امنیت در تجارت الکترونیکی

دکتر محمود زرگر*

تاریخ دریافت ۸۶/۷/۲۳	تاریخ پذیرش ۸۶/۱۱/۷

تجارت الکترونیکی زمانی به واقعیت می‌پیوندد که امنیت آن نیز تأمین شده باشد. در این مقاله ابتدا به ضرورت امنیت در تجارت الکترونیکی و مقایسه آن با امنیت در تجارت سنتی و سپس به تهدیدات و خدمات آن در چهار موضوع محرمانگی، تصدیق هویت و سندیت، تمامیت و انکارناپذیری پرداخته شده است. در واقع این چهار موضوع درد تجارت الکترونیکی است. چرا که در صورت تأمین این چهار خدمت امنیتی در سطح قابل قبول برای اجرا، تجارت الکترونیکی تأمین شده است. موضوع بعدی الگوریتم‌های رمزنگاری است که به‌عنوان زیربنای اصلی تأمین چهار خدمت امنیتی مطرح است. بخش انتهایی مقاله به امضا و گواهی الکترونیکی و دیگر روش‌ها یا خدمات تأمین امنیت در ابعاد مختلف تجارت الکترونیکی می‌پردازد.

کلیدواژه‌ها: امنیت تجارت الکترونیکی؛ محرمانگی؛ تصدیق هویت و سندیت؛ تمامیت و انکارناپذیری؛ رمزنگاری متقارن؛ رمزنگاری نامتقارن؛ رمزنگاری جفت کلیدی؛ رمزنگاری درهم‌ساز؛ امضای الکترونیکی؛ گواهی الکترونیکی؛ لایه حفره‌های امنیتی؛[1] مَهر زمانی

---

* استاد دانشگاه امام صادق (ع)، مدیر کل دفتر توسعه تجارت الکترونیکی، عضو کمیته راهبری تسهیل تجاری و توسعه تجارت الکترونیکی آسیا (AFACT).

E-mail: mahmood.zargar@gmail.com

1. Secure Sockets Layer (SSL)

مقدمه

یکی از مفاهیمی که ذهن بشر را در ادوار مختلف تاریخی به‌خود جلب کرده و ما همواره شاهد ظهور نوآوری‌هایی برای پاسخ‌گویی به این نیاز اساسی بشر بوده‌ایم؛ مسئله «برقراری امنیت» در حوزه ارتباطات است.

با نگاهی گذرا به تاریخ، به ابزارها و روش‌های مختلف برقراری امنیت در ارتباطات برمی‌خوریم. برای مثال می‌توان به شیوه رمزنگاری ناپلئون در مکاتبات نظامی اشاره کرد که با جابه‌جا کردن حروف براساس طرح مشخّصی انجام می‌شد. اما نکته قابل توجه در بررسی این روش‌ها اینکه همواره افزایش تهدیدات و شکل‌های نوین تهدیداتی ــ که متوجه ارتباطات درون و بین گروه‌ها بوده ــ موجب ایجاد روش‌های پیچیده‌تری در برقراری امنیت ارتباطات شده است.

امروزه با توسعه روزافزون اینترنت و فناوری‌های آن از یک‌سو و از سوی دیگر حرکت‌های جهانی در راستای انجام مبادلات تجاری اینترنتی، با هدف تسهیل فرایندهای تجارت داخلی و بین‌المللی، شاهد ظهور جنبه‌های جدیدی از تهدیدات امنیتی در جریان مبادلات تجاری هستیم. در نتیجه، کشورها برای مقابله با این تهدیدات به سمت ایجاد زیرساخت‌هایی حرکت کرده‌اند تا در راستای گسترش مبادلات تجارت الکترونیکی به اهداف ملی خود دست یابند.

اما برای برقراری امنیت در سطوح مختلف مربوط به فرایند مبادلات تجارت الکترونیکی باید روش‌های پیچیده و نوینی به‌کار گرفت؛ امری که با گسترش توانمندی‌های بشر درزمینه فناوری‌های رایانه و اینترنت، هر روز بر پیچیدگی‌های فنّی آن افزوده می‌شود.

برای برقراری امنیت در مبادلات تجارت الکترونیکی، به برقراری امنیت در دو سطح کلان به‌شرح زیر توجه می‌شود:

۱. **امنیت در سطح شبکه‌های مخابراتی**: منظور از امنیت در سطح شبکه‌های مخابراتی، تدارک راهکارهای جلوگیری از نفوذ غیرمجاز افراد به شبکه‌های مخابراتی است. برقراری

این سطح از امنیت به‌وسیله متخصّصان شبکه‌های ارتباطی و با استفاده از پروتکل‌ها و تجهیزات امنیتی شبکه‌های ارتباطی مانند دیوار آتش[1] و ... انجام می‌شود.

۲. **امنیت در سطح کاربردهای تجارت الکترونیکی**: برقراری امنیت در سطح کاربردهای تجارت الکترونیکی دقت بیشتری می‌طلبد. در این سطح، علاوه بر امنیت در ارسال و دریافت پیام، مفهوم دیگری به نام «اعتماد» نیز حائز اهمیت است. منظور از برقراری امنیت در سطح کاربردها این است که امنیت مبادلات تجارت الکترونیکی در شبکه‌های مخابراتی، با ورود و حضور مجاز یا غیرمجاز افراد به این شبکه‌ها تهدید نشود. برقراری این سطح از امنیت مستلزم استفاده از ابزارهای امنیتی تجارت الکترونیکی است. این ابزارها به‌نحوی طراحی شده‌اند که با توجه به ماهیت و پیچیدگی روش کار، استفاده از آنها در جریان انجام مبادلات تجارت الکترونیکی بسیار آسان است.

