هویتا

بستر زیرساخت کلید عمومی

احراز هویت الکترونیک امن . امضای دیجیتال

Hovita.ir

Public Key Infrastructure

شرکت فناوران هویت الکترونیکی امن (هویتا)

شرکت دانش بنیان فناوران هویت الکترونیکی امن (هویتا)، با هدف توسعه محصولات و خدمات حوزه زیرساخت کلید عمومی (PKI)، احراز هویت و هویت سنجی دیجیتال و ارائه راهکارهای مطمئن به جهت تأمین امنیت اطلاعات، ارتباطات و تبادلات الکترونیکی، تشکیل شده است.

HOVITA

Secure Electronic Identity Technologies Company

WWW.HOVITA.IR

هویتا

درباره شرکت فناوران هویت الکترونیکی امن (هویتا)

هسته اصلی شرکت فناوران هویت الکترونیکی امن (هویتا)، متشکل از متخصصین حوزه امنیت و زیرساخت کلید عمومی است که فعالیت خود را از سال ۱۳۸۱ در کشور آغاز نموده‌اند. این شرکت در زمینه طراحی و توسعه محصولات، خدمات و راهکارهای نوین مبتنی بر رمزنگاری، امضای دیجیتال، گواهی‌های الکترونیکی، توکن امضای دیجیتال، سخت‌افزارهای امنیتی و راه‌اندازی زیرساخت کلید عمومی، در سال ۱۳۹۵ به عنوان یک شرکت دانش بنیان در پارک علم و فناوری شریف ثبت و مستقر گردیده است.

این شرکت مفتخر به آن است که توانسته محصولات متعددی را با کیفیت بالا و دقت عملکرد، بر مبنای پژوهش، تحقیق و توسعه در حوزه زیرساخت کلید عمومی تولید نماید که این محصولات به‌لحاظ بومی‌سازی و فن‌آفرینی، موفق به کسب دریافت بالاترین تاییدیه‌های لازم از آزمایشگاه های معتبر کشور است. همچنین این شرکت علاوه بر طراحی، تولید و ارائه محصولات تخصصی درحوزه زیرساخت کلید عمومی، تا کنون چندین کارگاه تخصصی ارائه نموده و تهیه مقالات علمی و پژوهشی در حوزه زیرساخت کلید عمومی را در کارنامه خود دارد.

امید است فعالیت‌های این شرکت به همت نیروی جوان و با تمرکز بر فناوری‌های نوآورانه و نوظهور، گام موثری در پییشبرد اهداف میهن عزیزمان باشد.

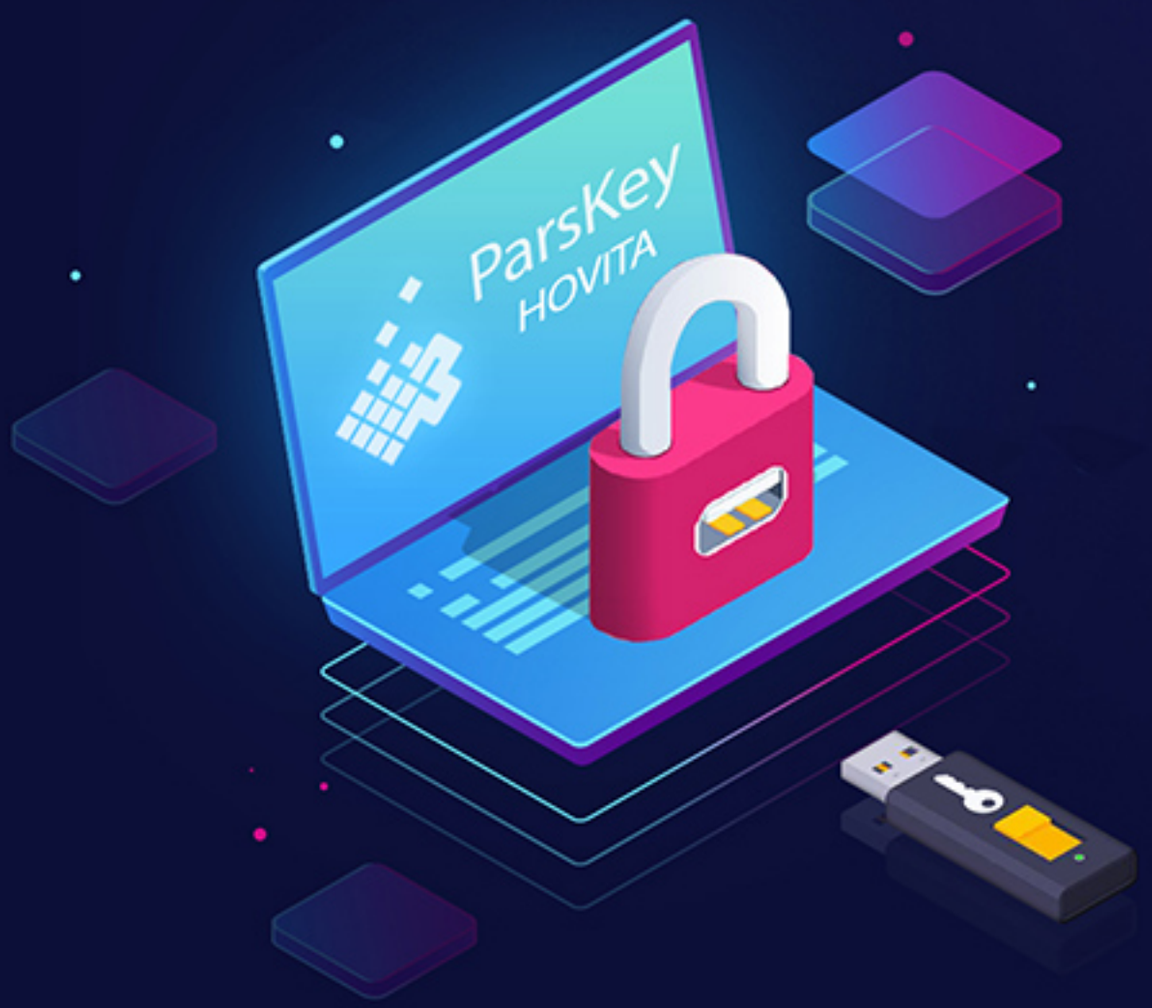
هـویتـا

توکن امضای دیجیتال پارس کی (ParsKey)

توکـن هوشـمند پارس‌کـی مـاژول رمـز کننـده‌ای بـا رابـط USB میباشـد. ایـن مـاژول تلفیقـی از امنیـت، کارآیـی، کاربـری آسـان، قابلیـت حمـل و صرفـه اقتصـادی را در اختیـار کاربـر قـرار میدهـد. پارس‌کـی بـه صـورت مسـتقل و بـدون نیـاز بـه سـخت‌افزارهـای اضافـی ماننـد کارت‌خـوان، قابل‌اسـتفاده بـوده و امـکان تولیـد کلیدهـای متقـارن و نامتقـارن، انجـام عملیـات رمزنـگاری و امضـای دیجیتالـی به‌صـورت On-Board در آن وجـود دارد. برخـورداری از رابـط اسـتاندارد (PKCS #11) به‌منظـور برقـراری ارتبـاط بـا توکـن و همچنیـن پشـتیبانی از زیرسـاخت کلیـد عمومـی، امـکان اسـتفاده از ایـن محصـول را در طیـف وسیعی از نرم‌افزارهای PK-Enabled فراهم کرده است.

تأییدیه‌ها و افتخارات

- کسب رتبهٔ نخست در آزمون عملکرد و انطباق از آزمایشگاه ارزیابی ماژول‌های رمزنگاری (۱۳۹۱، ۱۳۹۲ و ۱۳۹۳)
- دریافت اولین گواهی تأیید نمونه توکن امنیتی USB از سازمان تنظیم مقررات و ارتباطات رادیویی (۱۳۹۱)
- مطابقت کامل با سطح ۲ و برخی محورهای سطح ۳ از استاندارد FIPS 140-2
- مطابقت با Common Criteria EAL4+
- چهـار سـال متوالی برترین توکن امنیتـی کشـور



وظایف مورد انتظار از توکن هوشمند پارس‌کی

- نگهـداری امـن زوج کلیـد و گواهـی کلیـه کاربران سیسـتم‌های نرم‌افـزاری بـا قابلیـت عـدم اسـتخراج کلیـد خصوصـی جهـت جلوگیـری از نسـخه‌برداری (Duplication) و دسـترسـی غیـرمجـاز بـه کلیـد
- امضـای دیجیتـال مقـدار تصادفـی تولیدشـده توسـط سـرور در هنـگام احـراز هـویـت کـاربـران

هـویتـا

• امضـای دیجیـتالی فـرم‌ها و فـایل‌ها در سیـستم
• رمزگشـایی محتوای رمـز شده با کلید خصـوصی

کـاربرد هـا

بانکـداری الکترونیکـی- امضـای اظهارنامـه مالیاتـی - مبـادلات امـن در بـورس - ورود امـن بـه ویـنـدوز پسـت الکترونیـک امـن - اتوماسـیون اداری امـن - ثبت‌اسـناد حقوقـی (قراردادهـای خریدوفـروش و اجـاره مسـکن) - برقـراری ارتبـاطات امـن IPSec، SSH، SSL و VPN

قابلیـت هـای کلیـدی

پشـتیبانی از الگوریتم‌های مختلف رمزنگاری و امضا (DES, AES-3 ,RSA, DES) - پشـتیبانی از اسـتانداردهای PKCS MicrosoftCAPI و ISO 7816 - اجرای تمام عملیات به‌صورت on-board - پشـتیبانی از سیسـتم‌عامل هـای ویـنـدوز و لینوکـس ۳۲ و ۶۴ بیتـی - اسـتحکام بدنـه فوق‌العـاده، مقـاوم در برابـر ضربه، عـدم امکان باز شدن بـدون تشخیـص - بدون نیـاز به نصـب (driverless) - پشتیبـانی و خدمـات پس از فـروش گسـتـرده

مزایای توکن امضـای دیجیتـال ParsKey

بدون نیـاز به نصب نرم‌افزار در سمت کلاینت - قابل‌حمل (بدون نیاز به کارت‌خوان) - بدون نیاز به شـارژ و باتری - دارای نرم‌افـزار مخصوص برای مدیریت تمـام فرایندهای چرخه حیات - رابط کاربـری مناسـب برای مدیریت کلیـدهـا و گواهـی‌هـا - امکـان استفـاده مـوازی از چنـد توکـن - امـکان به اشتـراک‌گـذاری در شبـکه

