زیرساخت کلید عمومی[1]

• محمد سلطانی

دانشجوی دوره دکترای حقوق خصوصی دانشگاه استراسبورگ فرانسه و مشاور حقوقی سازمان بورس و اوراق بهادار

قبلاً مسألهٔ قابلیت استناد خرید فروش الکترونیک سهام را مورد بررسی قرار دادیم و در پایان اشاره نمودیم که امضای الکترونیکی مستلزم راه‌اندازی مراکز صدور گواهی دیجیتال است که علی‌الاصول بر مبنای زیر ساخت کلید عمومی عمل می‌کنند. آیین‌نامهٔ اجرایی مادهٔ ۳۲ قانون تجارت الکترونیکی مصوب ۱۳۸۶/۰۶/۱۱ هیأت وزیران نیز امکان صدور امضای الکترونیکی مطمئن را بر مبنای زیر ساخت کلید عمومی پیش‌بینی کرده است. با توجه به اینکه سازمان بورس و اوراق بهادار پیشگام در زمینه معاملات و انتقال ایمن اطلاعات الکترونیک می‌باشد، مناسب آن دیدیم که یکی از مجاری طرح موضوع بورس باشد. در این مقاله چارچوب زیرساخت کلید عمومی که تدبیر احراز هویت و تصدیق صحت و تمامیت پیام در محیط اینترنت است با سایر جوانب مرتبط با آن مورد مطالعه قرار می‌گیرد. به اینصورت که ماهیت، اجزاء و عملکرد تکنیکی زیرساخت کلید عمومی در مباحث اول تا سوم بررسی می‌شود. البته مسائلی همچون جنبه‌های بین‌المللی زیرساخت و مسئولیت مراجع گواهی به عنوان مهمترین رکن زیرساخت نیز از اهمیت خاص برخوردار است که جهت جلوگیری از تطویل مطلب در حال حاضر از آن سخنی نخواهد رفت.

مبحث اول

مفهوم زیرساخت کلید عمومی

زیرساخت کلید عمومی[2] در واقع مهندسی امنیت مبادله اطلاعات در محیط غیرایمن اینترنت است تا سطح بالایی از اعتماد و اطمینان را برای کاربران فراهم نماید. تجار و دولتها در سراسر جهان با مسأله عدم ایمن بودن مبادله اطلاعات در اینترنت مواجه هستند. این امر و ضرورت استفاده از اینترنت این نیاز را نشان می‌دهد که شرکتهای تجاری و دولتها باید راهکاری برای حل این مشکل بیابند. اینترنت اصولاً با توجه به فلسفه ایجادش که یک دسترسی باز به اطلاعات را اقتضاء می‌نمود دارای سطح پایینی از امنیت است. بنابراین معاملاتی که بدون زیرساخت امنیتی مناسب که بتواند سطح مناسبی از اعتماد را ایجاد کند انجام گیرد پرخطر و مشکل‌زا خواهند بود.

[1] این مقاله برگرفته از پایان‌نامه دوره کارشناسی ارشد با عنوان "ادله الکترونیک اثبات دعوا" می‌باشد که در سال ۱۳۸۴، در دانشگاه تهران دفاع شده است.

[2] Public Key Infrastructure (PKI)

در وهله اول اصطلاح "زیرساخت کلید عمومی" می‌تواند گیج‌کننده باشد، زیرا این اصطلاح معانی متفاوتی دارد. از یک سو PKI به معنای روشها، تکنولوژیها و تکنیکهایی است که با یکدیگر یک زیرساخت ایمن را فراهم می‌سازد. از سوی دیگر PKI به معنی استفاده از یک جفت کلید عمومی و خصوصی برای اثبات هویت فرستنده و تأیید محتوای پیام است.[۳] با این وجود از اصطلاح زیرساخت کلید عمومی ۵ معنا را می‌توان استنباط نمود.

زیرساخت کلید عمومی:

۱. یک زیرساخت ایمن است که افراد را قادر می‌سازد درون یک سازمان (مثل اینترانت) یا میان شرکای تجاری (اکسترانت) یا بین دو زیرساخت مشابه (اینترنت) به اطلاعات موردنظر اعتماد نمایند.

۲. یک زیرساخت ایمن مبتنی بر رمزنگاری کلید عمومی است.

۳. شبکه‌ای است که خدمات زیر را برای کاربرانش فراهم می‌سازد:

الف- هویت فرستنده پیام را تأیید می‌کند تا طرف دیگر مطمئن گردد، فرستنده پیام همانی است که ادعا می‌کند.[۴]

ب- تمامیت پیام را تضمین می‌کند به این معنا که پیام در هنگام انتقال در شبکه بصورت متقلبانه یا غیرعمدی تغییر نیافته است.[۵]

ج- تضمین می‌کند که اطلاعات از دسترسی افراد غیرمجاز به دور می‌ماند و بدین وسیله محرمانگی پیام حفظ می‌شود.[۶]

د- با دسترسی مطمئن به مدرک پیام، هویت دریافت‌کننده پیام و زمان و مکان ارسال آن، احتمال هرگونه عدم انکار بعدی از سوی فرستنده را منتفی می‌سازد.[۷]

۴. ترکیبی از سیستم نرم‌افزار و سخت‌افزار، اشخاص[۸]، سیاستها[۹] و فراگردها[۱۰] است که یک ارتباط و وابستگی قابل تأیید بین اجزاء عمومی یک جفت کلید عمومی نامتقارن و یک واحد سازمانی مشخص ایجاد می‌کند.

۵. ترکیبی از سیستم نرم‌افزار و سخت‌افزار، اشخاص، سیاستها و فراگردها است که:

الف- اطلاعات مورد اعتماد در خصوص اشخاص را در گواهینامه‌های دیجیتال نگهداری می‌کند.

ب- اطلاعات گواهینامه‌ها را براساس اطلاعات جدید به روز می‌نماید و یا از آنها رجوع می‌کند.

ج- این امکان را فراهم می‌سازد تا گواهینامه‌ها بطور ایمن بین اعضای زیرساخت انتقال یابند.

---

[3] Introduction to Public Key Infrastructure,www.articsoft.com/wp-pki-intro.htm تمامی آدرسهای سایتهای مورد ارجاع مربوط به زمان مشاهده متن میباشد، بر این مبنا ممکن است برخی از این مطالب به صفحه دیگری در سایت منتقل یا اساسا حذف شده باشند.

[4] Authentication

[5] Integrity

[6] Confidentiality

[7] Non-repudiation

[8] People

[9] Policies

[10] Procedures

د– این امکان را فراهم می‌سازد تا اطلاعات گواهینامه‌ها برای الزام‌آور ساختن سیاستهای زیرساخت مورد استفاده قرار گیرند.[11]

این تعاریف از زیرساخت کلید عمومی بیش از آنکه نشانگر مفهوم زیرساخت باشد، مجموعه‌ای از وظایف آن را به تصویر می‌کشد. اما از آنجا که شناخت و فهم یک مجموعه با شناخت وظایف آن ساده‌تر تحقق می‌یابد، کارکردهای کلی زیرساخت نیز ذکر شد. بنابراین زیرساخت کلید عمومی مجموعه‌ای از خدمات تکنیکی، سیاستها و رویه‌های تجاری است که می‌تواند با یکدیگر استفاده شود تا همان اثرات حقوقی که در مبادله اسناد بصورت کاغذی وجود دارد در ارتباطات شبکه‌ای فراهم شود.[12]

