

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.



WWW.HOVITA.IR



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 رمزگاری، 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 به لحاظ بومی‌سازی و فناورینی، موفق به کسب دریافت بالاترین تاییدیه‌های لازم از آزمایشگاه‌های معتبر کشور است. همچنین این شرکت علاوه بر طراحی، تولید و ارائه محصولات تخصصی در حوزه 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 پیشبرد اهداف میهن عزیzman باشد.



توكن امضای ديجيتال پارسکي (ParsKey)

توكن هوشمند پارسکي مازول رمز کننده‌اي با رابط USB ميباشد. اين مازول تلفيقی از امنيت، كارآيی، كاربری آسان، قابلیت حمل و صرفه اقتصادي را در اختيار کاربر قرار ميدهد. پارسکي به صورت مستقل و بدون نياز به سخت افزارهای اضافی مانند کارت خوان، قابل استفاده بوده و امكان تولید کلیدهای متقارن و نامتقارن، انجام عملیات رمزگاری و امضای ديجيتالی به صورت On-Board در آن وجود دارد. برخورداری از رابط استاندارد (PKCS #11) به منظور برقراری ارتباط با توکن و همچنین پشتيبانی از زيرساخت کلید عمومي، امكان استفاده از اين محصول را در طيف وسعي از نرم افزارهای PK-Enabled فراهم کرده است.

تأييديهها و افتخارات

- کسب رتبه نخست در آزمون عملکرد و انطباق از آزمایشگاه ارزیابی مازولهای رمزگاری (۱۳۹۲، ۱۳۹۱ و ۱۳۹۳)
- دریافت اولین گواهی تأیید نمونه توکن امنیتی USB از سازمان تنظیم مقررات و ارتباطات راديوسي (۱۳۹۱)
- مطابقت کامل با سطح ۲ و برخی محورهای سطح ۳ از استاندارد FIPS 140-2
- مطابقت با Common Criteria EAL4+
- چهار سال متوالی برترین توکن امنیتی کشور



وظايف مورد انتظار از توکن هوشمند پارسکي

- نگهداري امن زوج کلید و گواهی کليه کاربران
- سистемهای نرمافزاری با قابلیت عدم استخراج کلید خصوصی جهت جلوگیری از نسخهبرداری (Duplication) و دسترسی غيرمجاز به کلید
- امضای ديجيتال مقدار تصادفي تولیدشده
- توسط سرور در هنگام احراز هويت کاربران



- امضای دیجیتالی فرم‌ها و فایل‌ها در سیستم
- رمزگشایی محتوای رمز شده با کلید خصوصی

کاربردها

بانکداری الکترونیکی - امضای اظهارنامه مالیاتی - مبادلات امن در بورس - ورود امن به ویندوز پست الکترونیک امن - اتوماسیون اداری امن - ثبت اسناد حقوقی (قراردادهای خریدوفروش و اجاره مسکن) - برقراری ارتباطات امن SSL، SSH، IPSec و VPN

قابلیت‌های کلیدی

پشتیبانی از الگوریتم‌های مختلف رمزگاری و امضا (DES, AES-3, RSA, DES) - پشتیبانی از استانداردهای MicrosoftPKCS و ISO 7816 - اجرای تمام عملیات به صورت on-board - پشتیبانی از سیستم عامل‌های ویندوز و لینوکس ۳۲ و ۶۴ بیتی - استحکام بدنه فوق العاده، مقاوم در برابر ضربه، عدم امکان بازشدن بدون تشخیص - بدون نیاز به نصب (driverless) - پشتیبانی و خدمات پس از فروش گستردۀ

مزایای توکن امضای دیجیتال ParsKey

بدون نیاز به نصب نرمافزار در سمت کلاینت - قابل حمل (بدون نیاز به کارت‌خوان) - بدون نیاز به شارژ و باتری - دارای نرمافزار مخصوص برای مدیریت تمام فرایندهای چرخه حیات - رابط کاربری مناسب برای مدیریت کلیدها و گواهی‌ها - امکان استفاده موازی از چند توکن - امکان به اشتراک‌گذاری در شبکه

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

سامانه صدور و مدیریت گواهی الکترونیکی پارس تراست

سامانه پارس تراست 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، تعليق، 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 پارس تراست عبارت‌اند از: مرکز صدور گواهی (CA)، مرکز ثبت‌نام گواهی (RA)، مخزن گواهی و لیست ابطال (TSA)، پاسخگوی برخط وضعیت گواهی‌ها (OCSP Responder)، مرکز مهر زمانی (Repository)، مرکز اعتمادسنجی گواهی (VA) و مرکز مدیریت و احراز هویت (IdP).

