امضاء الکترونیکی

جمشید نورشرق*

چکیده

یکی از موضوعات مهم در باب بررسی تشکیل قراردادهای الکترونیکی به معنی قراردادهایی که با استفاده از وسائط الکترونیکی مختلف همچون تلفن، تلگرام، نمابر، در محیط شبکه و یا با استفاده از ایمیل منعقد می‌شوند، موضوع امضای الکترونیکی است درواقع اسناد الکترونیکی و به خصوص قراردادهای الکترونیکی با امضاء کامل شده و قابلیت انتساب پیدا می‌کنند، مقایسه‌ی امضای سنتی با امضای الکترونیکی به برداشتی بهتر از این موضوع کمک می‌کند، این بحث هم از جهت حمایت از حقوق قراردادی فرستنده‌ی داده پیام و هم مخاطب آن اهمیت پیدا می‌کند، بعبارت دیگر اعتقاد به تشکیل و یا عدم تشکیل قراردادی که با استفاده از وسائط الکترونیکی منعقد می‌گردد و متعاقباً استقرار حقوق و تعهدات متقابل طرفین، بطور اساسی بر این سؤال محوری متمرکز است که آیا انتساب داده پیام به فرستنده‌ی آن محرز است یا خیر؟ ایده‌ی داده پیام مطمئن و یا امضای مطمئن و همچنین پیشنهاد نهاد و مرجع گواهی و تصدیق بر این اساس متمرکز است که تا حد امکان از هرگونه تردید و خلل در اعتبار انتساب داده پیام پرهیز شود.

کلید واژه‌ها

تجارت الکترونیکی- قراردادهای الکترونیکی- امضاء سنتی- مرجع گواهی

* . دانش آموخته ی مقطع دکتری حقوق خصوصی دانشگاه آزاد اسلامی، واحد علوم و تحقیقات، گروه حقوق، تهران.

مقدمه

تردیدی نیست که رشد و گسترش روز افزون تجارت الکترونیکی مستلزم ایجاد اطمینان و اعتماد عمومی نسبت به این نوع از تجارت است و بدیهی است که این اطمینان باید از طریق تضمین امنیت و اعتبار تبادل الکترونیکی داده ها صورت گیرد.

یکی از مهمترین عواملی که باعث اعتبار قرارداد یا هر سند دیگری می‌شود صحت انتساب آن به صادر کننده آن سند یا قرارداد است این امر به طور معمول از طریق مهر نمودن یا امضاء کردن سند صورت می‌گرفته بر اساس آنچه متعارف است مهر و امضاء، دلایل قابل قبولی برای صحت انتساب سند به صادر کننده محسوب می‌گردند، در قراردادهای الکترونیکی نیز بایستی براساس ویژگی‌های خاص مربوط به این نوع قراردادها، صحت انتساب آنها را به صادرکننده احراز کرد، بنا براین در مورد امضاء اسنادی که به شیوه الکترونیکی صادر شده‌اند و به منظور امکان استناد به اینگونه اسناد به‌طرفیت صادرکننده، لازم است که علاوه بر بیان اقسام و انواع این امضاء (که به لحاظ موضوع بر وجوه فنی آن متمرکز است) ارکان و شرایط لازم برای تأثیرگذاری یک امضای الکترونیکی به طور دقیق معین شوند، بنابراین همانند حقوق سنتی، اثر مهم امضاء در حقوق تجارت الکترونیکی یعنی الزام صادرکننده به مفاد سند مورد بحث و همچنین بهره مندی از امتیازات آن در فرض وجود رابطه قراردادی، مبتنی بر این پیش فرض است که «اسناد بدون امضاء فاقد اعتبار و اثر حقوقی هستند.»

امضاء کردن شرط کامل بودن سند محسوب می‌گردد به این معنا که سند زمانی علیه صادرکننده قابلیت اتکاء دارد که به امضاء وی رسیده و یا واجد اثر انگشت او باشد، از این لحاظ گفته می‌شود که خطوط و عبارات نوشته، مربوط به کسی است که آن را امضاء کرده است، با توجه به آنچه گفته شد مشخص است که معنی و مفهوم امضاء سند این است که امضاءکننده، صحت صدور سند را نسبت به خود قبول نموده و به آثار حقوقی و قانونی سند مزبور پایبند باشد، در حال حاضر با توجه به فراگیر شدن تجارت الکترونیکی، امضاء الکترونیکی همسان با امضای دستی، مورد پذیرش نظام‌های حقوقی مختلف قرار گرفته است.

امضاء الکترونیکی از جهت احراز هویت طرفین در محیط سایبر حائز اهمیت فراوان است. عامل بسیار مهمی که با توجه به نقش مرجع گواهی تصدیق امضاء، بروز و نمود پیدا می‌کند، از طرفی در ارتباط با بحث تلقی داده پیام به عنوان یکی از ادله اثبات دعوی، سند الکترونیکی مزبور را می‌توان به عنوان دلیل اثبات تلقی و مورد استناد قرار داد، در بندهای ک و ی ماده۲ق.ت.ا و فصول اول و دوم قانون مزبور که مربوط به داده پیام مطمئن است، از مواد ۱۰ تا

۱۶ به بحث امضاء الکترونیکی تخصیص داده شده است، در این مقاله پس از بیان کلیاتی در مورد امضاء و آثار آن، به مقایسه امضای سنتی و مسلم الصدور پرداخته و پس از ذکر تاریخچه امضاء الکترونیکی و مفهوم آن، انواع امضاء الکترونیکی را مورد بحث قرار می‌دهیم.

گفتار اول : مفهوم و آثار امضاء

قانون مدنی ایران تعریفی از امضاء ارائه نکرده است، ماده ۱۳۰۱ قانون مذکور در مورد امضاء مقرر می‌دارد: «امضایی که در روی نوشته یا سندی باشد بر ضرر امضاء کننده دلیل است»، بنابراین اثر مهم امضاء متعهد شدن به تمام آثار و جنبه‌های سند یا قراردادی است که امضاء شده باشد. برخی عقیده دارند که امضاء جزیی از ماهیت معامله نیست بلکه مؤید شکل معامله است[1] ولی باید توجه کرد که در واقع امضاء سبب تحقق معامله می‌شود و پیش نویس قراردادی که متن آن مورد توافق طرفین قرار گرفته است، اصولاً تا زمانی که امضاء نشده، نسبت به طرفی که آن را امضاء ننموده، فاقد اثر خواهد بود. موارد ذیل را می توان به عنوان آثار امضاء ذکر نمود:

۱- **گواهی:** امضاء موجب تأیید و تصدیق یک نوشته از طریق شناسایی کردن امضاء کننده یا اسناد امضاء شده، می‌باشد، وقتی که امضاء کننده یک نشانه و علامتی را با یک ویژگی خاص به وجود می‌آورد، نوشته به امضاء کننده قابل انتساب خواهد بود.

۲- **تشریفات و رسوم:** اقدام به امضاء کردن یک سند، به طور معمول و متعارف قصد امضاء کننده را آشکار می‌سازد و مؤید قصد انشاء و تصمیم او بر التزام به مفاد آن است.

۳- **تأئید:** در حقیقت به موجب قانون یا عرف، امضاء را می توان به معنای تأئید یا تنفیذ نوشته تلقّی کرده و یا به معنای اینکه امضاء کننده قصد ایجاد آثار حقوقی دارد، محسوب نمود.

۴- **کارایی و قطعیت:** امضای مدرکی کتبی، غالباً مؤید وقوع، وضوح و قطعیت معامله است.

در ارتباط با بند ۴ فوق الذکر بایستی اذعان داشت که با توجه به نقش و کارکرد امضاء در انتساب مفاد نوشته یا سند به شخص امضاءکننده و اتکاء به مندرجات سند به طرفیت شخص مزبور، امضاء باید اوصاف ذیل را واجد باشد:

۱ – ۴ : تصدیق صاحب امضاء: امضاء باید نشان دهد چه کسی سند، پیام یا مدارک را امضاء کرده است.

۲ – ۴ : تصدیق مدرک: امضاء باید نشان دهد چه چیزی امضاء شده است و مانع انکار و تکذیب یا تغییر مدرک یا امضاء شود.

به هر حال از آنچه که در مورد امضاء گفته شد، مشخص می‌شود که هیچ سندی در عالم حقوق اعتبار ندارد مگر اینکه دارای علامتی باشد دال بر انتساب آن به مرجع صدور، که موجب رسمیت یافتن اسناد، تأئید و قطعیت آنها می‌گردد.[۲] تصدیق امضاء کننده و تصدیق مدرک، ابزارهایی برای مقابله با تحریف و تغییر غیر مجاز در سند است، در واژه شناسی امنیت اطلاعات این ابزارها، مانع انکار و تکذیب می‌گردند و «خدمات پیش گیری از انکار و تکذیب» نامیده شده‌اند، این خدمات، منشاء داده پیام یا ارسال داده پیام از سوی فرستنده را تثبیت می‌کنند و اصولاً مانع انکار و تکذیب دریافت کننده می‌شوند.

۳ – ۴ : اقدام مثبت و عملی: درج امضاء باید عمل مثبتی باشد که دلالت بر انجام معامله داشته باشد.

۴ – ۴ : کارآیی: روند ایجاد و تصدیق امضاء، باید موجب اصالت آن بوده و نیز کمترین هزینه را در بر داشته باشد.

