امضاء دیجیتالی، فن آوری نوین امنیت اطلاعات در فرایندهای کسب و کار

اسماعیل ملک اخلاق[1]، علی قلی زاده باریس[3]، ابوالقاسم زارعی دودجی[3]

[1]دکتری مدیریت استراتژیک، دانشکده علوم انسانی، دانشگاه گیلان
رشت، ایران
Dr.Malekakhlagh@yahoo.com

[2] دانشجوی کارشناسی ارشد مدیریت بازرگانی، دانشکده علوم انسانی، دانشگاه گیلان
رشت، ایران
Aliqulizade@yahoo.com

[3]دانشجوی کارشناسی ارشد مدیریت صنعتی، دانشکده علوم انسانی، دانشگاه گیلان
رشت، ایران
Ghasem.zd@gmail.com

چکیده

در جهان امروز مدیریت اسناد الکترونیکی، ارسال و دریافت آن‌ها بخش بزرگی از فعالیت‌های اجرایی را شامل می‌شود و هنوز انتظار می‌رود که استفاده از اطلاعات و اسناد الکترونیکی در سطح جهان به طرز قابل توجهی در حال گسترش باشد. یکی از تکنولوژی‌هایی که موجب افزایش اعتماد به این فرایند گردیده، امضای دیجیتالی است. این تکنیک مبتنی بر رمزنگاری، باعث به رسمیت شناختن اطلاعات الکترونیکی شده بطوریکه هویت پدید آورنده، محرمانگی و جامعیت اطلاعات آن، قابل بازیابی و کنترل می‌باشد. در اسناد مکتوب، امضا، نشان تایید تعهدات قبول شده در آن سند به شمار می‌آید و از آن جهت که در تجارت الکترونیکی «مدرک الکترونیکی» دارای جایگاهی همانند اسناد مکتوب هستند، لذا در این مدارک نیز نیازمند امضای دیجیتالی می‌باشیم. با توجه به ضرورت این امر، در این مقاله ابتدا به بیان اهمیت و ضرورت امنیت اطلاعات و مبادلات الکترونیکی در فضای سایبری پرداخته می‌شود و در ادامه به معرفی امضای دیجیتالی و الگوریتم‌های رمزنگاری به عنوان راهکار و ابزار امنیتی مناسب در این خصوص پرداخته می‌شود و کاربردهای مهم امضای دیجیتالی در تبادلات اینترنتی و انواع کسب و کار نیز معرفی می‌شود.

کلید واژه

امضای دیجیتالی، گواهی دیجیتالی، امنیت اطلاعات، رمزنگاری

1- مقدمه

مهم‌ترین مزیت و رسالت شبکه‌های رایانه‌ای، اشتراک منابع سخت‌افزاری و نرم‌افزاری و دست‌یابی سریع و آسان به اطلاعات است. علیرغم تمامی مزایا و دستاوردهای اینترنت، این شبکه عظیم به همراه فن‌آوری‌های مربوطه، دریچه‌ای را در مقابل تعداد زیادی از تهدیدات امنیتی برای تمامی استفاده کنندگان اعم از افراد، سازمان‌ها، مؤسسات و دولت‌ها گشوده است [14].

اطمینان از ایمن بودن سرمایه‌های اطلاعاتی و تجهیزات زیرساختی کشور گذشته از ابعاد گسترده امنیت ملی، کلید قفل فرصت‌های بی‌شمار تجاری و غیرتجاری جدید اینترنتی است. امروزه امنیت فضای دیجیتال، وجهه‌ای از امنیت ملی هر کشور را به تصویر می‌کشد [1]. در دنیای امروز، اعتبارات مالی بیشتر و بیشتر به صورت الکترونیکی جا بجا می‌شوند، اطلاعات مختلف با حساسیت‌های کم و زیاد از طریق شبکه‌ها منتقل می‌شوند، سامانه‌های رایانه‌ای با سرعت بسیار زیادی پیچیده‌تر و مرتبطتر با دنیای بیرونی می‌گردند، و ابزارهای ساده نفوذ و بهره‌برداری از آسیب‌پذیری‌ها بیش از هر زمان دیگری در دسترس ماجراجویان و جاسوسان دنیای مجازی قرار دارد و هر یک از این عوامل خود به تنهایی دلیل محکمی برای جدی گرفتن موضوع امنیت اطلاعات است [5].

2- امنیت اطلاعات[1]

امنیت اطلاعات در واقع محافظت از اطلاعات در برابر طیف وسیعی از تهدیدات و به حداقل رساندن خطر افشای اطلاعات در بخش‌های غیرمجاز است [7] که با هدف تضمین استمرار فعالیت‌ها، به حداقل رساندن ریسک‌های کاری و به حداکثر رساندن میزان بازده سرمایه‌گذاری‌ها صورت می‌پذیرد و فناوری امنیت اطلاعات[2] به بهره‌گیری مناسب از تمامی فناوری‌های امنیتی پیشرفته برای حفاظت از تمام اطلاعات احتمالی اشاره دارد. امنیت اطلاعات در محیط‌های مجازی همواره به عنوان یکی از زیرساخت‌ها و الزامات اساسی توسعه فناوری اطلاعات مورد تاکید قرار گرفته است. گرچه امنیت مطلق چه در محیط واقعی و چه در فضای مجازی دست نیافتنی است، اما ایجاد سطحی از امنیت که به اندازه کافی و متناسب با نیازها و سرمایه‌گذاری انجام شده باشد، تقریباً در تمامی شرایط محیطی امکان پذیر است [6].

