جمهوری اسلامی ایران
وزارت صنعت، معدن و تجارت

مرکز توسعه تجارت الکترونیکی

مرکز دولتی صدور گواهی الکترونیکی ریشه

I.R.Iran Root Certification Authority

جمهوری اسلامی ایران
وزارت صنعت، معدن و تجارت

مرکز توسعه تجارت الکترونیکی

نشانی پستی: تهران- بلوار کشاورز- خیابان شهید نادری
جنب کوچه حجت دوست- ساختمان نادری
وزارت صنعت، معدن و تجارت- طبقه پنجم-
مرکز دولتی صدور گواهی الکترونیکی ریشه
کد پستی ۱۴۱۶۶۴۳۸۵۱
شماره تلفن ۸۵۱۹۳۷۱۱
شماره فاکس ۸۸۹۶۸۰۷۲
وب‌سایت مرکز www.rca.gov.ir

I.R.Iran Root Certification Authority

مقدمه

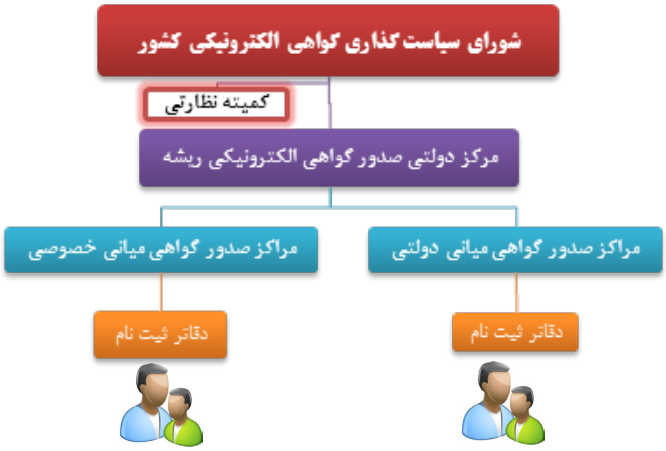
با توجه به گسترش روز افزون فناوری اطلاعات و جایگاه آن در کشور و همچنین تبدیل عملیات و نمادهای فیزیکی به دیجیتالی، تبادل اطلاعات به صورت محرمانه، به همراه احرازهویت مبادله‌کنندگان و انکارناپذیری اطلاعات مبادله شده، به امری ضروری و اجتناب ناپذیر تبدیل شده است

اعتماد شالوده اصلی هر نوع تعاملی است. به دنبال ارتقای سطح تعاملات نیاز به اعتماد، بیشتر و پیچیده‌تر می‌شود. اما ابزار اعتماد در فضای مجازی چیست؟ چگونه طرف‌های درگیر در یک تعامل، با توجه به ویژگی‌های فضای مجازی باید به یکدیگر اعتماد کنند؟ چگونه نسبت به امن بودن تراکنش مطمئن شوند؟ چگونه از سوء استفاده خرابکاران در فضای مجازی در امان باشند؟ ...

یکی از راه‌کارهای عملی برای رفع مشکلات تعامل در فضای مجازی، استفاده از زیر ساخت کلید عمومی (PKI) می‌باشد. زیرساخت کلید عمومی کشور، با هدف ایجاد امنیت و اعتماد در فضای تبادل اطلاعات، احراز هویت در فضای مجازی در سطح ملی و بین المللی، و در نهایت جلب اعتماد در استفاده از خدمات الکترونیکی شکل گرفته‌است.

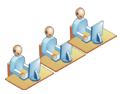
زیرساخت کلید عمومی کشور به عنوان یکی از ابزارهای ایجاد اعتماد، درواقع چارچوبی برای تولید، توزیع، کنترل، ممیزی و ابطال گواهی‌های الکترونیکی فراهم می‌کند. در این زیرساخت از گواهی‌های الکترونیکی صادره توسط مراکز صدور گواهی الکترونیکی میانی استفاده می‌کند تا اعتبار طرفین یک تراکنش الکترونیکی را ممیزی وتصدیق‌نماید.