گفتار دوّم : تعریف و مفهوم امضاء سنّتی و امضاء مسلّم الصّدور

امضاء سنتی به مفهوم اعم، هرگونه علامت انحصاری شخصی است که زیرِ نوشته ترسیم یا گذارده شده و دلالت بر هویّت امضاء کننده و تأئید متن نوشته توسط او می‌نماید، بنابراین می‌تواند بوسیله دست در سند ترسیم شده «امضاء به معنای اخص» و یا بوسیله دیگری نقش بسته و یا منحصراً مهر یا اثر انگشت باشد.[۳]

همچنین گفته است که امضاء عبارت از ترسیمی شخصی است که بطور معمول حاوی نام شخص است.[۴] همچنین امضاء نشان تأئید اعلام‌های مندرج در سند و پذیرش تعهدهای ناشی از آن است و پیش از آن، نوشته را باید طرحی به حساب آورد که موضوع مطالعه و تدبر است و هنوز تصمیم نهایی دربارهٔ آن گرفته نشده است.[۵]

برخی گفته اند امضاء عبارت از نگارش نام نویسنده در ذیل نوشته‌ای به منظور تصریح صحت تحقق تعهداتی است که در سند مذکور برای وی درج شده است،[۶] بنابر آنچه گفته شد امضاء باید در محلی قرار گیرد که در نظر عرف نشان رضایت باشد، اثر انگشت نیز وسیله امضاء است که گاه ضرورت و اصالت پیدا می‌کند. [۷] بر این اساس وقتی امضاء یا اثر انگشت شخصی ذیل سندی باشد علیه آن شخص سندیت دارد، برخی نیز گفته‌اند امضاء عبارت از اسم و علامتی است که در ذیل اسناد و نوشته‌ها گذارده شده و کاشف از این است که مدلول و مفاد آن مستند به فعل و تصدیق امضاء کننده بوده و یا بر طبق اراده او تنظیم گردیده است.[۸]

بر این مبنا امضاء در اسناد سنتی، ترسیم یا اثر انگشتی است که به وسیله دست در ذیل اسناد تنظیمی شخصی به کار می‌رود تا بدین وسیله امضاء کننده بیان نماید که محتوای سند مزبور را با اراده خویش تنظیم نموده و به آثار حقوقی آن ملتزم می‌باشد. ممکن است گفته شود که امضاء باید به دست صاحب امضاء انجام شود بنابراین نمی‌تواند با استفاده از ماشین باشد و نباید در قالب یک شکل یا علامت باشد، بنظر می‌رسد که این منع به لحاظ عدم توانایی اثبات هویّت امضاء کننده است، بنابراین اگر چنین محدودیتی وجود نداشته و بنا به شرایط و اوضاع و احوال پیرامونی، تردیدی درانتساب آن وجود نداشته باشد، منعی برای امضاء با ماشین به چشم نمی‌خورد، برخلاف آنچه گفته شده است لازم نیست امضاء لزوماً به صورت علامت خطی دست نویس باشد و فقط مقصود این است که با استفاده از علامتی صاحب امضاء را مشخص کنند و او را از دیگران کاملاً متمایز کنند.[۹] بنابراین امضاء می‌تواند همان تحریر نام و نام خانوادگی شخص باشد.

البته به نظر می‌رسد که اولاً عرف، زمانی که مفهوم اخص امضاء، را مدنظر دارد، مهر، مهرِ امضاء یا اثر انگشت را داخل در معنای آن نمی‌داند و بیشتر به ترسیم دستی توجه دارد، ثانیاً هر چند قانون‌گذار به طور عام بر اثر انگشت و امضاء یک اثر قائل است و هر یک از آن ها چنانچه به شخصی منتسب شوند دارای اثر حقوقی برای آن شخص خواهند بود. به عنوان مثال چنانچه در ماده ۲۲۳ قانون تجارت بیان نموده «برات علاوه بر امضاء یا مهر برات دهنده باید دارای شرایط ذیل باشد ...» که ملاحظه می شود حتی مهر را نیز در ردیف امضاء دانسته است، با این وجود در مواردی بر امضاء به مفهوم آنچه با دست ترسیم شده، موضوعیت قائل شده و ایجاد سند را به جز از طریق امضاء مورد پذیرش قرار نداده و حتی مهر و اثر انگشت را نیز نپذیرفته است، همچون ماده ۳۱۱ قانون تجارت که مقرر می‌دارد «در چک باید محل و تاریخ صدور قید شده و به امضای صادر کننده برسد.»

امضای مسلم الصدور، امضایی است که دعوی انکار و تکذیب نسبت به آن شنیده نشود. مانند امضای ذیل سند رسمی یا امضایی که صاحب امضاء معترف و مقرّ به صدور آن از سوی خویش باشد،[۱۰] این امضاء در زمان رسیدگی به صحت و اصالت امضای مورد انکار و تردید، اساس تطبیق قرار می‌گیرد.[۱۱] با توجه به آنچه گفته شد به نظر می‌رسد که امضای الکترونیکی ثبت و تودیع شده نزد مرجع تصدیق یا گواهی،[۱۲] امضای مسلم الصدور محسوب می‌گردد.

گفتار سوّم : تاریخچه امضای الکترونیکی

گسترش تجارت الکترونیکی و رشد روزافزون آن مستلزم ایجاد اطمینان و اعتماد در افکار عمومی نسبت به این نوع از تجارت می‌باشد و این اطمینان بایستی از طریق تضمین امنیت و اعتبار تبادل الکترونیکی داده‌ها صورت گیرد، تبعاً در این میان آنچه بعنوان عاملی اصلی در خصوص صحت انتساب سند به صادر کنندهٔ آن نقش مهمی را ایفا می‌نماید به طور معمول امضاء و مهر درج شده در ذیل سند است، در این قسمت لازم است ابتدا در خصوص تاریخچه‌ی امضای الکترونیکی توضیحاتی بیان گردند: در سال ۱۹۹۶ میلادی کمیسیون حقوق تجارت بین الملل‌سازمان ملل متحد (آنسیترال) قانون نمونه‌ای در باب تجارت الکترونیکی[۱۳] تدوین کرد، در ماده ۷ این قانون نمونه، امضای واجد شرایط الکترونیکی دارای همان آثار و ارزش اثباتی امضای سنتی شناخته شد.[۱۴] بنابر گزارش کارگروه تجارت الکترونیکی آنسیترال، با امضای الکترونیکی نیز اصالت سند و انتساب آن به امضاء کننده، اثبات و وی متعهد به محتوای سند، خواهد بود. اهمیت موضوع امضاء در تجارت الکترونیکی سبب شد تا آنسیترال در سال ۲۰۰۱، قانون نمونه جداگانه‌ای را درباره امضاهای الکترونیکی، در ۱۲ ماده به تصویب رساند. قانون نمونه آنسیترال در باره امضاهای الکترونیکی مصوب ۲۰۰۱، امضای الکترونیکی را به «داده‌ای در شکل الکترونیکی که به یک داده پیام، ضمیمه، یا جزء همسان، پیوسته و جدا ناپذیری از آن شده و می‌تواند برای شناسایی امضاکننده آن داده پیام و تأیید اطلاعات موجود در داده پیام از سوی امضاءکننده به کار گرفته شود»[۱۵] تعریف کرده است.

قانون نمونه دفاتر اسناد رسمی ایالات‌متحده، در بند ۷ ماده ۱۴، امضای الکترونیکی را به معنی «هرگونه صدا، علامت یا فرایند الکترونیکی که به مدرک الکترونیکی با در نظر گرفتن شرایط علمی مربوط بدان، الحاق یا با آن همسان شده و این امضاء از سوی شخصی که قصد پذیرش مدارک را دارد، درج شده یا به دستور و برای او طراحی شده است». دانسته است.[۱۶] قانون یوتا نیز، هرچند از امضاء، تعریفی به عمل نیاورده، اما «امضای الکترونیکی» را به عنوان « صدا،

نماد یا فرایندی الکترونیکی که منطقاً به همراه سابقه بوده یا به آن ضمیمه شده، و توسط شخصی که قصد دارد، آن سابقه را امضاء کند، اجرا شده و یا مورد پذیرش قرار گرفته باشد»، تعریف کرده است.[۱۷] در سطح اتحادیه اروپا نیز، دستورالعمل شماره 1999/93/ce ناظر به امضاهای الکترونیکی مصوب ۱۳ دسامبر ۱۹۹۹[۱۸] و دستورالعمل شماره 2000/31/ce مربوط به برخی جنبه‌های حقوقی تجارت الکترونیکی در بازار داخلی (مصوب ۸ ژوئن ۲۰۰۰) را که باید مبنای قانونی اعتبار امضاهای الکترونیکی دانست، به مفهوم امضای الکترونیکی، اشاره داشته‌اند. براساس دستورالعمل تجارت الکترونیکی، منظور از امضای الکترونیکی، داده‌ای الکترونیکی است که به سایر داده‌های الکترونیکی، متّصل یا به طور منطقی مرتبط است و روشی برای احراز اصالت به شمار می‌رود.

در حقوق فرانسه در ۱۳ مارس ۲۰۰۰ مجلس قانون‌گذاری این کشور، قانونی[۱۹] را برای پذیرش امضای الکترونیکی تصویب و از طریق آن مفهوم امضای الکترونیکی را وارد قانون مدنی فرانسه کرد. این قانون به سرعت قابلیت اجرایی یافت. علاوه بر آن دستورالعمل امضاهای الکترونیکی اتحادیه اروپا که در فرانسه هم به تصویب رسیده به بحث امضای الکترونیکی پرداخته است. ماده ۱۳۱۶ قانون مدنی فرانسه، به موجب اصلاحات مذکور، بیشتر به قواعد ماهوی امضای الکترونیکی می‌پردازد. به موجب بند۳ این ماده «... با اثبات صدور امضاء از سوی شخص معین، قرارداد (توافق)، دارای ارزش و اعتبار مساوی با معادل کاغذی آن خواهد بود»، علاوه بر تشخیص هویت امضاء کننده، امضای معتبر، بیانگر تنفیذ مدرک از سوی شخص اخیر و اثبات گر دخالت ارادی او، در تنظیم محتوای سند است، (بند۴ ماده ۱۳۱۶)، بند اخیر تصریح دارد که امضاء، اعلام قصد شخص بر التزام به قرارداد، به شمار می‌آید.نکته مهم، امکان انتساب امضاء به شخص و فعل ارادی امضاء کننده به هنگام قبول تعهد است، بنابراین با لحاظ بند ۴ ماده ۱۳۱۶ قانون مدنی فرانسه، چنین فرض می شود که امضاء، شرایط فنی و قانونی مقرر در مقررات خاص را داراست.

