آشنایی با رسید دیجیتالی (امضای الکترونیکی)

نگاهی فنی

این راهنما خلاصه ای است برای آشنایی شما با تکنولوژی استاندارد امضای دیجیتالی (Digital Certificate) و PKI.

امضای دیجیتالی به این معناست که طرف مصرف کننده و طرف تجاری بتوانند از امنیت ارتباطات و برنامه ها با استفاده از PKI (Public Key Infrastructure) بهره برداری کنند.

لزوم امنیت بر روی اینترنت !

ما اکنون درحال سپری کردن عصر اطلاعات هستیم. تعداد افراد و تجارتهایی که هر روزه به اینترنت ملحق میشوند به صورت بی سابقه ای در حال افزایش است . درحالیکه هر روز دسترسی به اینترنت آسان تر و سرعت آن سریعتر و قیمت آن ارزان تر میشود ، بسیاری از افراد میزان زیادی از وقت خود را بر روی اینترنت به تبادل اطلاعاتشان و همچنین تبادلات مالی میپردازند.

درحالیکه اینترنت یک شبکه ارتباطی باز است. هرکسی میتواند از اینترنت استفاده کند ، و درنتیجه هرکسی میتواند از آن برای استخراج اطلاعات از مناطق آسیب پذیر ، برای مقاصد سودجویانه و غیرقانونی استفاده کند. اگر اینترنت بخواهد به منبعی برای استفاده اهداف تجاری و انتقال اطلاعات تبدیل شود مطمئنا به یک بنیاد و مؤسسه امنیت هم نیاز دارد.

امنیت چه چیزی را تامین میکند ؟

تصدیق هویت / شناسایی

اطمینان از اینکه شخص یا طرفی که با آن درحال ارتباط هستیم همان کسی است که ما انتظار داریم و خودش میگوید.

محرمانه بودن

اطلاعات درون پیغامها و یا تبادلات محرمانه میشود. و تنها برای اشخاص دریافت کننده و ارسال کننده قابل فهم و خواندن میباشد .

امانت داری

اطلاعاتی که درون پیغام و یا تبادلات وجود دارد در طول مسیر به صورت اتفاقی یا عمدی مورد دستبرد قرارنمیگیرد .

غیر قابل انکار

ارسال کننده نمیتواند منکر ارسال پیام یا تبادل مالی شود ، و دریافت کننده هم نمیتواند منکر دریافت آن شود.

کنترل دسترسی

دسترسی به اطلاعات حفظ شده تنها برای طرفین و اشخاص انتخاب شده میسر میباشد.

PKI چیست ؟

PKI (Public Key Infrastructure) ، بازمیگردد به، تکنولوژی ، مراحل عملیاتی و خط مشیی که مجموعا محیطی را برای مقاصد تامین امنیت مطابق پاراگراف فوق فراهم میسازد – شناسایی ، محرمانه بودن ، امانت داری ، انکارناپذیری و کنترل دسترسی .

PKI به مردم و تجار این امکان را میدهد که از نرم افزارها و ابزارهای امن اینترنتی بهره ببرند. به طور مثال ترکیب قانونی و امن ایمیل و تبادلات مالی تحت اینترنت و انتقال خدمات، تماما در سایه PKI تحقق میابد.

PKI دو عامل اصلی را به خدمت میگیرد: کلید عمومی رمزگذاری و گواهینامه اعتبار.

پنهان سازی و آشکارسازی

فایده های PKI در استفاده ازکلید عمومی رمزگذاری مشخص میشود. اساسی ترین ثمره کلید عمومی رمزگذاری همان پنهان سازی (رمزگذاری) و آشکارسازی (رمزگشایی) اطلاعات دیجیتالی میباشد.

پنهان سازی (رمزگذاری) ، تبدیل اطلاعات به صورت اطلاعات اتفاقی و نامفهوم میباشد. حالت بدون معنای آن ما را از محفوظ ماندن اطلاعات رمزگذاری شده حتی اگر افراد غیر مجاز به آنها دسترسی پیدا کنند ، مطمئن میسازد.

