نام مقاله: مرکز صدور گواهینامه ملاحظات امنیت و تجارت

ارائه دهنده: افسانه کربلائي زاده

تاریخ ارائه:۴ /۸۳/۱۲

گروه مطالعاتی: امنیت

سرپرست گروه کاری: طیبه میرزائی

اصلاح کننده: افسانه کربلائي زاده

تاریخ اصلاح: ۸۳/۱۲/۶

بسم الله الرحمن الرحیم

مرکز صدور گواهینامه
(Certificate Authority)
CA

با توجه به گسترش روزافزون فناوری و انجام تجارت ها بـه صـورت اینترنتـی ، ایجاد فضایی امن برای اینگونه فعالیت ها امری ضروری به نظر می رسـد.
ما در این مقاله به برسـی مرکـز صـدور گواهینامـه و لـزوم ایجـاد آن در کشـور پرداخته ایم.

مرکز صدور گواهینامه چیست؟

مرکزی برای صدور گواهینامه و تایید هویت سـرویس گیرنده و سـرویس دهنده می باشـد.و بدین صورت عمل مـی کنـد کـه پـس از درخواسـت گواهینامـه از طرف کـاربر، CA بـه آن دو کلیـد خصوصـی و عمـومی داده میشـود کـه کلیـد خصوصی را در اختیار کاربر قرار میگیرد و باید در جای امنی ذخیره شود..CA با استفاده از کلید عمومی و مشخصات کاربر برای آن گواهینامه ای صـادر مـی کند ، که این گواهینامه شـامل مشخصـات کـاربر و تـاریخ اعتبـار آن و امضـای صادر کننده گواهینامه می باشد .

مرکز صدور گواهینامه دارای بخش های مختلفی است که به توضیح هر کدام از آن ها می پردازیم.

۱ - مرجع صدور گواهینامه ریشه (Root CA) :این مرکز چون باید امنیت بالایی داشته باشد و کسی به کلید خصوصی آن دسترسی پیدا نکند و به این علت وظیفه اعطا گواهینامه را بهCA محول می کند .

۲-مرجع صدور گواهینامه (CA) : این مرجع وظیفه اعطا گواهینامه را به کاربران بعهده دارد و دارای گواهینامه ای از سوی مرجع صدور گواهینامه ریشه برای اطمینان کاربران می باشد .

۳-مرجع ثبت نام (RA) : این مرجع وظیفه ثبت درخواست گواهینامه کاربر و اعلام آن بهCA و اعطا گواهینامه را ازCA به کاربر بعهره دارد .

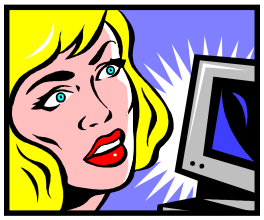
پس از گرفتن کلید خصوصی وعمومی ،کاربر امکان رمزنگاری و امضا کردن متن ارسالی را پیدا می کند .

CA ها دارای لیستی به نام CRL میباشند که در آن لیست گواهینامه هایی که کلید خصوصی آن ها لو رفته وجود دارد و آن را به صورت مداوم به اطلاع کاربران می رساند.