تأییدیه‌ها 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 جما سازمان بورس و اوراق بهادار، شرکت همراه اول مرکز میانی صدور گواهی پارس‌ساین و بیش از ۱۰ زیرساخت کلید عمومی درون سازمانی

قابلیت‌ها و استانداردها

- منطبق با استانداردهای IETF PKIX
- قابلیت تعریف و پیکربندی انواع پروفایل‌های گواهی مطابق X.509 و RFC5280
- پشتیبانی از تعیین سیاست‌های مدیریت گواهی از طریق پروفایل‌های پویا
- قابلیت تعیین قالب برای محتوای هر یک از فیلد‌های Subject گواهی
- امکان تعریف افزونه‌های Extensions مختلف برای درج در گواهی
- قابلیت صدور و مدیریت چندین گواهی متفاوت با یک پروفایل
- امکان مدیریت پروفایل کلید شامل طول کلید، الگوریتم تولید کلید، طول عمر کلید، رسانه ذخیره‌سازی کلید
- قابلیت تعیین بازه مجاز در خواست تمدید گواهی (Renew margin)
- قابلیت صدور، ابطال، تعلیق و رفع تعلیق انواع گواهی
- قابلیت تمدید و تجدید کلید انواع گواهی‌های صادر شده
- قابلیت مدیریت خودکار و نیمه خودکار گواهی
- پشتیبانی از تعیین زمان عملیات بر روی گواهی برای آینده
- پشتیبانی از کارکرد های مدیریت کلید شامل تولید، نگهداری، ابطال و تعلیق
- قابلیت مدیریت درخواست (ثبت، بازنگری و ویرایش، لغو و حذف انواع درخواست‌های گواهی)
- قابلیت بایگانی، جستجو و بازیابی درخواست‌ها و گواهی‌ها
- قابلیت مشاهده فرآیند کاری درخواست‌ها
- قابلیت نمایش و کنترل چرخه حیات گواهی
- قابلیت تعريف و مدیریت نقش‌های مختلف برای هر مولفه براساس سرویس‌های ارائه شده توسط مولفه‌ها
- قابلیت تعريف و مدیریت سازمان‌ها به صورت چندسطحی تا ۵ سطح
- قابلیت تعريف، 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
- کنترل دسترسی کاربران چندسطحی به صورت Record-level و Role-based



- پشتیبانی از شبیه ساز نرم افزاری HSM پارس کی به صورت Built-in
- امکان کار با انواع تجهیزات HSM با واسطه های Java JCA/JCE CSP و PKCS #11
- سازگاری با توکن پارس کی (ParsKey) و سایر توکن های مورد تائید در زیرساخت کلید عمومی کشور
- قابلیت تعیین بازه اعتبار، به روزرسانی و انتشار دوره ای CRL سازگار با RFC5280
- پشتیبانی از مکانیزم های انتشار گواهی ها و CRL در مخزن، سازگار با پروتکل LDAP RFC2253
- امکان آدرس دهی و تمایز گواهی بر اساس نام متمایز کننده (DN) سازگار با RFC2396
- قابلیت به روزرسانی همزمان چندین OCSP، RA و مخزن گواهی
- پشتیبانی از الگوریتم های RSA و ECDSA در تمامی مؤلفه ها
- پشتیبانی از کار کرد تولید مهر زمانی (TSP) سازگار با استاندارد RFC3161
- پشتیبانی از سرویس مرکزی اعتبار سنجی گواهی و امضای دیجیتال از طریق مؤلفه VA
- پشتیبانی از مکانیزم های برخط استعلام وضعیت گواهی در مؤلفه OCSP سازگار با RFC5019
- امضای دیجیتال رویدادهای ممیزی به صورت Chain signing در تمامی مؤلفه ها
- قابلیت رویدادنگاری عادی با امکان ذخیره در انواع فایل، پایگاه داده یا ارسال رویدادها تحت شبکه
- پشتیبانی از گواهی های کلید عمومی X509 v3 and v1 و لیست گواهی های باطله CRL v2
- پشتیبانی از PKCS #1، #5، #7، #8، #9، #10، #11، #12