برای دریافت اطلاعات بیشتر و مشخصات فنی محصول به سایت هویتا مراجعه نمایید

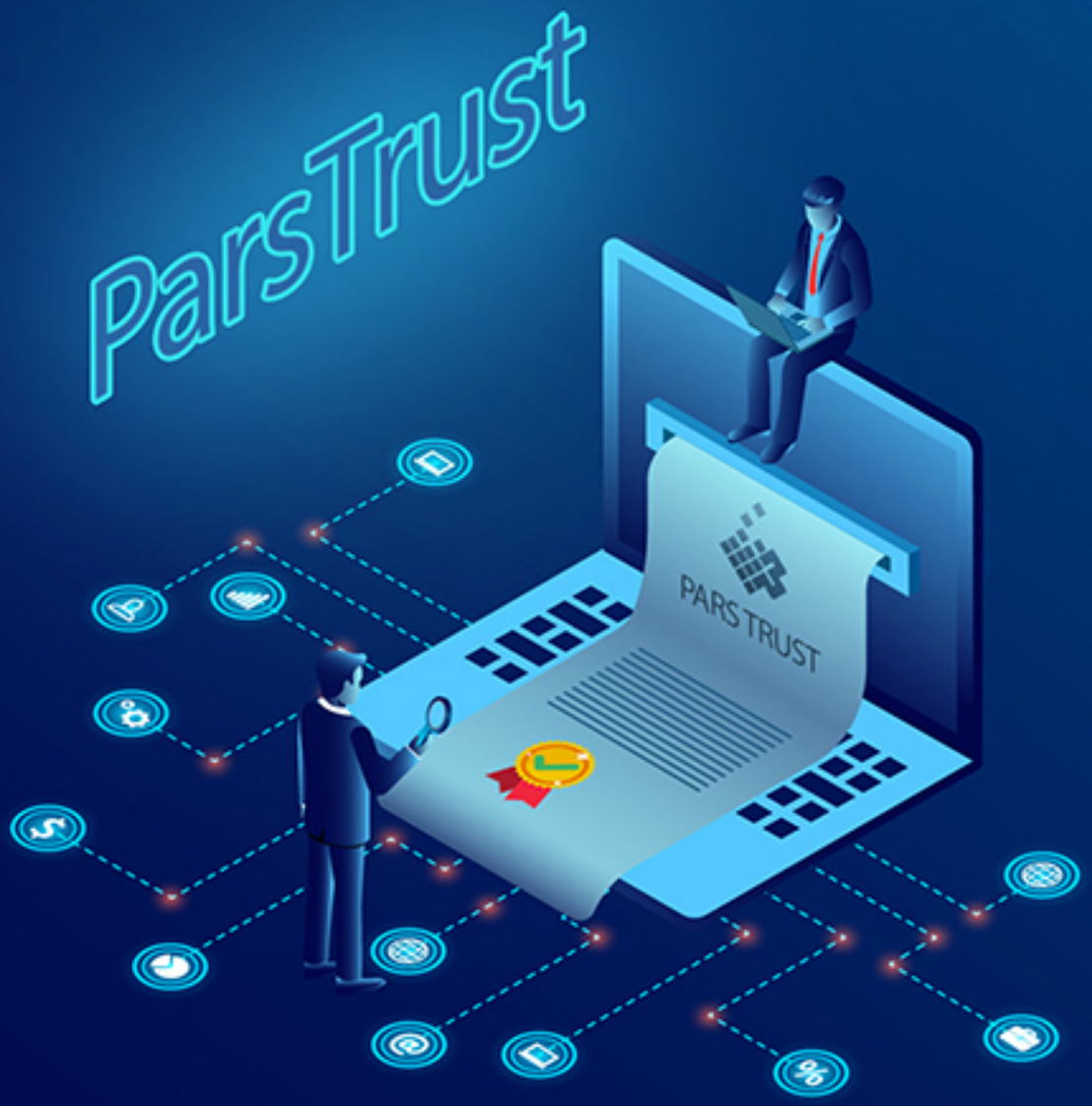
WWW.HOVITA.IR

هویتا

معرفی محصول ParsTrust

سامانه صدور و مدیریت گواهی الکترونیکی پارس‌تراست

سامانه پارس‌تراست مجموعه‌ای است متشکل از مؤلفه‌های نرم‌افزاری موردنیاز جهت صدور و مدیریت گواهی الکترونیکی کلید عمومی (Public Key Certificate X509)، می‌باشد. این سامانه، کلیه فرایندهای ثبت‌نام، صدور، ابطال، تعلیق، تمدید، تجدید و اعتبارسنجی گواهی الکترونیکی را منطبق بر استانداردهای کشور و با توجه به نیازمندی‌ها، سیاست‌ها و الزامات زیرساخت کلید عمومی در انواع دامنه‌ها و کاربردها، فراهم می‌نماید. مؤلفه‌های اصلی سامانه پارس‌تراست عبارت‌اند از: مرکز صدور گواهی (CA)، مرکز ثبت‌نام گواهی (RA)، مخزن گواهی و لیست ابطال (Repository)، پاسخگوی برخط وضعیت گواهی‌ها (OCSP Responder)، مرکز مهر زمانی (TSA) مرکز اعتبارسنجی گواهی (VA) و مرکز مدیریت و احراز هویت (IdP)



تاییدیه ها و افتخارات

- اولین نرم‌افزار صدور و مدیریت گواهی‌های الکترونیکی بومی تولید شده در سال ۱۳۸۱
- کسب رتبه پلاتین از آزمایشگاه مرکز ریشه وزارت صنعت، معدن و تجارت
- ثبت رسمی نرم‌افزار در شورای عالی انفورماتیک در سال ۱۳۸۵
- مورد استفاده در مراکز صدور گواهی الکترونیکی کشور از قبیل بانک مرکزی ج.ا.ا سازمان بورس و اوراق بهادار، شرکت همراه اول
- مرکز میانی صدور گواهی پارس‌ساین و بیش از ۱۰ زیرساخت کلید عمومی درون سازمانی

هـویتـا

قابلیـت‌ها و اسـتانداردها

- منطبـق با اسـتانداردهـای IETF PKIX
- قابلیـت تعریف و پیـکربندی انواع پروفـایل‌های گـواهـی مطابـق X.509 و RFC5280
- پشتیـبانی از تعییـن سیاسـت هـای مدیریـت گـواهـی از طـریق پروفـایل‌هـای پویـا
- قابلیـت تعییـن قالـب بـرای محتـوای هـر یـک از فیـلد هـای Subject گـواهـی
- امـکان تعـریـف افـزونه هـای (Extensions) مختـلف بـرای درج در گـواهـی
- قـابلیـت صـدور و مدیـریـت چنـدیـن گـواهـی متفـاوت بـا یک پروفـایل
- امکان مدیریت پروفـایل کلیـد شامل طول کلید، الگوریتم تولید کلید، طول عمر کلید، رسـانه ذخیره‌سازی کلید
- قابلیـت تعییـن بـازه مـجـاز در خواسـت تمـدید گـواهـی (Renew margin)
- قابلیـت صـدور، ابـطال، تعلیـق و رفـع‌تعلیـق انـواع گـواهـی
- قابلیـت تمـدید و تجـدید کلید انواع گواهـی‌های صـادر شده
- قابلیـت مدیریـت خـودکار و نیمـه خـودکـار گـواهـی
- پشتیبـانی از تعییـن زمان عملیات بر روی گواهـی برای آینده
- پشتیبـانی از کارکرد هـای مدیریـت کلیـد شـامل تولیـد، نگهـداری، ابطال و تعلیـق
- قابلیت مدیریت درخواست (ثبت، بازنگری و ویرایش، لغو و حذف انواع درخواست‌های گواهی)
- قابلیـت بـایگانـی، جستـجـو و بـازیابـی درخـواسـت ها و گـواهـی‌هـا
- قابلیـت مشـاهـده فرآینـد کـاری درخـواسـت هـا
- قابلیـت نمـایش و کنتـرل چرخـه حیـات گـواهـی
- قابلیـت تعـریف و مدیریت نقـش های مختـلف برای هر مولفه براسـاس سـرویس‌های ارائه شده توسـط مولفه‌ها
- قابلیـت تعـریف و مدیریـت سـازمان ها به صـورت چنـدسـطحـی تا ۵ سـطـح
- قابلیت تعریف، و مدیریت کاربران برای هر مولفه با قابلیت انتصاب نقش و سازمان
- احراز هویت کاربران (اپراتورهای مراکز ثبت‌نام و صدور گواهی و راهبران) با استفاده از توکن امضای دیجیتال PKI
- کنتـرل دسـتـرسی کاربران چندسطحـی به صـورت Role-based و Record-level

هویتا

- پشتیبانی از شبیه ساز نرم‌افزاری HSM پارس‌کی به‌صورت Built-in
- امکان کار با انواع تجهیزات HSM با واسطهای Java JCA/JCE CSP و PKCS #11
- سازگاری با توکن پارس‌کی (ParsKey) و سایر توکن‌های مورد تائید در زیرساخت کلید عمومی کشور
ا قابلیت تعیین بازه اعتبار، به‌روزرسانی و انتشار دوره‌ای CRL سازگار با RFC5280
- پشتیبانی از مکانیزم‌های انتشار گواهی‌ها و CRL در مخزن، سازگار با پروتکل LDAP RFC2253
- امکان آدرس‌دهی و تمایز گواهی براساس نام متمایزکننده (DN) سازگار با RFC2396
- قابلیت به‌روزرسانی همزمان چندین RA، OCSP و مخزن گواهی
- پشتیبانی از الگوریتم‌های RSA و ECDSA در تمامی مؤلفه ها
- پشتیبانی از کارکرد تولید مهر زمانی (TSP) سازگار با استاندارد RFC3161
- پشتیبانی از سرویس مرکزی اعتبارسنجی گواهی و امضای دیجیتال از طریق مؤلفه VA
- پشتیبانی از مکانیزم‌های برخط استعلام وضعیت گواهی در مؤلفه OCSP سازگار با RFC5019
- امضای دیجیتال رویدادهای ممیزی به‌صورت Chain signing در تمامی مؤلفه‌ها
- قابلیت رویدادنگاری عادی با امکان ذخیره در انواع فایل، پایگاه داده یا ارسال رویدادها تحت شبکه
- پشتیبانی از گواهی‌های کلید عمومی X509 v3 and v1 و لیست گواهی‌های باطله CRL v2
- پشتیبانی از PKCS #1 ، #5 ، #7 ، #8 ، #9 ، #10 ، #11 ، #12