این گزارش به تشریح ابزارهای امنیتی تجارت الکترونیکی در سطح کاربردها می‌پردازد تا بتوان با به‌کارگیری این ابزارها، امنیت مبادلات تجاری را در سطح شبکه اینترنت امکان‌پذیر ساخت. البته باید گفت که هر کدام از این ابزارها و روش‌ها، سطحی از امنیت را برای مبادلات تجارت الکترونیکی فراهم می‌آورند و هیچ‌گاه نمی‌توان ادعا کرد که این ابزارها امنیت صد درصد را به وجود می‌آورند؛ بلکه در تجارت الکترونیکی به سطحی از امنیت نیاز داریم که به وجودآورنده اعتماد باشد. ازاین‌رو در بیشتر مستندات، کلمه اعتماد به‌همراه امنیت طرح می‌شود.

البته این نکته نیز حائز اهمیت است که سطحی از امنیت که به‌وسیله استفاده از این ابزارها و روش‌ها در جریان فرایند تجارت الکترونیکی به وجود می‌آید، از سطح امنیت موجود در تجارت سنّتی بسیار بیشتر است. نکته مهم اینکه برای انجام تجارت الکترونیکی ایمن، باید این ابزارها را شناخت و با به‌کارگیری آنها به سطح قابل قبول امنیت در این عرصه دست یافت.

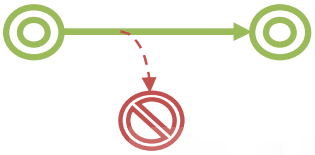
---

1. Fire wall

۱ خدمات امنیتی مورد نیاز در تجارت الکترونیکی

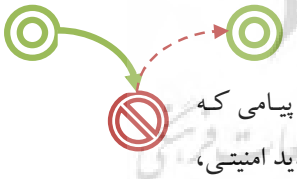
پرداختن به مقوله امنیت در تجارت الکترونیکی، باید هم‌زمان با مقوله تهدیدات و خطرها انجام شود. به‌طور کلی، برای مقابله با تهدیدات امنیتی موجود در مسیر فرایند مبادلات تجارت الکترونیکی، به خدمات چهارگانه امنیتی ذیل نیاز است:

۱. **محرمانگی**:[1] یکی از تهدیدات موجود در مسیر فرایند مبادلات تجارت الکترونیکی، استراق‌سمع[2] است. استراق‌سمع در مبادلات تجارت الکترونیکی به این معناست که نسخه‌ای از مبادلات انجام شده بین طرفین تجاری در دسترس فرد غیرمجازی قرار گیرد. برای مقابله با این حمله امنیتی به خدمت امنیتی محرمانگی نیاز داریم.



۲. **تصدیق هویت و سندیت**:[3] یکی دیگر از تهدیدات موجود، کلاهبرداری[4] است. کلاهبرداری در مبادلات تجارت الکترونیکی به این معناست که فرد غیرمجازی پیامی را، به جای یکی از طرفین تجاری، برای طرف دیگر ارسال می‌کند. برای مقابله با این تهدید امنیتی، به خدمت امنیتی احراز هویت نیازمندیم.

۳. **تمامیت**:[5] نوع دیگر تهدیدات امنیتی، دستکاری[6] است که عبارت است از قرار گرفتن فرد غیرمجاز در میانه مسیر مبادله پیام تجاری و دریافت پیام، اعمال تغییرات در پیام و سپس ارسال آن از طرف فرستنده پیام. ازاین‌رو پیامی که گیرنده دریافت می‌کند با پیامی که فرستنده ارسال کرده، متفاوت است. برای مقابله با این تهدید امنیتی،



1. Privacy
2. Interception
3. Authentication
4. Spoofing
5. Integrity
6. Modification

به خدمت امنیتی تمامیت نیاز داریم.

۴. **انکارناپذیری**:[1] آخرین نوع تهدیدات امنیتی، مسئله احراز هویت طرفین مبادله است. چرا که اگر خدمتی برای احراز هویت واقعی طرفین مبادله وجود نداشته باشد، تمام پیام‌ها و اسناد مبادله شده در جریان یک فرایند تجارت الکترونیکی، قابل انکار است. در نتیجه، برای جلوگیری از این تهدید به خدمت امنیتی انکارناپذیری نیازمندیم.

همان‌گونه که مشاهده شد، این نوع خدمات امنیتی تجارت الکترونیکی، ماهیت اعتمادسازی قابل توجهی دارند. برای برقراری این خدمات امنیتی، ترکیبی از راهکارهای مختلف به‌شرح ذیل، استفاده می‌شود:

۱. **الگوریتم‌های رمزنگاری متقارن**:[2] این الگوریتم‌ها از قدیم همواره با این شیوه که فرستنده داده‌ها را به‌وسیله یک کلید رمزنگاری می‌کند و گیرنده نیز داده رمزنگاری شده را با همان کلید رمزگشایی می‌کند، مورد استفاده بوده‌اند. به‌این‌ترتیب، در این الگوریتم از یک کلید برای هر دو عمل رمزنگاری و رمزگشایی بهره‌گیری می‌شود. این الگوریتم برای ایجاد محرمانگی در اسناد و پیام‌ها کاربرد دارد. برای مثال می‌توان استفاده رایج از کلمه عبور را برای دسترسی به اسناد و فایل‌ها بیان کرد.