ویژگی های غیر عملکردی و عملیاتی

- قابلیت مدیریت و راهبری مجازی مرکز صدور گواهی (CA) و دفاتر ثبت نام (RA)
- قابلیت پشتیبانی از چند CA در مؤلفه RA
- قابلیت پشتیبانی از چند CA در مؤلفه OCSP
- دارای درگاه وب کاربر پسند برای هر مؤلفه
- قابلیت افزایش مؤلفه های OCSP به صورت مجزا
- امکان استفاده از سرویس های اصلی ثبت نام و صدور گواهی از طریق وب سرویس

- قابلیت تعریف و افزایش دفاتر ثبت نام
- عدم محدودیت در تعداد سطوح سلسله مراتب اعتماد
- قابل ارائه به صورت بسته های نصب نرم افزار، ماشین مجازی و Container و Network Appliance
- طراحی مستقل از پایگاه داده و قابلیت کار با انواع پایگاه داده از قبیل Oracle، MySQL، PostgreSQL و Microsoft SQL Server
- قابلیت HA با مدیریت Fail-over و Load balancing
- قابلیت پشتیبان گیری، بازیابی، مانیتورینگ و نظارت مرکزی
- پشتیبانی از ارتباط SSL/TLS دو طرفه بین مؤلفه ها، بین مؤلفه ها و پایگاه داده و با مخزن
- قابل پیکربندی و انطباق با انواع سیاست های گواهی الکترونیکی
- امکان یکپارچه سازی با امضای همراه (Mobile Signature Service) از طریق ETSI TS 204 102

ParsTrust

سامانه صدور و مدیریت
گواهی الکترونیکی پارس تراست

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

WWW.HOVITA.IR





بسته توسعه نرم افزاری پارس کیت (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 نرم افزاری طرف اعتماد کننده، اصطلاحاً PKE یا Public Key Enabling گفته می‌شود و مجموعه ابزارها و بسته‌های نرم افزاری که در این خصوص مورد استفاده قرار می‌گیرند، PKE SDK نام دارند. این ابزارها با برخورداری از توابع و مazon‌های برنامه نویسی آماده و مورد تأیید آزمایشگاه‌های PKI در کشور، فرایند توسعه محصول را برای برنامه نویسان و تولیدکنندگان نرم افزار، 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 سامانه‌های نرم افزاری تحت وب، Desktop و سرویس‌های راه دور
- قابل استفاده در مرورگرهای وب متداول ویندوز لینوکس و اندروید
- امکان استفاده در سرورهای نرم افزار مبتنی بر PHP، Microsoft .NET Framework، Java Native C/C++ Library بر روی Wrapper



- قابل استفاده در کارگزارهای وب متداول از قبیل Apache IIS، Oracle WebLogic و
- قابل استفاده در سیستم عامل‌های ویندوز، لینوکس و اندروید

NIST Recommendation for RFC5280 ، مطابق با «الزامات تشکیل و اعتبارسنجی زنجیره گواهی مرکز دولتی صدور گواهی الکترونیکی ریشه» X509 Path Validation

- 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 با واسطه‌های MS CAPI و PKCS11# Java JCA/JCE CSP
- پشتیبانی از توکن نرم‌افزاری پارس‌کی با رابط # PKCS11 در سمت سرور و کاربر 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 Annex D 2005-ANSI X9.62 Appendix A2.4 ANSI X9.31 و FIPS196 برای تولید رشته تصادفی Challenge در مبحث احراز هویت مطابق با PKCS10#

- امکان تولید و بررسی درخواست صدور گواهی در قالب CSR منطبق با استاندارد CMS و PKCS7
- امکان تولید و اعتبارسنجی امضای دیجیتال در قالب # RSA و ECDSA در امضا و اعتبارسنجی
- پشتیبانی از الگوریتم‌های SHA1، SHA256، SHA384 و SHA512
- پشتیبانی از مکانیزم‌های امضای دیجیتال RSASSA-PKCS1v1.5 و RSASSA-PSS
- قابلیت رویدادنگاری مطابق سند «الزامات تشکیل و اعتبارسنجی زنجیره گواهی مرکز دولتی صدور گواهی الکترونیکی ریشه»
- امکان ارائه اپلت‌های PKI، FIDO و PIV برای کارت هوشمند و سیم‌کارت

معرفی محصول ParsPKE

درگاه نرم افزاری امضای دیجیتال مبتنی بر سرویس

محصول ParsPKE امکان تجهیز سامانه‌های نرم‌افزاری به خدمات احراز هویت و امضای تراکنش‌ها و اسناد را مبتنی بر وب‌سرویس، فراهم می‌کند. سامانه‌های نرم‌افزاری با فرخوانی سرویس‌های این سامانه می‌توانند کاربران خود را مبتنی بر PKI، احراز هویت کرده و همچنین اسناد و تراکنش‌های را به صورت دیجیتالی امضانمایند. فرمات اسنادی که این سامانه قادر به امضای آن‌ها می‌باشد شامل انواع فایل‌های مجموعه Office (نظیر Word، Excel، وغیره)، فایل‌های ZIP، XML، PDF وغیره است.