ویژگی های غیر عملکردی و عملیاتی

- قابلیت مدیریت و راهبری مجزای مرکز صدور گواهی (CA) و دفاتر ثبت‌نام (RA)
- قابلیت پشتیبانی از چند CA در مؤلفه RA
- قابلیت پشتیبانی از چند CA در مؤلفه OCSP
- دارای درگاه وب کاربرپسند برای هر مؤلفه
- قابلیت افزایش مؤلفه‌های OCSP به‌صورت مجزا
- امکان استفاده از سرویس‌های اصلی ثبت‌نام و صدور گواهی از طریق وب‌سرویس

هویتا

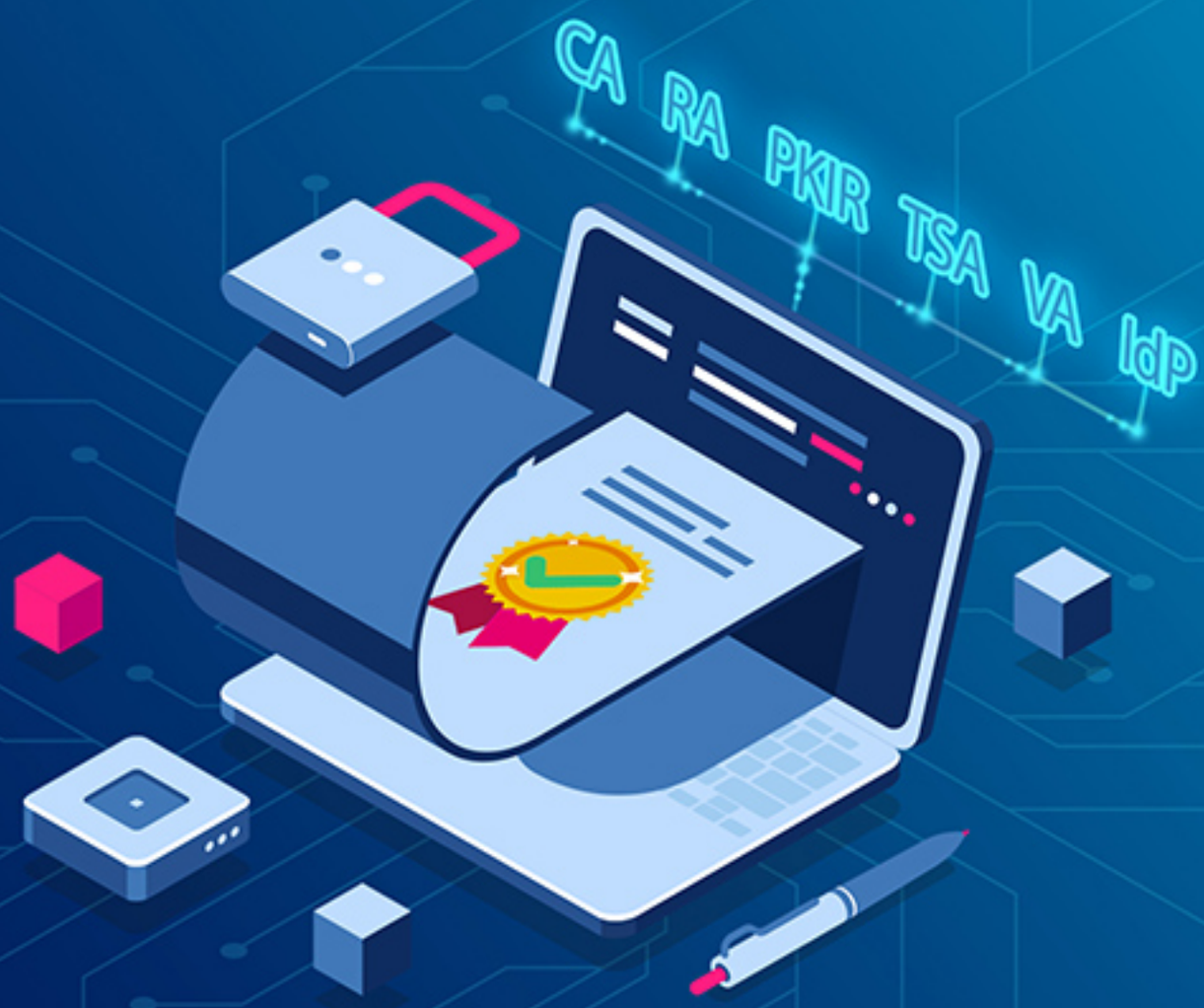
- قابلیت تعریف و افزایش دفاتر ثبت نام
- عدم محدودیت در تعداد سطوح سلسله مراتب اعتماد
- قابل‌ارائه به‌صورت بسته‌های نصب نرم‌افزار، ماشین مجازی و Container و Network Appliance
- طراحی مستقل از پایگاه داده و قابلیت کار با انواع پایگاه داده از قبیل PostgreSQL، MySQL، Oracle و Microsoft SQL Server
- قابلیت HA با مدیریت Load balancing و Fail-over
- قابلیت پشتیبان‌گیری، بازیابی، مانیتورینگ و نظارت مرکزی
- پشتیبانی از ارتباط SSL/TLS دوطرفه بین مؤلفه‌ها، بین مؤلفه‌ها و پایگاه داده و با مخزن
- قابل پیکربندی و انطباق با انواع سیاست‌های گواهی الکترونیکی
- امکان یکپارچه‌سازی با امضای همراه (Mobile Signature Service) از طریق ETSI TS 204 102

ParsTrust

سامانه صدور و مدیریت گواهی الکترونیکی پارس‌تراست

برای دریافت اطلاعات بیشتر و مشخصات فنی محصول به سایت هویتا مراجعه نمایید

WWW.HOVITA.IR

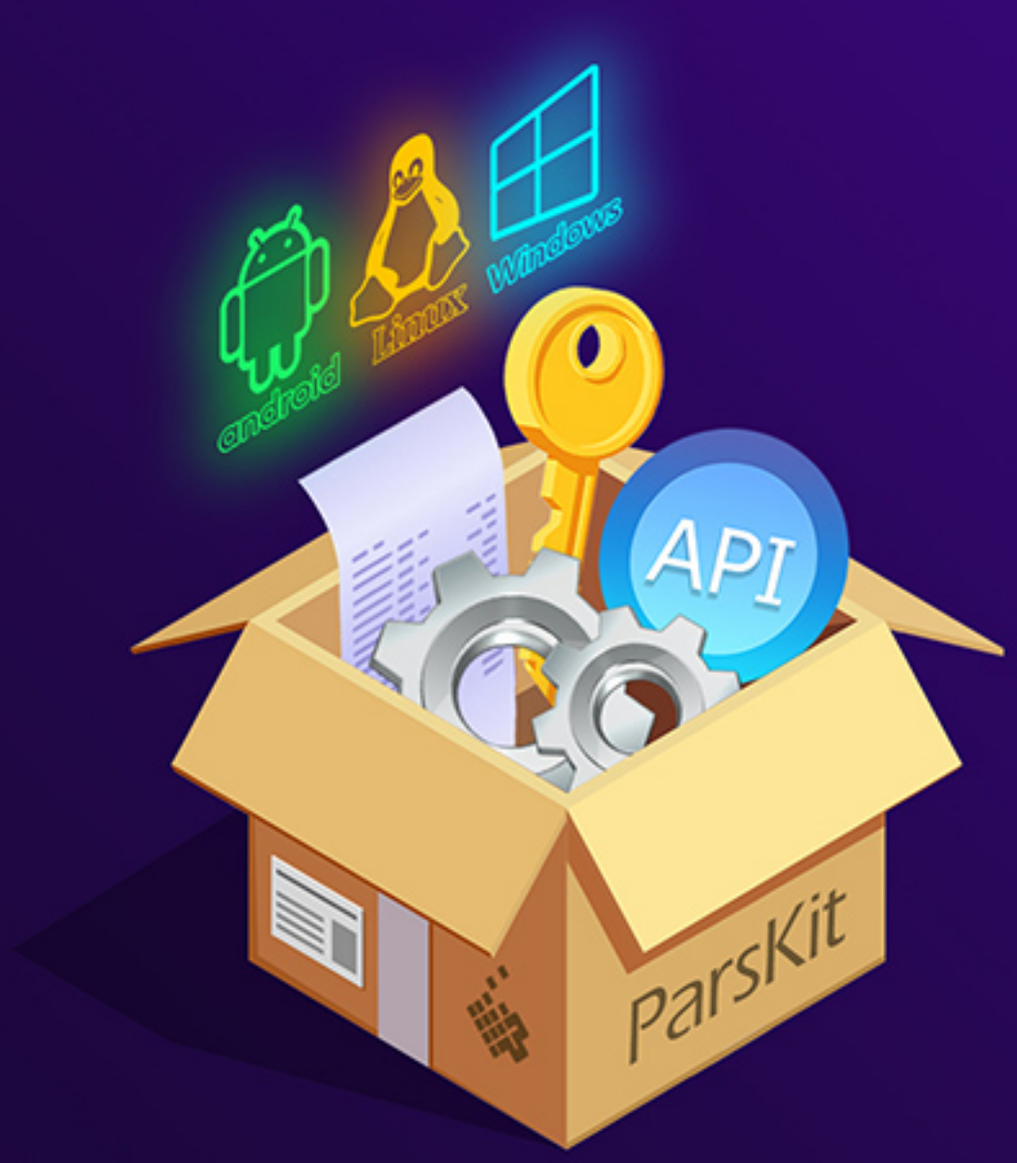


هویتا

بسته توسعه نرم افزاری پارس‌کیت (ParsKit PKE SDK)

زیرساخت کلید عمومی، با هدف تأمین امنیت و اعتماد در فضای تولید و تبادل اطلاعات الکترونیکی، مورد استفاده قرار می‌گیرد. یکی از عناصر اصلی این زیرساخت، نهاد یا طرف اعتماد کننده (Relying Party) نام دارد. این نهاد با توجه به الزامات و سیاست‌های مرکز صدور گواهی، امضای دیجیتال و گواهی الکترونیکی طرف امضاکننده را اعتبارسنجی کرده و پس از تائید هویت و اعتبار امضا ، خدمات مربوطه را به ایشان ارائه می‌کند.