گفتار چهارم : تعریف و مفهوم امضاء الکترونیکی

همان‌طوری که گفته شد امضاء به معنای پایان رساندن یا نافذ دانستن امری در عالم خارج است، البته این نکته را هم باید در نظر داشت که امضاء لزوماً ناظر به شکل یا علامت خاصی نیست، بلکه هر علامت یا رمزی که مبین قصد انشاء فرد در قرارداد باشد در تجارت الکترونیکی پذیرفتنی است. امضاء الکترونیکی معادل کاربردی برای یک امضای دستی است، مفهوم امضای

الکترونیکی تمامی آثار امضای دست نویس از نظر ایجاد آثار حقوقی را دارا است. هر دو هویّت و ارتباط وی با متن امضاء شده را تائید می‌کنند و این امر در واقع وجه اشتراک امضاء در تمامی نظام‌های حقوقی است. بنابراین برای اینکه امضای الکترونیکی نشان دهنده تائید اطلاعات باشد وجود فناوری که قادر به ایجاد چنین امضایی برای تحقق کارکردهای امضای دستی باشد یک پیش شرط ضروری است.

در فضای الکترونیکی که نوشته‌ها صورت مادی ندارند و نمی‌توانند لمس شوند و تبادل آگاهی‌ها در محیطی مجازی صورت می‌گیرد، هر علامتی (برای نمونه شمارهٔ رمز) که شناسایی امضا کنندهٔ داده پیام را امکان پذیر نماید، امضای الکترونیکی شمرده می‌شود.[۲۰]

امضاء الکترونیکی، وظیفه معرفی شخص ارسال کننده و نیز انتساب داده پیام به وی را بر عهده دارد، وقتی شخصی از طریق رایانه اقدام به خرید کتابی می‌کند، تا زمانی که خریدار، داده پیام را امضاء نکند و هویّت وی توسط مراجع گواهی تأئید نشود، نمی‌توان اطمینان حاصل کرد که خریدار اهلیت معامله دارد و این امر به بحث امضاء الکترونیکی و مراجع گواهی ارتباط نزدیک پیدا می‌نماید. در تعریف امضاء الکترونیکی گفته شده است: ۱ـ رشته‌ای از داده‌ها که برای شناسایی مورد استفاده قرار می‌گیرد، مثلاً متنی که به انتهای پیام، پست الکترونیکی یا نمابر ضمیمه می‌شود. ۲ـ یک شماره منحصر به فرد که برای شناسایی یک سخت افزار یا نرم افزار اختصاص می‌یابد.[۲۱]

برخی گفته‌اند امضای الکترونیکی هرگونه تصدیقی است که به شکل الکترونیکی ایجاد شده باشد و می‌تواند یک علامت رمز، کلمه، عدد، اسم تایپ شده، تصویر اسکن شده یک امضای دستی و یا هر نوع نشانه الکترونیکی باشد که به وسیله صادر کننده و یا قائم مقام وی صورت پذیرفته و به یک سند ملحق شده است.[۲۲] همچنین گفته شده است، امضای الکترونیکی هر علامت یا روش الکترونیکی است که به وسیله یک طرف پذیرفته شده تا قصد او به تصدیق صحت سند یا ملزم شدن او به وسیله سند را نشان دهد.[۲۳] باید توجه نمود که هرگونه علامت و نشانه‌ای که به صورت رمزی نباشد در صورتی امضاء محسوب می‌شود که به گونه ای موجب انتساب بین ایجاد کننده نشانه و علامت مورد نظر باشد.

امضاء دیجیتالی اجازه می‌دهد تا اسناد ارسال شده به صورت الکترونیکی امضاء شده و رسمیت یابند،گیرنده پیامی که به صورت دیجیتالی امضاء شده است، می‌تواند هویّت فرستنده را شناسایی کرده و در صورتی که تغییری در پیام بعد از ارسال داده شده باشد آن را تشخیص دهد و پیام رمز گذاری شده را رمزگشایی کرده و بتواند آن را بخواند.

بعلاوه در بند ی ماده ۲ ق.ت.ا.ا، امضای الکترونیکی «عبارت از هر نوع علامت منضم شده یا به نحو منطقی متصل شده به (داده پیام) است که برای شناسایی امضاء کننده (داده پیام)، مورد استفاده قرار می‌گیرد»، تعریف شده است. با دقت در تعاریف ارائه شده از امضای الکترونیکی، می‌توان به این نتیجه رسید که امضای مذکور باید به گونه‌ای باشد که بتوان موارد زیر را از طریق آن اثبات نمود :

۱- **اِسناد** : با امضای الکترونیکی یک سند، محتوای آن به شخص امضاء کننده منتسب می‌شود و به نفع و به ضرر او قابل استناد است.

۲- **انجام تشریفات:** امضای الکترونیکی یک سند الکترونیکی، حاکی از انجام تمام تشریفات مقرر قانونی برای تنظیم آن است.

۳- **کارکرد یکسان:** در صورت استفاده از امضای الکترونیکی، برای تأیید محتوای مدارک الکترونیکی، این نوع امضاء کارکردی همانند امضاء در اسناد کاغذی خواهد داشت.

۴- **داشتن آثار حقوقی** : امضای الکترونیکی دارای تمام آثار حقوقی مقرر برای امضای سنتی می‌باشد. چنانچه در ماده ۷ قانون نمونه آنسیترال (۱۹۹۶) و ماده ۳ قانون نمونه آنسیترال (۲۰۰۱)، «اصل اتحاد آثار امضاء و مدارک الکترونیکی و سنتی» مورد تأکید قرار گرفته است.

شرایط ذکر شده در قانون ق.ت.ا.ا برای احراز مطمئن بودن یک امضای الکترونیکی، عبارتست از این که نسبت به امضاء کننده منحصر به فرد باشد، هویّت امضاء کننده ی داده پیام را معلوم کند، به وسیله ی امضاء کننده یا تحت اراده انحصاری وی صادر و به نحوی به یک داده پیام متصل شده باشد که هر تغییر در آن داده پیام، قابل تشخیص و کشف باشد، در ماده ۱۰ قانون تجارت الکترونیکی ایران، این شرایط تقریباً به صورت یکسان و بدون تغییر مطابق شرایط پذیرفته شده‌ی بین‌المللی در قوانین مشابه در سایر کشورهاست، در بررسی و تدوین این قانون، قوانین کشورهای مختلف خصوصاً قوانین مرجع سازمان ملل‌متحد (آنسیترال) و اتحادیه‌ی اروپا مورد استفاده و مقایسه‌ی تطبیقی قرار گرفته‌اند. به طور کلی موادی که در این قانون به امضاء الکترونیکی اشاره شده و در مورد آن نکاتی را بیان شده است به شرح زیر می‌باشند:

یک) بند (ی) ماده دو: امضاء الکترونیکی[۲۴] عبارت از هر نوع علامت منضم شده یا به نحو منطقی متصل شده به «داده پیام» است که برای شناسایی امضاء کننده‌ی «داده پیام» مورد استفاده قرار می‌گیرد.

دو) بند (ک) ماده دو: امضای الکترونیکی مطمئن،[۲۵] هر امضای الکترونیکی است که مطابق با ماده ۱۰ این قانون باشد.

سه) بند (ل) ماده دو: امضاء کننده،[۲۶] هر شخص یا قائم مقام وی که امضای الکترونیکی را تولید می‌کند.

چهار) ماده هفت: هرگاه قانون وجود امضاء را لازم بداند امضای الکترونیکی مکفی است.

پنج) ماده ۱۰: امضاء الکترونیکی مطمئن باید دارای شرایط زیر باشد:

- ❖ نسبت به امضاء کننده منحصر به فرد باشد.
- ❖ هویت امضاء کننده «داده پیام» را معلوم نماید.
- ❖ به وسیله امضاء کننده و یا تحت اراده انحصاری وی صادر شده باشد.
- ❖ به نحوی به یک «داده پیام» متصل شود که هر تغییری در آن «داده پیام» قابل تشخیص و کشف باشد.

شش) ماده ۱۴: کلیه «داده پیام» هایی که به طریق مطمئن ایجاد و نگهداری شده‌اند از حیث محتویات و امضای مندرج در آن، تعهدات طرفین یا طرفی که تعهد کرده و کلیه اشخاصی که قائم مقام قانونی آنان محسوب می‌شوند، اجرای مفاد آن و سایر آثار در حکم اسناد معتبر و قابل استناد در مراجع قضایی و حقوقی است.

هفت) ماده ۱۵: نسبت به «داده پیام» مطمئن، سوابق الکترونیکی مطمئن و امضای الکترونیکی مطمئن انکار و تردید مسموع نیست و تنها می‌توان ادعای جعلیت به «داده پیام» مزبور وارد و یا ثابت نمود که «داده پیام» مزبور به جهتی از جهات قانونی، از اعتبار افتاده است. علاوه بر تعریف مذکور در بند «ی» ماده ۲ ق.ت.ا.ا مصوب ۱۳۸۲، در بند ک همان ماده امضای مطمئن را چنین تعریف می‌کند: «هر امضای الکترونیکی است که مطابق با ماده ۱۰ این قانون باشد»[۲۷] متعاقباً قانون‌گذار در ماده ۷ ق.ت.ا.ا بیان نموده «هرگاه قانون وجود امضاء را لازم بداند امضای الکترونیکی مکفی است». این تعریف برگرفته از ماده ۷ قانون نمونه تجارت الکترونیکی آنستیرال در مورد امضاء می‌باشد که بیان می‌دارد در جایی که قانون امضاء شخصی را شرط بداند، این شرط در رابطه با داده پیام در صورتی که شرایط زیر مهیا باشد، محقق می‌گردد:

الف –از روشی برای تعیین هویّت شخصی و تائید اطلاعات موجود در داده پیام استفاده شود.

ب – متناسب با موضوعی که داده پیام برای آن ایجاد یا ارسال شده، روش به کار گرفته شده با توجه به اوضاع و احوال از جمله هرگونه توافق خصوصی مطمئن باشد. ماده ۷ قانون نمونه

آنستیرال براساس شناسایی کارکرد امضاء در محیط کاغذی و نه الکترونیکی بنا شده است، در تنظیم قانون فوق، کارکردهای زیر در مورد امضاء مدنظر قرار گرفته شده است:

۱- شناسایی هویّت افراد.

۲- فراهم آوردن این اطمینان که براساس آن دخالت شخص امضاء کننده مستفاد گردد.

۳- ارتباط شخصی امضاء کننده با محتویات سند.

