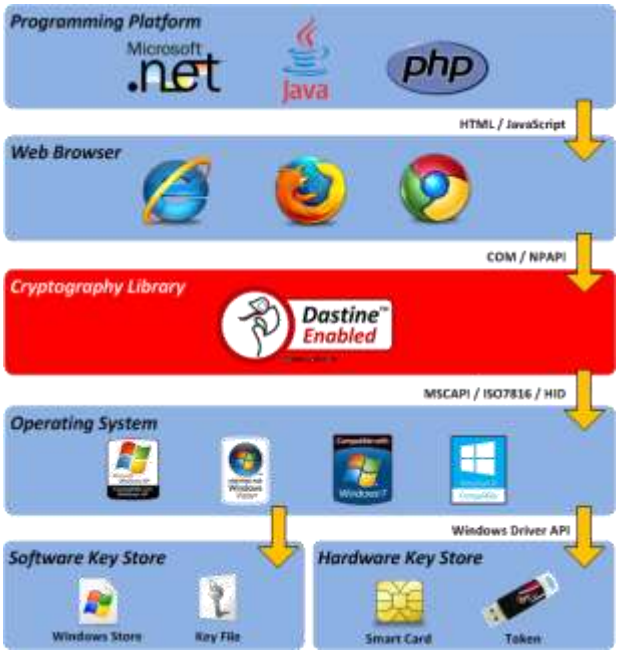
- Less than 1 MB
- No dependency
- No requirement to
  .Net Framework or
  Java Virtual Machine

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 به صورت پلاگین برای سه مرورگر پر استفاده Microsoft IE، Mozilla Firefox و Google Chrome در دسترس است. نسخه پلاگین دستینه نیازی به نصب دستی توسط کاربر نداشته و با حجم بسیار کم به صورت خودکار بارگذاری و اجرا می‌شود. همچنین اجرای دستینه وابستگی به نصب بسته‌های نرم افزاری دیگر مانند Net Framework. و یا Java بر روی رایانه کاربران ندارد. از طرف دیگر، دستینه توسط گواهینامه امضای کد (CodeSign) معتبر از شرکت VeriSign امضا شده است و بدون نیاز به هیچگونه تنظیم امنیتی اضافه برروی سیستم کاربر قابل نصب و استفاده می‌باشد.

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 XP، Windows Vista، Windows 7 و یا Windows 8 را داشته باشد. همچنین دستینه به شکلی طراحی شده است که می‌تواند برروی انواع معماری ۳۲□□□ و ۶۴□□□ بدون مشکل استفاده شود. دستینه همچنین برای انواع پراستفاده مرورگر وب شامل Microsoft IE، Mozilla Firefox و Google Chrome نسخه اختصاصی دارد و به صورت خودکار با تشخیص نسخه سیستم‌عامل و مرورگر، پلاگین مناسب را برروی کلاینت کاربر بارگذاری می‌نماید.



Key Stores

- Secure Token by MS-CAPI
- Smart Card by MS-CAPI
- Windows Key Store
- File Key Store (PKCS#12)
- IDin without Driver
- ParsKey without Driver
- KeyA3 without Driver

Programming Platform

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

Operating System

- Windows XP(SP1/SP2/SP3)(32/64)
- Windows Vista (SP1/SP2) (32/64)
- Windows 7 (SP1) (32/64)
- Windows 8/8.1 (32/64)

Web Browser

- Microsoft Internet Explorer (IE) (6 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)

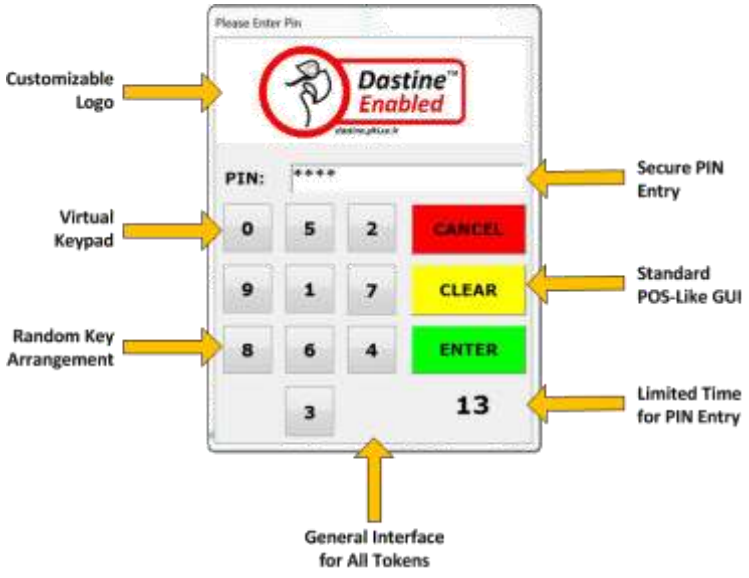
مستقل از پلتفرم و زبان‌های برنامه‌سازی

دستینه به شکلی طراحی شده است که مستقل از زبان‌های برنامه‌سازی بوده و قابل استفاده در انواع پروژه‌های مبتنی بر .Net Framework، J2EE/J2SE و یا PHP می‌باشد. در واقع زبان ارتباط با دستینه، زبان JavaScript بوده که در تمامی سیستم‌عامل‌ها و مرورگرها، بدون نصب هیچگونه بسته نرم‌افزاری، قابل استفاده است. بدین ترتیب می‌توان از دستینه در انواع مختلف پروژه‌های نرم‌افزاری تحت وب استفاده نمود و در عین حال نیازی به نصب هیچگونه بسته نرم‌افزاری در طرف کلاینت ندارد.

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 قادر است بدون نیاز به نصب درایور توکن، با کارت هوشمند ایرانی آیدین و همچنین توکن‌های رمزنگاری ParsKey از شرکت امن افزار گستر شریف و KeyA3 از شرکت مهندسی پیام پرداز تعامل داشته باشد. بدین ترتیب در صورتی که از ابزار دستینه برای PKI-Enabling نرم‌افزار استفاده شود، توکن‌های شرکت‌های ایرانی مذکور، بدون نیاز به نصب هیچگونه درایور و یا میان‌افزار، قابل استفاده در طرف کلاینت هستند و به عبارت دیگر تنها یک درگاه USB کافیست تا کاربر بتواند از توکن 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.)

ایران، تهران، خیابان کارگر شمالی، پردیس شمالی دانشگاه تهران، پارک علم و فناوری، ساختمان شماره ۲، واحد ۲۰۵

۸۸۲۲۰۷۱۵ و ۸۸۲۲۰۶۹۰ ۲۱ ۹۸+

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