مبحث دوم

اجزاء زیرساخت کلید عمومی

عملکرد زیرساخت کلید عمومی مبتنی بر روابط ۳ جزء اصلی زیرساخت یعنی امضاءکننده[13]، تأمین‌کننده خدمات گواهی[14] و طرف اعتمادکننده[15] است. با این حال برای توضیح دقیق‌تر موضوع، مرجع ثبت[16] و فهرست زیرساخت[17] نیز مورد بحث قرار گرفته‌اند. آنچه که اینجا بررسی می‌شود منطبق با یکی از مدلهای زیرساخت کلید عمومی و البته عمومی‌ترین و دقیق‌ترین آن است اما مدلهای دیگری مثل جایی که مرجع خدمات گواهی مستقلی وجود ندارد نیز قبلاً در بازار استفاده شده‌اند. دو عامل ایجاد و اتکا بر امضای الکترونیکی در تمام مدلهای زیرساخت وجود دارند اما عنصر سوم یعنی تأیید امضای الکترونیکی نه در همه بلکه در بیشتر مدلها یافت میشود. در بررسی ساختار PKI هر سه عنصر باید لحاظ شود، خواه این عناصر به وسیله ۳ عامل یا بیشتر اداره شود (مثل جایی که تأیید امضای الکترونیکی به وسیله بیش از یک عامل اداره می‌شود) یا ۲ عنصر را یک عامل اداره نماید (مثل جایی که مرجع گواهی طرف اعتمادکننده نیز هست). تمرکز بر عملکردهای انجام شده در یک PKI بدون تأکید بر یک مدل معین این حسن را دارد تا به صرف تغییر تکنولوژی بکار رفته در امضاء ارزش آن زیر سئوال نرود[18] و محافظت از عملکردهای مشابه در تکنولوژیهای غیر PKI را آسانتر سازد.[19]

---

[11] Leo Pluswick, PKI Technical Concepts and Backgrounds, www.icsalabs.com/html/communities/pki/pki-faq.pdf
[12] Mark Lucker, What is a Public Key Infrastructure, www.educause.edu.ir/library/pdf/DEC 0103.pdf
[13] Signatory
[14] Certification Authority
[15] Relying-Party
[16] Registration Authority
[17] Repository
[18] Media- Neutural
[19] . Uncitral Model Law on Electronic Signatures with Guide to Enactment 2001, United Nations Publication, New York, 2002, www.uncitral.org/english/texts/electcom/ml-elecsig-e.pdf
, PP.20-21

گفتار اول

مرجع گواهی[20]

برای انجام تجارت یا غیر آن باید شرایطی فراهم شود تا طرفین بتوانند به یکدیگر اعتماد کنند. در معاملات کاغذی این اعتماد به واسطه مواجهه حضوری طرفین و شناخت آنان نسبت به یکدیگر و یا از طریق دفاتر اسناد رسمی حاصل می‌شود. در تجارت الکترونیکی که در شبکه باز اینترنت انجام می‌شود، گواهی نقشی حیاتی در شناسایی هویت اشخاص و الزام‌آور ساختن معامله ایفاء می‌کند. فعالیت اصلی مراجع گواهی مبتنی بر تضمین صحت فرایند تصدیق امضای دیجیتال است. همانطور که بعداً توضیح خواهیم داد، امضای دیجیتال با استفاده از کلید خصوصی امضاکننده ایجاد شده و با کلید عمومی وی تصدیق می‌شود. برای تصدیق یک امضای دیجیتال، تصدیق‌کننده–شخصی که می‌خواهد از هویت طرف دیگر اطمینان یابد– باید به کلید عمومی امضاکننده دسترسی و اطمینان داشته باشد که آن با کلید خصوصی امضاکننده مطابقت می‌کند. از آنجا که جفت کلید عمومی و خصوصی هیچ ارتباط و همراهی ذاتی با شخص ندارد لذا لازم است مکانیسمی پیش‌بینی شود تا چنین همراهی و ارتباطی را ایجاد نماید. برای اینکه امضاء از طریق جفت کلید عمومی و خصوصی نتیجه‌بخش باشد لازم است کلید عمومی به نحوی شایسته در دسترس اشخاصی که خواهان استفاده از آن هستند قرار گیرد. از طرف دیگر بسیاری از این افراد امضاکننده را نمی‌شناسند و فقط از طریق اینترنت با او آشنا شده‌اند و لذا لازم است یک سیستم قابل اعتماد بین این دو قرار گیرد تا ضمن پخش کلید عمومی به نحو مقتضی صحت کلیدهای عمومی و خصوصی افراد را تضمین و بدین وسیله اطمینان لازم را در جهت شناسایی هویت و انجام معاملات مورد نظر جلب نماید.

مراجع گواهی شباهت فراوانی با دفاتر اسناد رسمی دارند. همانطور که این دفاتر هویت طرفین قرارداد و وقوع معامله و زمان و مکان آن را با تأیید قصد و رضای طرفین تصدیق می‌کنند مراجع گواهی یا بنابر عبارت قانون تجارت الکترونیک ایران "دفاتر خدمات صدور گواهی الکترونیکی" [21] نیز هویت درخواست‌کنندگان صدور گواهی را به عنوان یک نهاد ثالث شناسایی و سلامت و امنیت انجام معاملات در یک محیط بسته یا باز را تضمین می‌نمایند. براین اساس تفاوت دفاتر اسناد رسمی و دفاتر خدمات صدور گواهی الکترونیکی نه از جهت ماهوی بلکه به جهت شکل اجرای تصدیق هویت است. البته در دفاتر خدمات الکترونیکی آن قسمت از وظیفه دفتر که شناسایی هویت درخواست‌کننده است معمولاً به عهده مرجع ثبت است که در قسمت بعدی از آن سخن خواهیم گفت. بنابراین بطور خاص مرجع گواهی واحدی است که گواهیها را براساس اطلاعات ارائه شده توسط مرجع ثبت صادر می‌کند. گواهینامه‌های صادره

– مقررات مربوط به مرجع گواهی در مادهٔ ۸ آیین‌نامهٔ اجرایی مادهٔ ۳۲ قانون آمده است. با توجه به آیین‌نامهٔ مزبور، سازمان بورس می‌تواند با مجوز مرکز ریشه یک مرجع گواهی میانی به منظور ایمن‌سازی معاملات الکترونیکی در بورس تأسیس کند.

[20] Certification Authority
[21] Certification Service Provider

ممکن است بصورت برخط[۲۲] و از طریق زیرساختهای شبکه بدست آید و یا اینکه بصورت off-line در یک محل غیرقابل دسترس نگهداری شوند و با استفاده از دیسکت[۲۳] از طریق خدمات انتقال ایمن ارسال شوند. در خصوص نوع اول می‌توان از Verisign [۲۴] نام برد و [۲۵] European Sesame Project نیز از نمونه‌های نوع دوم می‌باشد.

براساس بند ۱۱ ماده ۲ دستورالعمل اتحادیه اروپا[۲۶]، تأمین‌کننده خدمات گواهی، واحد یا شخص حقیقی یا حقوقی است که گواهینامه‌ها را صادر نموده یا سایر خدمات مرتبط با امضای الکترونیکی را فراهم می‌سازد. براساس بند ۲ ماده ۲ قانون امضای دیجیتال آلمان، گواهی‌کننده در چارچوب این قانون شخص حقیقی یا حقوقی است که اسناد کلیدهای امضای عمومی را برای اشخاص حقیقی تصدیق نموده و برای انجام این منظور لازمه – مجوز مذکور در ماده ۴ آن قانون – را داراست.[۲۷] براین اساس تأمین‌کننده خدمات گواهی ممکن است شخص حقیقی، شخص حقوق خصوصی یا شخص حقوق عمومی باشد. در تعدادی کشورها به دلایل مربوط به نظم عمومی پیش‌بینی شده که فقط مؤسسات دولتی مجاز هستند به عنوان مراجع گواهی عمل نمایند، در حالی که در بسیاری از کشورها به این موضوع توجه شده است که برای صدور گواهی بخش خصوصی بتواند اقدام نماید تا با رقابتهای حاصله از این امر کیفیت کار بالا رود. در کشور ما بند الف مادهٔ ۴ آیین‌نامهٔ اجرایی مادهٔ ۳۲ قانون تجارت الکترونیکی، صدور گواهی الکترونیکی ریشه را منحصراً در اختیار بخش دولتی قرار داده است. با این وجود مطابق مادهٔ ۷، مرکز صدور گواهی الکترونیکی میانی می‌تواند توسط دستگاه‌های دولتی یا غیر دولتی تأسیس شود.

