

عنوان مقاله:

**آخرین وضعیت زیرساخت های موجود در زمینه گواهی الکترونیکی در ایران**

**و همچنین موارد بکارگیری آن**

گردآوری از: محمد اسماعیلی

نام و نام خانوادگی: محمد اسماعیلی(پرسنلی 25056)

مدارک و رشته های تحصیلی: مهندسی کامپیوتر – سخت افزار

 دانشجوی کارشناسی ارشد مهندسی کشاورزی-ترویج و آموزش کشاورزی

سمت و محل خدمت فعلی در بانک: مسئول قسمت رایانه و نظارت تصویری مدیریت استان قم

پست الکترونیک:mo-esmaili@agri-bank.com

همراه:09194525633

مقدمه

امروزه یکی از موضوعات اصلی در مباحث مربوط به اسناد و پیامهای الکترونیکی و کد گذاری و امضا های دیجیتالی مربوط به آنها، ایجاد این تضمین است که کسی نتواند کلید عمومی خود را انکار کرده و یا اینکه اخلال گران نتوانند خودشان را به جای دیگری جا بزنند. وجود یک مرکز مورد وثوق و اطمینان راه حل مسئله انکار پذیری پیامها می باشد. اما این مشکل بروز می کند که چنین مراکزی به خودی خود به پاشنه آشیل سیستم تبدیل می شوند زیرا همیشه باید فعال و online باشند که این موضوع می تواند منجر به ایجاد گلوگاه و نقطه حساس به خرابی شود . بدیهی است که هرگونه نفوذ در این مراکز، بنیان خدمات سیستم را به باد خواهد داد و کلیدهای همه را افشا خواهد کرد حال می خواهیم مکانیزمهایی را مورد بررسی قرار دهیم که بر اساس آنها برای همه افراد گواهینامه دیجیتالی صادر می شود. این گواهینامه بایستی غیر قابل جعل بوده و درون آن ، هویت هر فرد به همراه کلید عمومی او درج شده باشد. این گواهینامه ها توسط مراکز مجاز و معتبر ، صادر و امضا می شوند. مراکز صدور گواهینامه ، پشتوانه حقوقی دارند و گواهینامه ها را بصورت Offline صادر می کنند. در ضمن برای افزایش ضریب امنیت ، می توان دسترسی همگانی به این مراکز را محدود نمود زیرا پس از صدور گواهینامه ، نیازی به حضور فعال آنها برای تایید گواهینامه نیست.بدیهی است اولین شرط در داشتن یک ارتباط امن ، راهکاری است که بر اساس آن مطمئن شویم کلید عمومی اصالت دارد و واقعا متعلق به همان کسی است که ادعا می کند. چنین پیش شرطی با روش گواهینامه دیجیتالی برآورده خواهد شد

**1-گواهی دیجیتالی چیست؟**

گواهینامه دیجیتالی حاوی پاره ای از اطلاعات در خصوص کاربر ، تاریخ صدور و انقضاء و از همه مهمتر کلید عمومی کاربر است.سازمان صادر کننده گواهی دیجیتالی را CA: certificate Authority می نامند که پس ازصدور گواهینامه و استخراج چکیده محتویات گواهینامه ، آن را با کلید خصوصی خود امضاء (رمز) می کند.سپس گواهینامه را به هر روش دلخواه (مثل ذخیره روی کارتهای هوشمند ، دیسک فشرده یا فلاپی) به کاربر تسلیم می نماید. مهمترین بخش قضیه آن است که افراد با مراجعه حضوری یا روشی مطمئن ، پس از تسلیم مدارک مورد نیاز، هویت خود را اثبات و با پرداخت هزینه اندک، گواهینامه خود را دریافت می کنند. فرض بر آن است که مرکز گواهی امضاء (CA) همان لحظه ای که گواهینامه فرد را به او تسلیم میکند کلید عمومی خود را نیز به کاربر می دهد تا کاربر کلید عمومی این مرکز را از طریق محیطهای نا امن مثل وب سایتها یا e-mail در یافت نکند.