3- مشکلات و مسائل امنیتی در مبادلات الکترونیکی

در یک ارتباط ایده‌آل روی شبکه، مبدأ و مقصد یکدیگر را می‌شناسند و با هم در ارتباطند و هیچ شخص ثالثی در این میان به اطلاعات مبادله شده بین آن‌ها دسترسی ندارد و اطلاعات ارسالی به طور کامل و سالم به مقصد می‌رسند. اما در یک سیستم واقعی هر لحظه امکان دارد ارتباط بین مبدأ و مقصد مورد حمله قرار گیرد، ممکن است مبدأ یا مقصد جعلی باشند، داده‌ها مخدوش یا مفقود شوند و یا مورد استراق سمع واقع شوند [3]. از طرفی هنگام بازدید از یک وب سایت نمی‌توان به وب سرور مربوطه اطمینان حاصل کرد زیرا ممکن است رابطه گرافیکی یک پایگاه اینترنتی معتبر جهت ربودن اطلاعات محرمانه دقیقاً کپی شده باشد[3] و از آنجایی که ایجاد پایگاه اینترنتی و ثبت دامنه، کاری آسان و کم هزینه است، لذا امکان ساخت پایگاه‌های جعلی و انجام کلاه‌برداری از این طریق وجود دارد [8]. همچنین احتمال دارد شخصی لحظه به لحظه هر آنچه را که شما با رایانه انجام می‌دهید مشاهده و ثبت کند[4]، زمانی که شمارهٔ کارت اعتباری و پسورد خود را برای خرید اینترنتی وارد می‌کنید از آن آگاه شود، از گشت‌وگذار شما در پایگاه‌های وب مختلف مطلع باشد، و زمانی که با پایگاه وب یا سیستم‌ها ارتباط برقرار می‌کنید بتواند نام کاربری و رمز عبور را به سرقت ببرد [1].

علاوه بر این، سرویس پست الکترونیکی[5] که جزء قدیمی‌ترین و پراستفاده‌ترین خدمات مورد استفاده در شبکه‌های کامپیوتری می‌باشد، دارای مشکلات امنیتی بسیاری است. یکی از این مشکلات عدم تضمین هویت فردی است که نام او به عنوان فرستنده نامه ذکر می‌شود [15]، به عبارت دیگر به سهولت می‌توان هر آدرس دلخواهی را به جای فرستنده‌ی نامه قرار داد و نامه‌های جعلی ارسال کرد. دومین مشکل اساسی آن است که هیچ تضمینی وجود ندارد که نامه‌های الکترونیکی فقط توسط گیرنده قابل دسترسی باشند. به بیان دیگر محرمانه بودن[6] صندوق‌های پست الکترونیکی تضمین نمی‌شود [3]. کسانی که بخواهند از این مشکلات سوء استفاده کنند، به سادگی می‌توانند به نامه‌های خصوصی افراد دسترسی پیدا کنند و از طرف آن‌ها برای دیگران نامه بنویسند.

4- الزامات و مفاهیم امنیتی در دنیای مجازی

در واقع امنیت اطلاعات یعنی حفظ محرمانگی، قابل دسترس بودن و تمامیت[7] اطلاعات از افراد غیرمجاز [10]. البته در بین متخصصان این رشته علاوه بر این سه مفهوم موارد دیگری هم مانند احراز هویت[8] و انکار ناپذیری[9] مطرح است که به این شرح می‌باشد [4] :

4-1- محرمانگی

به معنای جلوگیری از افشای اطلاعات به افراد غیر مجاز می‌باشد. به عنوان مثال، برای خرید با کارت‌های اعتباری بر روی اینترنت نیاز به ارسال شماره کارت اعتباری از خریدار به فروشنده و سپس به مرکز پردازش معامله است. در این مورد شماره کارت و دیگر اطلاعات مربوط به خریدار و کارت اعتباری او نباید در اختیار افراد غیرمجاز قرار گیرد و این اطلاعات باید محرمانه بماند.

4-2- تمامیت

به مفهوم عدم دستکاری و جلوگیری از تغییر داده‌ها به طور غیرمجاز و تشخیص تغییر در صورت دستکاری غیر مجاز اطلاعات می‌باشد.

4-3- قابل دسترس بودن

اطلاعات باید زمانی که مورد نیاز افراد مجاز هستند، در دسترس باشند. این بدان معناست که باید از درست کار کردن و جلوگیری از اختلال در سیستم‌های ذخیره و پردازش اطلاعات و کانال‌های ارتباطی مورد استفاده برای دسترسی به اطلاعات اطمینان حاصل کرد.

4-4- انکار ناپذیری

در انتقال اطلاعات و یا انجام عملی روی اطلاعات، گیرنده و فرستنده و یا عمل کننده روی اطلاعات نباید قادر به انکار عمل خود باشد. مثلاً فرستنده یا گیرنده نتواند ارسال یا دریافت پیامی را انکار کند.

4-5- احراز و تصدیق هویت

در مبادلات حضوری علاوه بر استفاده از کارت شناسایی، پاسپورت، امضاء و... از علائم زیست‌سنجی مانند صدا، اثر انگشت، تپش قلب، عنبیه و... نیز به صورت گسترده برای تشخیص هویت استفاده می‌کنند اما در مبادلات مجازی(اینترنتی)، امکان برگزاری جلسات حضوری وجود ندارد. طرفین نمی‌توانند با روش‌های فیزیکی از صحت ادعاها و اسناد اطمینان حاصل کنند. در این محیط فرایند احراز و تصدیق هویت از طریق روش‌های زیر صورت می‌گیرد.

4-5-1- دانش و دانسته‌های فرد

در این روش با استفاده از کلمات رمز که متداول‌ترین روش احراز هویت کاربران است، اطلاعات محرمانه مانند کد رمز یا کلمات عبور با اطلاعات ذخیره شده در سیستم مطابقت داده می‌شود و عملیات احراز هویت صورت می‌گیرد.