زیرساخت کلید عمومی مطابق قانون تجارت الکترونیکی و آیین نامه ماده ۳۲ آن، دارای ساختار سلسله مراتبی نهادهای متولی در زیرساخت کلید عمومی کشور مطابق شکل زیر می‌باشد:



گواهی الکترونیکی چیست؟

گواهی‌ها جزء اساسی زیرساخت کلید عمومی هستند و راهکاری عملی جهت ایجاد امنیت و اعتماد در فضای مجازی در کاربردهای مختلف می‌باشند. وظیفه صدور گواهی الکترونیکی بر عهده مراکز صدور گواهی الکترونیکی می‌باشد. این گواهیها مطابق با سطح امنیتی تعریف شده، بر روی سخت‌افزارهایی نظیر: کارت هوشمند، توکن‌های USB و ... صادر می‌شوند که به آنها سخت‌افزارهای PKI می‌گویند.
گواهی الکترونیکی، فایل الکترونیکی است که حاوی مجموعه‌ای از اطلاعات در مورد مالک گواهی، مرکز صادر کننده گواهی، تاریخ صدور و انقضاء گواهی، حوزه کاربرد، ... می‌باشد. این گواهی :


بر اساس تأیید هویتی که توسط یک دفترثبت نام (RA) انجام می‌گیرد، صادر می‌شود.


برای افراد حقیقی، حقوقی و وسایل کاربردی صادر می‌گردد.


حاوی کلید عمومی مالک گواهی است.

دربردارنده مورد استفاده یا کاربرد گواهی است.

انـواع کاربردهـای گواهی الکترونیکی

گواهی امضای الکترونیکی - عملیات امضاء با اسـتفاده از این گواهی انجـام می‌گیـرد.

گواهی مهرسازمانی - در نقش یک مهر برای سازمان مورد استفاده قرار می‌گیـرد.

گواهی احراز هویت - جهت شناسایی و احراز هویت استفاده می‌گردد.

گواهی سـرور - در کاربردهایی نظیر SSL، گواهی تجهیزات شـبکه اسـتفاده می‌گردد.

گواهی پسـت الکترونیکی امن - جهت کاربرد ایمیل استفاده می‌گردد.

گواهی امضای کد - برنامه نویسان جهت جلوگیری از تغییر کد توسط افراد غیرمجاز اسـتفاده می‌کنند.

گواهی مراکزمهرزمانی - جهت ثبت زمان دقیق بر روی اسـناد الکترونیکی اسـتفاده می‌شـود.

برخی نمونه های کاربردی گواهی الکترونیکی

- امضا و محرمانگی اسـناد
- احراز اصالت اسـناد و داده های الکترونیکی
- مبـادلات تجـاری الکترونیکـی امـن
- تراکنـش هـای بانکـی امـن (بانکـداری الکترونیکـی)
- صـدور مجـوز جهـت انجـام عملیـات
- ارتباط با سـرویس‌دهنده‌ها در کانال ارتباطی امن
- رای‌گیـری الکترونیکـی
- بیمـه الکترونیکـی
- سـلامت الکترونیکی
- آمـوزش الکترونیکـی
- دولـت الکترونیکـی

مرکز دولتی صدور گواهی الکترونیکی

مرکز دولتی صدور گواهی الکترونیکی ریشه بر طبق آیین نامه ماده ۳۲ قانون تجارت الکترونیک، مسئول مجوز ایجاد، امضا، صدور و ابطال گواهی الکترونیکی، مراکز صدور گواهی الکترونیکی میانی می‌باشد. برخی از وظایف این مرکز به شرح ذیل می‌باشد

- مسئولیت تمام ابعاد صدور و مدیریت مراکز صدور گواهی الکترونیکی میانی، شامل نظارت بر فرایندهای ثبت نام، احراز هویت، صدور گواهی‌های میانی، انتشار و ابطال گواهی‌ها و تجدید کلید
- تضمین تطابق تمام ابعاد خدمات و عملیات این مرکز با زیرساخت مربوط به صدور گواهی الکترونیکی، تحت سیاست‌های گواهی الکترونیکی و مطابق با خواسته ها و ضمانت‌های آن سیاست‌ها.