اما این روش با دو محدودیت عمده مواجه است:

الف) هر فرد باید در مبادلات خود با فرد دیگر، یک کلید مشترک داشته باشد. بنابراین با افزایش تعداد افراد، تعداد کلیدهای مورد نیاز برای رمزنگاری و رمزگشایی اسناد و پیام‌ها، تصاعدی افزایش می‌یابد.

ب) محدودیت اساسی در انتقال ایمن کلیدهاست. به‌این‌ترتیب که فرستنده پس از رمزنگاری و ارسال پیام یا سند خود، باید کلید رمزگشایی آن پیام یا سند را نیز برای

---

1. Non-repudiation
2. Symmetric Encryption Algorithms

گیرنده ارسال کند و اگر بخواهد کلید را با همین شیوه رمزنگاری کرده و ارسال کند؛ با مشکل محدودیت انتقال کلید مواجه می‌شود.

در نتیجه استفاده صِرف از این شیوه رمزنگاری نمی‌تواند محرمانگی اسناد را تضمین کند. برای حل این مشکل باید از شیوه رمزنگاری نامتقارن یا ترکیب این دو شیوه استفاده کرد.

۲. الگوریتم‌های رمزنگاری نامتقارن:[1] در این الگوریتم، برخلاف الگوریتم رمزنگاری متقارن، از یک کلید برای رمزنگاری سند یا پیام و از کلید دیگر برای رمزگشایی آن استفاده می‌شود. با این توضیح که این دو کلید با یک رابطه ریاضی به هم مرتبط هستند که کشف آن به تلاش بلندمدت ابررایانه‌ها نیازمند است.

به کلید مورد استفاده برای رمزنگاری، «کلید عمومی»[2] و به کلید مورد استفاده برای رمزگشایی، «کلید خصوصی»[3] گفته می‌شود. ازاین‌رو، کلید خصوصی هر فرد فقط نزد خود او و کلید عمومی وی در دسترس تمامی افراد دیگر قرار می‌گیرد. حال هنگامی که فرستنده می‌خواهد سند یا پیامی را به‌صورت امن و محرمانه برای گیرنده ارسال کند؛ آن را با کلید عمومی گیرنده، رمزنگاری کرده و در طرف دیگر، گیرنده با کلید خصوصی خود آن پیام را رمزگشایی می‌کند.

همان‌گونه که اشاره شد، ارتباط ریاضی میان کلید عمومی و خصوصی، ارتباط بسیار پیچیده‌ای است و گشایش آن به سال‌ها تلاش ابررایانه‌ها نیازمند است. به‌علاوه از یک‌سو این پیچیدگی موجب کُند شدن سرعت رمزنگاری و رمزگشایی اسناد و پیام‌ها شده و از سوی دیگر (همان‌طور که در الگوریتم رمزنگاری متقارن اشاره شد) مشکل چگونگی ارسال محرمانه و ایمن کلمه رمز متقارن وجود دارد.

حال راه حل ترکیبی پیشنهادی، استفاده از هر دو روش است. یعنی ابتدا سند یا پیام با استفاده از الگوریتم رمزنگاری متقارن به‌صورت رمز درآورده شود و سپس کلید

---

1. Asymmetric Encryption Algorithms
2. Public Key
3. Private Key

رمزگشایی آن با استفاده از الگوریتم رمزنگاری نامتقارن به‌صورت ایمن و محرمانه ارسال شود. به‌این‌ترتیب دو مشکل کُندی الگوریتم رمزنگاری نامتقارن و ارسال کلمه رمز در الگوریتم رمزنگاری متقارن به‌طور هم‌زمان حل می‌شود.

کلیدهای خصوصی و عمومی مورد استفاده در این الگوریتم‌ها به‌صورت فایل‌های رایانه‌ای هستند و برای نصب آنها بر رایانه، کافی است روی آنها کلیک کنیم.

۳. **الگوریتم‌های درهم‌ساز**:[1] نوع سوم الگوریتم‌های رمزنگاری، الگوریتم درهم‌ساز نام دارد. تفاوت این الگوریتم با دو الگوریتم رمزنگاری متقارن و نامتقارن در این است که این الگوریتم رمزنگاری را به‌صورت یک‌طرفه انجام می‌دهد؛ یعنی با استفاده از روش‌های مختلف ریاضی، سند یا پیام را به رشته‌ای از اعداد، حروف و علائم با طول مشخص تبدیل می‌کند؛ اما این رشته قابلیت بازگشت به سند یا پیام اصلی را ندارد.

مزیت اصلی این الگوریتم، در ارائه خدمت امنیتی «تمامیت» است. دلیل آن هم این است که با درهم‌سازی دو سند یا پیام مختلف، احتمال ایجاد رشته‌های یکسان از (۰/۰۰۱ درصد) کمتر است؛ درحالی‌که رشته ایجاد شده از درهم‌سازی یک سند، همواره رشته‌ای ثابت است.