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



ویژگی‌ها و قابلیت‌های محصول

- **معماری مبتنی بر سرویس:** این سامانه با بهره‌گیری از معماری سرویس محور می‌تواند مستقل از پلتفرم سامانه نرم‌افزاری، مورد استفاده در انواع زبان‌های برنامه‌نویسی قرار گیرد.

- **برخورداری از پشتونه حقوقی و قانونی:** امضای الکترونیکی در این سامانه منطبق با استانداردها و قوانین کشور انجام می‌گیرد و مؤلفه‌های مرتبط با زیرساخت کلید عمومی، دارای تأییدیه از آزمایشگاه مرکز توسعه تجارت الکترونیکی هستند. لذا امکان ارائه

- 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، XAdES، CAdES، PAdES، ASiC-E و 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 می‌کند.
- قابلیت امضاء با توکن: امکان استفاده از PKI USB Token‌ها (مورد تأیید مرکز ریشه وزارت صنعت معدن و تجارت) در فرایند احراز هویت کاربران و امضای اسناد و تراکنش‌ها (توسط کاربران در مرورگرهای مطرح سیستم عامل‌های 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 رمزگاری مبتنی بر استاندارد PKCS#11 (مورد تأیید 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 "الزمات 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 به صورت پیش‌فرض براساس استاندارهای اعتبارسنجی ETSI عملیات مذکور را انجام می‌دهد.
- استفاده از استانداردهای بین‌المللی و قوانین بومی: محصول مبتنی بر استانداردهای بین‌المللی معتبر توسعه داده شده 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

امضای همراه دیجیتال مبتنی بر سیم کارت و گوشی تلفن همراه

سرвис امضای همراه (Mobile Signature Service) راهکاری نوین در حوزه احراز هویت و امضای دیجیتال با استفاده از تلفن همراه کاربران (به عنوان 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 به صورت دوامده و دوکاناله تأمین می‌نماید. این راهکار مبتنی برای استانداردهای داخلی و بین‌المللی توسعه یافته و می‌تواند مبتنی بر سیم کارت (SIM-based) و بدون سیم کارت (SIM-less) ارائه شود.

مشخصات فنی

ارائه خدمات احراز هویت دوامله 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 سیم کارت - امکان ارسال پیام عادی و محترمانه به کاربر - پشتیبانی از سرویس ارائه رسید تراکنش‌ها - پشتیبانی از پروفایل‌های امضای دیجیتال
ارائه خدمات بر روی API‌های SOAP و REST - پشتیبانی از الگوریتم‌ها و مکانیزم‌های رمزگاری 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 متتنوع ارائه خدمت: Client-Server - Server-Server - Synchronous

مزایا

- عدم نیاز به حمل ابزارهای اضافه و سهولت استفاده
- بالاترین سطح امنیت و محافظت از کلیدهای خصوصی (GSMA مطابق LoA4)
- تبادل نشدن پین کد روی شبکه و عدم امکان شنود آن
- احراز هویت دوکاناله (شبکه GSM و شبکه اینترنت / اینترانت)
- برخورداری از پشتونه حقوقی و قانونی
- کاهش هزینه‌ها، پیچیدگی و زمان پیاده‌سازی و نگهداری کاربردهای زیرساخت کلید عمومی

تأییدیه‌ها و گواهی‌نامه‌ها

گواهی تأیید اپلت امضای همراه از آزمایشگاه امنیت سیستم عامل مراجع ذیصلاح

- مورد تأیید کمیته سیم کارت شرکت ارتباطات سیار ایران (همراه اول)
- استفاده از مازول PKE دارای تأییدیه سطح پلاتین از آزمایشگاه مرکز توسعه تجارت الکترونیکی ایران