لازم به ذکر است وظیفه صدور گواهی موجودیتهای نهایی برعهده مراکز صدور گواهی الکترونیکی میانی اعم از دولتی و یا خصوصی می‌باشد.

واحد تدوین ،سیاست‌ها دستورالعمل ها و رویه ها

- تدوین و بکارگیری ملزومات و خط و مشـی ها، جهت اعمال یکپارچگی و انسـجام بسـترهای زیرسـاخت کلید عمومی؛
- ارائه پیشـنهاد تدوین مقررات و آیین‌نامه‌های مربوطه

واحد مراکز صدور گواهی الکترونیکی میانی

- هماهنگی و مدیریت راه‌اندازی مراکز صدور گواهی الکترونیکی در کشـور
- هماهنگی، مدیریت منسـجم و نظارت برفعالیت‌های مراکز صـدور گواهی الکترونیکی میانی در کشـور به منظور حصول اطمینان از عملکرد صحیح مراکز میانی

واحد آزمایشگاه‌ها

- آزمایشگاه تست و ارزیابی محصولات صدور و مدیریت گواهی الکترونیکی
- آزمایشگاه تست و ارزیابی برنامه های کاربردی مجهز به زیرساخت کلید عمومی (PKE)
- آزمایشگاه تست وارزیابی ماژولهای امنیتی
- آزمایشگاه الگوریتمهای PKI

واحد تحقیق و توسعه

- تحقیق و پژوهش به منظور برنامه‌ریزی جهت تسهیل در ایجاد و توسعه زیرساخت‌های امنیتی
- تحقیق و پژوهش در حوزه کاربردهای مختلف امضای دیجیتال و توسعه کاربردهای آن
- تحقیق و پژوهش در زمینه الگوریتم ها و پروتکل های امنیتی موثر در زمینه زیر ساخت کلید عمومی

خدمات و سرویس‌ها

- مشاوره راه‌اندازی و تاسیس مراکز صدور گواهی الکترونیکی میانی
  - مشاوره در امور تدوین اسناد
  - مشاوره در امور تجهیز مراکز داده صدور گواهی
- مشاوره تجهیز برنامه کاربردی به زیرساخت کلید عمومی
  - برگزاری کارگاه‌های آشنایی با مفاهیم PKE
  - مشاوره پیاده‌سازی فنی
- مشاوره جهت ارزیابی تجهیزات سخت‌افزاری و نرم‌افزاری در آزمایشگاه‌های PKI
  - مشاوره در امور چگونگی ارزیابی
  - مشاوره جهت رفع مشکلات محصولات و بهبود آنها

خلاصه وضعیت عملکرد مرکز دولتی صدور گواهی الکترونیکی ریشه

PKE چیست؟

جهت اســتفاده از گواهی الکترونیکی در یک ســامانه، لازم اســت قابلیت اســتفاده از گواهی الکترونیکی به آن سامانه افزوده شود. قابلیت بهره گیری از گواهی الکترونیکی و فراتر از آن زیرساخت کلید عمومی در سیستم‌ها را Public Key Enabling یا به اختصار PKE گوییم. عملیات PKE کردن می‌باید توســط کارشناسان نرم‌افزار ارائه شــود و به ســامانه مورد نظر اضافه گردد.

آنچه اهمیت دارد این اســت که ســامانه‌ها باید بتوانند بمنظور

- محرمانگــی
- شناســایی
- احــراز هویــت
- جامع بودن و دســت نخوردگی اطلاعات

و همچنین امضای آنها مورد اســتفاده قرار گیرند. با این امر می‌توان مطمئن بود اطلاعات خوانده نشــده، تغییر نکرده، جعل نشــده و کاملا امن منتقل می‌شــوند.

تجهیز ســامانه ها به زیرســاخت کلید عمومی و اضافه کردن قابلیت اســتفاده از گواهی الکترونیکی در سامانه‌ها می‌باید بر اســاس مجموعه ای از اســتانداردها و الزامات صورت پذیرد.