به‌منظور تأمین خدمات امنیتی و اعتماد در سطح فرایندهای تجارت الکترونیکی به ابزارهایی نیاز است که مهم‌ترین آنها عبارت است از: «امضای الکترونیکی»، «گواهی الکترونیکی»، «لایه حفره‌های امنیتی» و «مَهر زمانی». البته ابزارهای متنوع دیگری نیز در این حوزه مطرح است که پرداختن به آنها در این مقاله نمی‌گنجد.

۲ امضای الکترونیکی

در تجارت سنّتی برای تأمین خدمات امنیتی از جمله «تمامیت»، «انکارناپذیری» و «احراز هویت» از ابزارهای مختلفی مانند امضا، دفاتر اسناد رسمی، شناسنامه، کارت‌های شناسایی و ... استفاده می‌شود. اما در فضای الکترونیکی به‌دلیل وجود سه ویژگی عمده، نمی‌توان از این ابزارها استفاده کرد:

1. Hash Algorithms

۱. در اسناد کاغذی، تشخیص نسخه اصلی از نسخه کپی‌شده به‌راحتی امکان‌پذیر است؛ اما اطلاعات الکترونیکی ترکیبی از بیت‌ها بوده و میان نسخه اصل و کپی شده تفاوتی وجود ندارد.

۲. معمولاً تغییر در اسناد کاغذی موجب ایجاد نشانه‌های فیزیکی بر روی سند می‌شود. برای مثال، پاک‌کردن حروف و اعداد در اسناد کاغذی می‌تواند موجب تغییر رنگ کاغذ شود؛ درحالی‌که حذف یا تغییر تعدادی بیت یا بایت از یک سند الکترونیکی، هیچ اثر فیزیکی برجای نمی‌گذارد.

۳. اثبات صحت مدارک کاغذی با بررسی برخی خواص و نشانه‌های فیزیکی آن مثل شکل ظاهری، دست‌خط، امضا و ... امکان‌پذیر است؛ حال آنکه اثبات صحت مدارک الکترونیکی فقط باید بر مبنای اطلاعات خود سند باشد.

در نتیجه، در فضای مبادلات تجارت الکترونیکی باید از ابزارهایی متناسب با ویژگی‌های آن استفاده کرد. به این منظور، با بهره‌گیری از الگوریتم‌های رمزنگاری نامتقارن و درهم‌سازی، ابزاری امنیتی با نام «امضای الکترونیکی» ابداع شد.

عمده‌ترین تفاوت میان دو روش مورد استفاده در امضای الکترونیکی و رمزنگاری نامتقارن این است که در امضای الکترونیکی، فرستنده برای امضای سند از کلید خصوصی خود و گیرنده برای تأیید امضای موجود بر روی سند، از کلید عمومی فرستنده استفاده می‌کند.

مراحل امضای یک سند یا پیام تجاری با استفاده از امضای الکترونیکی عبارتند از:

۱. فرستنده سند، با استفاده از الگوریتم درهم‌ساز، رشته درهم‌سازی شده سند را ایجاد می‌کند.

۲. فرستنده، رشته درهم‌سازی شده سند را با استفاده از کلید خصوصی خود رمزنگاری و آن را به سند مورد نظر الصاق می‌کند.

گیرنده، پس از دریافت سند مراحل زیر را طی می‌کند:

۱. گیرنده، با استفاده از الگوریتم درهم‌ساز، رشته درهم‌سازی شده سند را ایجاد می‌کند.

۲. گیرنده با استفاده از کلید عمومی فرستنده، به رمزگشایی رشته الصاق‌شده به سند اقدام می‌کند.

۳. گیرنده دو رشته درهم‌سازی شده را در اختیار دارد؛ یکی از رشته‌ها را خود تولید کرده و دیگری را فرستنده هنگام امضای سند تولید کرده است.

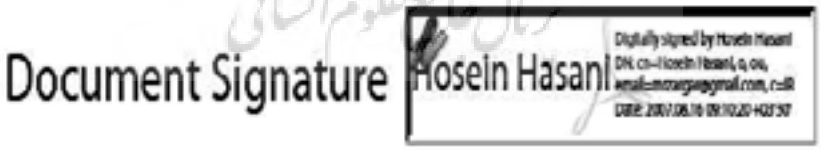
۴. حال اگر این دو رشته با هم یکسان باشند؛ گیرنده از تمامیت این سند اطمینان حاصل می‌کند.