مرجع گواهی خواه دولتی یا خصوصی برای مرتبط ساختن یک جفت کلید با یک امضاکننده معین اقدام به صدور گواهینامه[۲۸] می‌نماید. گواهینامه یک سند الکترونیکی است که یک کلید عمومی را با نام ثبت نام‌کننده گواهی به عنوان "موضوع"[۲۹] گواهی منتشر می‌کند و ممکن است تأیید نماید که امضاکننده معین شده در گواهینامه کلید خصوصی متناظر را در اختیار دارد. عملکرد اصلی یک گواهینامه، مرتبط ساختن کلید عمومی با یک امضاکننده خاص است.[۳۰]

براساس بند ۹ ماده ۲ دستورالعمل اتحادیه اروپا[۳۱] "گواهینامه، گواهی الکترونیکی است که داده تصدیق امضاء را به شخص مرتبط می‌سازد و هویت وی را تأیید می‌نماید." منظور از داده تصدیق امضاء در این ماده همان کلید عمومی است. بند ۳ ماده ۲ قانون امضای

---

[22] On-line
[23] Floppy-disk
[24] www.verisign.com
[25] www.mi-kun.nl/sesame/summary.htm
[26] Electronic Signature Directive, Electronic Signature Directive, European Union, December 1999, www.e-podpis.sk/laws/eu-ep-dir93-1999.pdf
[27] German Digital Signature Law,www.kuner.com/data/siyg/digsig4.htm
[28] Certificate
[29] Subject
[30] Uncitral Model Law on Electronic Signatures with Guide to Enactment 2001, op.cit,P.27
[31] Electronic Signature Directive, op.cit

دیجیتال آلمان[۳۲] در تعریف گواهینامه مقرر می‌دارد "گواهینامه در چارچوب این قانون یک گواهی دیجیتال مرتبط با اسناد کلید عمومی امضای یک شخص حقیقی است که به یک امضای دیجیتال ملحق شده (گواهی کلید امضاء) یا یک گواهی دیجیتال خاص است که به گونه‌ای مطمئن به یک گواهی کلید امضاء ارجاع دارد و شامل اطلاعات اضافی است (گواهی اسناد)."

یک گواهینامه دیجیتال شامل اطلاعات اساسی است که شخص ثالث نیاز دارد برای اطمینان از هویت طرف به آن دسترسی داشته باشد. وجود حداقل اطلاعات ذیل در گواهینامه ضروری است:

- هویت موضوع گواهی یعنی درخواست‌کننده صدور گواهی از قبیل نام و نام خانوادگی
- کلید عمومی موضوع گواهی (ثبت نام کننده)
- الگوریتم های رمزنگاری که با کلیدها استفاده شده است
- هویت مرجع گواهی از قبیل نام و محل آن
- تصریح به مدت زمان اعتبار گواهی
- امضای دیجیتال مرجع گواهی صادرکننده گواهی[۳۳]

یک دریافت‌کننده گواهی که مایل به اتکا به یک امضای دیجیتالی ایجادشده به وسیله امضاکننده که نامش در گواهی آمده است می‌باشد می‌تواند از کلید عمومی لیست شده در گواهی استفاده کند تا تأیید نماید امضای دیجیتال به وسیله کلید خصوصی متناظر ایجاد شده است. اگر چنین تصدیقی موفقیت آمیز باشد از نظر تکنیکی این سطح از تضمین تأیید می‌شود که پیام به وسیله امضاکننده ایجاد شده و پس از آن نیز تغییر ننموده است.[۳۴]

گفتار دوم

مرجع ثبت[۳۵]

یک مرجع ثبت، اطلاعاتی را که یک درخواست‌کننده هنگام ثبت نام ارائه می‌دهد بررسی نموده و تأیید می‌نماید. با توجه به اینکه تعداد افرادی که می‌خواهند هویت خود را به عنوان موضوع گواهی به ثبت برسانند زیاد و از نظر جغرافیایی پراکنده هستند باید مراجع ثبت متعدد در کشور پراکنده باشند تا با مراجعه به این مراجع، ثبت نام افراد با اعمال دقتهای لازم امکانپذیر گردد و از اتلاف وقت و هزینه و تجمع در یک مرجع گواهی خودداری گردد.

---

[32] German Digital Signature Law (sigG), www.kuner.com/data/sigdigsig4.htm

[33] Leo Pluswick, op.cit

[34] Uncitral Model Law on Electronic Signatures with Guide to Enactment 2001, op.cit, P.27

– مقررات مربوط به مرجع ثبت در مواد ۱۲ به بعد آیین‌نامهٔ اجرایی مادهٔ ۳۲ قانون پیش‌بینی شده‌اند.

[35] Registration Authority

اگر در یک PKI مرجع ثبت وجود نداشته باشد، مرجع گواهی خود، وظایف مرجع ثبت را انجام می‌دهد. در جریان ثبت نام، درخواست‌کنندگان باید هویت، حسن نیت و سایر موارد لازم را برای مرجع ثبت ثابت نمایند. در این حالت از آنجا که احراز هویت برای اولین بار صورت می‌گیرد، این ثبت نمی‌تواند بصورت برخط[۳۶] باشد.

ممکن است در صحت یکی از گواهینامه‌های مورد استفاده تردید شود، در این‌صورت، مرجع ثبت هویت و سایر مشخصات کاربر در گواهینامه دیجیتال را بررسی و در نتیجه گواهینامه را تأیید یا رد می‌نماید. در صورت لزوم، مرجع ثبت، مرجع گواهی را برای رجوع از اعتبار گواهینامه مطلع می‌سازد و گزارش تمامی گواهینامه‌های رجوع شده به وسیله مرجع گواهی را به فهرست PKI ارسال می‌دارد. ممکن است مدیریت کلیدهای کاربردی نیز در اختیار مرجع ثبت قرار گیرد. در اینصورت مرجع ثبت کلیدها را تولید نموده، کلیدهای معتبر را ذخیره نموده و بقیه را در فهرست خود نگهداری می‌نماید تا در صورت لزوم بازیابی شود.[۳۷]

مرجع ثبت ممکن است خود بصورت مستقیم و حضوری توسط مرجع گواهی، شناسایی و تصدیق هویت شده و یک گواهی برای آن صادر شده باشد. در این حالت مرجع ثبت پس از تنظیم یک گواهینامه برای شخص درخواست‌کننده آن را بصورت یک پیام دیجیتالی امضاء شده برای مرجع گواهی ارسال می‌نماید همچنان که ممکن است این وظیفه بصورت مستقیم و حضوری انجام پذیرد.[۳۸]

ممکن است ثبت نام‌کنندگان قادر به تمییز مرجع گواهی از مرجع ثبت نباشند اما در هر صورت وجه تمایز این دو آن است که مرجع ثبت گواهی را امضاء نمی‌نماید.[۳۹] استفاده از یک مرجع ثبت در جمع آوری اطلاعات بصورت جداگانه سیستم امنیتی مطمئن‌تری را فراهم نموده و در محافظت اطلاعات محرمانه مؤثرتر است.[۴۰]

---

[36] On-line
[37] Leo Pluswick, op.cit, P.6
[38] Local Registration Authority, www.fundserv.com/english/services/identity-Ira.shtml
[39] Introduction to PKI-Public Key Infrastructure, European Master in Multimedia Projects, www.k-binder.be/papers/PKI-V11.pdf, P.5
[40] Understanding Public Key Infrastructure, www.directoryservice.com/wp/psa/understanding-pki.pdf, P.3

گفتار سوم

ثبت نام کننده (موضوع گواهی)