ماده ۷ قانون نمونه آنستیرال با پذیرفتن یک راهکار وسیع و جامع، شرایط کلی را وضع می‌نماید که طبق آن داده پیام، انتساب داده شده، فرض گردیده و دارای اعتبار کافی برای لازم الاجرا شدن می باشد. بند ۱ ماده ۷ به دو موضوع تاکید می کند؛ یکی شناسایی هویّت امضاء کننده سند و دیگر اینکه امضاء کننده محتویات سند را تائید کرده است. در قانون نمونه نیز به صورت مطلق، استفاده از هر روشی و هرگونه امضایی پذیرفته شده و امضاء می‌تواند علامت، عدد، اسم شخص و ... باشد، مشروط بر اینکه امضای مزبور قادر به تعیین هویّت شخص و تائید اطلاعات داده پیام بوده و متناسب با اهمیت موضوع داده پیام اطمینان‌آور باشد.

قانون تجارت الکترونیکی ایران در ماده ۷ تنها به کافی بودن امضاء الکترونیکی در مواردی که قانون‌گذار، امضاء را لازم می‌داند، بسنده کرده است. امّا امضاء الکترونیکی برای اینکه مطمئن باشد باید، شرایطی داشته باشد که ماده ۱۰ ق.ت.ا.ا به آن موارد اشاره کرده است. آن شرایط به شرح زیر است:

۱- نسبت به امضاء کننده منحصر به فرد باشد.

۲- هویّت امضاء کننده داده پیام را معلوم نماید.

۳- به وسیله امضاء کننده و یا تحت اراده انحصاری وی صادر شده باشد.

۴- به نحوی به یک داده پیام متصل شود که هر تغییری در آن داده پیام قابل تشخیص و کشف باشد.

حسب ماده ۱۵ ق.ت.ا.ا در صورتی که امضاء الکترونیکی دارای شرایط فوق باشد، انکار و تردید در برابر آن مسموع نبوده و تنها می‌توان ادعای جعلیت به داده پیام مزبور وارد یا ثابت نمود که داده پیام مزبور به جهتی از جهات قانونی از اعتبار افتاده است.

دستورالعمل ۱۹۹۹/۹۳/EC پارلمان و شورای اتحادیه اروپا مصوب ۱۹۹۹[۲۸] در بند ۱ ماده ۲ امضای الکترونیکی را بدین نحو تعریف کرده است: «امضای الکترونیکی داده‌ای الکترونیکی است که به سایر داده‌های الکترونیکی متصل یا منطقاً مربوط بوده و روشی برای احراز اصالت به شمار می‌رود.» قانون نمونه آنستیرال در مورد امضای الکترونیکی مصوب ۲۰۰۱[۲۹] در بند۱

ماده ۲ در خصوص امضای الکترونیکی مقرر می‌دارد: «امضای الکترونیکی داده‌ای الکترونیکی است که ممکن است به یک داده پیام ملحق شده یا مطلقاً با آن همراه بوده و برای شناسایی هویّت امضاء کننده داده پیام و تائید قصد امضاء کننده نسبت به اطلاعات موجود در داده پیام به کار رود».

در حقوق فرانسه در تعریف امضای الکترونیکی، قسمت دوم ماده ۴ ـ ۱۳۱۶ قانون مدنی مقرر می‌کند: «هنگامی امضاء الکترونیکی است که امضاء در برگیرنده رویه مطمئنی است که شناسایی ارتباط امضاء را با سندی که به آن محلق شده است، تضمین می‌کند. قابلیت اعتماد چنین فرایندی مفروض است مگر اینکه دلیل مخالفی وجود داشته باشد. هنگامی که امضای الکترونیکی ایجاد می‌شود، هویّت امضاء کننده و تمامیت سند را با توجه به شرایط تعیین شده در مصوبه شورای دولتی تضمین می‌نماید» بند ۱ ماده ۱ مصوبه شورای دولتی، امضای الکترونیکی را داده‌ای می‌داند که با استفاده از فرایندی که شرایط ذکر شده در جمله اول زیر پاراگراف دوم ماده ۴ـ۱۳۱۶ ق.م را رعایت نموده ایجاد شده است.[۳۰]

بند ۵ ماده ۱۰۶ قانون معاملات الکترونیکی متّحدالشکل ایالات متحده آمریکا(یوتا) (۱۹۹۹)[۳۱] نیز اعلام می‌دارد: «امضای الکترونیکی به معنای هر صدا، نشانه یا فرایند الکترونیکی است که به یک قرارداد یا سند متصل بوده یا از لحاظ منطقی با آن همراه بوده و به وسیله مشخص با قصد امضای پیام، اعمال یا پذیرفته است»[۳۲] قانون مبادلات الکترونیکی سال ۱۹۹۸ سنگاپور یک تفکیک پایه ای بین سوابق الکترونیکی و امضاء از یک طرف و سوابق و امضای الکترونیکی مطمئن از طرف دیگر قائل شده است که از این جهت ماده ۷ قانون نمونه آنستیرال درباره تجارت الکترونیکی را تداعی می‌کند، در واقع در حقوق سنگاپور فقط امضاهای خاصی دارای ارزش و سندیت هستند و آن امضاهایی است که با کلید مشخص مطمئن و قابل اعتمادی زده شده باشد، به گونه ای که به راحتی قابل جعل نباشد، در این قانون آمده است: امضای الکترونیکی یعنی مجموعه‌ای از حروف، اعداد، یا علایم دیجیتالی که به سابقه (ثبت) الکترونیکی ضمیمه یا الصاق شده است و به قصد مستندسازی اطلاعات به عنوان یک سابقه ساخته می‌شود.

در قانون نمونه آنستیرال امضای الکترونیکی در واقع یک امضاء محسوب می‌شود (اگر چه محدودیت در ارتباط با قصد، انتقال مال غیر منقول، و اسناد مشابه وجود دارد) و به هر طریقی قابل اثبات است در عوض یک «امضای الکترونیکی مطمئن» یک امضای دیجیتال است که مطابق با استانداردهای امضای دیجیتال مندرج در قانون به وجود آمده و با یک فرآیند مطمئن

تجاری معقول، طرفین آن را به رسمیت شناخته‌اند. به این ترتیب یک امضای الکترونیکی مطمئن باید ۱ـ نسبت به شخص استفاده کننده منحصر به فرد باشد ۲ـ قابلیت تعیین هویّت شخص را داشته باشد ۳ـ به نحوی ایجاد شده باشد که تحت کنترل انحصاری شخص استفاده کننده بوده باشد ۴ـ به نحوی به سند الکترونیکی متصل شده باشد که تمامیت آن را بتوان تصدیق کرد.[۳۳]

اسنادی که به وسیله امضای الکترونیکی مطمئن تولید می‌شوند فرض تمامیت را با خود همراه دارند، این فرض که امضاء متعلق به شخص ایجاد کننده است و این فرض که کاربر، امضاء را به قصد امضاء به علاوه سایر تبعات حقوقی آن از جمله تأئید سند لحاظ کرده است. این قانون امضای دیجیتال را به عنوان یک امضای الکترونیکی مطمئن محسوب و یک رژیم جامع راجع به آن تدوین کرده است. بنابراین بین امضای الکترونیکی در مفهوم مطلق آن و امضای الکترونیکی مطمئن (امضای الکترونیکی دارای امنیت)[۳۴] تفاوت قائل شده است.[۳۵]

در واقع می‌توان گفت که امضای الکترونیکی هویّت امضاء کننده را معلوم می‌کند. در نتیجه امضاء باید به گونه‌ای صورت پذیرد که این کارکرد را تحقق بخشد، بنابراین صرف تایپ نمودن اسم یک شخص در پایان یک متن بدون اینکه هیچ نوع رمزنگاری در آن بکار گرفته باشد، به ندرت می‌تواند مثبت هویّت امضاء کننده باشد، زیرا بر خلاف نوشتن نام به صورت دستی که امکان تطبیق دستخط وجود دارد، در اینجا چنین امکانی وجود ندارد و لذا امکان کشف هویّت امضاء کننده وجود نخواهد داشت. بر این اساس، هر نوع علامت به خودی خود نمی‌تواند امضای الکترونیکی محسوب شود بلکه این علامت باید با نوعی رمزنگاری همراه باشد تا امضاء محسوب شود. رمزنگاری در معنای اعم هرگونه مخفی کردن اطلاعات است یعنی روشی که طی آن فقط طرف مقصود امضاء کننده بتواند مطلب را دریافت کرده و مقصود امضاء کننده را استنباط نماید و به واسطه این انحصار از هویّت واقعی ارسال کننده اطمینان یابد. برخی معتقدند ساده ترین و اساسی ترین دیدگاه در خصوص امضاء، تایپ نام شخص است و ممکن است نام شخص بر روی یک نامه الکترونیکی امضاء محسوب شود. همچنان که ممکن است از تصویر اسکن شده امضای شخصی در یک سند برای تائید محتویات سند و تعیین هویّت فرستنده استفاده کرد. این نوع امضاها بیشتر برای معاملات جزئی و کم اهمیت کاربرد دارند.[۳۶] با وجود این به نظر می‌رسد در یک نامه الکترونیکی نیز بیش از آنکه اسم شخصی مؤثر در اعتبار پیام باشد، شناخت قبلی گیرنده از آدرس ارسال کننده و اطمینان کافی از این نکته که رمز عبور الکترونیکی فقط در اختیار فرستنده است، موجب اعتماد به هویّت فرستنده و محتویات نامه می‌گردد.

در واقع امضای الکترونیکی چیزی جز یک سری فرمول‌های ریاضی نیست که از سوی مراجع گواهی امضاء، تأئید و در اختیار افراد قرار می‌گیرد و اگر چه تحت عنوان امضاء، نام گرفته‌اند، ولی چون توسط شخص ثالثی تولید و به اشخاص اختصاص داده می‌شوند و اشخاص فقط آنها را به شکلی که هستند مورد استفاده قرار می‌دهند، در تحلیل حقوقی در ردیف مهر قرار می‌گیرد.

بهرحال طبق ماده ۷ قانون تجارت الکترونیکی ایران «هرگاه قانون، وجود امضاء را لازم بداند، امضاء الکترونیکی مکفی است» یعنی امضای الکترونیکی هر ماهیتی که داشته باشد (مهر، امضاء یا ماهیت دیگر) از نظر قانون جایگزین امضای دست نویس با آثار حقوقی مشابه شده است، همچنین در بند (ی) ماده دو اعلام می‌کند که: امضای الکترونیکی عبارتست از هر نوع علامت منضم شده یا به نحو منطقی متصل شده به داده پیام است که برای شناسایی امضاء کننده داده پیام مورد استفاده قرار می‌گیرد.