سرвис امضای همراه
Mobile Signature Service

سامانه احراز هویت یکپارچه ParsSSO

سامانه ParsSSO، سرویس احراز هویت را ارائه می‌دهد. احراز هویت در این سامانه به صورت Single Sign-On است یعنی تنها با یکبار احراز هویت کاربر می‌تواند از تمامی نرمافزارهای سازمان بدون نیاز به احراز هویت مجدد استفاده نماید. علاوه بر این مدیریت کاربران یکپارچه مشکلات مربوط به سرپرستی سامانه‌های این سامانه را به صورت چشمگیری کاهش می‌دهد. با تعریف یک کاربر، دسترسی کاربر در تمامی سامانه‌ها به صورت خودکار ایجاد می‌گردد و با حذف دسترسی کاربر، تمامی سامانه‌ها از ورود کاربر جلوگیری خواهند کرد. مهم‌ترین بخش سامانه مؤلفه SSO است که به اختصار IdP نامیده می‌شود، مؤلفه ارائه‌دهنده خدمات سفارشی‌سازی شده‌ی AA شامل، احراز هویت و کنترل دسترسی است. تمامی فراهم‌کنندگان خدمت می‌توانند با ثبت‌نام در این مؤلفه، خدمات AA را به آن برونق‌سپاری کنند. از ویژگی‌های اصلی این مؤلفه ارائه‌های خدمات به صورت Single Sign-On با ضریب امنیتی بالا است. همچنین این مؤلفه از جانب فراهم‌کنندگان خدمت مسئولیت Policy Enforcement را بر عهده دارد.

قابلیت‌های مؤلفه Identity Provider



- احراز هویت: در مؤلفه IdP احراز هویت به سه روش انجام می‌شود: «احراز هویت با نام کاربری و رمز عبور»، «احراز هویت به صورت OTP از طریق ارسال پیامک»، «احراز هویت با توکن (برای انجام این نوع از احراز هویت از گواهی استفاده شده و به صورت Challenge-Response انجام می‌شود).»
- کنترل دسترسی: در این مؤلفه به دو صورت Record-Based و Role-Based انجام می‌شود. کنترل دسترسی Role-Based براساس سطح دسترسی تعیین شده به سرویس‌های ارائه شده از جانب فراهم‌کنندگان خدمت در نقش مناسب به کاربر و کنترل



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

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

Credentials : برای احراز هویت کاربر در سامانه استفاده شده و شامل

«گواهی با کاربرد کلید Authentication» و «نام کاربری و رمز عبور» می‌باشد.

اطلاعات هویتی : شامل نام و نام خانوادگی، شماره تماس

نقش : سطح دسترسی کاربر به سرویس‌های فراهم‌کننده خدمت مربوطه را مشخص می‌کند.

سازمان : سطح دسترسی کاربر به سازمان‌های فراهم‌کننده خدمت مربوطه تعیین می‌کند.

سرویس‌هایی که در این بخش ارائه می‌شوند، شامل:

ایجاد کاربر-ویرایش کاربر-اختصاص نقش به کاربر-حذف کاربر و مشاهده لیست کاربران

• مدیریت نقش : هر فراهم‌کننده خدمت امکانات خود را در قالب سرویس به کاربران ارائه می‌دهد. نقش بهمنظور

تعیین دسترسی به سرویس‌های فراهم‌کننده خدمت تعریف می‌شود. هر سرویس می‌تواند یک یا چند Entity داشته

باشد که هنگام تعیین دسترسی به سرویس، امکان تعیین سطح دسترسی از طریق Entity‌ها نیز موجود است.

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

• مدیریت سازمان‌ها : سازمان‌ها به صورت یک درختواره تعریف می‌شوند. هر سازمان می‌تواند تا ۵ سطح زیر سازمان داشته

باشد. سازمان‌ها به منظور اعمال سطح دسترسی Record-Level استفاده می‌شوند. در هر سطح سازمان دسترسی به

اطلاعات زیر سازمان‌ها وجود دارد، در حالی که دسترسی به اطلاعات سازمان‌های هم‌سطح امکان‌پذیر نیست.

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

• مدیریت فراهم‌کنندگان خدمت : اطلاعاتی که به هنگام ثبت، از فراهم‌کننده خدمت دریافت می‌شود به منظور 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 فراهم‌کننده خدمت، ویرایش فراهم‌کننده خدمت، حذف

فراهم‌کننده خدمت و مشاهده 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 سرسید احراز هویت کاربر باطل شده و کاربر برای ادامه فعالیت

نیاز به احراز هویت مجدد دارد.