4-5-2- علائم زیست‌سنجی[10] فرد

نوعی فناوری است که برای احراز هویت از سنجش و تحلیل خصوصیات منحصربه‌فرد شخصی استفاده می‌کند. این خصوصیات ممکن است فیزیولوژیکی یا رفتاری باشند. اثر انگشت، شکل عنبیه یا شبکیه چشم، فرم دست و چهره فرد همگی مثال‌هایی از خصوصیات فیزیولوژیکی می‌باشند.

4-5-3- چیزی که در تصرف فرد است

روشی مطمئن‌تر، استفاده از دستگاه‌ها و ابزارهایی است که یک کد دیجیتال درون آن‌ها قرار داده می‌شود و مانند یک کلید الکترونیکی عمل می‌کنند برخی از این ابزارها که برای دسترسی به شبکه‌های رایانه‌ای مورد استفاده قرار می‌گیرند عبارتند از [2] :

4-5-3-1- کارت‌های هوشمند: این کارت‌ها که در ابعاد کارت‌های اعتباری عرضه می‌شوند، هنگام احراز هویت درون شکاف کارت خوان قرار داده می‌شوند. این کارت‌ها می‌توانند حاوی کلید خصوصی افراد، گواهی‌نامه کلید عمومی و دیگر اطلاعات مفید باشند.

4-5-3-2- توکن‌های امنیتی[11] : سخت افزاری کوچک است که برای ورود کاربر یک سرویس رایانه‌ای به سامانه بکار می‌رود و جهت احراز هویت، تعیین اعتبار، نگهداری امن و جلوگیری از دسترسی غیر مجاز داده‌های حساس کاربر و همچنین تولید کدهای تصادفی، انجام اعمال رمزنگاری و امضای دیجیتالی و امنیت نرم افزار بکار می‌رود [9].

5- راهکارها و ابزارهای امنیتی در دنیای مجازی

5-1- رمزنگاری[12]

اغلب این مسئله باید تضمین شود که یک پیام یا سند فقط می‌تواند توسط کسانی خوانده شود که برای آن‌ها ارسال شده است و دیگران این اجازه را ندارند. روشی که تامین کننده امنیت این مسئله باشد رمزنگاری نام دارد. رمزنگاری مجموعه‌ای از فنون ریاضی برای حفاظت از اطلاعات و هنر نوشتن به صورت رمز است بطوریکه هیچ‌کس به غیر از دریافت کننده مورد نظر نتواند محتوای پیام یا مستندات را بخواند.

از لحاظ نظری وقتی قطعه‌ای از اطلاعات رمزگذاری شود و سپس به طور تصادفی توسط یک شخص ثالث از میان راه دزدیده یا افشا گردد امنیت آن خدشه‌دار نخواهد شد، مشروط بر آن که کلید لازم برای رمزگشایی اطلاعات افشا نشده باشد و بدین ترتیب روش رمزگذاری در مقابل تلاش برای رمزگشایی، مقاومت می‌کند.

با استفاده از رمزنگاری می‌توان کلمات مکتوب و دیگر انواع پیام را به گونه‌ای تبدیل کرد که اگر کسی یک کلید ویژه ریاضی که برای باز کردن قفل پیام‌ها لازم است را در اختیار نداشته باشد آن پیام‌ها برایش بی‌مفهوم به نظر بیاید. استفاده از رمزنگاری برای تغییر ظاهری یک پیام، رمزگذاری[13] نامیده می‌شود؛ و فرآیند بازگشت یک پیام رمز شده به قالب اولیه با استفاده از کلید مناسب نیز رمزگشایی[14] نام دارد [6].

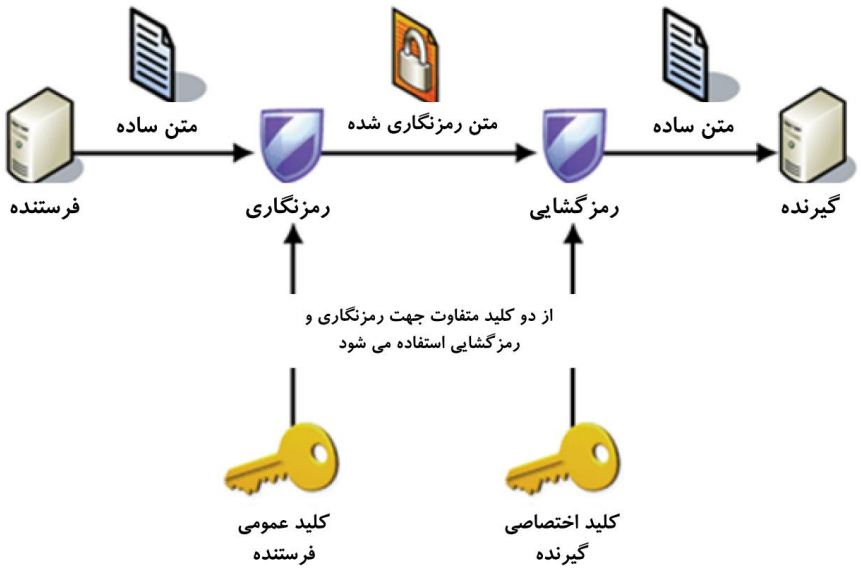
2-5- الگوریتم‌های رمزنگاری

1-2-5- الگوریتم متقارن[15]

در این روش از یک کلید مشترک برای رمزنگاری و رمزگشایی استفاده می‌شود. در صورتیکه گیرنده با کلید مشترک خود با فرستنده، پیام را رمزگشایی نماید، متن رمز نگاری شده قابل مشاهده بوده و با فرض محرمانه بودن کلید، گیرنده می‌تواند از اینکه پیام از سوی فرستنده مورد نظر ارسال شده، اطمینان کند [2].