تنها راه جهت تبدیل اطلاعات به صورت قابل فهم انجام عملیات عکس عملیات پنهان سازی (رمز گذاری) است که با نام آشکارسازی (رمزگشایی) معروف است . رمزگذاری عمومی شامل پنهان سازی و آشکارسازی، بوسیله کلیدهای عمومی و خصوصی انجام میگیرد.

کلیدهای عمومی و کلیدهای خصوصی

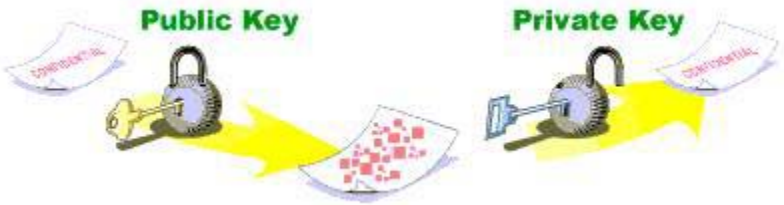
کلیدهای عمومی و خصوصی هردو از دو کلید رمزگذاری مرتبط و مجزا (معمولا رشته بلندی از اعداد) تشکیل شده اند. در زیر نمونه ای از یک کلید عمومی را مشاهده میکنید.

3048 0241 00C9 18FA CF8D EB2D EFD5 FD37 89B9 E069 EA97 FC20 5E35
F577 EE31 C4FB C6E4 4811 7D86 BC8F BAFA 362F 922B F01B 2F40 C744
2654 C0DD 2881 D673 CA2B 4003 C266 E2CD CB02 0301 0001

کلید عمومی همانی است که ازمعنای آن استخراج میشود – عمومی . این کلید دراختیار تمام کسانی که از یک منبع خاص یا فهرست مشخص استفاده میکنند قراردارد. در حالیکه کلید خصوصی بایستی به صورت محرمانه نزد دارندگان مجاز آن باقی بماند.

چون هردو کلید به صورت محاسباتی به هم مربوط میباشند ، هرچیزی که با یک کلید عمومی رمزگذاری میشود تنها با کلید خصوصی مربوط به آن قابل رمزگشایی است و بالعکس .

برای مثال ، اگر **باب** بخواهد اطلاعات محرمانه ای را برای **آلیس** ارسال کند ، و میخواهد مطمئن باشد که تنها آلیس قابلیت دسترسی و خواندن آن را داشته باشد او میتواند با کلید عمومی آلیس آنرا رمزگذاری کند . تنها آلیس به کلید خصوصی مربوطه خودش دسترسی دارد در نتیجه تنها شخصی که قابلیت رمزگشایی اطلاعات رمزگذاری شده را دارد آلیس است .



چون آلیس تنها کسی است که به کلید خصوصی خود دسترسی دارد، لذا تنها کسی است که قابلیت خواند اطلاعات رمزگذاری شده را دارد. حتی اگر شخصی هم به اطلاعات رمزگذاری شده دسترسی پیدا کند چون به کلید خصوصی آلیس دسترسی ندارد، نمیتواند آنرا بخواند.

کلیدهای عمومی اینگونه امنیت را به ارمغان میآورند. درحالیکه یکی دیگر از قابلیتهای مهم کلید عمومی رمزگذاری، امکان بوجود آوردن امضای الکترونیکی (دیجیتالی) میباشد.

امضای دیجیتالی

امضای دیجیتالی برای ایمیل و فایلهای اطلاعاتی همان کاری را انجام میدهد که امضای شما بر روی یک مدرک کاغذی انجام میدهد. امضای دیجیتالی اصل بودن و صداقت یک پیغام یا سند و یا فایل اطلاعاتی را تضمین میکند.