معرفی محصول ParsSign

مرکز صدور گواهی الکترونیکی ParsSign، نهادی است که برای اشخاص حقیقی و حقوقی گواهی الکترونیکی صادر می‌کند و به هویت آن‌ها در فضای دیجیتال اعتبار قانونی و حقوقی می‌بخشد. این مرکز از سال ۱۳۸۱ باهدف آموزش، فرهنگ‌سازی عمومی در زمینه صدور گواهی الکترونیکی و امضای دیجیتال فعالیت کرده است و تابه‌حال چندین هزار گواهی الکترونیکی برای کاربردهایی مانند امضا، پست الکترونیکی و SSL صادر نموده است.

افتخارات و دستاوردها

- توسعه‌دهنده اولین نرم‌افزارهای بومی مدیریت گواهی الکترونیکی (CA)، مدیریت مرکز ثبت‌نام (RA) و OCSP
- تأثیرگذاری شده در زیر ساخت کلید عمومی کشور
- نخستین و تنها مرکز صدور گواهی الکترونیکی خصوصی کشور
- دارای مجوز فعالیت از وزارت صنعت، معدن و تجارت
- زیر نظر مرکز دولتی صدور گواهی الکترونیکی ریشه
- برخورداری از دفاتر ثبت‌نام گواهی در سراسر کشور



کاربردها

- صدور گواهی امضای دیجیتال با کاربرد امضای دیجیتال
داده‌ها و احراز هویت کاربران
- صدور گواهی SSL/TLS با کاربرد تصدیق اصالت یک سرویس‌دهنده، تصدیق اصالت یک سرویس گیرنده ایجاد ارتباط امن و رمزگذاری شده بین سرویس‌دهنده و سرویس گیرنده

- 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 مرکز صدور گواهی



- طراحی، راه اندازی و پشتیبانی مرکز صدور گواهی
 - اخذ مجوز از مرکز ریشه
 - طراحی و راه اندازی مرکز داده
 - طراحی و تأمین سخت افزار و نرم افزار مرکز صدور
 - تهیه و تدوین اسناد سیاست های گواهی و دستور العمل اجرایی گواهی
 - تهیه، تدوین و پیاده سازی سیاست های امنیتی
 - ارائه آموزش های مرتبط با زیر ساخت کلید عمومی
 - مشاوره و نظارت بر طراحی و پیاده سازی
 - نگهداری و پشتیبانی
- میزبانی و اجاره مرکز صدور گواهی

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

راه حل شبکه خصوصی مجازی ParsVPN

محصول ParsVPN به منظور برقراری ارتباط کاربر با شبکه‌ای خصوصی در بستر یک شبکه عمومی و همچنین رفع مشکلات احراز هویت کاربر، حفظ محترمانگی و جامعیت اطلاعات در حال انتقال، توسعه یافته است. سامانه ParsVPN امکان ایجاد ارتباط امن بین چندین کاربر و تعدادی سرویس‌دهنده یا تنها بین چندین کاربر را فراهم می‌آورد که از اهداف اصلی آن ایجاد حداکثر امنیت با انجام ساده‌ترین تنظیمات، قابلیت بالای مدیریت هویت کاربران و کنترل دسترسی آن‌هاست. این محصول، راه حل شبکه‌ای خصوصی مجازی (Virtual Private Network) به منظور برقراری ارتباط کاربر با شبکه‌ای خصوصی در بستر یک شبکه عمومی و همچنین رفع مشکلات هویت شناسی کاربر، حفظ محترمانگی و جامعیت اطلاعات در حال انتقال است.



کاربردها

دور کاری امن - اختصاص پهنه‌ای باند و محدودیت در ارسال و دریافت داده جدا سازی اینترنت و اینترانet احراز هویت دو عامله مستقل از محیط امن سازی شبکه (حفظ محترمانگی و جامعیت، احراز هویت و جلوگیری از حملات) - امن سازی سرویس‌های تحت وب و پورتال‌ها - مدیریت هویت و کنترل دسترسی کاربران با استفاده از گواهی الکترونیکی و توکن قابلیت استفاده از شتاب دهنده‌های رمز نگاری از جمله HSM سربار ترافیکی بسیار پایین

قابلیت ها

قابلیت های کلاینت

- امکان استفاده از برندهای مختلف توکن برای اتصال
- مدیریت توکن های سخت افزاری و نرم افزاری
- قابلیت حمل تمامی پیکربندی بر روی توکن
- امضای معتبر درایور شبکه
- قابلیت افزودن زبان Proxy
- قابلیت کار با