اســتانداردهای زیرســاخت کلید عمومی مصوب شــورای سیاســتگذاری گواهی الکترونیکی کشور

- **پروفایل‌های گواهی الکترونیکی**
- **الگوریتم‌های زیرساخت کلید عمومی**
- **پروتکل‌های مدیریتی**
- **پروتکل‌های عملیاتی**
- **پروتکل‌های زنجیره گواهی**
- **ماژولهای امنیتی سخت‌افزاری**
- **ملزومات برنامههای کاربردی مجهز به زیرساخت کلید عمومی کشور**

آزمایشگاه ارزیابی سخت افزارهای PKI

گواهی های الکترونیکی به صورت نرم‌افزاری و یا بر روی سخت افزارهای PKI از قبیل کارت های هوشمند ، توکنهای USB و HSM صادر می‌شـوند. انتخاب یکی از این موارد مذکور، بسـتگی به سطح امنیت گواهی الکترونیکی فرد متقاضی گواهی دارد. صدور گواهی الکترونیکی به صورت نرم‌افزاری کمترین و HSM دارای بالاترین سطح امنیتی اسـت. از آن جایی‌که سـخت‌افزارها بعنوان یکی از مهمترین ارکان اعمال امنیت و اعتمادسازی در تراکنش های الکترونیکی و انجام عملیات امضای دیجیتال، محسوب می گردند، مهم است که بدانیم؛

آیا کارت های هوشمند، توکن های USB و HSM های ارائه شده در بازار، دارای امنیت لازم هستند؟

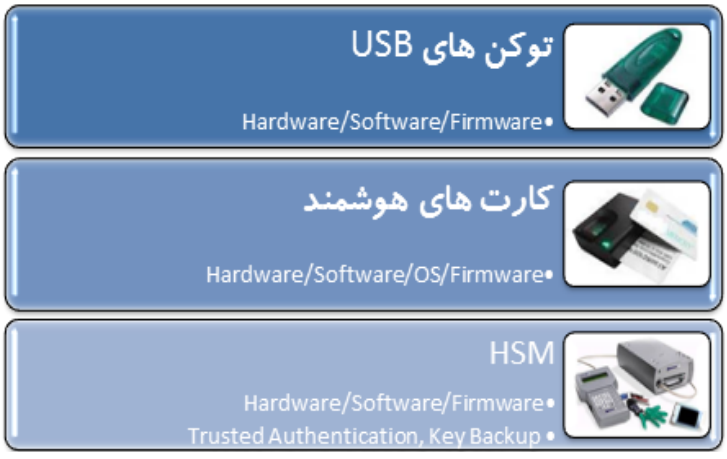
سخت افزارهای PKI بصورت بالقوه و بالفعل ممکن است دارای آسیب پذیری های امنیتی بسیار جدی و بحرانی باشند. پاره ای از این آسیب پذیری ها شامل موارد ذیل می باشند:

- وجود رخنه های امنیتی تعمدی و غیر تعمدی؛
- امکان استخراج و جعل کلیدهای محرمانه و مدیریت کلید ضعیف؛
- عدم اجرای درست و مطمئن الگوریتم های رمزنگاری؛
- امکان تغییر مشخصه های حساس و فقط خواندنی کلید؛
- عدم تعامل پذیری مناسب؛
- امکان اعمال انواع حملات سخت افزاری و نرم افزاری

راه حل: بکارگیری محصولات دارای گواهی تاییدیه PKI : ویژه سخت افزارهای PKI

آزمایشـگاه ارزیابی سخت افزارهای PKI با هدف تسـت و ارزیابی انواع سخت افزارهای PKI توسط مرکز دولتی صدور گواهی الکترونیکی ریشه راه اندازی شده است. این آزمایشگاه ارزیابی های خود را با بکارگیری انواع تجهیزات سـخت-افزاری و نرم افزاری در حوزه های عملیاتی و انطباق با اسـتانداردهای ملی و بین المللی، امنیت، کارایی و پایداری انجام می دهد. عبور موفقیت آمیز یک محصول از آزمون های آزمایشگاه، منجر به اعطای گواهی تاییدیه PKI برای آن محصول خواهد شد.