حال افراد می توانند گواهینامه های صادره برای خود را در وب سایت شخصی گذاشته یا از هر طریق نا امن دیگر آن را برای متقاضیان ارسال کنند زیرا هیچکس در جهان قادر نیست در محتویات آن تغییری ایجاد کند و این تغییر قابل کشف نباشد. از طرفی دیگر هیچ کس نمی تواند خود را جای صاحب گواهینامه جا بزند زیرا کسی که گواهی را از صاحب آن دریافت می کند ابتدا آن را با کمک کلید عمومی مرکز CA اعتبارسنجی نموده و در صورتی به آن استناد می کند که امضای آن با محتوا مطابقت داشته باشد. با این روش هم حمله MITM ناکام می ماند و هم اینکه صاحب گواهینامه تعلق این کلید به خودش را نمی تواند منکر شود.

اما یکی از چالشهای پیش روی گواهینامه های دیجیتالی آن است که محتوای این گواهینامه ها (بغیر از وجود کلید عمومی که جزء لاینفک آن است) بسته به نوع کاربرد متفاوت است. بعنوان مثال گواهینامه برای مشتری یک بانک با گواهینامه برای دانشجوی یک دانشگاه یا حتی گواهینامه برای یک شیء که می تواند حتی یک فایل باشد ، با یکدیگر متفاوتند زیرا اطلاعات مورد نیاز برای این گواهینامه از هم متفاوتند. برای مثال یکی شماره حساب و رمز عبور کارت اعتباری را داراست و دیگری شماره دانشجویی و اطلاعاتی از این قبیل را در خود دارد.

بنابراین از همین ابتدا ، حجم انبوهی از نیاز ها باعث می شود که در تدوین ساختار گواهینامه های دیجیتالی ، پراکندگی و ناهمگونی بوجود بیاید.لذا قبل از هر چیزی به استانداردی منعطف و جهانی برای توصیف ،سازماندهی و ایجاد گواهینامه های دیجیتالی نیاز خواهیم داشت.

2-استاندارد x.509 برای گواهینامه های دیجیتالی

این استاندارد در سال ١٩٨٨ توسط ITU-T بمنظور ایجاد یک شکل متحد و یکنواخت جهانی برای گواهینامه های دیجیتالی تصویب و معرفی شد. این استاندارد که امروزه کاربرد بسیار گسترده ای یافته است تا به امروز سه بار بهبود یافته و اکنون نسخه سوم آن با ویژگیهای فراوان و انعطاف پذیری چشمگیر در دسترس عموم است. در این استاندارد مرکز صدور گواهینامه باید برای یک شخص حقیقی یا حقوقی یا برای یک آدرس پست الکترونیکی ، آدرس DNS یا اشیاء گواهینامه x.509 با ساختار استاندارد، تولید و آن را امضاء کند.در حقیقتx.509 روشی برای تعریف و تبیین گواهینامه های دیجیتالی است.فیلدهای یک گواهینامه موارد ذیل می باشد :

* **شماره نسخه**
* **شماره سریال گواهی**
* **نام فرستنده**
* **مدت اعتبار**
* **اطلاعات کلید عمومی مالک**
* **شناسه الگوریتم**
* **مقدار کلید عمومی**
* **صادر کننده منحصر بفرد شناسه**
* **امضای دیجیتالی سازمان ارائه دهنده مجوز**

3-اجزای زیر ساخت عمومی کلید عمومی

زیرساخت کلید عمومی (PKI) مجموعه‌ای متشکل از سخت افزار، نرم‌افزار، افراد، سیاست‌ها و دستورالعمل‌های مورد نیاز برای مدیریت، توزیع، استفاده، ذخیره و ابطال گواهی‌های دیجیتال می‌باشد.