I am Alice

Is KU_A really Alice's

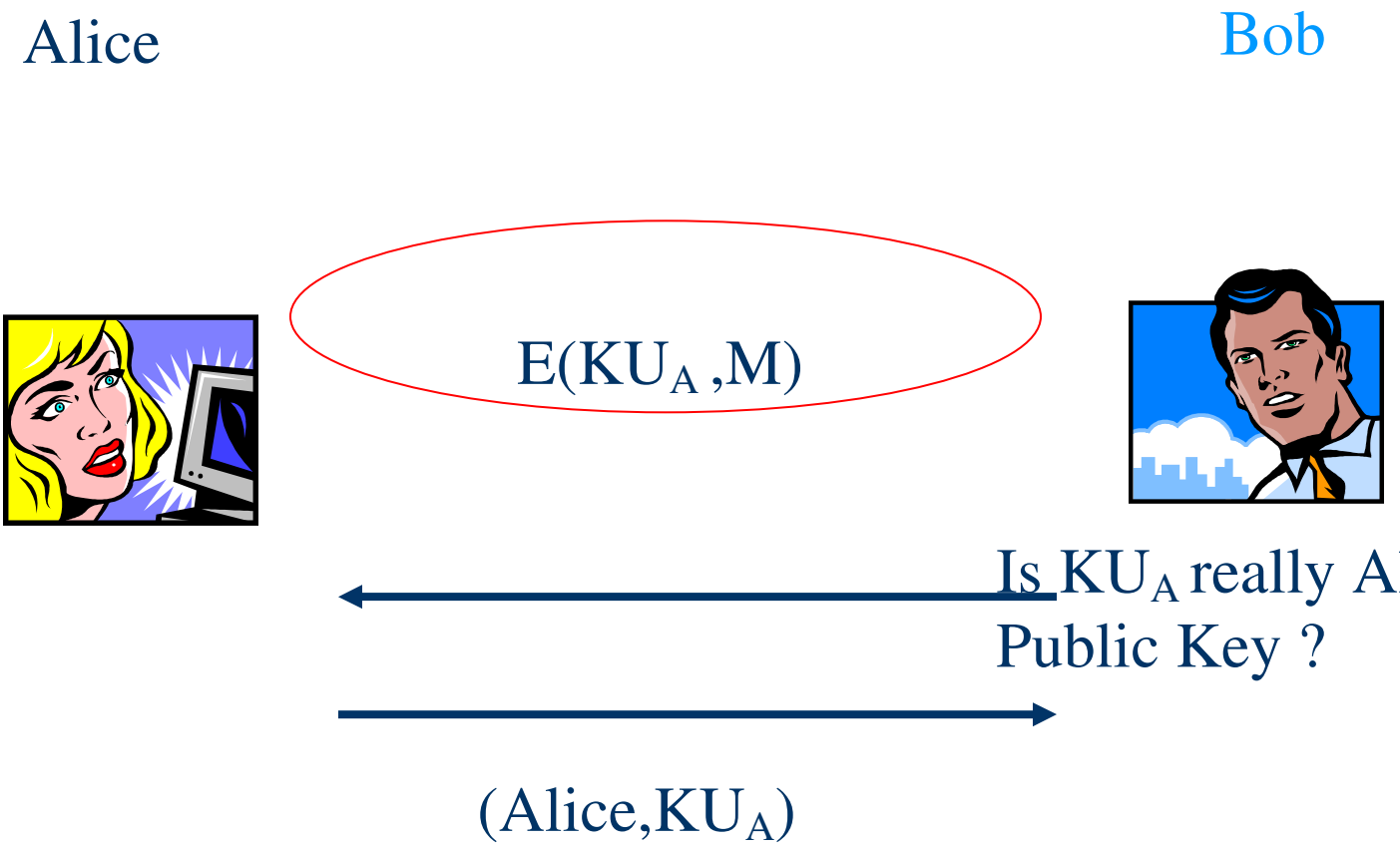
Yes



$(Alice, KU_A)$

رمزنگاری چیست؟

رمزنگاری اعتبار است بهم ریختگی اطلاعات طوری که برای کسی قابل فهم نباشد .در رمزنگاری کاربر با استفاده از کلید عمومی گیرنده، اطلاعات را رمز می کند وبرای گیرنده اطلاعات ارسال می کند . گیرنده اطلاعات ،اطلاعات رمز شده را توسط کلید خصوصی رمزگشایی می کند و چون کلید خصوصی هر شخص فقط در اختیار خودش است تنها همان فرد امکان رمزگشایی اطلاعات را دارد.



امضای دیجیتالی چیست؟

امضای دیجیتالی عبارتست از امضا کردن اطلاعات ارسالی برای اطمینان گیرنده از فرستنده اطلاعات . طریقه کار آن به این ترتیب است که فرستنده، اطلاعات را توسط الگوریتم هشینگ (که شامل MD5,SHV است) به حجم خاصی کاهش می دهد که به آن Digest می گویند سپس اطلاعات igestD شده را توسط کلید خصوصی رمز می کند وهمراه با اطلاعات ارسال می کند در سمت گیرنده اطلاعاتDigest شده توسط کلید عمومی رمزگشایی می شود و اگر با اطلاعات ارسالی یکی بود نشانه اینست که اطلاعات در بین راه دستخوش تغییر قرار نگرفته.

اهداف CA:

۱-تامین امنیت لازم در انجام معاملات و محیط های الکترونیکی و ترویج فرهنگ استفاده از هویت الکترونیکی است .
۲- تولید و ارائه گواهینامه دیجیتال برای تبادلات تجارت الکترونیکی B۲B,B۲C (در حوزه کالا و خدمات)
۳- تدوین آیین نامه ها و مقررات مربوط به مدیریت بر گواهی دیجیتال تولید و عرضه شده .
۴- ارائه خدمت به دفاتر ثبت گواهی دیجیتال (RA) و دفاتر خدمات گواهی دیجیتال در سراسر کشور .
۵- ارائه خدمات آموزشی برای استفاده از این فناوری در سراسر کشور .