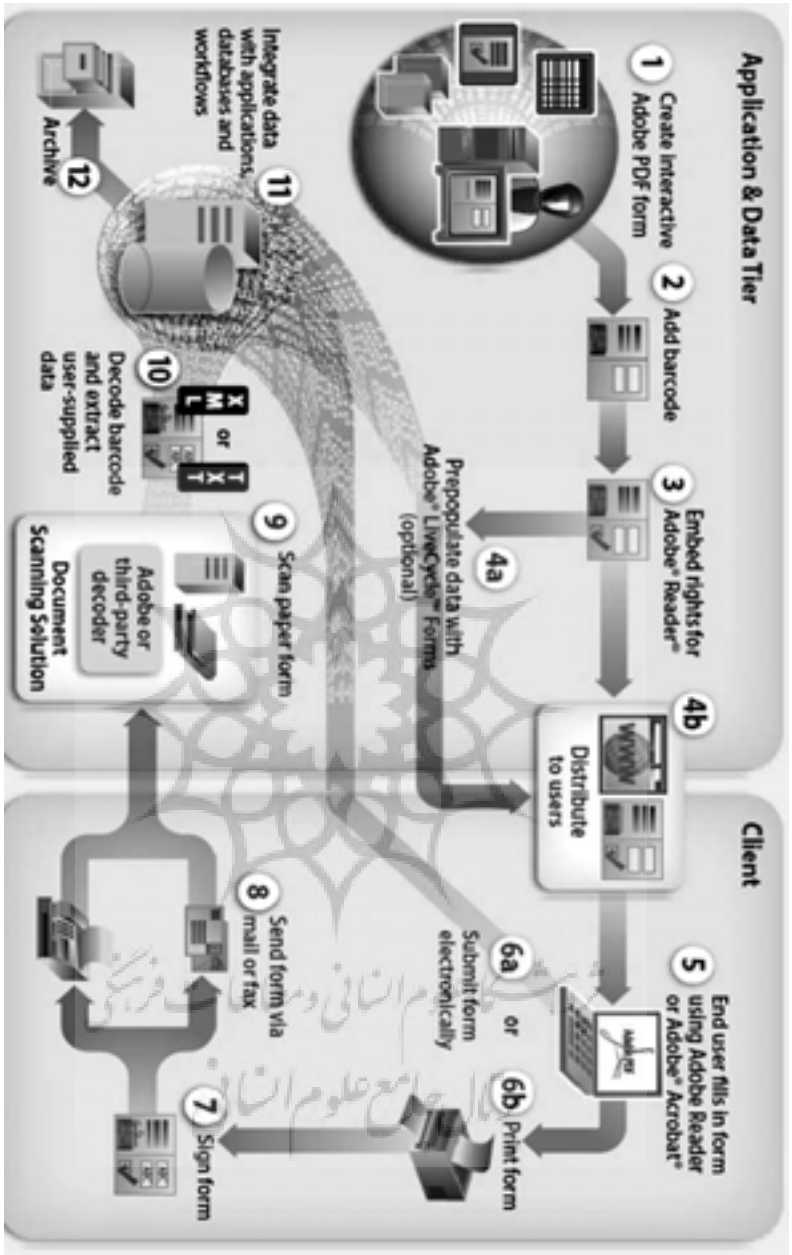
تمام این مراحل فقط با چند کلیک ساده ماوس رخ می‌دهد. در حقیقت، برای استفاده از امضای الکترونیکی در مبادلات تجارت الکترونیکی به انجام این عملیات امنیتی به‌وسیله کاربر نیازی نیست، بلکه تمام این مراحل در پشت پرده نرم‌افزارهای تجارت الکترونیکی به وقوع می‌پیوندد.

برای مثال، در حوزه جریان کار فرم‌های مورد استفاده در تجارت الکترونیکی، شرکت‌های بزرگ رایانه‌ای هریک به ایجاد راهکارهایی برای تسهیل فرایندهای تجاری الکترونیکی اقدام کرده‌اند که دو نمونه جهانی موفّق آن نرم‌افزار Infopath از شرکت مایکروسافت و نرم‌افزار LiveCycle از شرکت Adobe است. در شکل ۱ جریان کار اسناد الکترونیکی در نرم‌افزار LiveCycle نشان داده شده است.

برای امضای یک سند تجاری در این نرم‌افزار، کافی است روی مکان امضا کلیک کنید تا نرم‌افزار به‌صورت خودکار، امضای الکترونیکی را در پای آن قرار دهد. گیرنده سند، امضای الکترونیکی موجود در سند تجاری را به شکل زیر مشاهده می‌کند و با کلیک کردن روی آن می‌تواند به مشخّصات دقیق امضاکننده سند، اعتبار یا عدم اعتبار امضا، زمان دقیق امضای سند و ... پی ببرد.

این به زمانی مربوط می‌شود که تمامیت سند حفظ شده است. در هر نرم‌افزاری که امضای الکترونیکی را پشتیبانی می‌کند با علامت خاصی این مهم نشان داده می‌شود.





شکل ۱ نمودار فرایند صدور و تأیید گواهی الکترونیکی

حالت دیگر اینکه محتوای سند پس از قرار گرفتن امضای فرستنده روی آن، تغییر کرده است. این امر را می‌توان از علامت روی آن فهمید. زیرا همان‌طور که گفته شد هر نرم‌افزاری که امضای الکترونیکی را پشتیبانی می‌کند برای نشان دادن عدم تأمین تمامیت محتوای سند از علامت خاصّی استفاده می‌کند.

در اینجا دو سؤال اساسی در راستای خدمات امنیتی «احراز هویت» و «انکارناپذیری» طرح می‌شود:

۱. گیرنده با چه مکانیسمی باید اطمینان حاصل کند که شخص امضاکننده سند در دنیای فیزیکی واقعاً همان کسی است که ادعا می‌کند. به‌عبارت‌دیگر، چه نهادی در دنیای فیزیکی بر صدور و ایجاد امضاهای الکترونیکی نظارت می‌کند؟

۲. همان‌گونه که گفته شد، فرستنده سند برای رمزنگاری آن باید از کلید عمومی گیرنده استفاده کند؛ اما چه اطمینانی وجود دارد که کلید عمومی دریافتی همان کلید عمومی گیرنده سند باشد؟

برای حل این دو مشکل، کشورها به ایجاد زیرساختی به نام زیرساخت کلید عمومی[1] اقدام کرده‌اند.