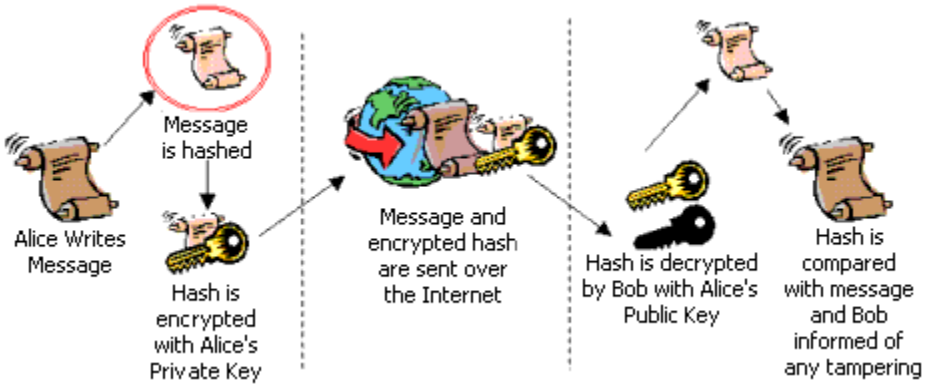
چگونه یک امضای دیجیتالی درست کنیم؟

بوجود آمدن یک امضای دیجیتالی مراحل محاسباتی پیچیده ای دارد. درحالیکه این مراحل پیچیده بوسیله کامپیوتر انجام میگیرد ، درست کردن امضای دیجیتالی دیگر حتی از یک امضای دستی هم آسان تر است.

مراحل زیر نشان دهنده اعمالی است که در حین ساخته شدن یک امضای دیجیتالی صورت میگیرد:

۱) آلیس دکمه "sign" را در نرم افزار ایمیل خود کلیک میکند و یا فایلی را که نیاز به امضا دارد انتخاب میکند.
۲) کامپیوتر آلیس رمزگذاری را محاسبه میکند . (پیغام به یک تابع عمومی جهت رمزگذاری برده میشود)
۳) این تابع توسط کلید خصوصی آلیس رمزگزاری شده است (در این حالت آنرا کلید امضا میخوانیم) برای بوجود آوردن یک رمز دیجیتالی .
۴) پیغام اصلی و امضای دیجیتالی آن برای باب ارساب میشود.
۵) باب پیغام امضا شده را دریافت میکند. درآنجا مشخص شده است که این پیغام امضا شده است ، و نرم افزار ایمیل باب میداند که چگونه آن امضا را تایید کند.
۶) کامپیوتر باب امضای دیجیتالی آلیس را توسط کلید عمومی آلیس رمزگشایی میکند.
۷) کامپیوتر باب کد رمزگذار را از امضای دیجیتالی استخراج میکند.
۸) سپس کامپیوتر باب کدرمزگذاری را که خود استخراج کرده است با کدی که با پیغام آلیس ارسال شده است مطابقت میکند.

شکل زیر همین مراحل را نشان میدهد :

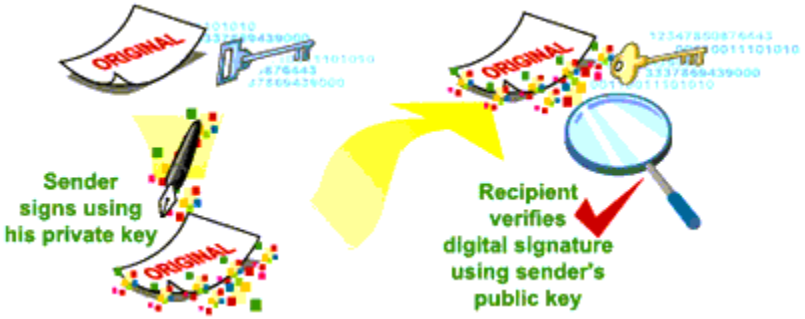


اگر پیغام آلیس صحیح انتقال یافته باشد و در طول راه مورد دستبرد واقع نشده باشد هردو کلید استخراج شده یکسان میباشند.