محصولات تحت آزمون



آزمایشگاه ارزیابی نرم افزارهای PKE

نرم افزارهای PKE به نرم افزارهایی گفته می شـود که از قابلیت‌های گواهی الکترونیکی اسـتفاده می‌کنند، این نرم‌افزارها قابلیت انجام عملیات امضای دیجیتال را دارا می باشند.

امضای دیجیتال، اعتماد یا عدم اعتماد؟

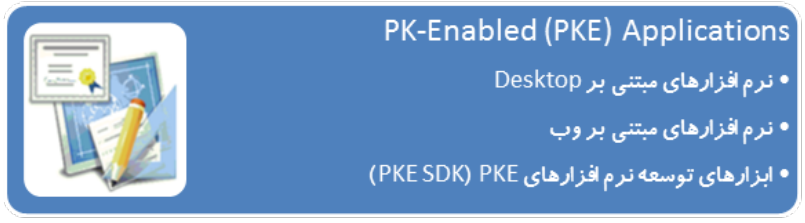
نرم افزارهای PKE بدون استانداردسـازی و اعمال الزامات لازم دارای آسیب پذیری های امنیتی و اشکالات بسیار جدی و بحرانی باشند. پاره ای از این آسیب پذیری ها و اشکالات شامل موارد ذیل می باشد:

- عدم اطمینان از امضای اطلاعات درست و مورد نظر؛
- عدم انجام فرآیند احرازهویت بصورت درست و مطمئن؛
- دسترسی غیر مجاز؛
- خطر جعل امضا؛
- عدم انجام درست و مطمئن عملیات اعتبارسنجی زنجیره گواهی؛
- مدیریت کلید ضعیف؛

راه حل: بکارگیری نرم افزارهای دارای گواهی تاییدیه PKI : ویژه نرم افزارهای PKE

آزمایشگاه ارزیابی نرم افزارهای PKE با هدف تست و ارزیابی انواع نرم افزارهای PKE توسط مرکز دولتی صدور گواهی الکترونیکی ریشـه راه اندازی شـده است. این آزمایشـگاه ارزیابی های خود را با بکارگیری انواع تجهیزات سخت-افزاری و نرم افزاری در حوزه های مختلف شامل امنیت، انطباق پذیری با استانداردهای ملی و بین المللی، استفاده-پذیری و پایداری انجام می دهد. عبور موفقیت آمیز یک نرم افزار از آزمون های آزمایشگاه، منجر به اعطای گواهی تاییدیه PKI برای آن نرم افزار خواهد شد.

محصولات تحت آزمون



آزمایشگاه ارزیابی الگوریتم

زیرساخت کلید عمومی یا PKI از الگوریتم های مختلف رمزنگاری جهت ارائه خدمات اعتمادسازی در فضای مجازی استفاده می‌کنند. بنابراین یکی ارکان بسیار مهم امنیت در این زیرساخت وابسته به امنیت الگوریتم های رمزنگاری می-باشد.

آیا الگوریتم های رمزنگاری در PKI قابل اعتماد هستند؟

الگوریتم های رمزنگاری بکارگرفته شـــده در سخت افزارها و نرم افزارهای PKI بعنوان هسته اصلی امنیت در این محصولات ممکن است دارای آسیب پذیری های و روزنه های امنیتی بسیار جدی و بحرانی باشند. پاره ای از این آسیب-پذیری ها شامل موارد ذیل می باشند:

- وجود رخنه های امنیتی؛
- تولید کلیدهای ضعیف و آسیب پذیر؛
- عدم اجرای درست و مطمئن الگوریتم های رمزنگاری؛
- بکارگیری الگوریتم های رمزنگاری جعلی؛
- عدم پیاده سازی درست و مطمئن الگوریتم های رمزنگاری؛
- عدم انطباق با استانداردها و عدم تعامل پذیری مناسب؛