۳ گواهی الکترونیکی و زیرساخت کلید عمومی

برای رفع مشکلات یاد شده، طرفین باید فرد ثالثی را برای تأیید هویت خود انتخاب کنند. اما از یک‌سو با توجه به گستردگی مبادلات تجارت الکترونیکی بین‌المللی و از سوی دیگر حساسیت این مبادلات، کشورها به ایجاد زیرساختی به نام زیرساخت کلید عمومی برای تصدیق هویت طرفین درگیر در معاملات تجارت الکترونیکی اقدام کرده‌اند.

1. Public Key Infrastructure (PKI)

زیرساخت تأمین خدمات امنیت تجارت الکترونیکی را زیرساخت کلید عمومی می‌گویند که دارای اجزای مهم زیر است:

۱-۳ مرکز صدور گواهی[1]

این مرکز موظف است برای افراد حقیقی و حقوقی متقاضی، گواهی‌های الکترونیکی صادر کند. این گواهی‌ها شامل کلید خصوصی و عمومی متقاضی و مشخّصات مرکز صادرکننده گواهی الکترونیکی است. این مرکز به‌صورت مستمر بر گواهی‌های الکترونیکی صادرشده نظارت دارد و به محض خدشه‌دار شدن هویت فرد حقیقی یا حقوقی دارنده گواهی الکترونیکی و یا انقضای تاریخ گواهی مزبور، برای لغو اعتبار گواهی اقدام کرده و آن را در فهرست گواهی‌های باطل شده[2] قرار می‌دهد. این مرکز به دو نوع مرکز اصلی تقسیم می‌شود:

الف) مراکز صدور گواهی ریشه:[3] وظیفه این مرکز صدور گواهی برای مراکز صدور گواهی میانی است. ایجاد و راهبری این مرکز در بسیاری کشورها از وظایف دولت است و فقط در کشورهای معدودی به‌وسیله بخش خصوصی ایجاد می‌شود که آن هم تحت قوانین و نظارت دولت فعالیت می‌کنند.

معمولاً در هر کشور فقط به یک مرکز ریشه نیاز است؛ اما در برخی کشورها از جمله آمریکا، هر ایالت دارای یک مرکز ریشه فعال است. باوجود این، به‌دلیل ایجاد اعتماد ملی، این مراکز به یکدیگر مرتبط و با یک قانون و نظارت ملی راهبری می‌شوند. در کشور ما، براساس مصوبه قانونی، یک مرکز ریشه برای سیستم بانکی و یک مرکز برای بقیه کاربردها پیش‌بینی شده است. اما هر دو ریشه با مجوز و نظارت یک شورای سیاست‌گذاری ایجاد خواهند شد.

ب) مراکز صدور گواهی میانی:[4] وظیفه این مراکز، صدور گواهی برای متقاضیانی است که

---

1. Certification Authority (CA)
2. Revocation List
3. Root Certification Authority (Root CA)
4. Intermediate Certification Authority

هویت آنها مورد تأیید دفاتر ثبت‌نام است. ایجاد و راهبری این مراکز درباره خدمات خاص، دولتی و در موارد عام، خصوصی است. در کشور ما این مراکز می‌توانند هم خصوصی و هم دولتی باشند.

در واقع نقطه اتّکای رسمیت مراکز صدور گواهی الکترونیکی معروف به مراکز میانی، از طریق گواهی صادر شده به‌وسیله مراکز صدور گواهی ریشه حاصل می‌شود.

۲-۳ مخزن[1]

این مورد یکی از اجزای مهم مراکز صدور گواهی الکترونیکی است که از آن برای استفاده از خدمات گواهی‌های الکترونیکی استفاده می‌شود و دارای دو وظیفه اصلی به‌شرح ذیل است:

الف) ارائه کلیدهای عمومی افراد عضو به متقاضیان برای حصول اطمینان از صحت کلید عمومی مورد استفاده در مبادلات تجاری.

ب) تأیید اعتبار گواهی‌های الکترونیکی صادر شده با استفاده از فهرست به‌روز شده گواهی‌های باطل‌شده.

این ساختار در برخی از کشورها به‌وسیله نهادهای دولتی و در برخی دیگر به‌وسیله شرکت‌های مورد اعتماد دولت انجام می‌شود. شرکت Verisign از جمله شرکت‌های مشهور در امر صدور گواهی‌های الکترونیکی است.

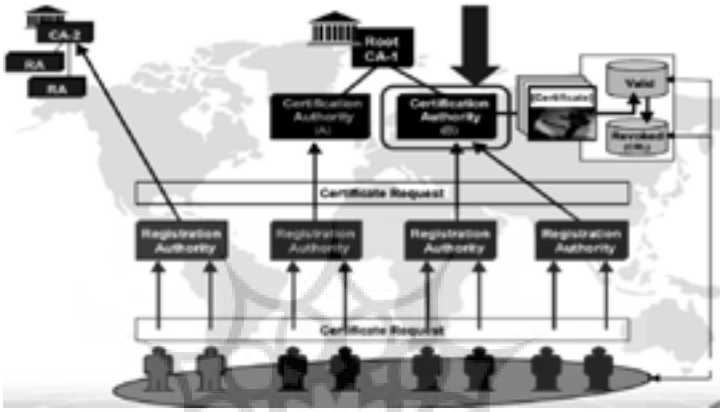
۳-۳ دفاتر ثبت‌نام[2]