اگر دو کد رمزگذاری که استخراج شده اند با یکدیگر مطابقت نداشته باشند صلاحیت نامه منتفی است. اگر پیغام اصلی مورد سرقت قرارگرفته باشد کدرمزگذاری که در کامپیوتر باب استخراج میشود متفاوت خواهد بود و در اینصورت کامپیوتر باب به او اطلاع خواهد داد.

مناشاء ، درستی و انکارناپذیری

جولیا ، که میخواهد خود را بجای آلیس جا بزند ، نمیتواند کدی را همانند امضای دیجیتالی آلیس تولید کند زیرا او کلید خصوصی آلیس را ندارد. اگر درمقابل ، جولیا بخواهد محتویات نامه آلیس را در حین انتقال دستکاری کند ، پیغام مورد دستبرد قرارگرفته، کدی را غیر از کد پیغام اصلی تولید میکند ، و کامپیوتر باب قابلیت شناسایی آنرا خواهد داشت. بعلاوه ، آلیس نمیتواند ارسال نامه به باب را انکار کند زیرا که به صورت دیجیتالی و با استفاده از کد خصوصی او امضا شده است، که باعث انکارناپذیر بودن آن میشود.



با توجه به قانون عمومی امضای دیجیتالی آلیس ممکن است که یک تبادل مالی ، یا یک پیغام و یا یک فایل اطلاعاتی را امضا کند، و با توجه به اینکه اگر دریافت کننده امضا را با موفقیت تایید کند این مفهوم به راحتی قابل اثبات است که آلیس این تبادل مالی را انجام داده و یا آن پیغام را نوشته است.

قبلا گفتیم که کلیدهای عمومی در دسترس همه قراردارند ، سؤال بعدی این است که چگونه آنرا به صورتی امن ، محافظت شده و قابل دسترسی در اختیار همه قرار دهیم . به طور کلی از یک فایل بسیار کوچک استفاده میکنیم که به آن گواهینامه دیجیتالی میگوییم.

گواهینامه دیجیتالی چیست و چرا ما به یکی نیاز داریم؟

یک گواهینامه دیجیتالی یک فایل دیجیتالی است که به صورت رمزگذاری شده ای حاوی اطلاعاتی از قبیل کلید عمومی و سایر اطلاعات دارنده خود است. دارنده میتواند یک شخص ، یک شرکت ، یک سایت و یا یک نرم افزار باشد. مانند یک گواهینامه رانندگی که عکس صاحب خود را به همراه سایر اطلاعات در مورد دارنده آن، شامل میشود ، یک گواهینامه دیجیتالی نیز یک کلید عمومی را به اطلاعاتی در مورد دارنده آن متصل میکند.

در کلام دیگر ، گواهینامه دیجیتالی آلیس ، تصدیق میکند که کلید عمومی به او و تنها او تعلق دارد. به همراه کلید عمومی ، یک گواهینامه دیجیتالی حاوی اطلاعاتی در مورد شخص حقیقی یا حقوقی دارنده آن میباشد ،که برای شناسایی دارنده، و (براین اساس که گواهینامه ها محدود میباشند) ، تاریخ ابطال آنرا نمایش میدهد.

گواهینامه دیجیتالی و دفاتر صدور گواهینامه

گواهینامه های دیجیتالی به وسیله دفاتر صدور گواهینامه (CA) صادر میشوند. مانند دفاتر قابل اطمینانی که برای صدور گواهینامه رانندگی و یا گذرنامه مشخص شده اند. دفاتر CA (Certificate Authorities) تعیین کننده وظیفه اشخاص ثالث برای قبول کردن گواهینامه های دیجیتالی ، معتبرکردن گواهینامه ها ، صدور آنها و نگهداری از وضعیت اطلاعات گواهینامه های صادر شده از اشخاص، هستند.

تلفیق و همکاری CA و PKI باعث میشود که افراد برروی اینترنت نتوانند با هویت جعلی و صدور گواهینامه های تقلبی دست به کارهای خلاف و نامشروع بزنند.