در اکثر کشورها از امضای الکترونیکی به عنوان داده پیام یاد شده که با هر نوع علامتی به نحو منطقی به دیگر داده پیام ها متصل می‌شود در حالیکه در حقوق آلمان امضای الکترونیکی را مهری دانسته اند که با کلید خصوصی تولید می‌گردد و به دیگر داده‌ها ضمیمه می‌شود،[۳۷] این در حالی‌ست که میان مهر و امضاء در حقوق موضوعه کشورها تفاوت‌های بسیاری وجود دارد.

با توجه به آنچه گفته شد، می‌توان گفت که:

- ❖ امضای الکترونیکی، یک داده الکترونیکی است.
- ❖ این داده به داده‌های الکترونیکی نیز منضم می‌شود یا منطقاً با آنها مرتبط است.
- ❖ این امضاء رابطه امضاء کننده را با داده‌هایی که با آن مرتبط است مشخص می‌کند.

با عنایت به مطالب فوق‌الذکر می‌توان گفت که در قالب نظام‌ها و متون حقوقی کارکردهای ذیل برای امضای الکترونیکی، به رسمیت شناخته شده است:

- ❖ انتساب به امضاء کننده: با امضای الکترونیکی یک سند، محتوای آن قابل انتساب به شخص امضاء کننده بوده، بنابراین له و یا علیه وی قابلیت استناد را دارد.
- ❖ انجام تشریفات: امضای الکترونیکی یک سند الکترونیکی حاکی از رعایت تمامی تشریفات مقرر قانونی در تنظیم این سند است.
- ❖ داشتن آثار حقوقی: امضای الکترونیکی نیز همانند سایر امضاهای سنتی دارای آثار حقوقی می‌باشد.

همچنین قانون متحدالشکل معاملات الکترونیکی آمریکا (یوتا) نیز تصریح می‌دارد که اگر بر طبق قانون، امضای قراردادی الزامی باشد، این شرط شکلی می‌تواند با وسایل الکترونیکی که منجر به فناوری تولید امضاء هستند، محقق شود، مشروط بر اینکه قصد امضاء محرز باشد. اگر چه قلمرو امضای الکترونیکی وسیع است و اصل بر امکان امضاء اسناد به طریق الکترونیکی است، امّا طبق این قانون، امضای الکترونیکی وصیت‌نامه و قراردادهای امانی، فرزند خواندگی و یا طلاق، رسمیت و اعتبار ندارد.

نکته مهم در قانون یوتا این است که شرکت‌ها و مؤسسات را مجاز ساخته تا با توجه به اوضاع و احوال، تصدیق یا ثبت امضاهای الکترونیکی را شرط پذیرش آن بدانند. اعطای این اختیار به ویژه از لحاظ کاهش مخاطرات تجاری دارای اهمیت فوق‌العاده ای می‌باشد. با توجه به ویژگی‌های تجارت الکترونیکی و جنبه‌های حقوقی آن، امضای الکترونیکی به منظور تسری تجارت الکترونیکی به فراسوی قراردادهای کتبی به رسمیت شناخته شده است.

گفتار پنجم : تفاوت امضاء الکترونیکی و امضاء دستی

برابر ماده ۷ قانون نمونه آنسیترال، امضای الکترونیکی در اسناد و مقررات بین‌المللی دارای همان ارزش و آثار اثباتی است که امضای سنتی دارا می‌باشد. بنابر گزارش کارگروه تجارت الکترونیکی آنسیترال، با امضای الکترونیکی نیز اصالت سند و انتساب آن به امضاء کننده اثبات و وی متعهد به محتوای سند خواهد بود.

همچنین بنابر ماده ۳ قانون نمونه آنسیترال مصوب ۲۰۰۱ میلادی، در صورت داشتن شرایط ایمنی به هیچ‌وجه نمی‌توان میان فناوری‌های گوناگون ایجاد امضاء تفاوت قایل شد و تمام آنها معتبر و دارای آثار حقوقی یکسان خواهند بود. شناسایی اصل «کارکرد یکسان» در این ماده از آن جهت دارای اهمیت است که هیچ تردیدی در عدم امکان تبعیض میان امضای دستی (مکتوب) و امضای الکترونیکی باقی نمی‌گذارد. تعریف سنتی ارائه شده از امضاء وجود یک نوشته را ضروری می‌داند. همانطوری‌که قانون مدنی ایران در ماده ۱۳۰۱ بدون تعریف امضاء مقرر می‌دارد: « امضایی که روی نوشته یا سندی باشد بر ضرر امضاء کننده دلیل است » اگر چه نام «امضاء» برای هر دو نوع امضای دستی (سنتی) و الکترونیکی به کار می‌رود، اما در تفاوت ماهوی این دو نباید تردید کرد، امضای دستی نشان می‌دهد که شخصی آن سند را تنفیذ نموده، حال آنکه امضای الکترونیکی (دیجیتال) دلیل تصدیق بکارگیری کلید خصوصی متعلق به فرد معین برای رمزگذاری آن است. در حقیقت بدون وجود سابقه ثبتی مربوطه،

امضای الکترونیکی دلالتی بر دخالت یک فرد در محتوای سندی که امضاء در آن به کار گرفته شده، ندارد. بهرحال موارد ذیل را می‌توان به عنوان تفاوت‌های خاص امضاهای دستی و الکترونیکی برشمرد:

الف) امضای یک شخص در فرم دستی (سنتی) معمولاً برای تمام مدارک معمولاً یکسان است ولی در امضای الکترونیکی، برای تولید امضاء از اطلاعاتی که به طور منحصر به فرد در اختیار امضاء کننده است استفاده می‌شود، بنابراین ممکن است با صدور گواهی‌های مختلف، امضاهای متفاوتی نیز در روابط تجاری گوناگون درج گردد.

ب) در روش امضای دستی، امضاء به راحتی توسط خود فرد تولید می‌شود ولی در روش الکترونیکی، امضای افراد به طور خودکار و توسط رایانه تولید می‌گردند.

ج) در روش امضای دستی، امضاء شخص یا اشخاص به راحتی تمییز داده می‌شوند ولی در امضای الکترونیکی، امضاء هر پیام وابسته به کلیه بیت‌های پیام است و هر گونه دست کاری و تغییر در متن سند موجب مخدوش شدن امضاء پیام می‌گردد.

د) تصدیق و صحت امضاء دستی، در نظام سنتی ثبت اسناد از جمله وظایفی است که بر عهده مسئولین دفاتر اسناد رسمی نهاده شده است (بند ۳ ماده ۴۹ قانون ثبت) و در قانون دفاتر اسناد رسمی و کانون سر دفتران و دفتر یاران، دفتری به نام «دفتر گواهی امضاء» پیش‌بینی شده که بنابر ماده ۲۰ قانون ثبت «دفتری است که منحصراً مخصوص تصدیق امضاء ذیل نوشته‌های عادی است و نوشته تصدیق امضاء شده با توجه به ماده ۳۷۵ قانون آئین دادرسی مدنی مسلم الصدور شناخته می‌شود »، در صورتی که در خصوص امضای الکترونیکی طبق باب دوم قانون تجارت الکترونیکی ایران این وظیفه توسط « دفاتر خدمات صدور گواهی الکترونیکی» موضوع مواد ۳۱و ۳۲ قانون اخیرالذکر، انجام می‌پذیرد.

قانون تجارت الکترونیکی ایران فاقد ضابطه کلی برای همسانی دلیل الکترونیکی با دلایل غیرالکترونیکی است، علاوه بر این، قانون مذکور برابری نوشته و امضاء الکترونیک با نوشته و امضای دستی (سنتی) را نیز مشروط به شرایط خاص ننموده و به صرف بیان قاعده برابری آنها اکتفا می‌کند، امری که اطلاق آن به لحاظ عدم برابری منطقی داده پیام غیر مطمئن با نوشته و امضاء دستی قابل انتقاد به نظر می‌رسد.

شاید به جهت جبران همین نقیصه باشد که ماده ۱۴ قانون تجارت الکترونیکی اعلام می‌نماید: «کلیه داده پیام‌هایی که به طریق مطمئن ایجاد و نگهداری شده‌اند از حیث محتویات و امضای مندرج در آن، تعهدات یا طرفی که تعهد کرده و کلیه اشخاصی که قائم‌مقام قانونی آنان

محسوب می‌شوند اجرای مفاد آن و سایر آثار در حکم اسناد معتبر و قابل استناد در مراجع قضایی و حقوقی است» در ماده ۱۵ همین قانون، نیز نسبت به داده پیام مطمئن، سوابق الکترونیکی مطمئن و امضای الکترونیکی مطمئن، انکار و تردید مسموع دانسته نشده است.

گفتار ششم : تفاوت امضاء دیجیتال و امضاء الکترونیکی

گرچه در بیشتر متون، امضاء الکترونیکی و امضای دیجیتالی، مترادف دانسته شده‌اند ولی از جنبه علمی در تمایز این دو به اختصار می‌توان گفت که امضای دیجیتالی نمودار داده‌ای است که به شکل یک واحد داده، الصاق یا با رمزگذاری منتقل می‌شود به گیرنده اجازه می‌دهد تا سرمنشأ و اصالت آن را تشخیص دهد، این ساختار منطقی مانع از جعل امضاء می‌شود، در حالی که امضای الکترونیکی دارای معنای گسترده‌تری است و شامل امضای دستی و اسکن شده یا اسم شخص که در قسمت انتهای نامه الکترونیکی قید می‌گردد، نیز می‌شود. در واقع امضای دیجیتالی نوعی امضای الکترونیکی است که شامل یک رشته داده‌های کدهای ریاضی مختص شخص معین است که ارسال کننده مدارک الکترونیکی محسوب است، امضای دیجیتال به کمک برنامه تغییرات ریاضی به شکل رمز است و محتوای پیام و هویّت امضاء کننده را تصدیق می‌کند. در ارتباط با امضای دیجیتالی به کلمه‌هایی مثل کلید، حلقه کلید، اثر انگشت و گواهینامه کلید بر می‌خوریم، که می‌توان بطور مختصر بشرح ذیل عنوان نمود:

کلید : کلیدها برای ایجاد امضای دیجیتالی استفاده می‌شوند هر امضای دیجیتالی یک کلید عمومی[۳۸] و یک کلید خصوصی[۳۹] دارد.[۴۰]

کلید خصوصی : یک رمز حفاظت شده می‌باشد و نمی‌بایست آن را در اختیار دیگران قرار داد. اما امکان استفاده از کلید عمومی برای دیگران وجود دارد تا آنها با استفاده از آن بتوانند امضاء را بررسی کنند و متوجه درستی آن بشوند.