ثبت‌نام از افراد حقیقی و حقوقی متقاضی دریافت امضای گواهی الکترونیکی و احراز هویت واقعی آنان در دنیای فیزیکی با استفاده از اسناد فیزیکی بر عهده دفاتر ثبت‌نام است. این دفاتر جزء غیر فنّی ساختار کلید عمومی هر کشور را تشکیل می‌دهند. متقاضیان به

---

1. Repository
2. Registration Authority (RA)

جای مراجعه مستقیم به مراکز صدور گواهی الکترونیکی، باید به این مراکز مراجعه کرده و مدارک مورد نیاز را به این دفاتر ارائه کنند تا تقاضای آنها از طریق این دفاتر به مراکز صدور گواهی ارسال و امضا و گواهی مختص آنها صادر شود و در اختیار آنها قرار گیرد. دفاتر ثبت‌نام، پیش‌خوان زیرساخت کلید عمومی هستند.



شکل ۲ ساختار مراکز صدور گواهی الکترونیکی

۳-۴ قوانین و مقررات

بر روابط و فعالیت‌های اجزای زیرساخت کلید عمومی دو نوع اسناد مقرراتی حاکم است:

الف) «مقررات فنّی و اجرایی» که براساس استانداردهای بین‌المللی تنظیم می‌شوند. این مقررات با عنوان سیاست‌نامه گواهی الکترونیکی[1] و دستورالعمل اجرایی گواهی الکترونیکی،[2] روابط مراکز صدور گواهی ریشه را با مراکز صدور گواهی میانی و دفاتر ثبت گواهی و شیوه عملکرد آنها تعریف و ارزیابی می‌کند.

ب) آن چیزی که شکل قانون حاکمیتی دارد تا روابط مراکز و اجزای زیرساخت کلید

1. Certificate Policy (CP)
2. Certificate Practice Statement (CPS)

عمومی در ساختار حاکمیتی و قانونی کشور جایگاه مشخّص و تعریف‌شده‌ای داشته باشد.

در کشور ما، براساس مندرجات قانون تجارت الکترونیکی، دولت مأمور تدوین و تصویب آیین‌نامه ویژه‌ای برای قانونی‌کردن نقش و ارتباط تمام اجزای زیرساخت کلید عمومی با کاربران و کاربردهای امضا و گواهی الکترونیکی است. این آیین‌نامه با نام «آیین‌نامه دفاتر ثبت‌نام گواهی الکترونیکی» هم‌اکنون به تصویب کمیسیون اجتماعی دولت رسیده و برای تصویب در هیئت دولت آماده شده است.

بنابراین تا این مرحله با استفاده از ابزار امضای الکترونیکی، نیازهای تمامیت، احراز هویت و انکارناپذیری اسناد الکترونیکی تأمین می‌شود. به‌گونه‌ای که اگر فرستنده یک سند تجاری مثل صورتحساب یا فرم‌های سفارش و ... را امضا و برای گیرنده ارسال کند؛ گیرنده با مشاهده علامت روی امضای الکترونیکی سند می‌تواند نسبت به تمامیت سند اطمینان حاصل کند. همچنین با استفاده از گواهی الکترونیکی مورد استفاده در امضای الکترونیکی، هویت امضاکننده سند مشخّص شده و غیرقابل انکار است.

اما همان‌گونه که گفته شد، برای بهره‌مندی از تجارت الکترونیکی ایمن، به چهار خدمت امنیتی نیازمندیم. با استفاده از امضای الکترونیکی، «محرمانگی» اسناد تجاری تأمین نمی‌شود. برای تأمین این خدمت امنیتی، باید از گواهی الکترونیکی و الگوریتم‌های رمزنگاری متقارن و نامتقارن استفاده کرد. به‌این‌ترتیب که فرستنده، سند تجاری را به‌وسیله یکی از الگوریتم‌ها رمزنگاری و برای گیرنده ارسال می‌کند. حال در صورتی که در میانه فرایند، نسخه‌ای از سند رمزشده به دست فرد ثالثی برسد، از آن‌جا که این سند به شیوه رمزنگاری نامتقارن یا ترکیب آن با رمزنگاری متقارن رمز شده و برای رمزگشایی آن در زمان معقول، فرد ثالث به کلید خصوصی گیرنده نیاز دارد، در نتیجه، امکان مشاهده سند برای وی وجود ندارد. البته همان‌گونه که گفته شد، سطحی از امنیت که از این طریق حاصل می‌شود، صد درصد نیست؛ اما در حدی است که اعتماد مورد نیاز فرایند مبادلات تجاری الکترونیکی را تأمین کند.