دفاتر ثانویه مطمئن صادرکننده گواهینامه ، هویت شخص دارنده گواهینامه را قبل از آنکه تصدیق کنند ، چک میکنند . بخاطر اینکه گواهینامه دیجیتالی اکنون یک فایل اطلاعاتی کوچک است ، اصل بودن آن توسط امضای دیجیتالی خودش

قابل بررسی است. لذا به همان صورتی که یک امضای دیجیتالی را تایید میکنیم به همان صورت از صحت امضای دیجیتالی به اصل بودن گواهینامه پی خواهیم برد.

چون دفاتر صدور گواهینامه (CA) قابل اطمینان هستند ، دسترسی به کلیدهای عمومی آنها برای امضای گواهینامه های دیجیتالی از راه های بسیاری ممکن میباشد.

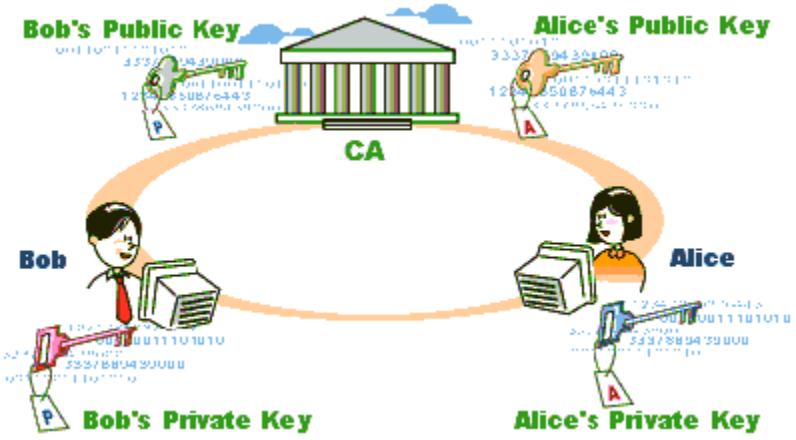
گواهینامه های دیجیتالی تحت قالب توصیه نامه های فنی " گواهینامه های دیجیتالی X.509 " و توسط سازمان ارتباطات بین المللی – بخش استانداردهای ارتباطی (ITU-T) ، صادر میشوند.

ثبت نام برای یک گواهینامه دیجیتالی

کاربران میتوانند از طریق وب برای یک گواهینامه دیجیتالی ثبت نام کنند. پس از کامل شدن فرمهای مورد نیاز ، مرورگر اینترنت کاربر یک جفت کلید عمومی درست میکند. نیمی از این کلید عمومی به دفتر صدور گواهینامه برای درج در مشخصات دارنده آن ارسال میشود. درحالیکه کلید خصوصی کاربر بر روی کامپیوتر او در جایی امن (هارد دیسک ، فلاپی درایو و ...) نگهداری خواهد شد.

دفتر صدور گواهینامه در ابتدا ملزم به تایید اطلاعات ارسال شده توسط کلید عمومی کاربر میباشد. اینکار از جازدن کسی به جای کسی دیگر و احتمال وقوع تبادلات نامشروع و غیرقانونی جلوگیری میکند.

اگر اطلاعات ارسال شده درست باشند ، دفتر صادرکننده گواهینامه ، یک گواهینامه دیجیتالی برای متقاضی خود صادر میکند . بمحض صدور ، دفتر صادرکننده گواهینامه امضای دیجیتالی را در یک بایگانی عمومی نگهداری میکند.



پخش کردن گواهینامه دیجیتالی

درحالیکه گواهینامه دیجیتالی در یک بایگانی عمومی ذخیره شده است ، نیز میتواند با استفاده از امضای دیجیتالی پخش گردد. به طور مثال زمانیکه آلیس نامه ای را برای باب به صورت دیجیتالی امضا میکند ، او همچنین گواهینامه خود را به آن نامه پیوست میکند. لذا همزمان با دریافت نامه دیجیتالی باب میتواند معتبر بودن گواهینامه آلیس را نیز بررسی کند. اگر با موفقیت تایید شد ، هم اکنون باب کلید عمومی آلیس را دارد و نیز میتواند اعتبار نامه ارسالی از طرف آلیس را بررسی کند.