ثبت نام‌کننده شخصی است که با مراجعه به یک مرجع ثبت و اثبات هویت خویش درخواست صدور یک گواهی را به نام خود نموده است. پس از صدور گواهی فرد مزبور "موضوع گواهی" نامیده می‌شود."موضوع گواهی" واحدی است که نامش به عنوان موضوع در یک گواهی نشان داده می‌شود و تصدیق می‌کند که جفت کلید عمومی و خصوصی و گواهی را در راستای سیاستهای گواهی که در خود گواهی بدان اشاره شده بکار می‌برد. موضوع گواهی ممکن است خود، یک مرجع گواهی یا مرجع ثبت باشد.[۴۱]

"موضوع گواهی" در مرحله بعد به عنوان "امضاکننده" ظاهر می‌شود. امضاکننده کسی است که وسیله ایجاد امضاء را در اختیار دارد[۴۲] و از طرف خود یا شخص حقیقی یا حقوقی سازمانی که نمایندگی آن را بر عهده دارد عمل می‌کند.[۴۳]

براساس بند (d) ماده ۲ قانون نمونه آنسیترال در مورد امضای الکترونیکی، امضاکننده کسی است که داده‌های ایجاد امضاء[۴۴] را در اختیار دارد و از سوی خود یا کسی که نمایندگی آن را به عهده دارد اقدام میکند. بند (ل) ماده ۲ قانون تجارت الکترونیک ایران نیز امضاکننده را به عنوان هر شخص یا قائم‌مقام وی که امضای الکترونیکی را تولید می‌کند تعریف کرده است. با توجه به سایر قوانین و به ویژه قانون نمونه آنسیترال که الگوی تدوین قانون تجارت الکترونیک ایران بوده است، منظور از قائم‌مقام طبق ماده ۳۹۵ قانون تجارت "...کسی است که رئیس تجارتخانه او را برای انجام کلیه امور مربوط به تجارتخانه یا یکی از شعب آن نایب خود قرار داده و امضای او برای تجارتخانه الزام آور است..." وگر نه در حقوق مدنی واژه قائم‌مقام به کسی اطلاق می‌شود که بطور مستقیم یا بوسیله نماینده خود در بستن قرارداد شرکت نداشته ولی به سبب انتقال حقی از دارایی یکی از دو طرف به او از عقد متأثر می‌شود.[۴۵] به هر صورت، قانونگذار می‌توانست از واژه مناسبتری استفاده کند.

در یک محیط کاغذی، به مفهوم مضیق اشخاص حقوقی نمی‌توانند امضاکننده اسنادی باشد که از جانب آنها تنظیم می‌شود، زیرا تنها اشخاص حقیقی می‌توانند امضاهای دستی ایجاد کنند. اما انتساب امضاهای الکترونیکی به شرکتهای تجاری یا سایر اشخاص حقوقی از قبیل مقامات عمومی و دولتی قابل تصور است و مواردی وجود دارد که هویت شخصی که امضاء را واقعاً به وجود آورده است تأثیری بر اهدافی که امضاء برای آن ایجاد شده است ندارد. با این وجود از آنجا که مفهوم امضاء نمی‌تواند از شخصی که واقعاً امضای الکترونیکی

---

[41] Leo Pluswick, op.cit,P.4

[۴۲] وسیله ایجاد امضاء (signature-creation device)سخت افزاری است که برای ایجاد امضای الکترونیکی بکار می رود. Electronic Signature Directive,op.cit

[43] Electronic Signature Directive,op.cit

[44] Signature Creation Data

[۵] دکتر ناصر کاتوزیان، دوره مقدماتی حقوق مدنی، اعمال حقوقی، شرکت سهامی انتشار با همکاری بهمن برنا، ۱۳۸۳، ش ۱۷۶

را ایجاد کرده جدا شود و برخی از تعهدات امضاکننده به کنترل واقعی به روی داده ایجاد امضاء مربوط می‌شود برای در نظرگرفتن مواردی که امضاکننده به نمایندگی از دیگر اشخاص اقدام می‌کند، این موضوع نیز در تعریف امضاکننده ملحوظ شده است.[۴۶]

وظایف ثبت نام‌کننده و در مرحله بعد امضاکننده به شرح زیر است:

۱. ثبت نام‌کننده نباید از گواهی برای اهدافی جز آنچه که در سیاستهای مرجع گواهی اعلام شده استفاده کند.

۲. ثبت نام‌کننده باید کلید خصوصی خود را بطور ایمن نگاه دارد و به محض آنکه تردیدی در تطابق دو کلید به وجود آید یا کلید خصوصی فاش شود درخواست رجوع از گواهی بنماید.

۳. ثبت نام‌کننده باید در صورت لزوم، حسب مورد مرجع گواهی یا مرجع ثبت را برای لغو ثبت نام یا تغییر اطلاعات مطلع سازد.[۴۷]

ماده ۸ قانون نمونه آنسیترال در این‌خصوص چنین مقرر کرده است:

"۱- هنگامی که داده ایجاد امضاء برای ایجاد امضایی که دارای اثر حقوقی است به کار رود هر امضاکننده باید:

الف- مراقبت معمول و متعارف برای پیشگیری از استفاده غیرمجاز از داده ایجاد امضای خود به عمل آورد.

ب- بدون تأخیر غیر موجه با استفاده از وسایل ایجاد شده توسط ارائه‌دهنده خدمات الکترونیکی بر طبق ماده ۹ این قانون، یا با بکار بردن تلاشهای متعارف هر شخصی را که امضاکننده بطور متعارف احتمال می‌دهد که بر امضای الکترونیکی اعتماد کرده یا خدماتی را بر مبنای امضای الکترونیکی فراهم کرده است، مطلع سازد اگر:

(i) امضاکننده بداند که داده ایجاد امضاء به خطر افتاده است.[۴۸] (ii) اوضاع و احوال نشانگر این خطر اساسی باشد که ممکن است داده ایجاد امضاء فاش شده باشد.

ج- هنگامی که برای تأیید امضای الکترونیکی از گواهی استفاده می‌شود امضاکننده باید برای تضمین درستی و کامل بودن همه اظهارات اساسی در گواهی یا مربوط به آن که در دوره اعتبار آن توسط وی ارائه شده دقت متعارفی را اعمال نماید.

۲- امضاکننده باید نتایج قانونی قصور در تحقق مقررات پاراگراف اول را بپذیرد."

بندهای (الف) و (ب) این ماده نسبت به همه امضاهای الکترونیکی اعمال میشوند، در حالی که بند (ج) تنها نسبت به امضاهای الکترونیکی که به وسیله گواهی تأیید شده‌اند اعمال می‌شود. تعهد مندرج در بند (الف) پاراگراف اول یعنی تعهد به اعمال دقت

[46] Uncitral Model Law on Electronic Signatures with Guide to Enactment,op.cit,P.46
[47] Proposal for Liability of Certification Authority, Authentication and Notary Working Group, Electronic Commerce Promotion Council of Japan (ECOM), May 2000
www.ecom.jp/ecom-e/report/full/proposalfor. pdf
[48] Compromise

متعارف برای پیشگیری از استفاده غیرمجاز از داده ایجاد امضاء یک تعهد مبنایی است که بعنوان مثال بطورکلی در قراردادهای مربوط به استفاده از کارتهای اعتباری گنجانده می‌شود.[۴۹]