2-2-5- الگوریتم نامتقارن[16]

دسته دوم الگوریتم‌های رمز نامتقارن می‌باشند که استفاده‌های بسیار جالبی دارند. در این‌گونه رمزنگاری‌ها، کلید رمز از دو قسمت تشکیل شده است. به جای یک کلید مشترک از یک جفت کلید به نام‌های کلید عمومی و خصوصی استفاده می‌شود. کلید عمومی همان‌گونه که از عنوان آن مشخص است می‌تواند در دسترسی عموم قرار گیرد. در این روش از کلید عمومی برای رمزگذاری اطلاعات استفاده می‌شود. طرفی که قصد انتقال اطلاعات را به صورت رمزگذاری شده دارد اطلاعات را رمزگذاری کرده و برای طرفی که مالک کلید خصوصی است فرستاده می‌شود. مالک کلید، کلید خصوصی را پیش خود به صورت محرمانه حفظ می‌کند و به کمک آن مطالب را رمزگشایی می‌کند. در این دسته، کلیدهای رمزنگاری و رمزگشایی متمایزند و یا اینکه چنان رابطه پیچیده‌ای بین آن‌ها حکم فرماست که کشف کلید رمزگشایی (خصوصی) با در اختیار داشتن کلید رمزنگاری (عمومی)، عملاً ناممکن است [4]. در شکل (1) فرایند رمزگذاری و رمزگشایی به وسیله کلید عمومی و خصوصی نشان داده شده است.



شکل (1) : فرایند رمزگذاری و رمزگشایی

3-2-5- الگوریتم هش[17] یا درهمساز

این الگوریتم‌ها توابعی هستند که از نظر ریاضیاتی یک طرفه هستند. به این معنی که نمی‌توان از روی خروجی تابع مذکور مقدار ورودی را بدست آورد. از این توابع در رمزنگاری برای تولید نوعی اثر انگشت استفاده می‌شود. به عبارت دیگر هنگامی که داده‌ای به عنوان ورودی به این تابع داده می‌شود، چکیده‌ای از آن مجموعه داده تولید می‌شود که منحصر به فرد و قابل بازگشت است. امر مهم در این تابع این است که با تغییر حتی یک بیت از داده های ورودی، باید کل مقدار خروجی تابع هش تغییر کند [11].

3-5- امضای دیجیتال

امضای دیجیتال[18] نوعی رمزنگاری نامتقارن است که خصوصیات امضای دستی را در فضای الکترونیکی فراهم می‌کند. هر موجودیت منحصر به فرد در فضای مجازی دارای امضای دیجیتالی خاص خود است و تنها این موجودیت یا فرد قادر به تولید این امضاست. در نتیجه می‌توان مستندات، پیغام‌ها و داده‌های الکترونیکی را توسط امضای دیجیتال تأیید کرده و سندیت بخشید، به شکلی که مطمئن بود که تولیدکننده امضا چه کسی است و متن پیغام امضا شده، پس از امضا تغییر نکرده است. بدین وسیله اسناد الکترونیکی قابل پیگیری بوده و با توجه به عدم امکان جعل امضای دیجیتال، اسناد یا پیام‌های امضاء شده غیر قابل انکار است و مراجع قضایی می‌توانند از این خصوصیت جهت استناد قانونی به سند الکترونیکی استفاده کنند و به کمک این خصیصه فعالیت افراد در فضای مجازی جنبه حقوقی پیدا می‌کند و قوانین حقوقی اسناد کاغذی در مورد اسناد الکترونیکی قابل اجرا می‌شود [12].

اما امضای دیجیتال دارای خصوصیت دیگری نیز هست که امضای دستی فاقد آن است. به وسیله امضای دیجیتال می‌توان مطمئن بود که محتوای سند یا پیام بعد از امضا تغییر نکرده و افراد غیرمجاز سند الکترونیکی مربوطه را مخدوش نکرده‌اند. این به دلیل نوع الگوریتمی است که در طراحی امضای دیجیتالی مورد استفاده قرار می‌گیرد که الگوریتم هش یا درهمساز نام دارد این الگوریتم‌ها توابعی هستند که از نظر ریاضیاتی یک طرفه هستند. به این معنی که نمی‌توان از روی خروجی تابع مذکور مقدار ورودی را بدست آورد. از این

توابع در رمزنگاری برای تولید نوعی اثر انگشت استفاده می‌شود. به عبارت دیگر هنگامی که داده‌ای به عنوان ورودی به این تابع داده می‌شود، چکیده‌ای از آن مجموعه داده تولید می‌شود که منحصر به فرد است و قابل بازگشت نیز است [13].

بدین ترتیب با در اختیار داشتن متن سند یا پیام در کنار امضای دیجیتالی آن، می‌توان با اعتبار سنجی امضای دیجیتال، در عین حال از عدم تغییر محتوای آن نیز مطمئن شد. در نتیجه به کمک امضای دیجیتال در کنار قابلیت شناسایی امضاء کننده، امنیت خاصی نیز به اسناد الکترونیکی اضافه می‌شود که همان تمامیت یا حفظ یکپارچگی سند می‌باشد. امضای دیجیتال برای هر مستند یا پیغام به وسیله کلید خصوصی فرد تولید می‌شود و در واقع یک عدد با طول بلند است. کلید خصوصی فرد به صورت امن در وسیله‌ای مانند کارت هوشمند یا توکن نگهداری می‌شود. بدین ترتیب جعل امضای دیجیتالی بسیار مشکل‌تر از امضای دستی است [12].