انواع مختلف گواهینامه های دیجیتالی

برحسب نوع استفاده از گواهینامه دیجیتالی ، چند نمونه مختلف از آن موجود میباشد :

- **شخصی** : قابل استفاده توسط اشخاص حقیقی برای امضای ایمیل و تبادلات مالی.
- **سازمانها** : قابل استفاده توسط اشخاص حقوقی برای شناساندن کارمندان برای ایمیلهای محفوظ و تبادلات تحت اینترنت.
- **سرور** : برای اثبات مالکیت یک دامین اینترنتی و برقراری SSL / TSL های رمزگذاری شده ما بین وب سایت و کاربران.
- **تولیدکنندگان** : برای اثبات حق تالیف و حفظ حقوق آن برای نشر برنامه نرم افزاری.

سطوح مختلف گواهینامه های الکترونیکی

گواهینامه های دیجیتالی در سطوح مختلفی بسته به میزان و سطح اطمینان خواسته شده از طرف متقاضی ، توسط دفاتر صدور گواهینامه موجود میباشند. در زبان ساده هرچه سطح گواهینامه بالاتر باشد به میزان بیشتری دارنده آنرا تایید میکند. یک گواهینامه سطح بالا میتواند به این معنا باشد که گواهینامه میتواند برای کارهای حساس تری مانند بانکداری آنلاین و معرفی هویت یک نفر برای تبادلات مالی و تجارت الکترونیکی ، مورد استفاده قراربگیرد.

سطح گواهینامه ارتباط نزدیکی با نوع گواهینامه دارد . سطوح پایین شامل اطلاعات شخصی کمتری و یا بدون اطلاعات شخصی میباشند (به طور مثال فقط یک آدرس ایمیل) . گواهینامه های متعلق به چنین سطحی میتوانند برای ارسال ایمیل حفاظت شده بکار بروند ، درحالیکه برای اثبات گواهینامه یک مؤسسه و یا یک سازمان نیاز به اطلاعات بیشتری و درنتیجه سطح بالاتری از گواهینامه است.

درخواستهای دنیای حقیقی برای گواهینامه های دیجیتالی

تاکنون به صورت خلاصه تئوری مخفی در گواهینامه های دیجیتالی را و نقشی را که در تحقق PKI بازی میکند نشان دادیم . پاراگرافهای آینده نگاهی بر جنبه عملی استفاده از گواهینامه های دیجیتالی و چگونگی یافتن آنها برروی کامپیوتر شما و چگونگی نمایش داده شدن آنها ، خواهد پرداخت.

استفاده از گواهینامه های دیجیتالی برای تحقق ۵ عملیات حفاظت در اینترنت

شناسایی و هویت

دفتر صادرکننده گواهینامه ، هویت دارنده گواهینامه را در زمان امضا تعیین میکند.

محرمانگی

کلید عمومی درون گواهینامه دیجیتالی به منظور رمزگذاری اطلاعات برای حصول اطمینان از اینکه تنها فرد واجد صلاحیت دریافت، میتواند آنرا بخواند استفاده میشود.

امانت داری

بوسیله امضاکردن دیجیتالی یک نامه یا اطلاعات ، دریافت کننده توانایی تشخیص این را دارد که آیا اطلاعات در حین مسیر دستکاری شده است یا خیر.

انکارناپذیری

یک پیام امضا شده اصل بودن خود را اثبات میکند ، به صورتیکه تنها ارسال کننده امکان دسترسی به کلید خصوصی برای امضا کردن پیغام یا اطلاعات را داشته است.

کنترل دسترسی

قابلیت دسترسی میتواند از طریق گواهینامه دیجیتالی برای شناسایی (به عنوان مثال بجای رمز عبور) استفاده شود. بعلاوه ، با توجه به اینکه اطلاعات را میتوان رمزگذاری کرد ، میتوان مطمئن بود که تنها فرد مورد نظر قابلیت و اجازه دسترسی به آن را خواهد داشت.