بند (ب) پاراگراف اول برای کاربرد تلاشهای متعارف برای آگاه ساختن هر شخصی که انتظار می رود در مواردی که امضای الکترونیکی در معرض خطر است بر آن امضا اتکا کند معیار قابل انعطافی ارائه می‌کند. برای امضاکننده غیرممکن است ردپای هر کسی را که ممکن است به امضای الکترونیکی اعتماد کرده باشد پیگیری نماید و بسیار مشکل است که امضاکننده را مکلف و متعهد به آگاهی واقعی و عملی هر شخص اعتمادکننده بدانیم. اشاره به وسایل ایجاد شده توسط ارائه دهنده خدمات الکترونیکی در بند (ب) منعکس کننده امکانات عملی است که توسط ارائه دهندگان خدمات گواهی در دسترس و اختیار امضاکننده قرار داده می‌شود که از جمله می‌توان به تشریفاتی که باید به هنگام به خطرافتادن امضای الکترونیکی اعمال شود اشاره کرد. این تشریفات نباید توسط امضاکننده تغییر یابند. این تشریفات این امکان را فراهم می‌سازد تا وی قادر باشد اثبات کند که در تلاش برای آگاه سازی طرفهای اعتمادکننده احتمالی به اندازه کافی کوشا بوده است. باید توجه داشت با توجه به عبارت بند (ب) تکلیف آگاه‌سازی شامل مرجع گواهی و هر شخص ذینفع دیگر نیز می‌شود.[۵۰] بند (ج) هنگامی اعمال می‌شود که گواهی برای تأیید داده ایجاد امضاء بکار رود. چرخه حیات گواهی از زمان درخواست صدور گواهی تا انقضای مدت گواهی یا رجوع از آن را دربرمی‌گیرد.[۵۱]

در پیش‌نویس قانون تجارت الکترونیک، با عنایت به قانون نمونه آنسیترال در مورد امضای الکترونیکی، وظایف امضاکننده به شرح زیر مقرر شده بود:

"ماده ۶۶- امضاکننده "داده" موظف به رعایت موارد زیر است والا مسئول خواهد بود:

۶۶-۱- مراقبت معقول در ممانعت از استفاده غیرمجاز از "داده" های تولید امضاء

۶۶-۲- بدون معطلی به اطراف اعتمادکننده پیام یا به دفتر خدمات الکترونیکی موارد زیر را اعلام کند:

۶۶-۲-۱- امضاکننده بداند که "داده" های تولید امضای وی به مخاطره افتاده است.

۶۶-۲-۲- از اوضاع و احوال بیم آن رود که "داده" های تولید امضاء در معرض خطر قرار گیرد.

۶۶-۳- زمانی که برای امضای خود از خدمات دفاتر الکترونیکی استفاده می‌کند بطور معقول از صحت و کمال اطلاعات اعلامی توسط خود که مربوط به گواهی است و در طول مرور زمان قانونی اعتماد حاصل کند."

[49] Uncitral Model Law on Electronic Signatures with Guide to Enactment,op.cit,P.62
[50] Ibid
[51] Ibid, P.63

گفتار چهارم

طرف اعتمادکننده[۵۲]

طرف اعتمادکننده کسی است که از اطلاعات موجود در گواهی یک ثبت نام‌کننده استفاده کرده و بـر رابطـه معتبـر بـین هویـت ثبـت نام‌کننده و کلید عمومی وی اعتماد میکند تا با تطبیق کلید عمومی فهرست شده با اطلاعات فرد مـورد ادعـا از هویـت فرسـتنده پیـام، صحت، تمامیت و محرمانگی پیام اطمینان حاصل کند.[۵۳]

براساس بند (f) ماده ۲ قانون نمونه آنسیترال در مورد امضای الکترونیکی، طرف اعتمادکننده "شخصی است که بر مبنای یک گـواهی یا یک امضای الکترونیکی عمل میکند." در پیش‌نویس قانون تجارت الکترونیک نیز به تبعیت از ایـن تعریـف طـرف اعتمادکننـده بـه عنوان شخصی که براساس گواهی یا امضای الکترونیکی اقدام می‌کند معرفی شده بود، اما این بند در نسخه نهایی قانون حذف شد.

براساس ماده ۱۱ قانون نمونه آنسیترال در مورد امضای الکترونیکی "طرف اعتمادکننده در صورت قصور در موارد ذیل باید نتایج قانونی آن را بپذیرد.

الف- انجام اقدامات متعارف برای بررسی قابلیت اعتماد امضای الکترونیکی یا

ب- جایی که امضای الکترونیکی توسط گواهی تأیید شده است در انجام اقدامات معقول در امور ذیل قصور کند.

۱. بررسی اعتبار، تعلیق یا الغای گواهی

۲. رعایت محدودیتهای اعمال شده نسبت به گواهی."

بسته به اوضاع و احوال، طرف "اعتمادکننده" می‌تواند هر شخصی باشد که با امضاکننده یا ارائه‌دهنده خدمات گواهی رابطه قـراردادی دارد یا ندارد. حتی ممکن است ارائه‌دهنده خدمات گواهی یا خود امضاکننده، "طرف اعتمادکننده" باشد. در واقع امضا کننده با تکیه بـر کلید خصوصی و عمومی تولید شده و ارائه‌دهنده خدمات گواهی در وضعیتی که به گواهی مراجع دیگر اتکا می‌کند، ممکن است طـرف اعتماد کننده محسوب شود. با این وجود مفهوم گسترده طرف اعتمادکننده نباید منجر به این نتیجه شود که تعهد بررسی اعتبار گـواهی که از ارائه‌دهنده گواهی خریداری شده است به عهده ثبت نام‌کننده (مشترک گواهی) قرار گیرد.[۵۴] طرف اعتمادکننده که می‌خواهـد بـه یک امضاء یا گواهی الکترونیکی استناد کند باید این پرسش را در ذهن داشته باشد که آیا چنین اعتمـاد و اتکـایی در اوضـاع و احـوال مربوطه معقول است یا خیر. طرف اعتمادکننده ممکن است یک مصرف‌کننده باشد، اما علیرغم ایجاد وظیفه بـرای طـرف اعتمادکننـده قواعد حمایت از مصرف‌کننده تحت تأثیر قرار نمی‌گیرد. با این حال این قواعد نقش مفیدی در آموزش همـه طرفهـای دخیـل از جملـه

[52] Relying Party
[53] Leo Pluswick, op.cit
[54] Uncitral Model Law on Electronic Signatures with Guide to Enactment, op.cit,P.68

طرف اعتمادکننده در خصوص استانداردهای رفتار متعارف ایفا می‌کند، ضمن اینکه این استانداردها و رعایت آنها برای گسترش زیرساخت کلید عمومی ضروری است.[۵۵]

گفتار پنجم

فهرست زیرساخت کلید عمومی[۵۶]

فهرست زیرساخت کلید عمومی یک پایگاه اطلاعاتی است که لیست گواهیهای معتبر و گواهیهای مرجوع شده [۵۷] را در اختیار اطراف معامله و سایر اجزاء عملیاتی زیرساخت کلید عمومی قرار می‌دهد.[۵۸] خدمات فهرست زیرساخت شامل تهیه و مدیریت کامل داده‌های مربوط به ثبت نام‌کننده است. این داده‌ها تنها گواهی را دربرنمی‌گیرد، بلکه اطلاعات دیگری از جمله آدرس پست الکترونیکی، شماره تلفن و ..... را نیز شامل می‌شود.[۵۹] هنگامی که مرجع گواهی، گواهی را صادر نمود، گواهی وارد فهرست PKI مربوط به گواهیهای معتبر می‌شود تا اشخاص ثالث بتوانند به آن دسترسی داشته باشند. در برخی موارد این فهرست به وسیله مرجع گواهی کنترل می‌شود و گاهی دیگر ثالثی بجز مرجع گواهی آن را اداره می‌کند. ممکن است برای دسترسی به فهرست مزبور محدودیتهایی وجود داشته باشد تا افراد غیرمجاز نتوانند به اطلاعات دست یابند.[۶۰] چنانچه این فهرست عمومیت نداشته باشد و بطورمثال مربوط به یک شرکت خاص باشد، علی الاصول دسترسی فقط برای کارمندان همان شرکت امکانپذیر خواهد بود، اما پایگاههای عمومی به روی همه باز هستند.[۶۱] دیگر لیست موجود در فهرست PKI ، لیست گواهیهای رجوع شده است. این گواهیها پیش از آنکه تاریخ انقضای اعتبار آنها فرا رسد به دلیلی بی‌اعتبار شده‌اند.[۶۲] با دسترسی به این فهرست می‌توان با اطلاعات دقیق‌تری راجع به هویت طرف معامله تصمیم‌گیری نمود. دلایل مختلفی می‌تواند برای رجوع از گواهی وجود داشته باشد. ممکن است کلید خصوصی کاربر فاش شده باشد یا یکی از ویژگیهای اساسی موضوع گواهی، همچون نام، شغل، آدرس، شماره حساب بانکی یا هر مشخصه مؤثر دیگری تغییر نموده باشد.