قابلیت های سرور ParsVPN

- پشتیبانی کامل از PKI
- بارگذاری الگوریتم های رمزنگاری سفارشی شده
- تنوع بالا در تعریف قواعد کنترل دسترسی
- امکان اتصال به چندین شبکه هدف
- سرویس دهی همزمان در حالت route و bridge
- مدیریت حساب کاربران
- مدیریت ارتباط کلاینت ها
- قابلیت تجمعیع با فایروال و سایر ابزارهای امنیت شبکه
- فشرده سازی و سربار ترافیکی پایین
- سرویس دهی همزمان روی پروتکل های TCP و UDP
- پایداری ارتباطات
- خارج سازی عملیات رمزنگاری از سرور و استفاده از شتاب دهنده های رمزنگاری
- قابلیت واگذاری اعتبار سنجی گواهی به سرور های بیرونی
- استفاده بهینه از منابع سخت افزاری

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

معرفی HSM بومی صدف

ماژول امنیت سخت افزاری (HSM) سامانه‌ای است که برای حفاظت از کلیدهای امنیتی و اجرای امن پردازش‌های رمزنگاری طراحی شده است. HSM با نگهداری، مدیریت، و به کارگیری کلیدهای رمزنگاری در یک بستر سخت افزاری غیرقابل نفوذ، به عنوان یک نگهبان و مجری قابل اعتماد، وظیفه حفاظت از مهم‌ترین زیرساخت‌های امنیتی را بر عهده دارد. شتابدهی به عملیات رمزنگاری و نیز برداشتن بار (offload) محاسبات رمزنگاری از روی پردازنده‌های همه‌منظوره در انواع کارگزارها (وب، پایگاه داده، فایروال) از دیگر وظایف اصلی آن است. معمولاً محصولات HSM به صورت توکن USB، کارت PCIe و یا دستگاه مستقل در شبکه (Network Appliance) ارائه می‌شوند.

موارد کاربرد

- تولید، محافظت، و به کارگیری امن کلیدهای رمزنگاری در مراکز نظامی و اطلاعاتی، مرکز صدور گواهی دیجیتال، شبکه بانکی، شبکه مخابرات و ارتباطات موبایل
- رمزگذاری و تضمین جامعیت داده‌های حساس در سیستم‌های مدیریت پایگاه داده‌ها
- محافظت از کلید و شتابدهی عملیات رمزنگاری در پروتکل‌های امنیتی HTTPS/SSL/TLS، IPSec، VPN



ماژول امنیت سخت افزاری صدف
Hardware Security Module

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

شرکت فناوران هویت الکترونیکی امن (هویتا) به سازمان‌ها و شرکت‌هایی که در زمینه خدمات و محصولات مرتبط با زیرساخت کلید عمومی (PKI) دچار ابهامات می‌شوند و برای پیشبرد اهدافشان به دنبال راه حل مناسب، سریع و کم هزینه هستند، راهکار استفاده از تیم مشاوران حرفه‌ای را ارائه می‌دهد. بیش از یک دهه سابقه درخشنان در زمینه زیرساخت کلید عمومی و بهره‌گیری از نیروهای متخصص، این شرکت را به یک شرکت حرفه‌ای 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 گواهی‌های الکترونیکی را برای افراد و سازمان‌های مختلفی در کشور ارائه کرده است. از جمله می‌توان به طراحی و تولید محصولات مدیریت گواهی الکترونیکی، طراحی و ساخت تجهیزات رمزگاری، صدور گواهی‌های الکترونیکی، امن سازی سرویس‌های 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 – راه اندازی مرکز میانی صدور گواهی الکترونیکی – مشاوره و ایمن سازی سامانه‌های زیرساخت، شبکه، ارتباط و کاربرد – مشاوره و نظارت در حوزه تجهیز نرم افزارهای کاربردی به زیرساخت کلید عمومی (PK-Enabling) – توسعه سامانه‌های زیرساختی در تجهیز نرم افزارهای کاربردی به زیرساخت کلید عمومی – ارزیابی برنامه‌های تجهیزشده به کلید عمومی – مشاوره به سازمان در مدیریت تعاملات فنی و اجرایی با مرکز میانی و مرکز ریشه کشور – مشاوره در حوزه ابزارهای مورد استفاده در سازمان در حوزه PKI اعم از سخت افزار و نرم افزار – توسعه خدمات مبتنی بر امضای دیجیتال و رمزگاری نامتقارن مبتنی بر PKI – توسعه محصولات نرم افزاری اختصاصی سازمان مبتنی بر PKI تولید محتوای آموزشی عمومی و تخصصی جهت فرهنگ سازی PKI و کاربردهای آن در سازمان – برگزاری دوره‌های آموزشی مدیریتی، عمومی و تخصصی در زمینه PKI