حلقه کلید :[۴۱] مجموعه‌ای از کلیدهای عمومی است که توسط دیگران ارسال می شود تا امکان بررسی امضاء آنها فراهم گردد.

گواهینامه کلید :[۴۲] عبارت است از اطلاعات متفاوت مانند نام صاحب کلید، تاریخ درست کردن و اعتبار کلید که موقع انتخاب یک کلید از میان حلقه کلید بررسی می‌شود. گفته شده است:[۴۳] امضای دیجیتالی یک مکانیزم امنیتی است که در اینترنت مورد استفاده قرار می‌گیرد و به دو کلید متکی است، یک کلید عمومی و یک کلید خصوصی. از این کلیدها برای رمزگذاری پیام هنگام انتقال و رمزگشایی آن‌ها در محل دریافت استفاده می‌شود. با توجه به

تعریف مذکور بحث رمزگذاری و رمزگشایی در امضای دیجیتالی مطرح است نه امضاء الکترونیکی که توسط یک طرف برای متعهد شدن و یا انتساب یک مدرک استفاده می‌شود. قلمرو این اصطلاح در حدی وسیع است که می‌تواند هر علامتی که تصویر دیجیتال شده یک امضاء کاغذی باشد را در برگیرد، مانند یک اسم درج شده در زیر یک سند الکترونیکی یا حتی آدرس قید شده در بالا و پائین نامه الکترونیکی. امضاء الکترونیکی هیچ گونه تضمینی بیشتر از یک رمز عبور ارایه نمی‌دهد و در صورتی که در سند تغییری حاصل شده باشد، این تغییر را نشان نمی‌دهد یعنی هیچ‌گونه ساماندهی برای تصدیق اسناد ندارد. ولی امضای دیجیتالی همان‌طور که ذکر شد، نوع خاصی از امضاء الکترونیکی است و از سایر انواع امضاهای الکترونیکی بیشتر قابل قبول و اطمینان است به طوری که هم به سند هم به امضاء کننده، قابلیت تصدیق را اعطاء می‌نماید. تصدیق امضاء کننده قابلیت شناسایی شخصی است که به صورت دیجیتالی سند را امضاء نموده است. تصدیق سند اطمینان حاصل می‌نماید که آن سند یا معامله (یا امضاء) نمی‌تواند به راحتی تغییر کند.[۴۴]

امضای دیجیتال، یک فرایند رمزنگاری[۴۵] است و به معنای رمز کردن پیام، با کلید خصوصی و رمزگشایی آن با کلید عمومی است. در این روش، طرفین بجای در اختیار داشتن یک کلید مشترک، هر کدام یک جفت کلید دارند. این جفت کلیدها که کلید عمومی و کلید خصوصی، نامیده می‌شوند، با یک دیگر قرینه و جفت هستند. کلید عمومی، سرّی نبوده و می‌تواند در اختیار همه مردم از جمله طرف معامله قرار گیرد، اما کلید خصوصی کاملاً محرمانه و تنها در اختیار مالک آن می‌باشد، از آنجا که کلید خصوصی از کلید عمومی قابل استنباط نیست، می‌توان از یک کلید برای رمز نگاری و از کلید دیگر، برای رمزگشایی استفاده کرد.

در مفهوم نیز امضای دیجیتالی در واقع یک کلید خصوصی رمز شده براساس پیام خلاصه شده است در سمت گیرنده نیز با استفاده از کلید عمومی امضاء دیجیتالی را رمزگشایی و صحت آن را مورد تأئید قرار می‌دهند. برای مثال دو کاربر «الف» و «ب» هر کدام یک جفت کلید دارند، طرفین با تبادل اطلاعات یا توسط شخص ثالث، کلید عمومی یکدیگر را در اختیار می‌گیرند، حال اگر کلید عمومی «الف» آن را به صورت رمز درآورده، پیام رمز شده را به مقصد «ب» ارسال می‌کند. از آنجا که «ب» تنها شخصی است که کلید قرینه کلید عمومی خود را داراست، می‌توان و البته تنها او می‌تواند رمز را بازگشایی کرده، پیام را بخواند. حال «ب» نیز می تواند پاسخ خود را با استفاده از کلید عمومی «الف» رمز گذاری و ارسال نماید تا «الف» آن را با کلید خصوصی خود بگشاید.[۴۶]

این امضاء شاخه ای از ریاضی کاربردی است که ابتدا، پیام را به اشکال نامفهوم تبدیل و سپس آن را به شکلی که قابل فهم باشد، در می آورد. بدیهی است که کلیدهای عمومی و خصوصی بکار گرفته شده در این نوع از امضاء فیزیکی نبوده، بلکه به صورت اعداد می‌باشند که در فرایند خاصی، ایجاد می‌شوند.

از لحاظ تخصصی به فرایندی که طی آن، نرم افزارها و سخت افزارهای رایانه ای، با استفاده از این دو نوع کلید، مبادرت به رمز نگاری و رمز گشایی می‌کنند، «رمز نگاری نامتقارن» یا رمز نگاری کلید عمومی[۴۷] گفته می‌شود.

قانون نمونه امضاء الکترونیکی آنستیرال در تفاوت بین امضاء الکترونیکی و دیجیتالی تأکید کرده است که امضای الکترونیکی براساس رمزنویسی کلید عمومی بنا شده است، اما وسایل دیگری نیز وجود دارد که در مفهوم موسّع امضاء الکترونیکی قرار می‌گیرند که می‌تواند کارکردهای امضاء دستی را برآورده سازد. برای مثال بعضی از تکنیک‌ها که برای تصدیق از ابزار بیومتریک[۴۸] استفاده می‌نمایند، بر مبنای امضاء دستی بنا شده‌اند، در این نوع دستگاه‌ها، امضاء کننده، به صورت دستی با استفاده از خودکار مخصوص بر روی صفحه نمایش رایانه و یا صفحه دیجیتالی امضاء می‌نماید، امضاء دستی توسط رایانه پردازش شده[۴۹] و به صورت مقدارهای عددی ذخیره می‌گردد که می‌تواند به داده پیام اضافه و سپس در رویه شناسایی طرف مقابل نمایش داده شود. در این روش از قبل نمونه امضاء از طرف گرفته و ذخیره گردیده و توسط دستگاه‌های بیومتریک پردازش گردیده است. تکنیک‌های دیگری نیز وجود دارد که استفاده از شماره شناسایی شخص یا (PIN)، نسخه دیجیتالی شده امضاء و یا کلیک کردن روی دکمه OK می‌باشد. در واقع می‌توان فرق امضای الکترونیکی و دیجیتالی را از لحاظ ضریب اطمینان دانست که در امضای الکترونیکی امکان جعل و سوء استفاده بیشتر ولی در امضای دیجیتالی این امکان کمتر است. بدیهی است که به لحاظ وسیع بودن مفهوم امضای الکترونیکی احکام آن در امضای دیجیتالی نیز جاری است.

گفتار هفتم : انواع امضاء الکترونیکی

برای ایجاد یک امضای الکترونیکی، ابتدا باید امضاء کننده از طریق کلید عمومی، امضای خود را رمزسازی کرده و سپس آنرا ضمیمه داده پیام کرده و برای مخاطب خویش ارسال نماید، مخاطب که اکنون داده پیام را به همراه امضای دیجیتالی منضم شده به آن دریافت کرده، باید امضای رمزنگاری شده را که قابل فهم نیست از داده پیام‌ها جدا ساخته و از طریق کلید عمومی

ارسال کننده «که در فهرست عمومی مرجع گواهی امضاء موجود است» پیام را برای وی ارسال می‌کند تا خود ارسال کننده (اصل ساز)[۵۰] با کلید خصوصی‌اش آن را رمزگشایی کند، در صورت مطابقت بین این دو، یعنی همان چیزی که امضاء کننده به عنوان امضای الکترونیکی دیجیتالی برای خود تعریف کرده بود آشکار شد، آنگاه معلوم و مشخص می‌شود که: اولاً: امضای مورد نظر به نحو صحیحی از طرف امضاء کننده ارسال شده است.ثانیاً: امضاء کننده نمی‌تواند ادعا کند که پیام را امضاء نکرده و یا اینکه پیام تغییر یافته است. پس از مقدمه فوق، در این قسمت به بیان اقسام امضاء الکترونیکی می‌پردازیم:

۱ – امضای ساده

همانطوری که ذکر گردید این امضاء در بند ی ماده ۲ ق.ت.ا.ا پیش‌بینی شده است.[۵۱] بنابراین هر گونه داده الکترونیکی که به پیامی ملحق شود یا منطقاً با آن مرتبط باشد و رابطه امضاء کننده را با داده‌هایی که با آن مرتبط است مشخص کند، امضای الکترونیکی ساده نامیده می شود، همین که این شرایط تحقق یافت امضای الکترونیکی انجام شده است، اما اگر شرایطی که در مورد امضای الکترونیکی مطمئن وجود دارد که در بحث بعدی به آن پرداخته می‌شود، وجود داشته باشد در آن صورت از آنجا که سطح بالاتری از امنیت ایجاد شده است با امضای الکترونیکی مطمئن مواجه هستیم، بنابراین هر گونه امضای الکترونیکی که شرایط عمومی امضاء را دارا باشد و فاقد شرایط ذکر شده در خصوص امضای الکترونیکی مطمئن باشد، امضای الکترونیکی ساده تلقی خواهد شد.

بر این اساس از جمله تفاوت‌هایی که میان امضای الکترونیکی ساده و مطمئن وجود دارد مربوط به حفظ تمامیت داده پیام است، به این صورت که اصولاً امضای الکترونیکی مطمئن، برخلاف امضاء ساده، هر گونه تغییر بعدی در پیام را قابل کشف می‌سازد، ضمن اینکه از آنجا که امضای عادی علی‌الاصول از طریق وسایلی تولید می‌شود که در کنترل انحصاری امضاء کننده نیست، انتساب سند به امضاء کننده در معرض تردید بیشتری است.