اخیراً به عنوان یک جایگزین برای CRL، از OCSP [۶۳] استفاده می‌شود تا بدین وسیله بررسی می‌شود که آیا گواهی در زمان مورد بررسی رجوع شده است یا خیر، زیرا در حالت قبلی یک فاصله زمانی بین موقعی که از گواهی رجوع می‌شود تا زمانی که درCRL

---

[55] Ibid,P.67
[56] Repository
[57] CRL(Certification Revocation List)
[58] Leo Pluswick,op.cit,P.4
[59] Proposal for Liability of Certification Authority, Authentication and Notary Working Group, Electronic Commerce Promotion Council of Japan (ECOM), May 2000, www.ecom.jp/ecom-e/report/fall/proposalfor.pdf, P.7
[60] Ibid,P.3
[61] Introduction to Public Key Infrasructure,op.cit,P.5
[62] Leo Pluswick ,op.cit,P.8
[63] Online Certificate Status Protocol

منتشر می‌گردد وجود خواهد داشت و در نتیجه خطر بروز اشتباه وجود دارد. این خطر در خود CRL به وسیله Delta-CRL [۶۴] که لیستی از آخرین تغییرات تا انتشار آخرین نسخه کامل CRL می‌باشد رفع می‌گردد.[۶۵]

گواهیهای صادر شده، لیست گواهیهای مرجوع یا معلق شده (تعلیق مربوط به دوره خاصی است و پس از آن گواهی بطور خودکار قدرت اجرای خود را باز می‌یابد. تعلیق در موقعیتهایی استفاده می‌شود که انجام درخواست رجوع از گواهی امکانپذیر نیست) و شبیه آن باید برای یک دوره زمانی بایگانی شوند. این بدان دلیل است که اسنادی که امضای دیجیتالی شده‌اند بیشتر از دوره اعتبار گواهی باقی می مانند بنابراین گواهیهایی که دوره اعتبارشان منقضی شده است باید در جایی نگهداری شوند تا در دسترس باشند.[۶۶] فهرست PKI باید گواهیهای جدید صادر شده و همچنین گواهیهای رجوع شده را در دوره زمانی از پیش تعیین شده منتشر نماید.

مبحث سوم

عملکرد تکنیکی زیرساخت کلید عمومی

منظور از عملکرد تکنیکی زیرساخت کلید عمومی فرایندی است که در این ساختار منجر به خلق امضای دیجیتالی مورد اعتماد و محرمانه ساختن پیام می‌گردد. در این مبحث ابتدا نحوه ایجاد امضای دیجیتال و سپس محرمانه ساختن پیام را بررسی می‌نماییم.

گفتار اول

امضای دیجیتال

امضای دیجیتال یک نوع امضای الکترونیکی است که از رمزنگاری کلید عمومی استفاده می‌کند.[۶۷] امضای الکترونیکی مفهومی عام‌تر از امضای دیجیتال است. امضای دیجیتال اغلب همراه با طرحها و نقشه‌های امضاء[۶۸] که در رمزنگاری نامتقارن استفاده می‌شود و مبتنی بر استفاده از فرایند ریاضیاتی است، بکار می رود.[۶۹] رمزنگاری ارتباط نزدیکی با امضای الکترونیکی دارد. در واقع امضاء بدون رمزنگاری ارزشی ندارد، لذا جهت تضمین معاملات رمزنگاری یک روش مناسب جهت حمایت از اطلاعات انتقال یافته ازطریق یک محیط باز مثل شبکه‌های کامپیوتری است. رمزنگاری با استفاده از کلید، پیام را به شکل اطلاعاتی که عموماً درهم و برهم و غیرقابل فهم به نظر می‌رسد تبدیل میکند.[۷۰]

---

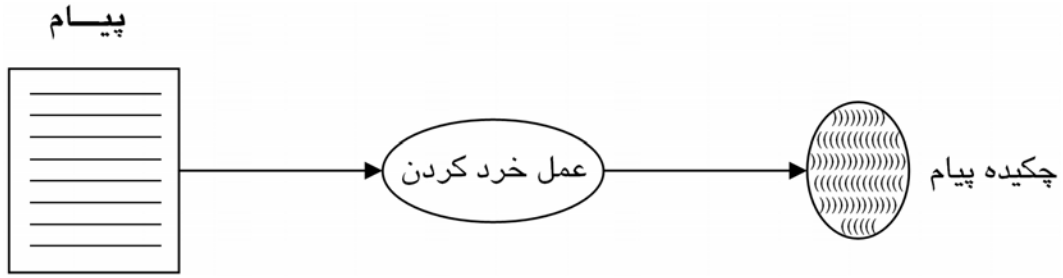
[64] www.LinuxSecurity.com/index2.php?option=com-content&do-pdf=1&id=117024
[65] Proposal for Liability of Certification Authority,op.cit,P.7
[66] Ibid ,P.3
[67] Bloemers, Ralph O, Electronic and Digital Signatures, www.stoel.com/resources/articles/ebusiness/ebi2-003.shtm
[68] Signature Schemes
[69] Ahto Buldas & Märt Saareperat,Electronic Signature System with Small Number of Private Keys, www.middleware.internet2.edu/pki03/presentations/08.pdf
[70] Jonathan Rosenoer, op.cit,P.239

در امضای دیجیتال با استفاده از رمزنگاری کلید عمومی از دو کلید عمومی و خصوصی برای ایجاد و تأیید امضاء استفاده می‌شود. علی الاصول کلید خصوصی که فقط در دسترس امضاکننده است برای ایجاد امضای دیجیتال استفاده می‌شود و کلید عمومی که در دسترس افراد معین یا در دسترس عموم قرار دارد به وسیله طرف اعتمادکننده برای تأیید امضاء استفاده می‌شود.[۷۱] برای بررسی نحوه ایجاد امضای دیجیتال، ابتدا لازم است مفهوم عمل "چکیده کردن پیام"[۷۲] توضیح داده شود.

۱- چکیده کردن پیام[۷۳]: چکیده کردن پیام یک فرایند ریاضیاتی مبتنی بر یک الگوریتم است که یک نمایش دیجیتالی از پیام ایجاد می‌کند یا شکل پیام را فشرده می‌کند که از آن به عنوان "چکیده[۷۴]" یا "اثر انگشت[۷۵]" پیام نام برده می‌شود. عمل خرد کردن نرم‌افزار را قادر می‌سازد تا روی مقادیر کوچکتر و قابل پیش‌بینی‌تری از داده‌ها عمل کند، در حالی که ارتباط قوی با محتوای پیام اصلی نیز وجود دارد و بدین وسیله بطور مؤثری این تضمین فراهم می‌شود که از زمانی که پیام، امضای دیجیتالی شده هیچ تغییر و اصلاحی در پیام صورت نگرفته است.[۷۶]

طول بیت پیام خرد شده معمولاً ۱۲۸ یا ۱۶۰ بیت است و به گونه‌ای طراحی شده که نسبت به پیام منحصر بفرد باشد به این معنی که هر پیام اصلی یک چکیده منحصر بفرد دارد و دو چکیده، دو پیام متفاوت همانند دو اثر انگشت متفاوت خواهند بود. برخی از نمونه‌های الگوریتم‌های چکیده کردن پیام، MD_2, MD_4, MD_5 و SHA1 [۷۷] هستند که اولی از طول ۱۲۸ بیت استفاده می‌کند و دومی که به وسیله مؤسسه ملی علوم و فنون ایالات متحده[۷۸] ایجاد شده از طول ۱۶۰بیت استفاده می‌کند.[۷۹] (شکل ۱)