تماس با ما

تهران خیابان حبیب الله خیابان قاسمی خیابان حبیبزادگان
پلاک ۶۹ طبقه ۶ واحد ۳۶
تلفن: ۰۲۱-۶۶۰۳۴۸۰۹

پست الکترونیک
info@hovita.ir

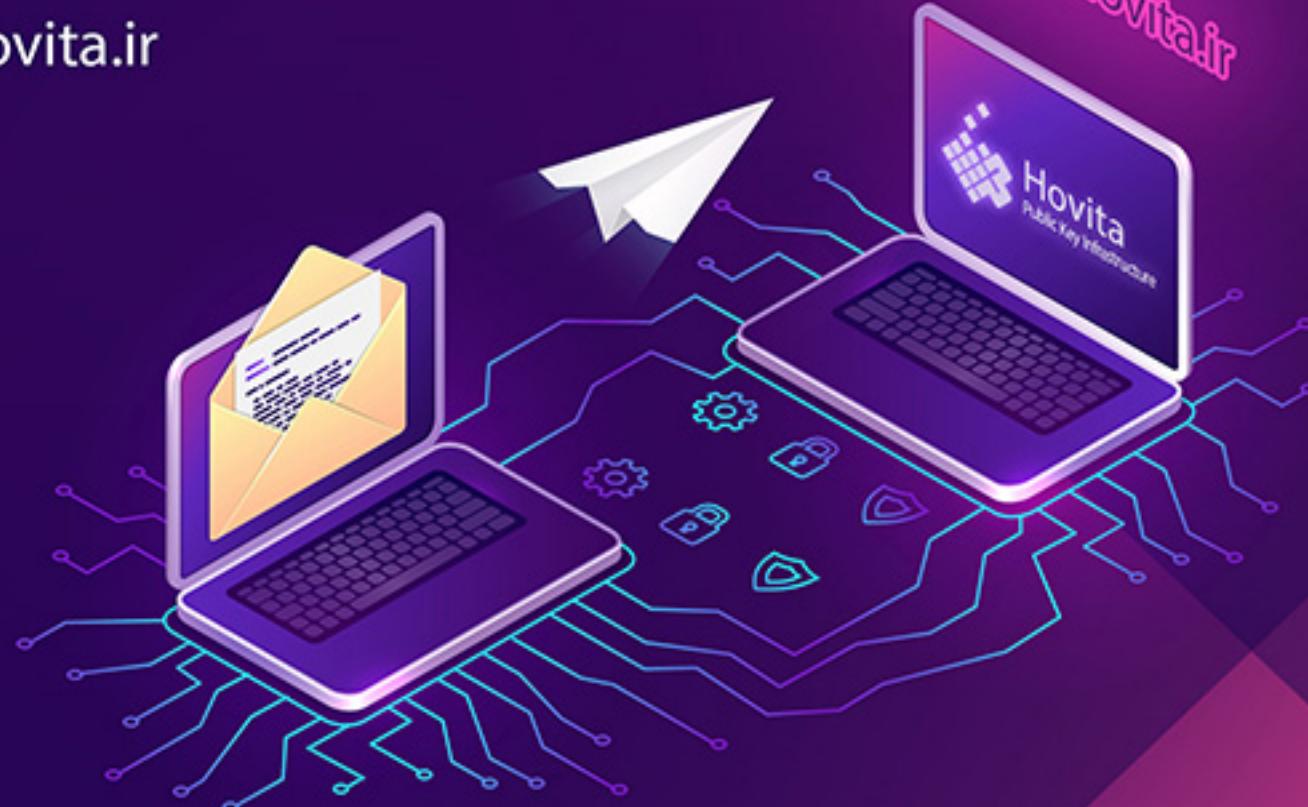
Contact Us

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

Phone Number: +982166034809

Email: info@hovita.ir

www.hovita.ir







شرکت فناوران هویت الکترونیکی امن (هویتا)

تمامی حقوق اطلاعات مندرج در کاتالوگ متعلق به شرکت هویتا می باشد