در رمزنگاری، PKI مقدمه‌ای است برای الصاق کلید عمومی به هویت کاربر، که با استفاده از یک مرکز صدور گواهی (CA) انجام می‌گیرد. هویت کاربر باید برای هر CA یکتا باشد. نسبت دادن کلید عمومی به هویت افراد مطابق با یک روند ثبت و صدور انجام می‌شود، که بر اساس سطح تضمین لازم ممکن است توسط یک نرم‌افزار در CA انجام شود و یا با نظارت انسان باشد. مسئولیت تضمین درستی در PKI بر عهدۀ مرکز ثبت نام یا RA است. مرکز ثبت نام یا RA، با استفاده از روش تضمین عدم انکار، از کلید عمومی مختص هر فرد، اطمینان حاصل پیدا می‌کند.

زیرساخت کلید عمومی از موارد زیر تشکیل شده‌است:

1-3 مراکز صدورگواهی

مراکز صدور گواهی الکترونیکی در زیرساخت کلید عمومی کشور از مراکز دولتی صدور گواهی الکترونیکی ریشه و مراکز صدور گواهی الکترونیکی میانی تشکیل شده است

* مراکز صدور گواهی الکترونیکی ریشه

این مرکز که به آن مرکز دولتی ریشه هم گفته میشود ، نقطه اطمینان در زیر ساخت عمومی کشور می باشد.این مرکز مجوز ایجاد ، امضا ، صدور و ابطال گواهینامه های الکترونیکی مراکز گواهی الکترونیکی میانی را دریافت کرده است.مرکز دولتی ریشه مسئول تمام ابعاد صدور و مدیریت مراکز صدور گواهی میانی ، شامل نظارت بر فرایندهای ثبت نام ، احراز هویت ، صدور گواهی های میانی ، ابطال و انتشار گواهی هاو تحدید کلید می باشد.

* مرکز دولتی میانی عام

مرکز منحصر به فردی است که به طور عام مبادرت به ارائه خدمات گواهی الکترونیکی برای تمامی کاربردهای مختلف به متقاضیان می نماید.

* مراکز میانی دولتی

هر یک از دستگاههای دولتی میی توانند با کسب مجوز و اخذ گواهی از مرکز دولتی ریشه ، در حوزه فعالیت خود ، مبادرت به تاسیس مرکز میانی دولتی نماید.

* مراکز میانی تابعه

مراکز میانی تابعه تا یک سطح بعدی دستگاه یا دستگاههای مطبوع خود در صورت داشتن شرایط مربوط، می توانند صرفا در حوزه فعالیت خود ایجاد به مراکز میانی تابعه و صدور گواهی برای آنها اقدام نمایند.

* مراکز میانی خصوصی

این مراکز برای صدور گواهی الکترونیکی مورد استفاده در بخش خصوصی برای کاربردهای آنها تعریف شده است.انها پس از احراز صلاحیتهای کیفی ، کمی و حقوق ،مجوز تاسیس از مرکز تاسیس ریشه خواهند گرفت.

* مراکز میانی بیرونی

مراکز میانی بیرونی با احراز شرایط لازم کسب گواهی تحت عنوان مراکز میانی بیرونی از مرکز دولتی ریشه می توانند، پی از انعقاد قرارداد با دستگاه دولتی مورد نظر اقدام به صدور گواهی الکترونیکی صرفا برای کاربردهای دولت با بنگاه و دولت با مشتری نمایند.

2-3 دفاتر ثبت نام

دفتر ثبت نام موجودیتی است اختیاری که وظیفه شناسایی و بررسی صحت اطلاعات دریافت شده از سوی درخواست کنندگان گواهی الکترونیکی بر عهده دارد.در واقع دفتر ثبت نام با بررسی هویت درخواست کننده ، وظیفه تنظیم درخواست صدور،ابطال و بروز رسانی گواهی و همچنین درخواست تجدید کلید را بر عهده دارد.دفتر ثبت نام می بایست مورد تایید مرکز صدور گواهی باشد و توافق نامه یا قراردادی بین این دو جهت متعهد شدن دختر ثبت نام بر ارائه خدمات منطبق با دستورالعمل اجرایی مرکز میانی ، منعقد گردد.