اكنون به بررسي ملاحظات امنيت و تجارت به عنوان رمز موفقيت CA مي پردازيم :

ابتدا اهداف و ديدگاه كلي يک Certificate Authority بررسي مي گردد .

١) CAها چه كساني هستند؟
٢) چگونه كاربران را تائيد مي كنند؟
٣) ويژگيهاي خاص CA چيست ؟
٤) CA چه نكات امنيتي را بايد مد نظر داشته باشد ؟

عناوين مهم CA دربعد تجاري چيست ؟

١) گواهي تائيد كل محصولات
٢) پشتيباني كامل از مشتريان
٣) تحويل به موقع
۴) تائيد مطمئن و محكم
۵) قابل اعتماد در هر مكاني
۶) امنيت كامل كليد خصوصي
٧) پول ساز باشد

عوامل موفقيت CA از ديدگاه مشتري ؟

١) اعتماد
٢) قيمت
٣) پشتيباني
٤) اعتبار

چه عواملي اعتبار CA را نزد مشتركين آن بالا مي برد ؟

١) در شرايط بحراني به كار خود ادامه دهد
٢) رابطه متقابل شهرت و اعتماد
٣) توجه به اينكه خطا ها هزينه بر هستند
۴) توجه به بعد زمان مهم است
۵) هزينه ها بايد حد اقل باشند

تعين حدود امنيت مورد نياز(مدل CERT)

١) هيچ گونه تائيدي مورد نياز نيست (پست الكترونيک)
٢) حداقل تائيد كفايت مي كند
٣) سطح قابل قبولي از تائيد جوابگو است
٤) حداكثر تائيد بايد وجود داشته باشد

CA بايد قابليت مالي بالايي داشته باشد زيرا:

١) هزينه هاي زير بنايي قابل توجه است
٢) امكان منسوخ شدن تكنولوژي هميشه وجود دارد
٣) منابع و سرمايه :
   - دراز مدت : حداقل
   - كوتاه مدت : قابل توجه
۴) سطح بالاي امنيت هزينه بر است
۵) سود سهام غير قابل پيش بيني است

مهارتهاي تكنيكي ذيل قدرت CA را افزايش مي دهد:

١) گواهينامه ها با پروتكل X.509 تعريف شده باشند
٢) توجه به ناقص بودن استاندارد ها و تنظيم استاندارد هاي جديد
٣) مهارتهاي بالاي اينترنتي و مديريت كليد و رمزنگاري
٤) انتشاردوره اي توانمندي و كارائيها
٥) در صورت شكست ،كليد از سرگيري تجارت

نيازهاي امنيتي كه بايد مورد توجه قرار گيرد:

١) صاحبان شركت درک كاملي از امنيت و كنترل داشته باشد
٢) از تجهيزات فيزيكي مطمئن و امن جهت ذخيره اطلاعات مشتريان استفاده كند
٣) ازتجهيزات سخت افزاري CRYPTOGRAPHY براي ذخيره كليد استفاده كند
٤) پرسنل قابل اعتماد باشند
٥) كنترل و عملكرد مطمئن
٦) مديريت كليد در شرايط بحراني
٧) رسيدگي به موقع به LOG سيستم

امنيت سايت فيزيكي چگونه بدست مي آيد ؟

۱) ازتجهيزات ايمن استفاده شود
۲) ملزومات كنترل دسترسي EXTERNAL
۳) مراقبت دائمي ۷×۲۴×۳۶۵ وجود داشته باشد
۴) قوانين محكم داخلي اجراء شوند
۵) ازتجهيزات كنترل امنيت داخلي استفاده شود
۶) كنترل دسترسي بيومتريک به توليد كننده كليد ومحل ذخيره آن وجود داشته باشد

با توجه به توضيحات داده شده و لزوم ايجاد CAدر كشور به برسی يكی از بزرگترينCA های جهان پرداخته ايم .

Verisign

اين CA در راسCA ROOT جهان قرار دارد و تمام CA هاي موجود به نحوي بايد مورد تائيد اين CA قرار گيرند .

تمام سرويسهايي كه اين CA ارائه مي دهد در اين ۳ دسته قرار مي گيرند كه به اجمال توضيح داده مي شوند :

۱- Products & services
۲- Solution
۳- Support

Products & services

۱- Security Services

این سرویس با ایجاد امنیت بالا از هر گونه سوء استفاده جلوگیری می کند .

۲- Payment Services

این سرویس امکان انجام تجارت ها را به صورتOnline فراهم می کند .

۳- Naming & Directory Services

این سرویس امکان شناساییDomain name ها را فراهم می کند .

۴- Communication Services

این سرویس امکان ایجاد ارتباط هوشمند را فراهم می کند .