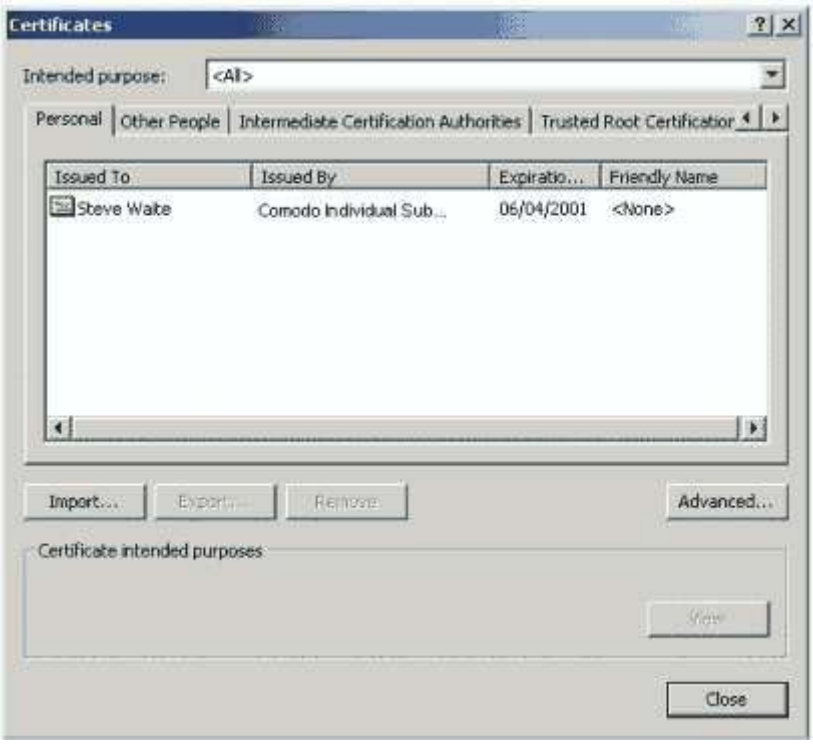
چگونه میتوانم گواهینامه های روی کامپیوتر خود را ببینم؟

شما میتوانید گواهینامه های دیجیتالی روی سیستم خود را به روش زیر ببینید :

برای استفاده کنندگان از MS Internet Explorer

۱) نرم افزار MS Internet Explorer خود را باز کنید
۲) برروی منوی Tools کلیک کنید
۳) از لیست گزینه ها ، گزینه Internet Options را انتخاب کنید
۴) صفحه Content را انتخاب کنید
۵) دکمه Certificates را فشار دهید

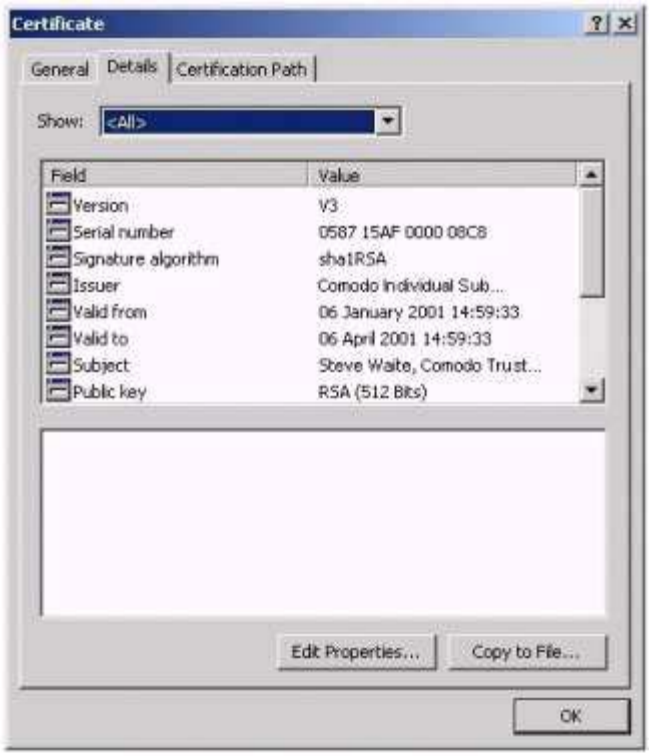
اگر برای یک یا چند گواهینامه دیجیتالی ثبت نام کرده باشید ، گواهینامه ها در بخش Personal به نمایش درخواهند آمد. اگر شما گواهینامه سایر افراد را دریافت یا دانلود کرده باشید ، آنها در بخش Other People نمایش داده خواهند شد. همچنین شما میتوانید واسطین و گواهینامه های ریشه (گواهینامه های دفاتر صدور گواهینامه) را در این پنجره ببینید.