3-3 مالکان گواهی

مالک گواهی به موجودیتی گفته می شود که از مرکز صدور گواهی ، گواهی دریافت کرده و نام او به عنوان مالک گواهی در گواهی الکترونیکی ، ثبت می شود.هویت مالک گواهی قبل از صدور گواهی ، توسط مرکز صدورگواهی یا دفتر ثبت نام بررسی و احراز می شود.

4-3 طرفهای اعتماد کننده

طرف اعتماد کننده موجودیتی است که به صحت تطابق میان مشخصات و کلید عمومی مالک گواهی الکترونیکی اعتماد کرده و گواهی الکترونیکی او مورد استناد قرار می دهد.

5-3 شورای سیاست گذاری گواهی الکترونیکی کشور

به منظور حفظ یکپارچگی و جلوگیری از تفکیک راهکارها و استانداردهای به کار گرفته شده ، سیاست گذاری در زمینه فعالیتهای مرکز دولتی ریشه و بروز رسانی سیاست گواهی این مرکز و تایید تطابق دستورالعمل اجرایی تمام مراکز میانی با این سند، شورایی به نام شورای سیاست گذاری گواهی الکترونیکی تشکیل شده است که از این پس در این سند به اختصار شورا نامیده میشود.

4- کاربردهای گواهی الکترونیکی

زیر ساخت عمومی کشور به منظور تامین سرویس های امنیتی تمامیت ، احراز هویت ، انکار ناپذیری و محرمانگی طراحی شده است .مراکز میانی در صورت استفاده از سطوح اطمینان مختلف ، می بایست تعریف این سطوح اطمینان و کاربردپذیری و شناسه هر سطح اطمینان را در دستورالعمل اجرایی گواهی خود قید کنند.موارد ذیل انواع گواهی تعریف شده و مورد استفاده در زیر ساخت عمومی کشور را نشان می دهد.

1-4 گواهی امضا

این گواهی جهت امضا اسناد و تراکنش های الکترونیکی و همچنین می توانند جهت احراز هویت کاربران مورد استفاده قرار می گیرد.

2-4 گواهی پست الکترونیکی

این گواهی از طریق پروتکل S/MIME امکان محرمانگی و امن کردن ایمیل را به واسطه رمز نگاری محتوای پیام و همچنین امضا نمودن ان فراهم می سازد.

3-4 گواهی احراز هویت

این گواهی جهت احراز هویت مالکان گواهی به منظور امکان دسترسی جهت ورود به سیستم مورد استفاده می گیرد .به عنوان مثال از این گواهی می توان برای ورود به سیستم از طریق احراز هویت دو عاملی مبتنی بر کلید عمومی ، در سیستم عامل های متعلق به مایکروسافت استفاده نمود.

4-4 گواهی مهر سازمانی

این گواهی به عنوان گواهی امضاء شرکت یا سازمان تلقی می شود و می تواند به عنوان مهر سازمانی آن شرکت یا سازمان در قالب امضای دیجیتال مورد استفاده قرار گیرد.

5-4 گواهی سرور

این گواهی جهت استفاده در سرور های مختلف در نظر گرفته شده است. دو نمونه از کاربردهای رایج این گواهی از گواهی SSL/TLS مختص نشانی اینترنتی صادر شده و به منظور تضمین اصالت یک سرور و به عبارتی تضمین ارتباط بین نشانی و وب سایتی که به آن مراجعه شده به کار می رود.

6-4 گواهی Code Signing

این گواهی جهت اطمینان از اصالت و حفظ جامعیت نرم افزارهای مختلف به ویژه نرم افزارهایی که از طریق اینترنت منتشر میشوند. نظیر ActiveX وJava Applet بکار می رود.