به فرایند تجهیز و فعال‌سازی قابلیت‌های PKI در سامانه‌های نرم‌افزاری طرف اعتماد کننده، اصطلاحاً PKE یا Public Key Enabling گفته می‌شود و مجموعه ابزارها و بسته‌های نرم‌افزاری که در این خصوص مورد استفاده قرار می‌گیرند، PKE SDK نام دارند. این ابزارها با برخورداری از توابع و ماژول‌های برنامه نویسی آماده و مورد تائید آزمایشگاه های PKI در کشور، فرایند توسعه محصول را برای برنامه نویسان و تولیدکنندگان نرم‌افزار، تسهیل کرده و باعث بهبود کیفیت و کاهش هزینه و زمان آماده‌سازی سامانه، می‌شوند.



تاییدیه‌ها و افتخارات

- کسب رتبه پلاتین از آزمایشگاه PKE مرکز ریشه وزارت صنعت، معدن و تجارت

قابلیت‌ها و استانداردها

- قابل استفاده در انواع سامانه های نرم‌افزاری تحت وب، Desktop و سرویس‌های راه دور
- قابل استفاده در مرورگرهای وب متداول ویندوز لینوکس و اندروید
- امکان استفاده در سرورهای نرم‌افزار مبتنی بر Java، Microsoft .NET Framework، PHP و سایر محیط ها به‌واسطه Wrapper بر روی Native C/C++ Library

هویتا

- قابل استفاده در کارگزارهای وب متداول از قبیل Oracle WebLogic، IIS و Apache
- قابل استفاده در سیستم عامل‌های ویندوز، لینوکس و اندروید
- تصدیق و اعتبارسنجی گواهی الکترونیکی کاربر مطابق با RFC5280 ، NIST Recommendation for Path Validation X509 و مطابق با سند «الزامات تشکیل و اعتبارسنجی زنجیره گواهی مرکز دولتی صدور گواهی الکترونیکی ریشه»
- پشتیبانی از پروتکل LDAP و HTTP برای اتصال به مخزن و دریافت زنجیره گواهی‌ها و لیست‌های ابطال
- قابلیت تعیین بازه زمانی دریافت و به‌روزرسانی CRL سازگار با RFC5280
- پشتیبانی از دریافت مهر زمانی (TSP) سازگار با استاندارد RFC3161
- پشتیبانی از مکانیزم‌های برخط استعلام وضعیت گواهی OCSP سازگار با RFC5019
- امکان دریافت اطلاعات گواهی براساس نام متمایزکننده (DN) سازگار با RFC2396
- پشتیبانی از انواع تجهیزات رمزنگاری از قبیل توکن، کارت هوشمند و HSM باواسطهای MS CAPI Java JCA/JCE CSP و PKCS11# در سمت سرور و کاربر
- پشتیبانی از توکن نرم‌افزاری پارس‌کی با رابط PKCS11# به‌صورت Built-in
- امکان استفاده از چندین تجهیز رمزنگاری متفاوت به‌صورت هم‌زمان
- امکان استخراج و بررسی الحاقیه‌های گواهی (Certificate Extensions) مطابق با RFC5280
- امکان تولید اعداد تصادفی مطابق با Appendix A2.4 ANSI X9.31 و Annex D 2005-ANSI X9.62 برای تولید رشته تصادفی Challenge در مبحث احراز هویت مطابق با FIPS196
- امکان تولید و بررسی درخواست صدور گواهی در قالب CSR منطبق با استاندارد#PKCS10
- امکان تولید و اعتبارسنجی امضای دیجیتال در قالب # PKCS7 و CMS
- پشتیبانی از الگوریتم‌های RSA و ECDSA در امضا و اعتبارسنجی
- پشتیبانی از الگوریتم های SHA1، SHA256، SHA384 و SHA512
- پشتیبانی از مکانیزم‌های امضای دیجیتال RSASSA-PSS و RSASSA-PKCS1v1.5
- قابلیت رویدادنگاری مطابق سند «الزامات تشکیل و اعتبارسنجی زنجیره گواهی مرکز دولتی صدور گواهی الکترونیکی ریشه»
- امکان ارائه اپلت های FIDO، PKI و PIV برای کارت هوشمند و سیم‌کارت

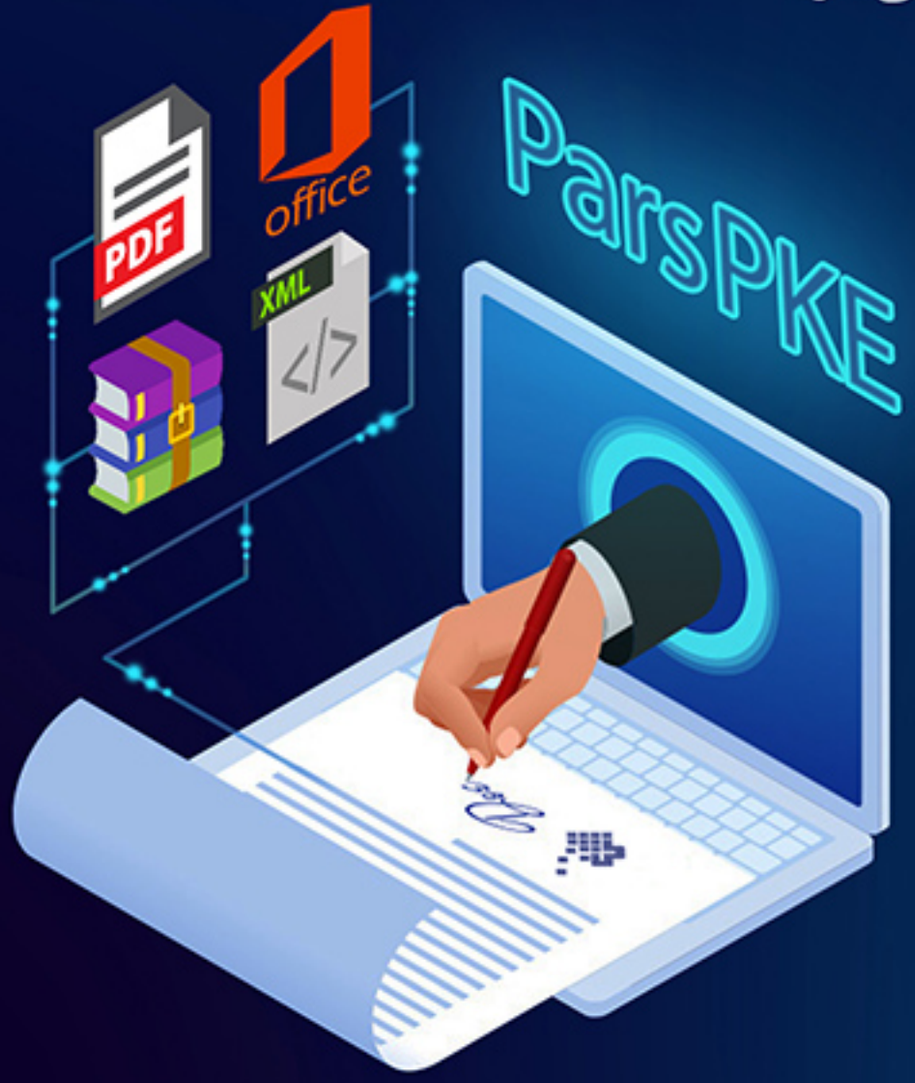
هویتا

معرفی محصول ParsPKE

درگاه نرم افزاری امضای دیجیتال مبتنی بر سرویس

محصول ParsPKE امکان تجهیز سامانه‌های نرم‌افزاری به خدمات احراز هویت و امضای تراکنش ها و اسناد را مبتنی بر وب‌سرویس ، فراهم می‌کند. سامانه‌های نرم‌افزاری با فراخوانی سرویس های این سامانه می‌توانند کاربران خود را مبتنی بر PKI، احراز هویت کرده و همچنین اسناد و تراکنش‌ها را به‌صورت دیجیتالی امضا نمایند. فرمت اسنادی که این سامانه قادر به امضای آن‌ها می‌باشد شامل انواع فایل‌های مجموعه Office (نظیر Word، Excel، و غیره)، فایل‌های ZIP ، XML، PDF و غیره است.

درواقع، این سامانه، با ارائه سرویس باعث تسریع فرآیند تجهیز سامانه‌ها به قابلیت‌های زیرساخت کلید عمومی مطابق استانداردهای داخلی و بین‌المللی می‌گردد و منجر به کاهش چشم‌گیر زمان و هزینه در به‌کارگیری زیرساخت کلید عمومی می‌شود.



ویژگی ها و قابلیت های محصول

- **معماری مبتنی بر سرویس :** این سامانه با بهره گیری از معماری سرویس محور می‌تواند مستقل از پلتفرم سامانه نرم‌افزاری، مورداستفاده در انواع زبان های برنامه‌نویسی قرار گیرد.
- **برخورداری از پشتوانه حقوقی و قانونی :** امضای الکترونیکی در این سامانه منطبق با استانداردها و قوانین کشور انجام می‌گیرد و مؤلفه های مرتبط با زیرساخت کلید عمومی، دارای تأییدیه از آزمایشگاه مرکز توسعه تجارت الکترونیکی هستند. لذا امکان ارائه

هویتا

خدمات به ذینفعان مراکز میانی صدور گواهی دولتی و خصوصی کشور توسط این سامانه وجود دارد.

• **قابلیت امضای اسناد :** این سامانه قادر است انواع فایل‌های مجموعه Office و قالب‌های اسناد XML، PDF و داده‌های باینری را براساس فرمت‌های امضای استاندارد ASiC-S، CAdES، XAdES، PAdES و ASiC-E امضا کند و در صورت نیاز، اسناد امضا شده را نیز مجهز به مهر زمانی و یا قابلیت اعتبار مدت‌دار (Long Term) نماید.

قابلیت امضای چندگانه : این سامانه مطابق با استانداردهای انواع قالب اسناد، امضا چندگانه را پشتیبانی می کند.

• **قابلیت امضاء با توکن :** امکان استفاده از PKI USB Token ها (مورد تائید مرکز ریشه وزارت صنعت معدن و تجارت) در فرایند احراز هویت کاربران و امضای اسناد و تراکنش‌ها (توسط کاربران در مرورگرهای مطرح سیستم عامل های ویندوز و لینوکس)

• **قابلیت امضاء با موبایل :** پشتیبانی از امضای الکترونیکی کاربران توسط سرویس امضای همراه مبتنی بر سیم‌کارت و بدون سیم‌کارت.