برای بدست آوردن مشخصات خاص یک گواهینامه ، آن گواهینامه را در لیست انتخاب کنید و دکمه View را فشاردهید. سپس جزئیات گواهینامه نمایش داده میشود. این جزئیات اطلاعات کلی را در مورد گواهینامه در اختیار شما قرارخواهد گذاشت. چه کسی مالک آن است ، چه کسی آنرا صادر کرده است ، و برای چه منظوری میتواند مورد استفاده قراربگیرد.

گواهینامه فوق نشان میدهد که کلید خصوصی مربوطه نیز همراه آن است. این مطلب ما رااز اینکه گواهینامه توسط مالک خود در حال ملاحظه است مطلع میسازد (که تنها مالک دارنده کلید خصوصی میباشد).

برای مشاهده جزئیات بیشتر بر روی صفحه Details کلیک کنید. این بخش جزئیات گواهینامه را که به صورت استاندارد x.509 میباشد نشان میدهد. با کلیک کردن بر روی هر فیلد میتوانید به اطلاعات موجود در آن دست یابید.



همانطور که قبلا بحث شد ، بسیار مهم است که یک صادرکننده معتبر گواهینامه آن را صادر کرده باشد. برای همین بایستی بررسی کنیم که یک گواهینامه توسط یک صادرکننده معتبر، صادر شده است.این اطلاعات را میتوانید در Certificate Path مشاهده کنید.

برای کاربران Netscape

۱) نرم افزار Netscape را باز کنید

۲) بر روی منوی Communicator کلیک کنید

۳) از لیست بازشونده گزینه Tools و سپس گزینه Security Info را انتخاب کنید.

۴) بر روی لینک Certificates کلیک کنید تا اطلاعات بیشتری را در مورد گواهینامه های موجود به دست آورید.

کلید خصوصی من چگونه است ؟

کلیدهای خصوصی را به آسانی نمیتوان دید بخاطر اینکه بایستی محفوظ بمانند. بخش زیادی از آن در حافظه رجیستری سیستم عامل قراردارد. درحالیکه اگر تعریف شده باشد میتوان کلید خصوصی را به صورت فایلی برای بازیابی آینده ذخیره کرد.مانند یک کلید رمزگذاری ، کلید خصوصی حاوی رشته طولانی از اعداد تصادفی میباشد.

جلوگیری از استفاده غیرمجاز از کلید خصوصی

برای جلوگیری از استفاده غیر مجاز از یک کلید خصوصی (علی الخصوص زمانیکه این کلید بر روی یک کامپیوتر عمومی قراردارد) شما میتوانید سطح دسترسی برای استفاده از کلید خصوصی تعریف کنید. لذا زمانیکه کلید خصوصی مورد نیاز هست (برای رمزگشایی و امضای دیجیتالی) ، از شما خواسته میشود که اجازه استفاده از کلید خصوصی را با وارد کردن رمز تایید کنید.

این خلاصه ای بود از چگونگی و نحوه عملکرد امضای دیجیتالی و گواهینامه دیجیتالی

http://www.IranSSL.com
Security Services CA

Under protect of E.G.S. Co. Ltd.
http://www.EastGoldenStar.com