5-4- الگوریتم امضای دیجیتال

هر طرح امضای دیجیتال شامل سه الگوریتم است که عبارتند از [12] :

1- **الگوریتم تولید کلید:** در این مرحله یک کلید محرمانه از یک سری کلیدهای محرمانه ممکن به صورت تصادفی انتخاب می شود. در واقع خروجی این الگوریتم کلید محرمانگی و یک کلید عمومی مترادف با آن است.

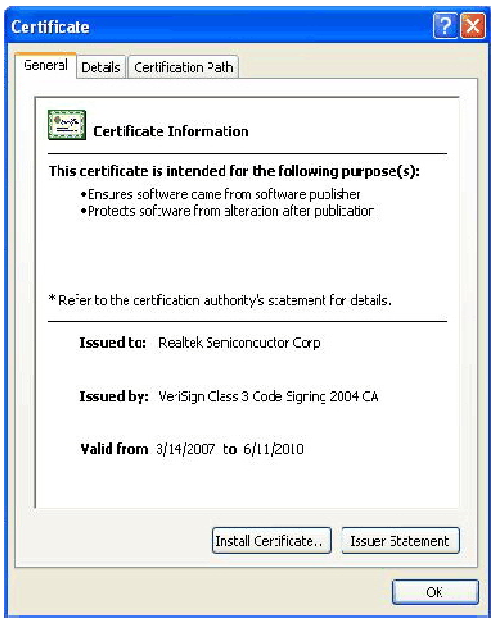
2- **الگوریتم امضا:** الگوریتمی است که با دادن پیام و کلید محرمانگی، امضای دیجیتال تولید می‌کند.

3- **الگوریتم شناسایی امضا:** الگوریتمی است که یک پیام، کلید عمومی و یک امضا را به صورت ورودی دریافت می‌کند و اعتبار آن پیام را تایید یا رد می‌کند.

5-5- گواهی دیجیتالی

گواهی دیجیتالی[19]، یک سند الکترونیکی امضاء شده و غیر قابل جعل است که هویت فرد را در فضای مجازی نشان می‌دهد به عبارتی معرف هویت فردی است که صاحب امضاء دیجیتالی است و توسط مرکز صدور گواهی[20] پس از اطمینان از صحت هویت فرد و تحت قوانین معینی برای یک شخص، سخت‌افزار یا نرم‌افزار صادر می‌شود و از اطلاعات درون آن می‌توان برای شناسایی دارنده‌ی گواهی و برقراری ارتباط امن با وی استفاده کرد [16].

متناظر با هر گواهی، داده یکتایی به نام کلید خصوصی وجود دارد. کلید خصوصی یک گواهی فقط باید در اختیار صاحب آن باشد، اما خود گواهی یک سند عمومی است که می‌توان آن را به همه نشان داد. پیام‌هایی را که با استفاده از یک گواهی رمز شده‌اند، تنها با کلید خصوصی مطابق به همان گواهی می‌توان رمزگشایی کرد. صدور یک گواهی به معنای آن است که دارندهٔ گواهی، کلید خصوصی متناظر با آن را در اختیار دارد [4]. در شکل (2) نمونه‌ای از گواهی دیجیتال آورده شده است.

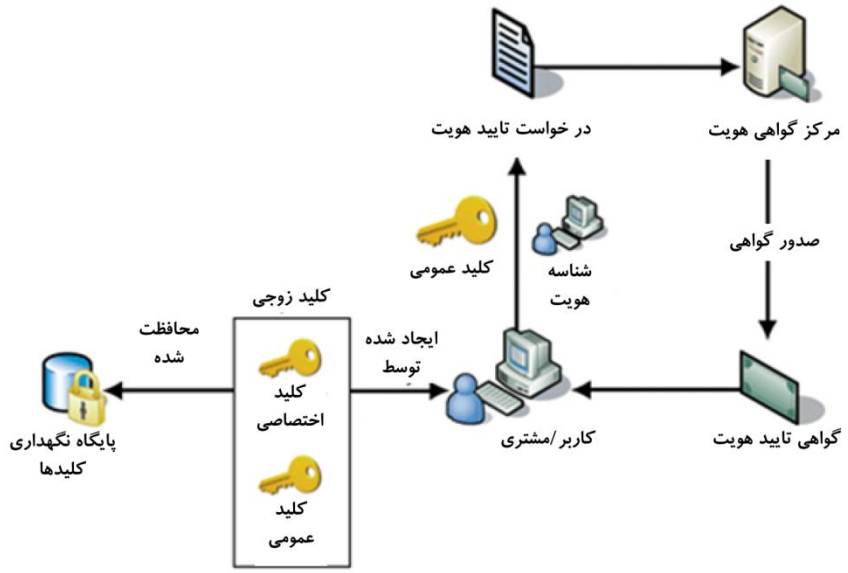


شکل (2) : نمونه‌ای از گواهی‌نامه دیجیتال

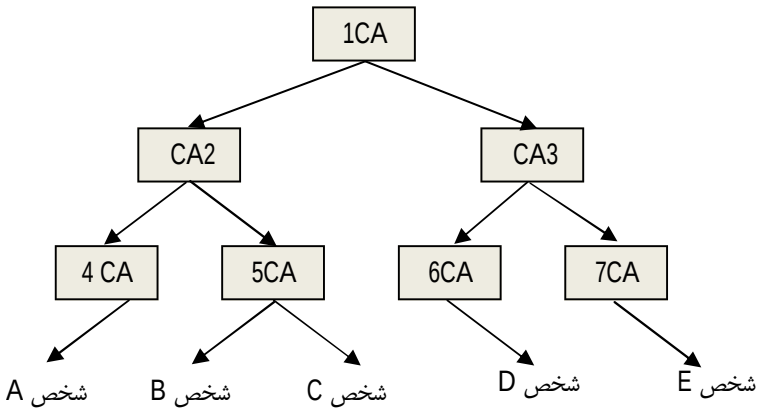
6- زیرساخت کلید عمومی

استفاده از گواهی‌های دیجیتالی و یک زیرساخت کلید عمومی[21] تلاش‌هایی برای وصل کردن هویت‌ها به امضاهای دیجیتالی [1] و یک معماری برای امن کردن مبادلات الکترونیکی است. این ساختار، استفاده از تعدادی طرف سوم مورد اعتماد را برای امن کردن مبادلات بین فرستنده و گیرنده پیشنهاد می کند (شکل3). هر یک از این مراکز مورد اطمینان، به نام مرکز گواهی هویت شناخته می‌شوند و وظیفهٔ اصلی آن‌ها صدور و نگهداری گواهی‌های الکترونیکی برای کاربران و مدیریت وضعیت گواهی‌ها است [3].