• **قابلیت امضا در سمت سرور :** این سامانه از پودمان‌های رمزنگاری مبتنی بر استاندارد#PKCS 11 (مورد تائید مرکز توسعه تجارت الکترونیکی) #PKCS12 ، JKS و MSCAPI پشتیبانی می‌نماید و بدین واسطه قادر به انجام انواع امضاهای سازمانی و توسط سرور می‌باشد.

• **قابلیت اعتبارسنجی امضا و گواهی :** این سامانه قادر است تا امضا و گواهی الکترونیکی را مطابق با استاندارد "الزامات تشکیل و اعتبارسنجی مسیر گواهی دیجیتالی" منتشرشده در تاریخ ۱۳۹۴/۰۳/۱۸ توسط مرکز ریشه وزارت صنعت، معدن و تجارت، اعتبارسنجی نماید. لازم به ذکر است که این سامانه به‌صورت پیش‌فرض براساس استانداردهای اعتبارسنجی ETSI عملیات مذکور را انجام می‌دهد.

• استفاده از استانداردهای بین‌المللی و قوانین بومی: محصول مبتنی بر استانداردهای بین‌المللی معتبر توسعه داده‌شده است و "استانداردهای منتشرشده توسط مرکز ریشه وزارت صنعت، معدن و تجارت" در آن رعایت شده است.

برای دریافت اطلاعات بیشتر و مشخصات فنی محصول به سایت هویتا مراجعه نمایید

WWW.HOVITA.IR

هویتا

امضای همراه ParsMSS

امضای همراه دیجیتال مبتنی بر سیم کارت و گوشی تلفن همراه

سرویس امضای همراه (Mobile Signature Service) راهکاری نوین در حوزه احراز هویت و امضای دیجیتال با استفاده از تلفن همراه کاربران (به‌عنوان رسانه تولید و نگهداری کلیدهای نامتقارن) می‌باشد. امضای همراه با ارائه سرویس‌های امضای دیجیتال و احراز هویت مبتنی بر زیرساخت کلید عمومی به فراهم‌کنندگان خدمات الکترونیکی از قبیل بانک‌ها، فروشگاه‌های آنلاین، دولت الکترونیک و سایر مؤسسات و نهادها، امنیت و اعتبار قانونی تراکنش‌های غیرحضوری را در بالاترین سطح به‌صورت دوعامله و دوکاناله تأمین می‌نماید. این راهکار مبتنی برای استانداردهای داخلی و بین‌المللی توسعه یافته و می‌تواند مبتنی بر سیم‌کارت (SIM-based) و بدون سیم کارت (SIM-less) ارائه شود.

مشخصات فنی

ارائه خدمات احراز هویت دوعامله مبتنی بر زیرساخت کلید عمومی - ارائه سرویس امضای دیجیتالی تراکنش‌ها و اسناد مطابق قوانین تجارت الکترونیکی کشور - پشتیبانی از سرویس اعتبارسنجی امضای دیجیتال و گواهی الکترونیکی - ارائه خدمات امضای همراه مبتنی بر سیم کارت و بدون سیم‌کارت- امکان ارسال پیام عادی و محرمانه به کاربر - پشتیبانی از سرویس ارائه رسید تراکنش‌ها - پشتیبانی از پروفایل‌های امضای دیجیتال

ارائه خدمات بر روی API های SOAP و REST - پشتیبانی از الگوریتم‌ها و مکانیزم‌های رمزنگاری معتبر در زیرساخت کلید عمومی کشور:

SHA-2(384) RSA PKCS #1 - SHA-2(256) RSA PKCS #1 - SHA-1 RSA PKCS #1 - RSA PKCS #1

SHA 2(512) RSA PKCS #1

- قالب‌های امضا: PKCS #1 - CAdES - CMS(PKCS #7)
- پشتیبانی از مدهای متنوع ارائه خدمت : Synchronous - Server–Server - Client–Server

هـویتـا

مزایا

- عـدم نیـاز بـه حمـل ابـزارهـای اضـافه و سهـولت استـفاده
- بالاترین سـطح امنیـت و محـافظت از کلیـدهـای خصوصی (LoA4 مطابق GSMA)
- تبـادل نشـدن پیـن کد روی شبـکه و عـدم امـکان شنـود آن
- احـراز هـویت دوکاناله (شبـکه GSM و شبـکه اینترنت / اینترانت)
- برخـورداری از پشتـوانه حقـوقـی و قـانونی
- کاهـش هزینه‌ها، پیچیدگی و زمـان پیاده‌سازی و نگهداری کاربردهـای زیرسـاخت کلیـد عمـومی

تأییدیه ها و گواهـی نامه‌هـا

گواهـــی تائیـــد اپلـــت امضـــای همـــراه از آزمایشـــگاه امنیـــت سیســـتم‌عامل مراجـــع ذیـصـلاح

- مـــورد تائیـــد کمیتـــه ســـیم‌کارت شـــرکت ارتبـاطـات سیـار ایـران (همـراه اول)
- اسـتفاده از مـاژولParsKit PKE دارای تأییدیـه سـطح پلاتیـن از آزمایشـگاه مرکـز توسـعه تجـارت الکتـرونیکـی ایـران

سرویـس امضـای همـراه
Mobile Signature Service

هـویتـا

سـامـانه احـراز هـویت یکپارچه ParsSSO

سامانه ParsSSO، سرویس احـراز هویت را ارائه می‌دهد. احراز هویت در این سامانه به‌صورت Single Sign-On است یعنی تنها با یک‌بار احـراز هویت کاربر می‌تواند از تمـامی نرم‌افـزارهای سازمان بدون نیـاز به احـراز هویـت مجـدد استفـاده نماید. علاوه بر این مدیریت کاربـران یکپـارچه مشـکلات مربـوط به سرپرستـی سامانـه‌هـا را به صـورت چشمگیری کاهـش می‌دهد. با تعـریف یک کاربر، دسـتـرسی کاربر در تمـامی سامانـه‌ها به صـورت خودکار ایجـاد میگردد و با حذف دسـتـرسی کاربر، تمامی سامانـه‌ها از ورود کاربر جلوگیری خواهند کرد. مهم‌ترین بخش سامانـه SSO مؤلفه Identity Provider است که به‌اختصار IdP نامیده می‌شود، مؤلفه ارائه‌دهنده‌ی خدمات سفارشی‌سـازی شده‌ی AA شامل، احراز هویت و کنترل دسترسی است. تمامی فراهم‌کنندگان خدمت می‌توانند با ثبت‌نام در این مؤلفـه، خدمـات AA را بـه آن برون‌سپـاری کننـد. از ویـژگی هـای اصلـی این مؤلفـه ارائـه‌ی خدمـات به صـورت Single Sign-On با ضـریب امنیتـی بالا است. همچنیـن این مؤلفـه از جانـب فراهـم‌کنندگان خدمـت مسئولیت Policy Enforcement را بـر عهـده دارد.

قابلیت های مولفه Identity Provider

• **احراز هویت** : در مؤلفـه IdP احراز هویـت به سه روش انجـام می شود: «احـراز هویت با نام کاربری و رمز عبور» «احـراز هویت به صـورت OTP از طریق ارسـال پیـامک» «احـراز هـویت با توکـن (بـرای انجـام این نـوع از احـراز هـویـت از گـواهـی استفـاده شـده و بـه صـورت Challenge-Response انجـام می شود.)»

• **کنترل دسترسی** : در ایـن مؤلفـه بـه دو صـورت Role-Based و Record-Level انجام می‌شود.

کنتـرل دسترسی Role-Based براسـاس سطح دسترسی تعییـن شـده به سـرویس‌های ارائه شده از جـانب فراهـم کننـده‌ی خدمـت در نقـش منتسب به کاربـر و کنتـرل

هویتا

دسترسی Record-Level براساس سازمان منتسب به کاربر انجام می‌شود.

• **مدیریت کاربران** : هر کاربر دارای چهار ویژگی اصلی است:

o Credentials : برای احراز هویت کاربر در سامانه استفاده شده و شامل «گواهی با کاربرد کلید Authentication» و «نام کاربری و رمز عبور» می‌باشد.

o اطلاعات هویتی : شامل نام و نام خانوادگی ، شماره تماس

o نقش : سطح دسترسی کاربر به سرویس‌های فراهم‌کننده‌ی خدمت مربوطه را مشخص می کند.

o سازمان : سطح دسترسی کاربر به سازمان‌های فراهم‌کننده‌ی خدمت مربوطه تعیین می کند.

سرویس‌هایی که در این بخش ارائه می‌شوند، شامل:

ایجاد کاربر- ویرایش کاربر- اختصاص نقش به کاربر- اختصاص سازمان به کاربر- حذف کاربر و مشاهده‌ی لیست کاربران

• **مدیریت نقش** : هر فراهم‌کننده‌ی خدمت امکانات خود را در قالب سرویس به کاربران ارائه می‌دهد. نقش به‌منظور تعیین دسترسی به سرویس‌های فراهم‌کننده‌ی خدمت تعریف می‌شود. هر سرویس می‌تواند یک یا چند Entity داشته باشد که هنگام تعیین دسترسی به سرویس، امکان تعیین سطح دسترسی از طریق Entity ها نیز موجود است.

سرویس‌های ارائه شده در این بخش شامل: ایجاد نقش، ویرایش نقش، حذف نقش و مشاهده‌ی لیست نقش‌ها می‌باشد.

• مدیریت سازمان‌ها : سازمان‌ها به‌صورت یک درختواره تعریف می‌شوند. هر سازمان می‌تواند تا ۵ سطح زیر سازمان داشته باشد. سازمان‌ها به‌منظور اعمال سطح دسترسی Record-Level استفاده می‌شوند. در هر سطح سازمان دسترسی به اطلاعات زیر سازمان‌ها وجود دارد، درحالی‌که دسترسی به اطلاعات سازمان‌های هم‌سطح امکان‌پذیر نیست.

سرویس‌های ارائه شده در این بخش شامل: ایجاد سازمان، ویرایش سازمان، حذف سازمان و مشاهده‌ی درخت سازمان‌ها می‌باشد.

• **مدیریت فراهم کنندگان خدمت** : اطلاعاتی که به هنگام ثبت، از فراهم‌کننده‌ی خدمت دریافت می‌شود به‌منظور ایجاد امکان برقراری ارتباط با IdP است. این اطلاعات شامل « نام»، «URL Callback»، «لیست سرویس‌ها» و «سیاست‌ها» میباشد. سرویس‌های ارائه شده در این بخش شامل: ثبت فراهم‌کننده‌ی خدمت، ویرایش فراهم‌کننده‌ی خدمت، حذف فراهم‌کننده‌ی خدمت و مشاهده‌ی لیست فراهم‌کنندگان خدمت می‌باشد.