Security Services

۱- SSL (Secure Socket Layer) Services

این سرویس با تامین امنیت بالا ، امکان انجام تجارت های امن را فراهم می کند .

۲- Email Security Services

این سرویس امکان چک کردن پست الکترونیکی(Email) کاربر را قبل از رسیدن به دست او را فراهم می کند .

۳- Managed Security Services

این سرویس امکان طبقه بندی شرکت ها برای تعیین سطح امنیت مورد نیاز را فراهم می کند .

۴- PKI and Authentication Services

این سرویس امکان تایید هویت طرفین معامله را فراهم می کند .

۵- Global Security Consulting

این سرویس احتمال خطر سوءاستفاده را به حداقل می رساند .

۶- Code Signing

این سرویس امکان شناسایی شرکت تولید کننده نرم افزار را فراهم می کند .

۷- Intelligence and Control Services

این سرویس امنیت لازم برای کاربران را فراهم می کند .

۸- Verisign Secured Seal Program

این سرویس امکان تجارت های امن را با مهر این شرکت را فراهم می کند

Payment Services

۱- Online Payment Services

این سرویس امکان پرداخت صورت حساب را به صورت Online فراهم می کند .

۲- Fraud Protection Services

این سرویس تجارت های Online امن را فراهم می کند .

۳- Recorring Biling Services

این سرویس جدول پرداخت صورت حساب های شما را به صورت منظم تنظیم می کند .

۴- Point_Of_Sale Payment Processing

این سرویس امکان تجارت های Onlineبا سرعت بالا را فراهم می کند .

۵- Wireless Payment Services

این سرویس امکان اضافه کردن سرویس هایی تلفن همراه با زدن یک Message برای مشترکش فراهم می کند .

۶- Smart Pay @ Wireless Repaid Biling

این سرویس مشترکین تلفن همراه گزارشی از موجودی حساب خود می توانند بگیرند .

۷- Biling and Payment Services

این امکان دریافت و پرداخت از حساب بانکی را فراهم می کند .

۸- Verisign Secured Seal Program

با این سرویس به اطلاعات به روز طرفین معامله می توانیم دسترسی پیدا کنیم .

Naming & Directory Services

۱- Naming Services

این سرویس امکان تایید هویت ۳۰ میلیون کاربر را با ۳۰۰زبان مختلف که عضو دامنه های نامی cccom,net,tv, باشند را فراهم می کند .

۲- Directory Services

این سرویس امکان رهبری جهانی را برای سرویس دایرکتوری فراهم می کند .

۳-Digitall Brand management services

این سرویس امکان مدیریت دامنه های نامی را برای دسترسی شرکت های دارای اعتبار فراهم می کند .

Communication Services

۱-Connectivity and Inteoperability Services

این سرویس امکان ایجاد ارتباط امن در شبکه های هوشمند را فراهم می کند .

۲- Intelligent database Services

این سرویس امکان همامنگی IP و شبکه مخابرات در ایجاد یک شبکه هوشمند فراهم می کند .

۳- Content and Application Services

این سرویس امکان ایجاد یک Platform قابل تنظیم با قابلیت ارسال پیغام را فراهم می کند .

۴- Biling and Payment Services

این سرویس امکان بررسی حساب بانکی شما را در موارد پرداختی و دریافتی فراهم می کند .

Business Solution

۱- Regulatory Compliance

این سرویس امکان انجام تنظیمات را توسط کاربر برای حداکثر استفاده با کمترین هزینه فراهم می کند .

۲- Anti_Phishing and Identify Thef

این سرویس امکان جلوگیری و ایجاد گزارشی از حمله های Phishing را فراهم می کند .

۳- Business Contiuity

این سرویس امکان ایجاد امنیت را در ۲۴ ساعت فراهم می کند .

۴- Business Partner Inteqration

با این سرویس امکان یکپارچگی همه شرکا ، با امنیت بالا را فراهم می کند

۵- Commerce Enablement

این سرویس امکان انجام تجارت های اینترنتی با امنیت بالا به وسیله پروتکل SSL را فراهم می کند .

۶- Interoperability

این سرویس امکان استفاده از سرویس های ذکر شده را برای دارندگان رایانه های قابل حمل فراهم می کند .

Industry Solution

۱- Telecommunication

این سرویس امکان ایجاد یک ارتباط با هزینه کم و امنیت بالا در مقوله صنعت را فراهم می کند .

۲- Finacial Institutions

این سرویس امکان محافظت از اطلاعات کاربران را فراهم می کند . گواهینامهSSL این سرویس با همه سرویس دهنده های بزرگ دنیا مانند Microsoft قابل اجرا است .