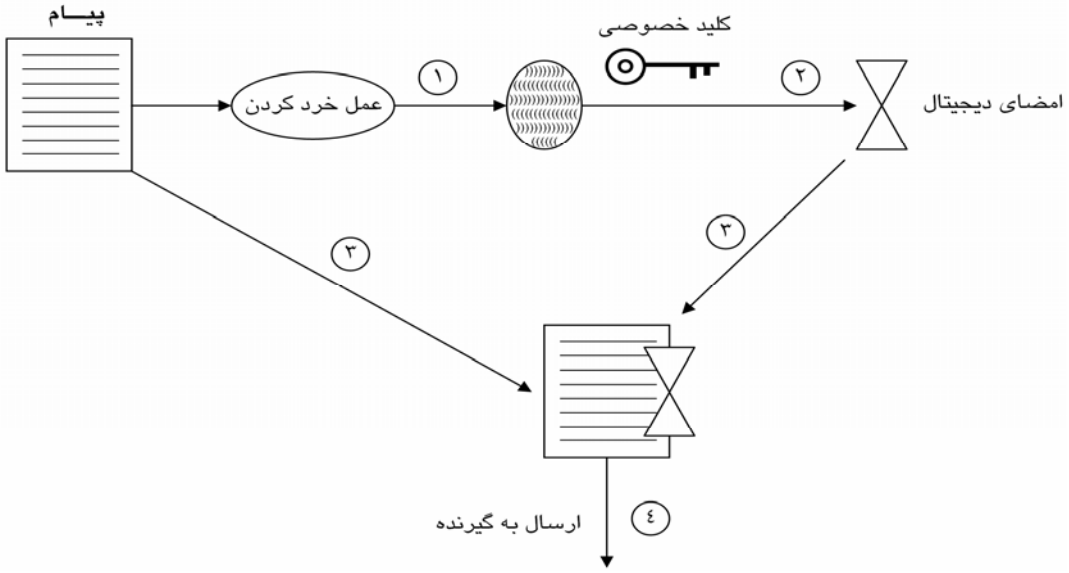
شکل ۱ : چکیده کردن پیام



[71] Uncitral Model Law on Electronic Signatures with Guide to Enactment, op.cit , PP.22-23
[72] Hash function
[73] Hashing
[74] Message Digest
[75] Fingerprint
[76] Uncitral Model Law on Electronic Signatures with Guide to Enactment, op.cit, PP.23-24
[77] Secure Hash Algorithm
[78] US National Institute of Science and Technology
[79] -What is a Hash Function? www.rsasecurity.com/rsalabs/fag/2-1-6.html
-Hashing, www.theory.dcs.st-and.ac.uk/ mda/cs2001/hashing/general.html

۲- ایجاد امضای دیجیتال: برای امضای سند، امضاکننده ابتدا بطور دقیق حدود آنچه را که باید امضاء شود تعیین می‌کند. سپس با استفاده از عمل خرد کردن در نرم‌افزار امضاکننده یک چکیده پیام منحصر بفرد ایجاد می‌شود(۱). پس از آن نرم‌افزار امضاکننده با استفاده از کلید خصوصی چکیده پیام را به یک امضای دیجیتال تبدیل می‌کند(۲). امضای دیجیتالی به دست آمده نسبت به پیام امضا شده و کلید خصوصی استفاده شده برای ایجاد امضاء منحصر بفرد است. معمولاً امضای دیجیتال به پیام ملحق می‌شود(۳) و حسب مورد ذخیره شده یا همراه آن انتقال می‌یابد(۴). با این وجود مشروط بر آنکه امضای دیجیتال همراهی قابل اعتمادی با پیام مرتبط داشته باشد ممکن است به عنوان یک داده جداگانه ذخیره شده یا ارسال شود.[۸۰](شکل ۲)

شکل ۲ : ایجاد امضای دیجیتال



۳- بررسی امضای دیجیتال و تمامیت پیام: فرایند بررسی امضای دیجیتال با مراجعه به پیام اصلی و کلید عمومی امضاکننده که از طریق گواهی صادر شده توسط مرجع گواهی یا به طریق دیگری در اختیار دریافت‌کننده پیام قرار گرفته است انجام می‌شود و بدان وسیله تعیین می‌کند که آیا امضای دیجیتال با استفاده از کلید خصوصی که با کلید عمومی مورد ارجاع مطابقت می‌کند و برای همان پیام ایجاد شده است یا خیر.

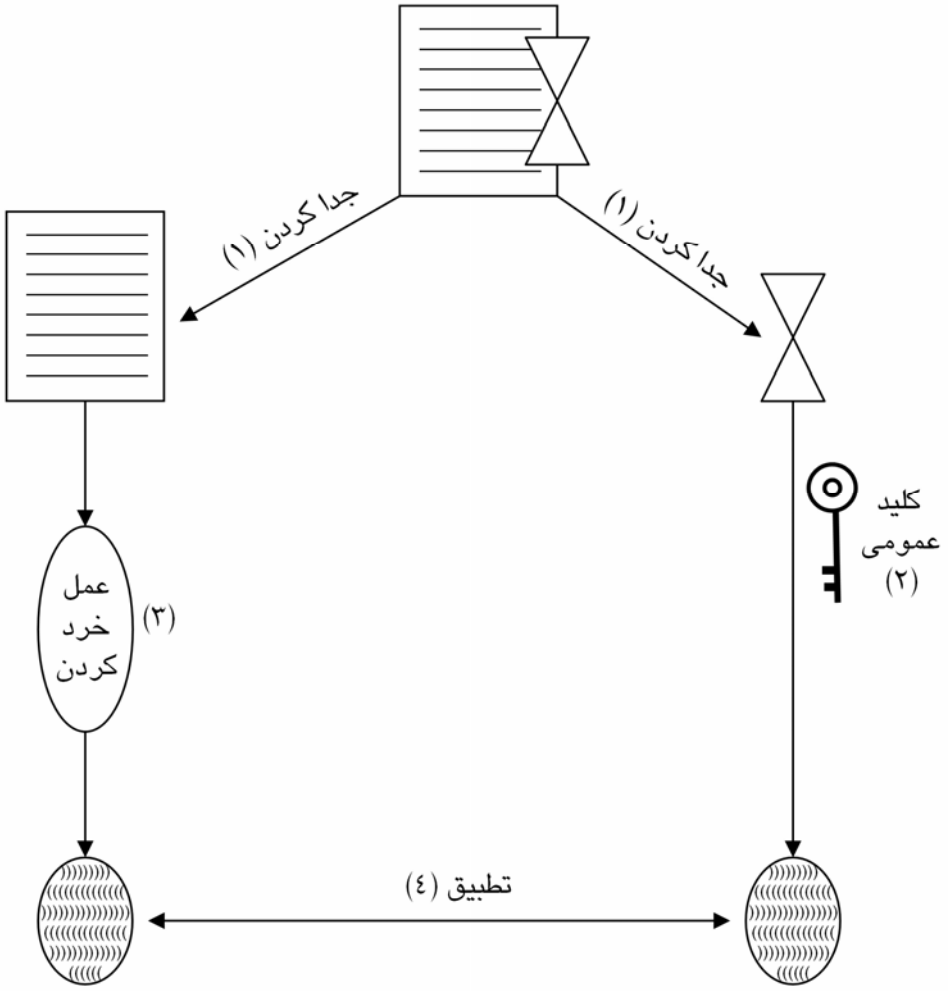
برای بررسی این موضوع پیام ارسالی از امضای دیجیتال جدا می‌شود(۱) و امضای دیجیتال با استفاده از کلید عمومی ارسال کننده رمزگشایی می‌شود(۲) سپس با استفاده از همان الگوریتمی که فرستنده استفاده کرده است عمل خرد کردن نسبت به پیام انجام می‌شود(۳) و پس از آن دو چکیده پیامی که در نتیجه این دو عمل ایجاد شده‌اند با یکدیگر مقایسه می‌شوند(۴) چنانچه تغییری در پیام صورت نگرفته باشد دو چکیده دقیقاً با یکدیگر منطبق خواهند بود. بنابراین با استفاده از امضای دیجیتال هویت فرستنده و تمامیت پیام