زیرساخت صنعت بانکداری و سازمان ثبت احوال کشور نمونه گویایی از این از این نوع زیر ساخت است، برای درک بهتر فرض کنید شخصی گواهی‌نامه دیجیتالی خود را برای شما ارسال نماید در صورتیکه شناختی نسبت به آن مرجع نداشته باشید چگونه می‌توانید به این گواهی‌نامه اعتماد کنید! ساده‌ترین راهکار این است که مرجعی معتبر که مورد اطمینان شماست، صلاحیت مرجع ناشناس را برای شما تضمین کند. اما در صورتیکه ارتباط مستقیمی میان مرجع معتبر شما و آن مرجع ناشناس وجود نداشته باشد، در این صورت از یک مرجع میانی شناخته شده استفاده می‌شود که مرجع ناشناس را تایید کند. شکل (4) نحوه انجام این فرایند را نشان می‌دهد به عنوان مثال فرض کنید کاربر B نیازمند تایید کاربر D است در این صورت برای تایید، مسیر CA6-CA3-CA1 باید طی شود. دقت داشته باشید که CA1 بالاترین مرجع شناخته شده است که تمامی کاربران و مراجع دیگر به آن اطمینان دارند [1].



شکل (3) : طرف سوم مورد اعتماد جهت تعیین هویت کاربران



شکل (4) : سلسله مراتب سه لایه‌ای از مراجع معتبر تایید هویت

7- کاربردهای گواهی دیجیتالی در تبادلات اینترنتی

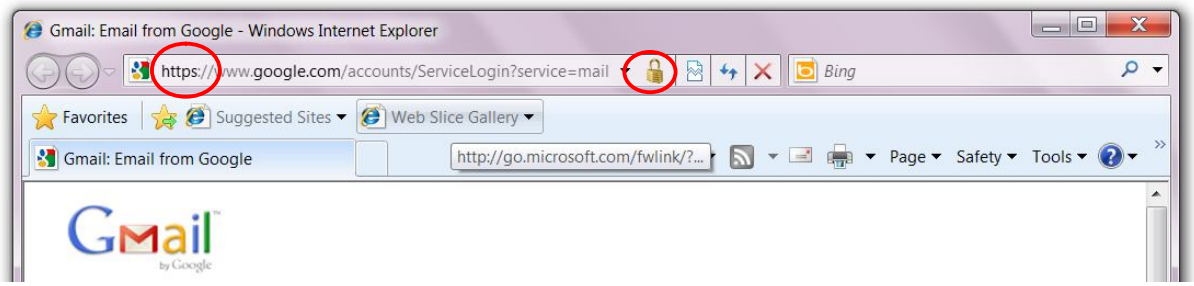
امضای دیجیتال در بسیاری از استانداردهای مبتنی بر وب مورد استفاده قرار می‌گیرد تا انتقال ایمن اطلاعات در بستر اینترنت را تضمین نماید. در اینجا به سه نمونه از این استانداردها اشاره می‌شود:

7-1- لایه اتصال امن[22] (SSL)

پروتکلی (مجموعه‌ای از قوانین) جهت برقراری ارتباطات ایمن میان سرویس دهنده و سرویس گیرنده در اینترنت است که توسط شرکت Netscape ابداع شده و از این پروتکل برای امن کردن پروتکل‌های غیر امن نظیر HTTP، LDAP، IMAP و ... استفاده می‌شود. بر این اساس یکسری الگوریتم‌های رمزنگاری بر روی داده‌های خام که قرار است از یک کانال ارتباطی غیر امن مثل اینترنت عبور کنند، اعمال می‌شود و محرمانه ماندن داده‌ها را در طول انتقال تضمین می‌کند [17].

به بیان دیگر شرکتی که صلاحیت صدور و اعطاء گواهی‌های دیجیتال SSL را دارد، برای هر کدام از دو طرفی که قرار است ارتباطات میان شبکه‌ای امن داشته باشند، گواهی‌های مخصوص سرویس دهنده و سرویس گیرنده را صادر می‌کند و با مکانیزم‌های احراز هویت خاص خود، هویت هر کدام از طرفین را برای طرف مقابل تأیید می‌کند. البته علاوه بر این تضمین می‌کند، اگر اطلاعات حین انتقال به سرقت رفت، برای رباینده قابل درک و استفاده نباشد که این کار را به کمک الگوریتم‌های رمزنگاری و کلیدهای رمزنگاری نامتقارن و متقارن انجام می‌دهد [17].

پروتکل SSL در تمامی مرورگرهای مهم و وب سرورها اجرا شده است. پیشوند https:// برای آدرس‌های اینترنتی (URL) با مشخصه قفل کوچکی که در گوشه نوار وضعیت[23] و یا نوار آدرس[24] مرور گر مشاهده می‌گردد، نشانه‌های استفاده از این پروتکل هستند. شکل (5) نمونه‌ای از وب سایت مجهز به این پروتکل را نشان می‌دهد.