• **مدیریت نشست** : در این مولفه امکان ایجاد و مدیریت نشست برای کاربری که احراز هویت شده است، وجود دارد. هر نشست دارای یک زمان انقضا است که در صورت سررسید احراز هویت کاربر باطل شده و کاربر برای ادامه‌ی فعالیت نیاز به احراز هویت مجدد دارد.

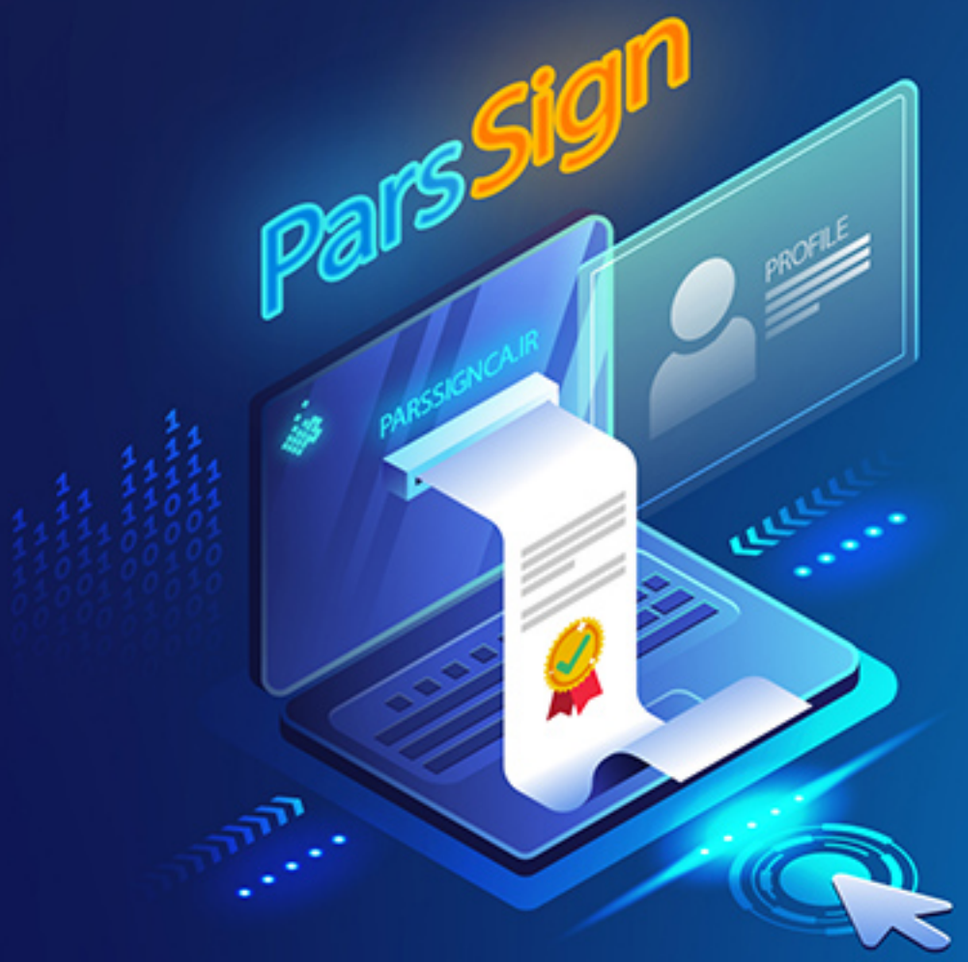
هـویتـا

معـرفی محصـول ParsSign

مرکـز صـدور گواهـی الکترونیکـی ParsSign ، نهـادی اسـت کـه بـرای اشـخاص حقیقـی و حقوقـی گواهـی الکترونیکـی صـادر می‌کنـد و بـه هویـت آن‌هـا در فضـای دیجیتـال اعتبـار قانونـی و حقوقـی می‌بخشـد. ایـن مرکـز از سـال ۱۳۸۱ باهـدف آمـوزش، فرهنگ‌سـازی عمومـی در زمینـهٔ صـدور گواهـی الکترونیکـی و امضـای دیجیتـال فعالیـت کـرده اسـت و تابه‌حـال چندیـن هـزار گواهـی الکترونیکـی بـرای کاربردهایی مانند امضا، پست الکترونیکی و SSL صادر نموده است.

افتخـارات و دستـاوردها

- توسعه‌دهنده اولین نرم‌افزارهای بومی مدیریت گواهی الکترونیکی (CA) ، مدیریت مرکز ثبت‌نام (RA) و OCSP تـأییـد شـده در زیـر سـاخـت کلیـد عمـومـی کشـور
- نخستین و تنها مرکز صدور گواهی الکترونیکی خصوصی کشور
- دارای مجـوز فعـالیـت از وزارت صنـعت، معـدن و تجـارت
- زیر نظـر مرکـز دولتـی صـدور گواهـی الکتـرونیکی ریشـه
- برخـورداری از دفـاتـر ثبـت‌نـام گواهـی در سراسـر کشـور



کـاربـردها

- صـدور گـواهی امضـای دیجیتال با کاربـرد امضـای دیجیتال داده هـا و احـراز هـویـت کـاربـران
- صـدور گـواهـی SSL/TLS بـا کـاربـرد تصـدیق اصـالت یـک سـرویس‌دهنـده، تصـدیق اصـالت یک سـرویس گیـرنده ایجاد ارتبـاط امـن و رمـزگـذاری شـده بیـن سـرویـس دهنـده و سـرویـس گیـرنـده

هویتا

• صدور گواهی پست الکترونیکی با کاربرد رمزگذاری محتوای ایمیل و تصدیق اصالت فرستنده ایمیل
• صدور گواهی احراز هویت با کاربرد ورود امن، امنیت ارتباطات SSH، امنیت ارتباطات VPN و امنیت ارتباطات بی‌سیم
• صدور گواهی مهر سازمانی با کاربرد امضای دیجیتال اسناد سازمانی
• صدور گواهی امضای کد با کاربرد اطمینان از اصالت و جامعیت نرم‌افزارها

طراحی و استقرار مراکز صدور گواهی

• طراحی، راه اندازی و پشتیبانی مراکز صدور گواهی
- اخذ مجوز از مرکز ریشه
- طراحی و راه اندازی مرکز داده
- طراحی و تأمین سخت‌افزار و نرم‌افزار مرکز صدور
- تهیه و تدوین اسناد سیاست های گواهی و دستورالعمل اجرایی گواهی
- تهیه ، تدوین و پیاده‌سازی سیاست های امنیتی
- ارائه آموزش‌های مرتبط با زیرساخت کلید عمومی
- مشاوره و نظارت بر طراحی و پیاده سازی
- نگهداری و پشتیبانی
• میزبانی و اجاره مراکز صدور گواهی

برای دریافت اطلاعات بیشتر و مشخصات فنی محصول به سایت هویتا مراجعه نمایید

WWW.PARSSIGNCA.IR

هـویتـا

راه‌حل شبکه خصـوصی مجـازی ParsVPN

محصول ParsVPN به‌منظور برقراری ارتباط کاربر با شبکه‌ای خصـوصی در بستر یک شبکه عمـومی و همچنین رفع مشکلات احـراز هویـت کاربـر، حفـظ محـرمانگی و جامعیـت اطلاعـات در حـال انتقـال، توسـعه یافته اسـت. سـامانه ParsVPN امکان ایجـاد ارتباط امن بین چندین کاربر و تعدادی سرویس‌دهنـده یا تنـها بین چندین کاربر را فراهـم می‌آورد که از اهداف اصلـی آن ایجاد حداکثر امنیـت با انجام سـاده‌ترین تنظیمات، قابلیـت بالای مدیریت هویت کاربران و کنترل دسترسی آن‌هاست. این محصول، راه‌حل شبکه‌ای خصوصی مجازی (Virtual Private Network) به منظور برقراری ارتباط کاربر با شبکه‌ای خصوصـی در بستر یک شبکهٔ عمـومی و همچنین رفع مشکلات هویت شناسی کاربر، حفظ محرمانگی و جامعیت اطلاعات در حال انتقال است.

کـاربرد هـا

دورکاری امن - اختصاص پهنای باند و محدودیـت در ارسـال و دریافـت داده جـدا سـازی اینتـرنـت و اینتـرانـت احـراز هویت دو عامله مستقل از محیط امن‌سـازی شبـکه (حفـظ محرمـانگی و جامعیـت، احـراز هویـت و جلوگیـری از حمـلات) - امن‌سـازی سـرویس‌هـای تحـت وب و پورتال‌ها - مدیریت هویت و کنترل دسترسی کاربران با استفاده از گـواهـی الکتـرونیکـی و تـوکـن قابلیـت استفـاده از شتـاب دهنـده های رمـز نگـاری از جمـله HSM سـربـار ترافیـکی بسیـار پاییـن

هویتا

قابلیت ها

قابلیت‌های سرور ParsVPN

- پشتیبانی کامل از PKI
- بارگذاری الگوریتم‌های رمزنگاری سفارشی شده
- تنوع بالا در تعریف قواعد کنترل دسترسی
- امکان اتصال به چندین شبکه هدف
- سرویس‌دهی هم‌زمان در حالت route و bridge
- مدیریت حساب کاربران
- مدیریت ارتباط کلاینت‌ها
- قابلیت تجمیع با فایروال و سایر ابزارهای امنیت شبکه
- فشرده‌سازی و سربار ترافیکی پایین
- سرویس‌دهی هم‌زمان روی پروتکل‌های TCP و UDP
- پایداری ارتباطات
- خارج‌سازی عملیات رمزنگاری از سرور و استفاده از شتاب‌دهنده های رمزنگاری
- قابلیت واگذاری اعتبار سنجی گواهی به سرور های بیرونی
- استفاده بهینه از منابع سخت‌افزاری

قابلیت‌های کلاینت

- امکان استفاده از برندهای مختلف توکن برای اتصال
- مدیریت توکن‌های سخت‌افزاری و نرم‌افزاری
- قابلیت حمل تمامی پیکربندی بر روی توکن
- امضای معتبر درایور شبکه
- قابلیت افزودن زبان
- قابلیت کار با Proxy