راه حل: استفاده از محصولات دارای گواهی تاییدیه PKI : ویژه الگوریتم های رمزنگاری

آزمایشگاه ارزیابی الگوریتم با هدف تست و ارزیابی انواع الگوریتم های رمزنگاری پذیرفته شده در زیرساخت کلید عمومی کشور راه اندازی شده است. این آزمایشگاه ارزیابی های خود را بر اساس مکانیزم های استاندارد و پذیرفته شده بین المللی، روال های طراحی شده داخلی و از طریق تجهیزات نرم افزاری و سخت افزاری مختلف و نزدیک به ده هزار بردار آزمون انجام می دهد.

الگوریتم های تحت آزمون

الگوریتم های متقارن	AES, 3DES• Encryption/Decryption/MACing•
الگوریتم های نامتقارن	RSA Algorithm • Signing, Verification, Encryption, Decryption •
الگوریتم های بدون کلید	Hash Functions: SHA1, SHA2 • RNGs •

آزمایشگاه ارزیابی سامانه های صدور و مدیریت گواهی الکترونیکی

در یک زیرساخت کلید عمومی، لازم است مراکز صدور گواهی الکترونیکی (مراکز CA) از طریق سامانه های نرم-افزاری و سخت افزاری امن و مورد اطمینان عملیات صدور و مدیریت گواهی الکترونیکی را انجام دهند تا بتوانند بعنوان مراجع اعتماد، خدمات مرتبط با امضای دیجیتال و گواهی الکترونیکی را ارائه نمایند.

مراکز صدور گواهی الکترونیکی (CA) دارای امنیت لازم و کافی هستند؟

سامانه های صدور و مدیریت گواهی الکترونیکی در مراکز CA بدلیل حساسیت بسیار بالا لازم است بطور دقیق ارزیابی شده و مورد بازرسی دوره ای قرار گیرند. پاره ای از این آسیب پذیری هایی که ممکن است در این سامانه ها وجود داشته باشد، شامل موارد ذیل می باشند:

- عدم ارتباط درست و مطمئن اجزای مختلف سامانه؛
- عدم تعامل پذیری درست و مطمئن، ناپایداری و عدم کارایی سامانه؛
- عدم رعایت سیاست ها، استانداردها و الزامات تعیین شده در زیرساخت کلید عمومی کشور؛
- عدم برآورده سازی سطح اطمینان لازم و کافی جهت ارائه خدمات صدور و مدیریت گواهی الکترونیکی؛
- عدم اعمال کنترل دسترسی مناسب؛
- مدیریت کلید ضعیف

راه حل: بکارگیری محصولات دارای گواهی تاییدیه PKI : ویژه سامانه¬های مرتبط با CA

آزمایشگاه ارزیابی سامانه های صدور و مدیریت گواهی الکترونیکی با هدف تست و ارزیابی انواع مولفه های سخت-افزاری و نرم افزاری مورد استفاده در مراکز صدور گواهی الکترونیکی، توسط مرکز دولتی صدور گواهی الکترونیکی ریشه راه اندازی شده است. این آزمایشگاه ارزیابی های خود را با بکارگیری انواع تجهیزات سخت افزاری و نرم افزاری در حوزه های مختلف انجام می دهد. عبور موفقیت آمیز یک محصول از آزمون های آزمایشگاه، منجر به اعطای گواهی تاییدیه PKI برای آن محصول خواهد شد.

مولفه های قابل ارزیابی در آزمایشگاه

نشانی پستی: تهران- بلوار کشاورز- خیابان شهید نادری
جنب کوچه حجت دوست- ساختمان نادری
وزارت صنعت، معدن و تجارت- طبقه پنجم-
مرکز دولتی صدور گواهی الکترونیکی ریشه
کد پستی ۱۴۱۶۶۴۳۸۵۱
شماره تلفن ۸۵۱۹۳۷۱۱
شماره فاکس ۸۸۹۶۸۰۷۲
وب‌سایت مرکز www.rca.gov.ir