5-وضعیت ایران در گواهی الکترونیکی

گواهی الکترونیک در ایران شرایط مناسبی دارد و در این عرصه در مقایسه با کشورهای خاورمیانه وضعیت بهتری داریم و همگام با تکنولوژی سایر کشورهای جهان در حال پیشرفت هستیم. در حال حاضر در کشور مرکز ریشه‌ای دولتی صدور گواهی الکترونیکی تأسیس شده که شرایط خوبی را برای پیشرفت تجارت الکترونیک فراهم آورد، با تأسیس این مرکز که اولین مرکز صدور گواهی الکترونیکی در کشور است تمامی اقدامات دسته بندی شده و به شکل منسجم و منظم در حال پیشرفت است. ایجاد فضای دیجیتال جهت ثبت سفارش به صورت 10 هزار شناسه برای بازرگانان صادر شده که این اقدام امکان سفارش‌پذیری به صورت آنلاین برای بازرگانان و تجار را فراهم آورده است از مهم‌ترین اقدامات این مرکز جهت پیشرفت به سمت تجارت الکترونیک است همچنین ایجاد پست الکترونیکی امن با ایجاد 2 هزار شناسه و ایجاد SSL جهت ارتباطات امن با سایت‌های تجارت الکترونیک از دیگر اقداماتی است که در مرکز میانی صدور گواهی الکترونیکی بازرگانی صورت گرفته و قابلیت توسعه برای آینده را نیز دارد. جهت آشنایی بیشتر مدیران و سازمان‌های دولتی و غیردولتی سایت‌های اطلاع‌رسانی مربوط به ریشه گواهی الکترونیکی و مرکز میانی تشکیل شده است. هزاران نفر از کارشناسان و مدیران دولتی درباره مباحث کلی و کاربردی تجارت الکترونیک و گواهی دیجیتال آموزش‌هایی ارائه شده و این در حالی است که برای توسعه استفاده از گواهی الکترونیکی سایر سیستم‌ها و بسترها باید به این سمت منتقل شوند.

نتیجه گیری

مرکز ریشه وابسته به مرکز توسعه تجارت الکترونیکی بوده و با مجوز از شورای سیاست گذاری گواهی الکترونیکی فعالیت می نماید. وب سایت مرکز دولتی صدور گواهی الکترونیکی ریشه، محل انتشار گواهی الکترونیکی ریشه و اسناد و اخبار مربوطه می باشد. از طریق این سایت همچنین می توان به آخرین نسخه های سیاست های گواهی الکترونیکی و دستورالعمل اجرایی گواهی الکترونیکی مرکز ریشه دسترسی پیدا کرد.

بررسی فنی و ساختاری مرکز ریشه نشان می دهد که در طول چند سال گذشته فعالیت های فراوانی در جهت اجرای این پروژه و تأمین زیرساخت آن انجام شده اما هنوز هم تا رسیدن به موفقیت در انجام این پروژه راه درازی در پیش است. سعی برآن شده از نتایج کاربردی و مهم کشورهای دیگر استفاده شود و همچنین از مشاوران خارج از کشور در راستای بهبود اجرای آن بهره کافی برده شود.

 لازم به ذکر است که هرچند امضاء الکترونیک اهمیت زیادی در گواهی دیجیتال دارد اما این دو بسیار متفاوت هستند. بر اساس نظر متخصصین مرکز دولتی ریشه ، این مرکز قرار است حداقل9گواهی الکترونیکی صادر کند که امضا یکی از آن هاست، مانند گواهی پست الکترونیک امن، گواهی مهر زمان، گواهی شخصیت های حقوقی، نرم افزارها، تجهیزات، سورس برنامه ها و غیره .

منابع:

1-انسان,مصطفی.(1387).وضعیت کنونی گواهی الکترونیکی در ایران.ماهنامه کانون(1387),شماره 81 و 82

2-فدوی,سلیمان و ملکی,محمدرضا.(1387).امضاهای دیجیتال,گواهی امضاءهای الکترونیکی و تجارت الکترونیک.ماهنامه کانون (1387),شماره60

3-http://enamad.ir

4-http://www.rca.gov.ir

5-http://nsecure.ir