تفاوت عمده ای که در امضای الکترونیکی ساده و مطمئن وجود دارد، وجود کلیدهای عمومی و اختصاصی در فرآیند امضاهاست، همین امر موجب شباهت امضای الکترونیکی مطمئن با امضای دیجیتال است، در امضاهای الکترونیکی ساده، فرآیندی با عنوان رمزنگاری وجود ندارد، امضای الکترونیکی در نوع معمولی خود روش بسیار ساده‌ای از وارد کردن متون و یا اشکالی خاص به درون دستگاه الکترونیکی است، هر شخصی می‌تواند بدون اتکاء به حضور شخص

ثالثی در تولید و استفاده از امضای الکترونیکی ساده آن را تولید و در اسناد الکترونیکی خود از آن استفاده نماید، البته طبق ماده ۱۲۸۷ قانون مدنی ایران در این مورد قطعاً نمی‌توان گفت اسنادی که بدین شکل تولید شده‌اند، اسناد رسمی و معتبر می‌باشند.

لازم به ذکر است برای اینکه این امضاها ارزش حقوقی به اسناد ببخشند، نیازمند شرایطی خاصی هستند که یکی از آن شرایط حضور یک مرجع ثالث در کنترل آنهاست که همانند یک دفتر اسناد رسمی عمل می کند، در اسناد تجاری که همواره از اهمیت ویژه‌ای برخوردارند، وجود یک امضای الکترونیکی ساده یا عادی قابل استناد نیست اما به هر حال تکنولوژی همواره به دنبال راهکارهایی است تا با کاستن از پیچیدگی‌ها و تشریفات امضاهای الکترونیکی پیشرفته، امضاهای ساده‌ای تولید کند که قابلیت حقوقی نیز دارا باشند.

۲ – امضاء مطمئن

امضای الکترونیکی مطمئن در بند ک ماده ۲ ق.ت.ا.ا پیش‌بینی شده است.[۵۲] امضای مطمئن، امضایی است که درجه بالایی از اطمینان را فراهم می‌سازد که امضاء متعلق به شخص مورد نظر است و در جریان انتقال نیز، پیام تغییری نیافته است. برای حصول این امر، امضاء باید شرایطی داشته باشد که ماده ۱۰ ق.ت.ا.ا آن را بدین شرح پیش‌بینی کرده است امضای الکترونیکی مطمئن باید دارای شرایط زیر باشد:

الف – نسبت به امضاء کننده منحصر به فرد باشد. ب – هویّت امضاء کننده «داده پیام» را معلوم نماید.ج – به وسیله امضاء کننده و یا تحت اراده انحصاری وی صادر شده باشد.د – به نحوی به یک «داده پیام» متصل شود که هر تغییری در آن «داده پیام» قابل تشخیص و کشف باشد[۵۳] بند ۳ ماده ۹ عهدنامه ۲۰۰۵ سازمان ملل متحد درباره استفاده از ارتباطات الکترونیکی در قراردادهای بین‌المللی، به منظور تحقق شرایط قانونی امضاء از طریق ارتباط الکترونیکی، اظهار می دارد: در مواردی که قانون مقرر می دارد ارتباط یا قرارداد باید توسط شخصی امضاء شود یا آثار فقدان امضاء را بیان می کند، این شرط از طریق ارتباط الکترونیکی محقق می شود، اگر:

الف) ارتباط الکترونیکی، متضمن روشی باشد که برای تعیین هویت طرف و معلوم کردن قصد او در خصوص اطلاعات، بکار می رود؛ و ب) روشی که بکار گرفته شده، یا ۱ – برای هدفی که ارتباط الکترونیکی، برای آن، تولید یا اعلام شده از حیث جمیع شرایط، از جمله هر گونه توافق

مربوطه، مطمئن و مناسب باشد؛ یا ۲ – در عمل ثابت شده باشد که کارکرد های موصوف در بند (الف) فوق را به تنهایی یا به همراه دلیل دیگر، داراست.[۵۴]

با استفاده از امضای الکترونیکی مطمئن، تمامیّت سند، محرمانه بودن اطلاعات و امنیّت داده‌ها، تضمین می‌شود، اما شناسایی هویّت امضاء کننده، یکی دیگر از مسائل مهم مطرح در باب امضاهای الکترونیکی است. در واقع، به لحاظ حقوقی مهم ترین اثر امضا، اثبات رابطه ی سند با کسی است که امضاء به او نسبت داده شده است. امضای الکترونیکی مطمئن، به تنهایی نمی‌تواند، هویّت امضاء کننده را تضمین کند، در فرضی که طرفین رابطه قراردادی شرکت‌های بزرگی هستند که به لحاظ سابقه مراودات تجاری و یا شهرت در عرصه بین‌المللی به خوبی یکدیگر را می‌شناسند، این مشکل کمتر بروز می‌کند. زیرا طرفین از توانائی‌های مالی و انسانی یکدیگر آگاهند. در این‌گونه موارد، صرف مبادله داده های رمزنگاری شده برای اثبات وجود رابطه حقوقی و محتوای آن، کفایت می‌کند. همچنین، در مواردی که طرفین مبادله الکترونیکی، پیش از ورود به محیط الکترونیکی، در خصوص چگونگی انجام معاملات خویش توافق می‌کنند و هویّت هر یک از طرفین برای دیگری، آشکار است، مشکل تعیین هویّت، اساساً فرصت بروز نمی‌یابد. برای نمونه در عملیات بانکی از طریق کارت‌های الکترونیکی بانکی، معمولاً مشتری با حضور در بانک، ضمن ارائه مدارک لازم برای تعیین هویّت، قراردادی را که بانک در خصوص چگونگی استفاده از کارت بانکی و مسائل حقوقی مرتبط با آن، تهیه کرده است، امضاء می‌کند. ولی مشکل تعیین هویّت در مواردی که طرفین از پیش، در خصوص تکالیف خود، توافقی نکرده‌اند و یا به هر نحو یکدیگر را نمی شناسند همچنان باقی است. برای نمونه در معاملات انجام شده از طریق شبکه جهانی اینترنت که در یک طرف آن، تاجران، شرکت‌ها و مؤسسه‌های تجاری و خدماتی و در طرف دیگر به طور عمده، مصرف کنندگان قراردارند، تعیین و تضمین هویت امضاکنندگان، ضرورت دارد. بدین لحاظ یکی از موضوعات اصلی مطرح شده در مقررات ملی و یا مقررات حاکم بر سازمانهای تجاری بین‌المللی، این است که مرجع ثالثی، اعتبار ارتباط الکترونیکی را از طریق تعیین هویت امضاء کننده ی الکترونیکی، تضمین کند، این مرجع، در اصطلاح، «دفاتر خدمات صدور گواهی الکترونیکی» یا «دفاتر خدمات الکترونیکی» یا «مراجع گواهی»، نامیده می‌شوند، عملکرد این دفترها با عملکرد دفاتر اسناد رسمی در محیط نوشته‌ها و اسناد کاغذی قابل مقایسه است. به بیان دیگر، همان‌گونه که دفاتر اسناد رسمی با احراز هویت امضاکنندگان سند و گذراندن تشریفات قانونی، به نوشته، سندیت و رسمیت می‌بخشند، دفاتر گواهی الکترونیکی، نیز هویت امضاء کننده را تضمین کرده

و در نتیجه، به اطلاعات و ارتباطات الکترونیکی، سندیت می‌دهند. در واقع، گواهی الکترونیکی‌ای که این دفاتر، صادر می‌کنند، هویت امضاء کننده را از طریق ارتباط میان کلید عمومی و دارنده کلید خصوصی مربوطه، تضمین می‌کند. به بیان دقیق تر، امضای الکترونیکی، دارای دو جزء متفاوت ولی از نظر ریاضی، مرتبط است؛ کلید خصوصی که در اختیار صاحب امضاست و کلید عمومی که در فهرست مرجع گواهی قراردارد. این مرجع، تضمین می‌کند که کلید عمومی مستقر در فهرست، به درستی اعلام و ایجاد شده است، زیرا هویت دارنده کلید خصوصی که با کلید عمومی، منطبق است، نزد مرجع گواهی وجود دارد، به عبارت دیگر برای اطمینان از صدور ارتباط از سوی کسی که ادعا می‌کند، وجود کلید عمومی، ضروری است. در واقع، مرجع گواهی، دو وظیفه مهم دارد: نخست، اختصاص دادن کلید خصوصی به دارنده و ثبت آن به منزله یک مستند اطلاعاتی و دوم، نگهداری کلید مکمل آن به نام کلید عمومی و در دسترس قراردادن فهرست نام دارندگان کلید عمومی از طریق سیستم درون خطی و بانک‌های اطلاعاتی ویژه. به نظر می رسد که گواهی یاد شده برای معتبر شناخته شدن، باید متضمن موارد دیگری از قبیل هویت خود مرجع گواهی و یا مدت اعتبار گواهی باشد.