شکل (5) : وب سایت مجهز به گواهی SSL

7-2- استاندارد تبادل الکترونیکی امن[25] (SET)

این استاندارد ابتدا مورد توجه شرکت‌هایی مانند Visa، MasterCard، Netscape و مایکروسافت قرار گرفت که به دنبال تامین امنیت و محرمانگی تبادلات مالی اینترنتی بودند. SET با استفاده از رمزنگاری و گواهی‌نامه‌های دیجیتال زنجیره‌ای از اعتماد بین فروشندگان، بانک‌ها و مشتریان ایجاد می‌کند. این استاندارد ممکن است به همراه پروتکل‌هایی مانند SSL مورد استفاده قرار گیرد.

به منظور فراهم سازی امکان خرید اینترنتی، گواهی دیجیتال مشتمل بر کلید عمومی خریدار و تاریخ انقضای آن از سوی بانک مورد نظر به مشتری داده می‌شود. سپس تبادل میان خریدار، فروشنده و بانک انجام می‌گیرد [18].

7-3- استاندارد secure MIME[26]

این استاندارد برای ارسال ایمن نامه‌های الکترونیکی طراحی شده است. در همین راستا، ابتدا استاندارد MIME معرفی شد که به کمک آن افراد می‌توانستند بدون نگرانی از دسترسی سایر افراد به نامه‌هایشان اقدام به مبادله الکترونیکی آن‌ها نمایند. سپس نسخه ایمن‌تر این استاندارد به نام S/MIME ارائه شد. بر اساس این استاندارد، الزامات امنیتی احراز هویت، تمامیت پیام، انکارناپذیری (با استفاده از امضای دیجیتال) و محرمانگی و امنیت (با استفاده از رمزنگاری) برای نامه‌ها و پیام‌های الکترونیکی تامین می‌گردد [19].

8- کاربردهای امضای دیجیتالی در انواع کسب و کار

کاربردهای امضای دیجیتالی به تفکیک انواع مدل‌های کسب و کار به قرار زیر است [1]. بدیهی است روز به روز بر کاربردهای جدید آن در این عرصه افزوده می‌شود.

تبادلات B2B[27]: استفاده از امضای دیجیتالی در تجارت کسب‌وکار ، باعث تایید هویت طرفین معامله شده و اطمینان لازم برای عدم تغییر و دستکاری ارتباطات مربوط به معامله را فراهم می‌کند. شرکت‌هایی که محصولات یا خدماتی از تامین کنندگان خریداری نموده و یا محصولات و خدماتی به مشتریان ارائه می‌دهند در سفارشات خرید، قبض‌های رسید، فرم‌های وب، یا سیستم‌های خرید آنلاین به امضای دیجیتالی نیاز دارند.

تبادلات B2C[28] : در تجارت کسب و کار با مشتری، امضای دیجیتال عمدتاً به منظور احراز هویت مشتری و اطمینان از عدم تغییر جزئیات معامله در حین ارتباط بکار برده می‌شود. همچنین علاوه بر کاربرد در زمینه فروش، در دیگر حوزه‌های کسب و کار با مشتری مانند خدمات مالی، بانکداری الکترونیک، تبادلات سهام و بیمه نیز به شکلی گسترده مورد استفاده قرار می‌گیرد.

تبادلات G2G[29] : در تعاملات بین نهادهای دولتی، استفاده از امضای دیجیتالی به دلیل اطمینان از احراز هویت و تمامیت پیام‌ها و اسناد مبادله شده بوده و اغلب انکارناپذیری از اهمیت کمتری برخوردار است. به عنوان مثال، در مورد ارتباط میان نهادهای اجرایی قانونی در خصوص تبهکاران بین‌المللی باید مطمئن شد که پیام‌ها از منبع درستی صادر شده‌اند، چون پیام‌های اشتباه و دستکاری شده می‌تواند پیامدهای خطرناکی به دنبال داشته باشد.

تبادلات G2B[30] : دولت‌ها هنگام تبادل با مراکز تجاری خواهان احراز هویت آن‌ها و اطمینان از عدم انکار و عدم تغییر ارتباطات فی‌مابین هستند. در بسیاری از موارد نیز دولت‌ها می‌خواهند شواهدی از ارتباطات خود با مراکز تجاری داشته باشند تا در صورت لزوم در دادگاه‌ها ارائه کنند.

شرکت‌های تولید کننده محصولات و خدمات دولتی می‌توانند پیشنهادات مناقصه‌ای خود را به صورت دیجیتالی امضاء می‌کنند و از سوی دیگر دولت‌ها نیز می‌توانند سفارشات خرید خود را به همین صورت تایید کنند. همچنین امضای دیجیتال را می‌توان در مورد اظهارنامه‌های مالیاتی کسب و کارها بکار برد.

تبادلات G2C[31] : در این نوع تبادلات، برای یک نهاد دولتی که با شهروندان سر و کار دارد احراز هویت شهروندان و اطمینان از عدم تغییر پیام‌ها در تبادلات از طریق بکارگیری امضای دیجیتال صورت می‌گیرد.

دولت‌ها می‌توانند برخی خدمات آنلاین خود مانند مجوز فعالیت، احداث یا بهره‌برداری، دریافت اظهار نامه مالیاتی از طرف اشخاص حقیقی را به صورت آنلاین و از طریق پرتال خود صادر کرده و یا حتی رای گیری الکترونیکی انجام دهند.