۴ امنیت سایت‌های تجاری در اینترنت

تا این مرحله به ابزارهای مورد استفاده در فرایند مبادلات تجارت الکترونیکی در بستر اینترنت برای ایمن‌سازی مبادلات و فراهم‌آوردن خدمات امنیتی چهارگانهٔ مورد نیاز پرداختیم. برای افزایش ضریب امنیت این فرایند، مراکز صدور گواهی الکترونیکی به ارائه دو سرویس امنیتی دیگر نیز اقدام کرده‌اند:

لایه حفره‌های امنیتی: گواهی لایه حفره‌های امنیتی یک گواهی دیجیتال است که مختص یک آدرس اینترنتی[1] صادر می‌شود. از این گواهی در تجارت الکترونیکی به دو منظور استفاده می‌شود:

الف) معرفی یک آدرس اینترنتی و تأییدکننده ارتباط بین آدرس وارد شده و سایت مورد مشاهده. به‌عبارت‌دیگر، با استفاده از این سرویس، روی صفحه مرورگر اینترنت سایتی مشاهده می‌شود. این سایت دقیقاً همان سایتی است که در نوار آدرس مرورگر وارد کرده‌ایم. چرا که در برخی موارد مشاهده می‌شود که هکر در هنگام مراجعه فرد به یک سایت تجاری، به‌صورت خودکار وی را به سایتی می‌برد که شبیه سایت مقصد طراحی شده است و از اطلاعات ورودی وی در آن سایت سوءاستفاده می‌کند. اما با بهره‌گیری از این سرویس، امکان این حملات از بین می‌رود.

ب) ایمن‌سازی مجرای ارتباطی رایانه‌های کاربران با سرورها با استفاده از گواهی‌های الکترونیکی و رمزنگاری تمامی اطلاعات مورد تبادل.

هم‌اکنون این سرویس در نسخه‌های دو و سه ارائه می‌شود و علامت نشان‌دهنده استفاده یک سایت از این سرویس است که آدرس آن به جای http با https آغاز می‌شود. البته به‌جز این نشانه، علامت یک قفل معمولی در قسمت پایین سمت راست مرورگر اینترنت نشان‌دهنده استفاده سایت از این ابزار امنیتی است.

---

1. Universal Resource Locator (URL)

۲-۴ مَهر زمانی[1]

یکی از نیازهای مهم در فرایندهای تجارت الکترونیکی، به‌ویژه در فرایند برگزاری مناقصات الکترونیکی، تعیین زمان دقیق ارسال اسناد است. توجه به این بحث به این علت است که زمان ارسال اسناد الکترونیکی روی رایانه‌ها و شبکه‌های رایانه‌ای، براساس تاریخ و ساعت سرور ارسال‌کننده در شبکه تنظیم می‌شود. از آنجا که این تاریخ و ساعت قابل تغییر بوده و با ساعت و تاریخ سرور گیرنده در شبکه متفاوت است، ریسک غیرقابل مدیریتی در استناد به زمان اسناد، به‌ویژه در فرایند مناقصات و دیگر فرایندهای تجاری، ایجاد خواهد شد. اگر برای تعیین زمان دقیق روی این اسناد مکانیسمی پیش‌بینی نشود، می‌تواند موجب ایجاد مناقشات متعددی در هنگام اجرا و بعد از اجرای فرایندهای تجاری شود. برای رفع این مشکل، مراکز صدور گواهی به ارائه خدمتی امنیتی به نام مَهر زمانی اقدام کرده‌اند. وظیفه این سرویس، تعیین زمان دقیق ایجاد و ارسال پیام‌های تجاری به‌گونه‌ای مستقل از تاریخ و ساعت رایانه‌هاست و در آن از فرایندهای رمزنگاری اسناد استفاده می‌شود. معمولاً این خدمت در کنار امضای الکترونیکی ارائه شده و زمان و تاریخ امضای سند الکترونیکی با شیوه مَهر زمانی در پایین امضای الکترونیکی قابل مشاهده است.

جمع‌بندی

در این بحث، ارتباط ساختاری نقش حاکمیت (از جمله قوانین و مقررات) با زیرساخت‌های فناوری و پیچیده برای تأمین امنیت و اعتماد مورد نیاز در بستر مدل‌ها و ارتباطات تجارت الکترونیکی نشان داده شده است. اما این مهم فقط یکی از سه بخش اساسی تأمین امنیت تجارت الکترونیکی است. در نتیجه می‌توان مباحث ارائه شده در این مقاله را در سه بخش زیر خلاصه کرد:

۱. ارائه خدمات امضا، گواهی الکترونیکی و سایر خدمات.

---

1. Time Stamp

۲. به‌کارگیری خدمات یاد شده از طریق نرم‌افزارهای خاص. اکثر نرم‌افزارهای موجود امکان به‌کارگیری امضا، گواهی الکترونیکی و مَهر زمانی را در متن یا محتوای اسناد تجاری ندارند. ازاین‌رو لازم است از نرم‌افزارهایی استفاده شود که این خدمات را پشتیبانی می‌کنند. به چنین نرم‌افزارهایی پشتیبان‌کننده[1] زیرساخت کلید عمومی می‌گویند.

۳. تغییر و مهندسی مجدد فرایندهای تجاری با هدف حذف فعالیت‌های فیزیکی احراز هویت و امضای طرف‌های تعاملات مهم تجاری در دنیای فیزیکی و جایگزینی این بخش از فرایندها با خدمات امضا و گواهی الکترونیکی به‌صورت خودکار.

1. Enabled PKI

منابع و مآخذ

Understanding Public Key Infrastructure (PKI), An RSA Data Security White Paper, RSA Data Security Inc., www.rsa.com.

Public Key Infrastructure and It's Application in the New Economy, Rick LaRowe, www.baltimore.com, 2000.

Public Key Infrastructure, Wikipedia Encyclopedia.

What Is Public Key Infrastructure Or PKI?, Mark Luker, E2001 Evolving Technology Committee Site.

www.adobe.com