برای دریافت اطلاعات بیشتر و مشخصات فنی محصول به سایت هویتا مراجعه نمایید

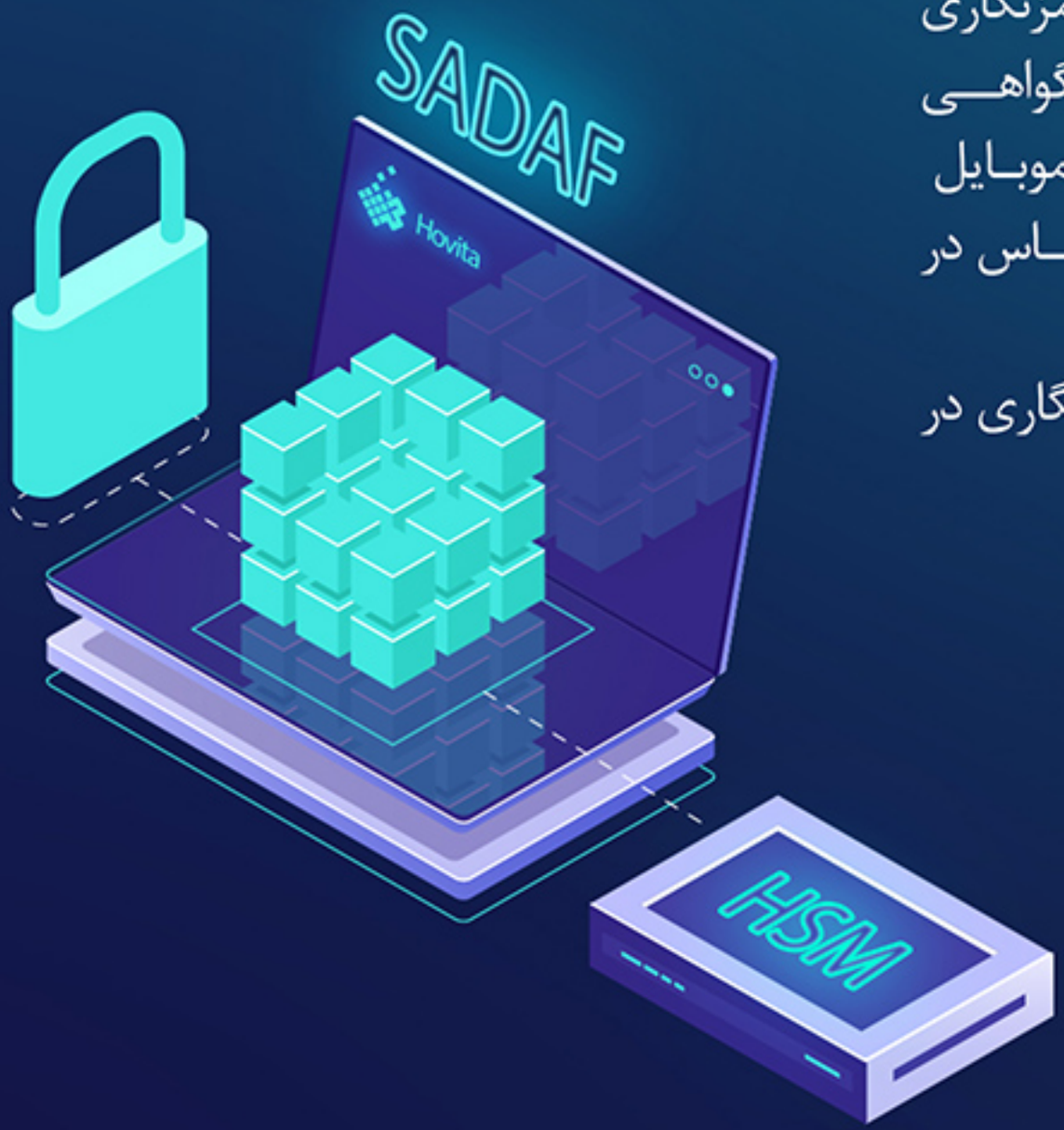
WWW.HOVITA.IR

هـویتـا

معرفی HSM بومی صدف

مـاژول امنیـت سـخت‌افزاری (HSM) سـامانه‌ای اسـت کـه بـرای حفاظـت از کلیدهـای امنیتی و اجـرای امن پردازش‌هـای رمزنـگاری طراحی‌شـده اسـت. HSM بـا نگهـداری، مدیریـت، و به‌کارگیـری کلیدهـای رمزنـگاری در یـک بسـتر سـخت‌افزاری غیرقابـل نفـوذ، به‌عنـوان یـک نگهبـان و مجـری قابل‌اعتمـاد، وظیفـه حفاظـت از مهم‌تریـن زیرسـاخت‌های امنیتـی را بـر عهـده دارد. شـتابدهی بـه عملیـات رمزنـگاری و نیـز برداشـتن بـار (offload) محاسـبات رمزنـگاری از روی پردازنده‌هـای همه‌منظـوره در انـواع کارگزارهـا (وب، پایـگاه داده، فایروال) از دیگر وظایف اصلی آن اسـت. معمـولاً محصولات HSM به‌صورت توکن USB، کارت PCIe و یا دستگاه مستقل در شبکه (Network Appliance) ارائه می‌شوند.

مـوارد کاربرد



- تولیـد، محافظـت، و به‌کارگیـری امـن کلیدهـای رمزنگاری در مراکـز نظامـی و اطلاعاتـی، مرکـز صـدور گواهـی دیجیتـال، شبکـه بانکی، شبکـه مخـابرات و ارتبـاطات موبـایل
- رمزگـذاری و تضمیـن جامعیـت داده‌هـای حسـاس در سیـستم هـای مدیریـت پایگـاه داده ها
- محافظـت از کلیـد و شـتاب‌دهی عملیـات رمزنـگاری در پروتکل هـای امنیتـی VPN، IPSec، HTTPS/SSL/TLS

ماژول امنیـت سخت‌افزاری صدف
Hardwae Security Module

هویتا

مشاوره در حوزه PKI

مشاوره در حوزه توسعه زیرساخت کلید عمومی، مرکز میانی و تکنولوژی PKI

شرکت فناوران هویت الکترونیکی امن (هویتا) به سازمان ها و شرکت هایی که در زمینه خدمات و محصولات مرتبط با زیرساخت کلید عمومی (PKI) دچار ابهامات می شوند و برای پیشبرد اهدافشان به دنبال راه حل مناسب، سریع و کم هزینه هستند، راهکار استفاده از تیم مشاوران حرفه ای را ارائه می دهد. بیش از یک دهه سابقه درخشان در زمینه زیرساخت کلید عمومی و بهره گیری از نیروهای متخصص، این شرکت را به یک شرکت حرفه ای و کارآمد در ارائه خدمات مشاوره ای PK-Enabling مبدل ساخته است.

شرکت فناوران هویت الکترونیکی امن(هویتا) تاکنون، خدمات و محصولات مرتبط با زیرساخت کلید عمومی (PKI) و گواهی های الکترونیکی را برای افراد و سازمان‌های مختلفی در کشور ارائه کرده است. از جمله می توان به طراحی و تولید محصولات مدیریت گواهی الکترونیکی، طراحی و ساخت تجهیزات رمزنگاری، صدور گواهی های الکترونیکی، امن سازی سرویس های مختلف مبتنی بر PKI، راه اندازی مراکز صدور گواهی الکترونیکی و ارایه راهکار و مشاوره در این حوزه، اشاره کرد.

خدمات قابل ارائه

طراحی و تهیه پروفایل امنیتی نرم‌افزار ـ راه اندازی مرکز میانی صدور گواهی الکترونیکی ـ مشاوره و ایمن سازی سامانه ها در لایه های زیرساخت، شبکه، ارتباط و کاربرد ـ مشاوره و نظارت در حوزه تجهیز نرم افزارهای کاربردی به زیرساخت کلید عمومی (PK-Enabling) ـ توسعه سامانه های زیرساختی در تجهیز نرم افزارهای کاربردی به زیرساخت کلید عمومی ـ ارزیابی برنامه‌های تجهیزشده به کلید عمومی ـ مشاوره به سازمان در مدیریت تعاملات فنی و اجرایی با مرکز میانی و مرکز ریشه کشور ـ مشاوره در حوزه ابزارهای مورد استفاده در سازمان در حوزه PKI اعم از سخت افزار و نرم افزار ـ توسعه خدمات مبتنی بر امضای دیجیتال و رمزنگاری نامتقارن مبتنی بر PKI ـ توسعه محصولات نرم افزاری اختصاصی سازمان مبتنی بر PKI تولید محتوای آموزشی عمومی و تخصصی جهت فرهنگ سازی PKI و کاربردهای آن در سازمان ـ برگزاری دوره های آموزشی مدیریتی، عمومی و تخصصی در زمینه PKI