9- نتیجه گیری

در حال حاضر امنیت در فضای اینترنت یکی از مهم‌ترین مسایل حوزه ارتباطات است. چرا که در نبود امنیت، سارقان می‌توانند اطلاعات افراد را بربایند یا خودشان را به جای دیگری جا بزنند و اطلاعات دیگران را دریافت و یا جعل نمایند. امضای دیجیتالی یکی از راهکارهایی است که برای جلوگیری از بروز این مشکل معرفی گردید. امضای دیجیتال مزایای بیشتری نسبت به امضای دستی دارد زیرا به کمک الگوریتم‌های پیچیده‌ای که در طراحی امضای دیجیتالی مورد استفاده قرار می‌گیرد و مراکز تعیین هویتی که گواهی‌های دیجیتالی را تایید می‌کنند می‌توان مطمئن شد که محتوای سند یا پیام بعد از امضا، تغییر نکرده و افراد غیرمجاز سند الکترونیکی مربوطه را مخدوش نکرده‌اند و محتوای پیام بدون اجازه برای سایرین افشا نشده است.

دولت نیز برای توسعه زیر ساخت های دولت الکترونیک و تشویق شهروندان و بخش‌های مختلف تجاری جهت استفاده از تجارت الکترونیک می‌بایست به مسئله حفظ دارایی‌های شخصی و ایجاد یک محیط امن جهت تبادل الکترونیک به کمک امضای دیجیتالی توجه ویژه‌ای نماید. به هر حال تا زمانی که امنیت اطلاعات و مواردی مانند امضای دیجیتالی، کاملاً جا نیافتد نمی‌توان به همه‌گیری بخش‌هایی چون دولت الکترونیک و یا تجارت الکترونیک امیدوار بود.

خوشبختانه در بورس اوراق بهادار و نظام بانکی کشور گام‌های خوبی در جهت بکارگیری از امضای دیجیتالی برداشته شده است که این امر می‌تواند با تبلیغات بیشتر، بالا بردن آگاهی مدیران سایر بخش‌های درگیر و حمایت‌های دولت زمینه مناسبی را برای توسعه فضای سالم سایبری، فراهم سازد.

منابع

[1] سادوسکای جورج، دمپزی جیمز اکس و دیگران، **راهنمای امنیت فناوری اطلاعات**، ترجمه مهدی میردامادی و دیگران، دبیرخانه شورای عالی اطلاع رسانی،1384

[2] عبداللهی علی و دیگران، **مفاهیم و راهنمای امضاء دیجیتال**، جلد اول، سازمان بورس اوراق بهادار، شرکت اطلاع رسانی و خدمات بورس، 1389

[3] سایت رسمی مرکز صدور گواهی دیجیتالی پارس‌ساین، http://www.parssign.com تاریخ بهره برداری: فروردین 1390

[4] Vacca, J. R. (2007). *Practical internet security*, Springer-Verlag New York Inc.

[5] Crescenzo, G. D. and A. Rubin.(2007). *Financial cryptography and data security*, Springer.

[6] McCarthy, M. P. and S. Campbell. "*Security transformation.*" New York. 2001

[7] King, C. M., Curtis E. Dalton, and T. Ertem Osmanoglu. *Security Architecture: Design, Deployment & Operations*. New York: Osborne, McGraw-Hill. 2001

[8] Grant, G. L. *Understanding digital signatures: establishing trust over the Internet and other networks*, McGraw-Hill. 1998

[9] Kennedy, P. R., T. G. Hall, et al. *Security token and method for wireless applications*, Google Patents. 2000)

[10] Singhal, A. *Data warehousing and data mining techniques for cyber security*, Springer-Verlag New York Inc. 2007

[11] Stanger, J., P. T. Lane, et al. CIW: *security professional: study guide*, Sybex Inc. 2002

[12] Gupta, K. N., K. N. Agarwala, et al. *Digital Signature: Network Security Practices*, PHI Learning Pvt. Ltd. 2005

[13] Laborde, C. M. *Electronic Signatures in International Contracts*, Peter Lang. 2010

[14] Scott, M. D. *Internet and technology law desk reference*, Aspen Law & Business. 2004

[15] Stallings, W. *Cryptography and network security*, Prentice Hall New Jersey; 2003

[16] Garfinkel, S. and G. Spafford. *Web security, privacy and commerce*, O'Reilly Media. 2002

[17] Davies, J. *Implementing SSL/TLS Using Cryptography and PKI*, Wiley.2011

[18] Bagad, V. *Management information systems*, Technical Publications. 2009

[19] HAUSMAN, K., E. TITTEL, et al.. "*Security+ exam cram 2 (exam cram syo-101).*" 2003

[ć] Information security

[2] Information security system

[3] فیشینگ(Phishing): در زمینه امنیت رایانه‌ای به تلاش برای سرقت و دستیابی به اطلاعات حساس افراد مانند نام کاربری، کلمه عبور و اطلاعات کارت‌های اعتباری به‌وسیله جازدن خود به جای یک وب‌گاه معتبر گفته می‌شود.

[4] نرم افزار های جاسوسی مانند keylogger ها می توانند بر روی سیستم قربانی نصب شوند و هر کاری که کاربر انجام می دهد را ثبت و برای هکرها ارسال نمایند و از این طریق اطلاعات محرمانه و شناسه های کاربری ربوده می شود.

[5] E-mail

[6] Confidentiality

[7] Integrity

[8] Authentication

[9] Non-repudiation

[10] Biometrics

[11] Security token

[12] Cryptography

[13] Encryption

[14] Decryption

[15] Symmetric algorithms

[16] Asymmetric algorithms

[17] Hash

[18] Digital signature

[19] Digital certificate

[20] Certificate Authority

[21] Public key infrustructure

[22] Secure Socket Layer

[23] Status bar

[24] Address bar

[25] Secure Electronic Transaction

[26] Secure/Multipurpose Internet Mail Extension

[27] Business to business

[28] Business to customer

[29] Government to government

[30] Government to business

[31] Government to customer