[80] Introduction to Public Key Infrastructure, op.cit

هر دو تضمین خواهد شد. زیرا کلید عمومی امضاکننده فقط زمانی امضای دیجیتال را رمزگشایی می‌کند که کلید خصوصی امضاکننده برای امضای آن استفاده شده باشد و به این ترتیب هویت فرستنده اثبات می‌شود، از طرفی چنانچه هر دو چکیده پیام، یعنی هم چکیده پیام محاسبه شده به وسیله اعمال الگوریتم خرد کردن و هم چکیده پیام ایجاد شده به وسیله امضای دیجیتال رمزگشایی شده یکسان باشند تمامیت پیام و عدم تغییر آن نیز اثبات می‌شود.[۸۱] (شکل۳)

[81] Uncitral Model Law on Electronic Signatures with Guide to Enactment,op.cit, P.24

شکل ۳ : بررسی امضای دیجیتال



گفتار دوم

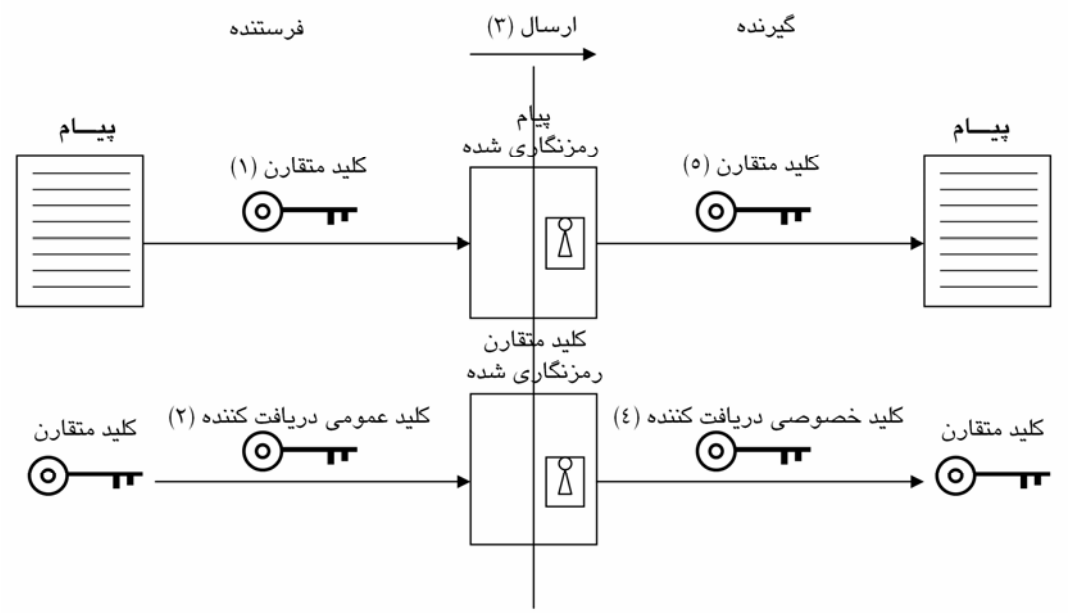
محرمانگی پیام

همانطور که دیدیم در امضای دیجیتال، اصل پیام به صورت ساده همراه امضاء ارسال می‌شود، بنابراین محتوای پیام برای هرکس که به آن دسترسی پیدا نماید قابل ملاحظه است. برای اینکه پیام فقط برای دریافت‌کننده قابل خواندن باشد لازم است پیام رمزنگاری گردد. بنابراین نرم‌افزار رمزنگاری برای محرمانه ماندن ارتباطات اینترنتی تهیه شده است.

رمزنگاری از یک الگوریتم ریاضی استفاده می‌کند تا یک متن ساده را به یک متن رمزنگاری شده ناخوانا تبدیل کند و آن را انتقال دهد و سپس از یک کلید دیگر استفاده می‌شود تا متن رمزنگاری شده را برای دریافت‌کننده، به شکل متن ساده تبدیل کند. بیشتر وب سایتها از نرم‌افزار رمزنگاری برای حفاظت از شماره کارتهای اعتباری استفاده می‌کنند. برای این امر می‌توان از سیستم رمزنگاری متقارن و نامتقارن استفاده نمود. اما در زیرساخت کلید عمومی برای رمزنگاری و محرمانه ساختن پیام با توجه به ایرادات دو نوع

سیستم یعنی مشکل انتقال کلید در رمزنگاری متقارن و کندی سرعت محاسباتی رمزنگاری نامتقارن ترکیبی از دو نوع رمزنگاری استفاده می‌شود. در این ترکیب، فرستنده برای سرعت بیشتر با استفاده از یک کلید متقارن پیام را رمزنگاری می‌کند(۱) این کلید متقارن که بطور تصادفی[۸۲] انتخاب شده با استفاده از کلید عمومی دریافت‌کننده رمزنگاری می‌شود(۲) سپس پیام رمزنگاری شده و کلید متقارن برای گیرنده ارسال می‌شود(۳) دریافت‌کننده با استفاده از کلید خصوصی خود کلید متقارن را رمزگشایی نموده و به آن دسترسی پیدا می‌کند(۴) و نهایتاً با استفاده از کلید متقارن که فرستنده به وسیله آن پیام را رمزنگاری و محرمانه ساخته است پیام را رمزگشایی می‌نماید(۵).[۸۳] (شکل۴)

شکل ۴ : محرمانه ساختن پیام



بنابراین در نهایت برای اینکه یک پیام بصورت محرمانه امضاء شود تا هم هویت فرستنده و تمامیت پیام و هم محرمانگی آن تضمین شود فرایند زیر صورت می‌پذیرد:

پیام با استفاده از یک کلید تصادفی که یک کلید متقارن است رمزنگاری می‌شود(۱) این کلید متقارن با استفاده از کلید عمومی دریافت‌کننده رمزنگاری می‌شود(۲) کلید متقارن رمزنگاری شده با امضای دیجیتالی که قبلاً در خصوص آن بحث کردیم و پیام رمزنگاری شده به وسیله کلید متقارن ترکیب شده(۳) و برای گیرنده مورد نظر ارسال می‌شود(۴). پس از آنکه گیرنده پیام را دریافت نمود، امضای دیجیتال، پیام رمزنگاری شده به وسیله کلید متقارن و کلید متقارن رمزنگاری شده به وسیله کلید عمومی خود را جدا می‌نماید(۵) کلید متقارن با استفاده از کلید خصوصی دریافت‌کننده رمزگشایی می‌شود(۶) سپس پیام با استفاده از این کلید متقارن

[82] Random Key
[83]- Introduction to Public Key Infrastructure, op.cit
-Cryptography: The Study of Encryption, http://world.std.com/franl/crypto.html

رمزگشایی و قابل خواندن می‌شود(۷) در مرحله بعدی برای اینکه تمامیت پیام و هویت ارسال کننده نیز اثبات شود با استفاده از الگوریتم خرد کردن، چکیده پیام ایجاد می‌شود تا با چکیده پیام حاصل از امضای دیجیتالی که با اعمال کلید عمومی فرستنده به آن به دست آمده، مقایسه شود(۸). (شکل۵)

شکل ۵ : پیام محرمانه امضاء شده