تماس با ما

تهران خیابان حبیب اللّه خیابان قاسمی خیابان حبیب زادگان
پلاک ۶۹ طبقه ۶ واحد ۳۶

تلفن: ۶۶۰۳۴۸۰۹ - ۰۲۱

پست الکترونیک
info@hovita.ir

Contact Us

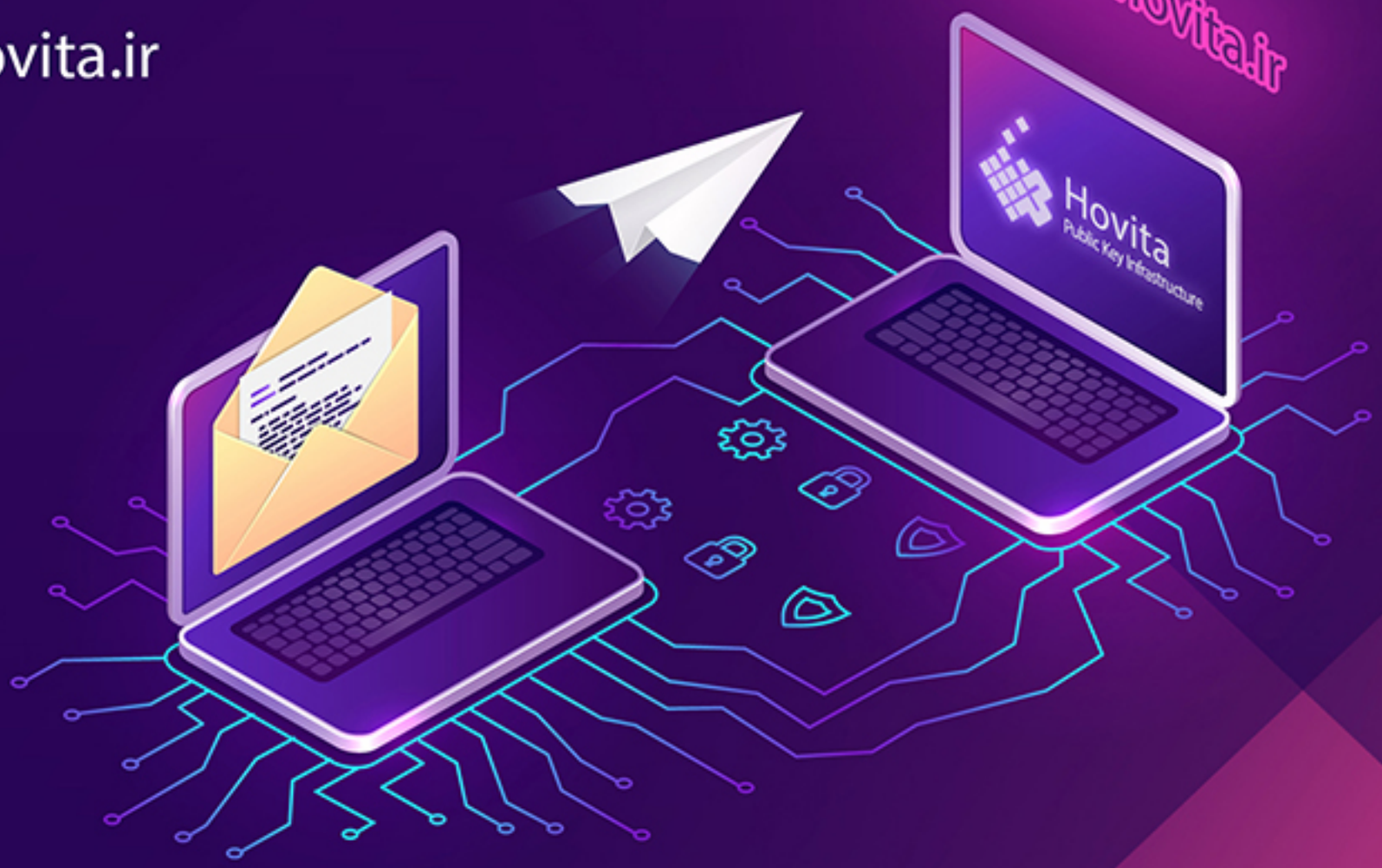
Unit 36, Floor 6, No 69, Habibzadegan St
Qasemi Ave, Habibollah Ave, Tehran

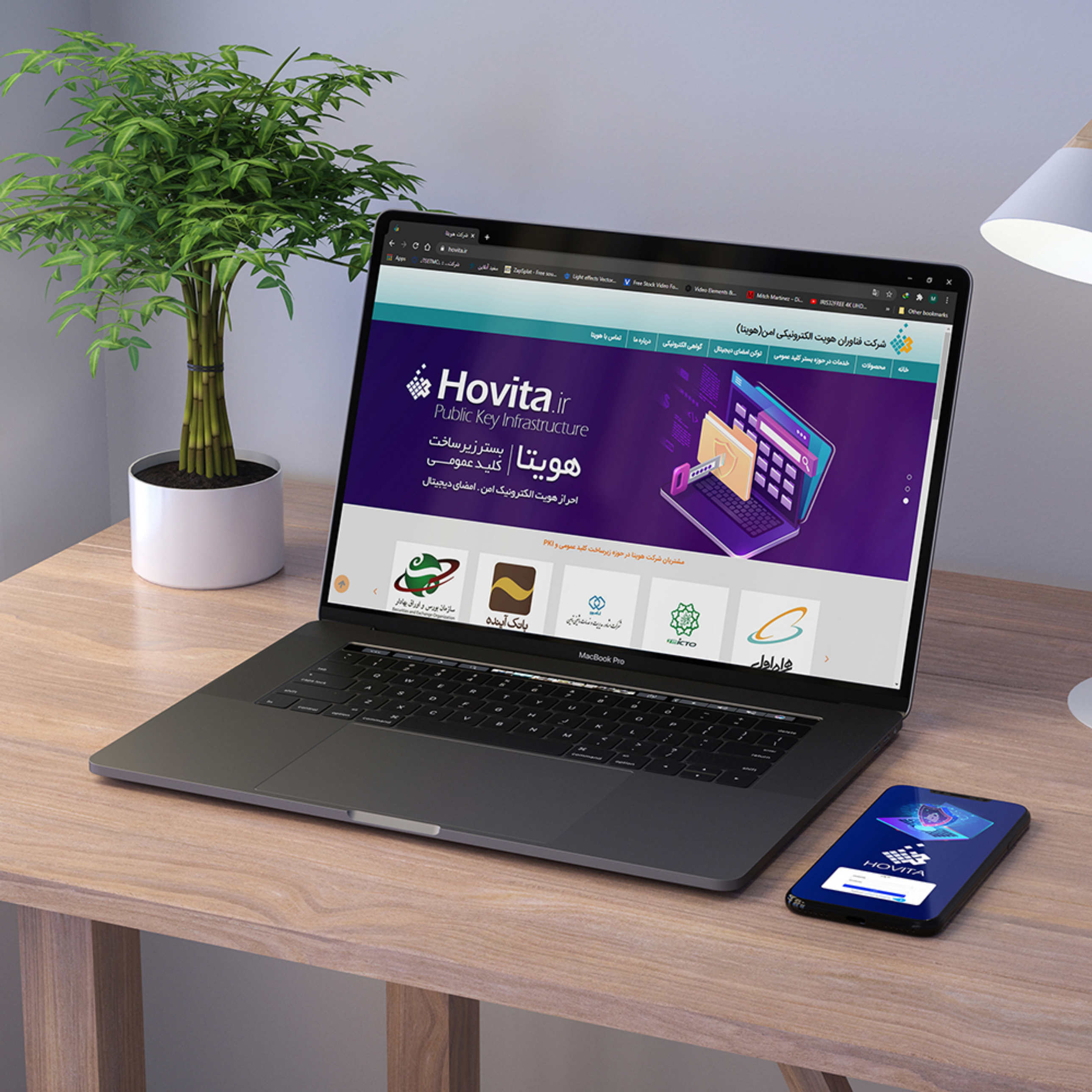
Phone Number: +982166034809

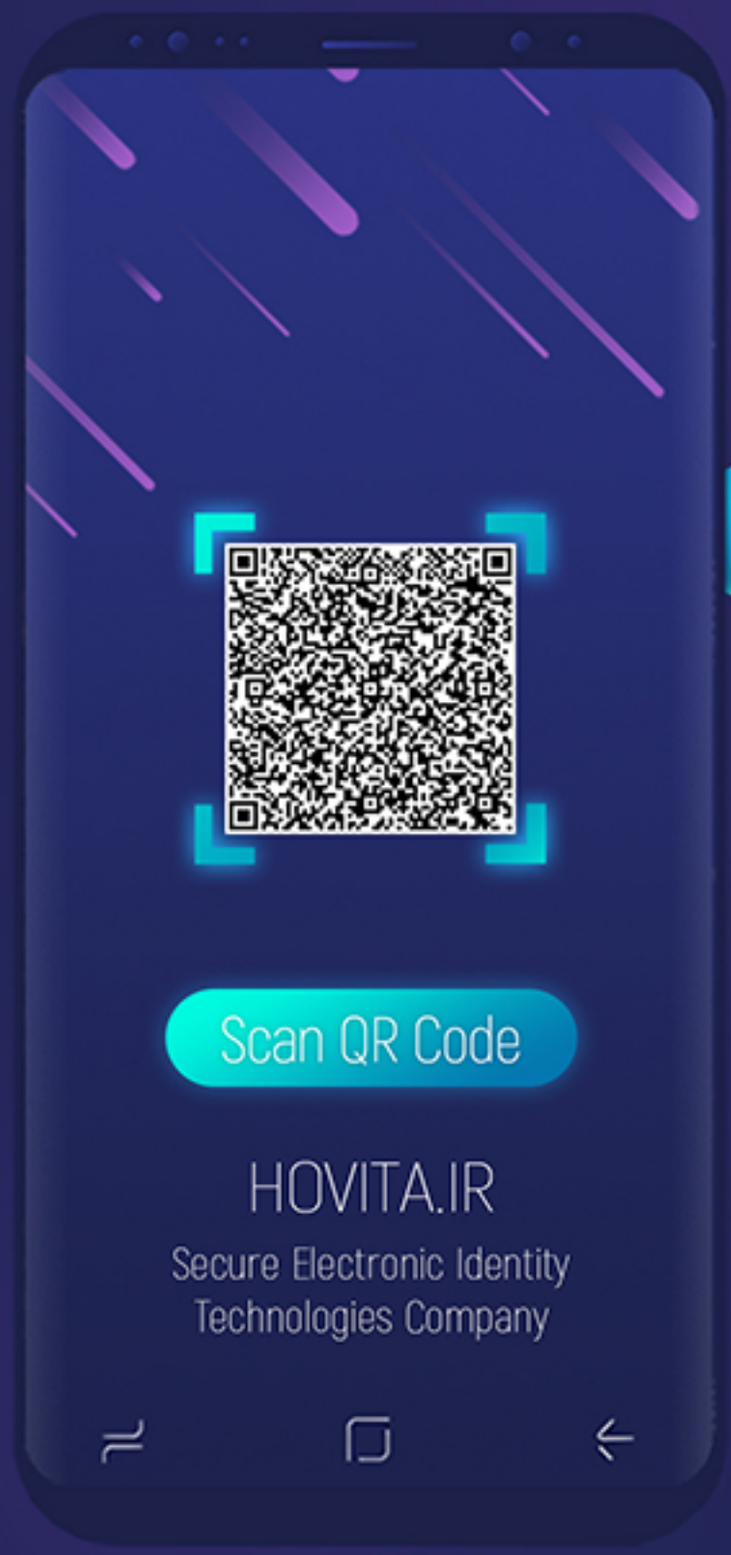
Email: info@hovita.ir

www.hovita.ir

https://hovita.ir




شرکت فناوران هویت الکترونیکی امن(هویتا)
خانه
محصولات
خدمات در حوزه بستر کلید عمومی
توکن امضای دیجیتال
گواهی الکترونیکی
درباره ما
تماس با هویتا
Hovita.ir
Public Key Infrastructure
هویتا | بستر زیرساخت کلید عمومی
احراز هویت الکترونیک امن . امضای دیجیتال
مشتریان شرکت هویتا در حوزه زیرساخت کلید عمومی و PKI
بانک آینده
MacBook Pro
HOVITA



شرکت فناوران هویت الکترونیکی امن (هویتا)