صرف نظر از اینکه برای احراز اینکه روش بکار گرفته شده، مطمئن و مناسب بوده یا خیر، عواملی چون: پیشرفته بودن تجهیزات بکار گرفته شده توسط طرفین، ماهیت فعالیت تجاری طرفین، کثرت فعالیت های تجاری که طرفین با یکدیگر دارند، رعایت شرایط قانونی مربوط به امضاء، نوع و میزان معامله، قابلیت نظام های ارتباطی، انجام تشریفات مربوط به تأئید و تصدیق که توسط واسطه ها تعریف شده است، حدود تشریفات تأیید که توسط واسطه ها، در دسترس قرار گرفته‌اند[۵۵] می‌توانند مورد توجه قرار گیرند، ذکر این نکته ضروری است، که در تشخیص مطمئن بودن روش بکار گرفته شده برای امضاء، دو حالت قابل تصور است: در حالت نخست، طرفین هیچ‌گونه ارتباطی از قبل با یکدیگر ند، بدیهی است که در این موارد احراز مطمئن بودن روش مورد استفاده، با توجه به دیگر عوامل خواهد بود. اما اگر طرفین، از قبل با یکدیگر ارتباط داشته باشند: دو حال را باید از یکدیگر تفکیک نمود: در حالت اول، طرفین بر استفاده از یک روش امضای مطمئن، با یکدیگر به توافق می‌رسند، در این حالت، توجه به روش توافق شده، جهت احراز اطمینان، یکی ازمعیارها خواهد بود اما معیار انحصاری نمی‌باشد. به بیان دیگر، اگر طرفین، در خصوص روشی که برای امضای مطمئن بکار گرفته می‌شود، به توافق برسند، توجه به این روش، تنها دلیل تشخیص این امر که آیا روش مورد استفاده، مطمئن هست یا خیر، نمی‌باشد؛ لذا روش توافقی لزوماً، روش مطمئن نخواهد بود. اما در حالت دوم، هرچند طرفین از

پیش نیز با یکدیگر در ارتباط بوده‌اند، اما در خصوص روش امضاء، به توافق نرسیده و یا اصلاً، صحبتی در این خصوص، بین طرفین، رد و بدل نشده است، در این حالت، احراز مطمئن بودن، براساس عوامل فوق الذکر صورت خواهد پذیرفت. در واقع در حالت اخیر، بین وضعیتی که طرفین، از قبل با یکدیگر ارتباط داشته و وضعیتی که طرفین، هیچگونه ارتباطی با یکدیگر نداشته‌اند، تفاوتی قائل نشده است.(۵۶)

نکته دیگر آنکه، توافق میان اصل ساز و مخاطب ارتباط الکترونیکی، باید به گونه ای تفسیر شود که نه تنها توافقات دو یا چند جانبه که میان طرفین به طور مستقیم، صورت گرفته را پوشش دهد، بلکه توافقاتی که از طریق واسطه‌ها، همچون شبکه های رایانه‌ای، برای مثال، توافق مربوط به ارائه خدمات توسط شخص ثالث را نیز در برگیرد، مگر اینکه توافق طرفین متضمن شمول انحصاری آن بر روابط آنها، از جمله در مقام تعیین مطمئن بودن روش مورد بحث باشد. لازم به ذکر است که در ماده ۷ ق. ت.ا.ا، قبل از بیان شرایط لازم برای یک امضای الکترونیکی مطمئن در حکمی مشابه با بند۳ ماده ۹ عهد نامه ۲۰۰۵، مقرر شده است «هرگاه قانون وجود امضاء را لازم بداند امضای الکترونیکی مکفی است.»

مفاد ماده ۷ فوق الذکر با توجه به آنچه در ماده ۱۰ این قانون در خصوص شرایط لازم برای امضاء الکترونیکی مطمئن، نشان دهنده این نکته است که قانون‌گذار با اشاره به عبارت مطلق «امضای الکترونیکی»، مبادرت به بیان این قاعده نموده است که در مواردی که قانون، امضاء را الزامی بدارد، امضای الکترونیکی، مکفی است و به بیان بهتر، این الزام از طریق امضایی که در محیط الکترونیکی صورت پذیرفته، یک امضای ساده الکترونیکی، محسوب می‌شود و طبیعی است که چنین امضائی ممکن است شرایط مذکور در ماده ۱۰ این قانون را نداشته و طبعاً امضای الکترونیکی مطمئن، محسوب نگردد، در این صورت این سوال مطرح می‌گردد که آیا باز هم این امضاء، کارکردی همسان امضای دستی در محیط واقعی دارد؟ روشن است که پاسخ منفی است. امّا، اطلاق امضای الکترونیکی مندرج در ماده ۷، این فرض را تقویت می‌کند که به صرف امضای الکترونیکی ساده نیز این الزام قانونی محقق می شود؛ در حالی که خود قانون‌گذار با بیان شرایط و خصایص یک امضای الکترونیکی مطمئن، در ماده ۱۰، این هدف را دنبال می‌کرده است که نشان دهد، تنها با امضای الکترونیکی مطمئن، است که این نیاز قانونی برآورده می‌گردد، بنابراین می‌توان نتیجه گرفت بنا به اطلاق ماده ۷ ق.ت.ا.ا امضاء الکترونیکی مکفی می‌تواند امضایی ساده و یا امضایی مطمئن باشد. همچنین ق.ت.ا.ا، در خصوص ارزش اثباتی امضای الکترونیکی، متضمن مطالبی است که در قانون نمونه آنسیترال و عهد نامه

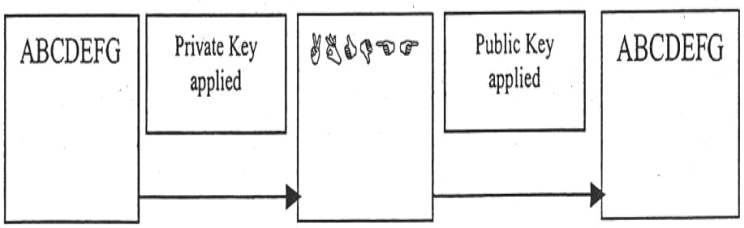
۲۰۰۵، راجع به آن مقرره ای وجود ندارد. به موجب ماده ۱۵ ق.ت.ا.ا «نسبت به "داده پیام" مطمئن، سوابق الکترونیکی مطمئن و امضای الکترونیکی مطئمن انکار و تردید مسموع نیست و تنها می‌توان ادعا جعلیت به "داده پیام" مزبور وارد و یا ثابت نمود"داده پیام" مزبور به جهتی از جهات قانونی از اعتبار افتاده است.» در واقع در این قسمت قانون‌گذار با توجه به آنچه در خصوص ارزش اثباتی سند عادی در برابر سند رسمی، در مقررات ملی آمده است قائل به تمایز بین ارزش اثباتی داده پیام یا امضاء ساده از یک سو و داده پیام یا امضاء مطمئن از سوی دیگر شده است. درخصوص ماده ۱۵ ق.ت.ا.ا از لحاظ تلقی سوابق الکترونیکی و امضاء الکترونیکی مطمئن، در حکم اسناد رسمی برخی گفته‌اند که سند الکترونیکی در صورتی که نوع رسمی آن مد نظر باشد باید سه شرط اصلی سند رسمی یعنی تنظیم توسط مأمور صالح، در حدود صلاحیت او و تنظیم مطابق مقررات، در آن محقق گردد. درغیر اینصورت سند تولید یا امضاء شده با وسائط الکترونیکی را به هیچ‌وجه نمی‌توان رسمی محسوب داشت. همین اثر خود بیانگر آن است که نمی‌توان صرف اطلاق عنوان سند رسمی یا در حکم سند رسمی به یک مدرک را موجب رسمی تلقی شدن آن محسوب داشت. تسری آثار حقوقی امضای الکترونیکی که ماهیتاً می‌تواند مجزای از متن بوده یا تنها برای امضای قسمتی از متن بکار رود، در مورد تمام متن صحیح نمی باشد مگر اینکه دفتر اسناد رسمی، اصالت امضای الکترونیکی و شمول آن را بر تمام متن تصدیق نماید.[۵۷]

در پاسخ به نظر فوق گفته شده است که هرچند در روند شکل گیری داده پیام مطمئن همانند روند تنظیم اسناد رسمی کاغذی مأمور رسمی حکومت یعنی دفاتر خدمات صدور گواهی الکترونیکی دخالت دارند ولی دایره وظایف و اختیارات مأمور رسمی که در تنظیم سند رسمی کاغذی دخالت دارد بسیار وسیع تر از دفاتر خدمات صدور گواهی الکترونیکی است، مهمترین وظیفه دفاتر این است که با صدور گواهی، هویّت طرفین معامله را تأیید می‌کنند و اساساً وظیفه یا اختیاری در زمینه کنترل شرایط قانونی لازم برای انعقاد قرارداد ندارند. درحالی‌که مأمور رسمی که در تنظیم سند رسمی کاغذی دخالت دارد نه تنها هویّت و تمامیت سند را به عنوان مأمور ممتاز و ویژه حکومت تأیید می‌کند بلکه شرایط قانونی لازم برای تنظیم سند رسمی همانند اهلیت، ایجاب و قبول و احیاناً پرداخت عوض و تحویل کالا یا مبیع را فراهم می‌کند.[۵۸] برابر آنچه که گفته شد بنظر می‌رسد عبارت مندرج در ماده ۱۵ ق.ت.ا.ا از حیث عدم امکان انکار یا تردید نسبت به سوابق الکترونیکی و امضاء الکترونیکی مطمئن، موجب نمی‌شود که آن را از تمامی اوصاف و خصوصیات اسناد رسمی برخوردار بدانیم، بعبارت دیگر

تصدیق و تأیید صحت امضاء و انتساب آن به ارسال کننده داده پیام، اصولاً نمی‌تواند به معنای سند رسمی محسوب شدن متن داده پیام، مشابه اسناد رسمی تنظیمی در دفاتر اسناد رسمی گردد. بررسی قوانین راجع به ارتباطات الکترونیکی دیگر کشورها، گویای آنست که در خصوص ارزش اثباتی امضاهای الکترونیکی، قواعدی مطرح شده است. برای مثال، دستورالعمل اتحادیه اروپا، در ماده ۵، با عنوان، «آثار حقوقی امضای الکترونیکی» دولت‌های عضو را مکلف ساخته است تا (۱) برای امضای الکترونیکی پیشرفته، همان آثاری را قائل شوند که برای امضای دستی قائل هستند و (۲) امضای الکترونیکی را به عنوان دلیل، در دادگاه بپذیرند. قانون مدنی فرانسه نیز در بند ۱ ماده ۱۳۱۶، بیان داشته است که نوشته الکترونیکی، همانند نوشته کاغذی، به عنوان دلیل در دادگاه پذیرفته می‌شود؛ البته مشروط بر آنکه، هویت امضاءکننده را تعیین و تمامیت آن را تضمین نماید.[۵۹]

۳ – روشهای ایجاد امضاء الکترونیکی مطمئن

امضای الکترونیکی توسط علم رمزگذاری[۶۰] بوجود آمده است، علم رمزگذاری علمی است که با استفاده از ریاضیات و روش‌های سخت‌افزاری و نرم‌افزاری، پیامی را به یک متن بی معنی تبدیل می‌نماید و گیرنده دوباره با همان الگوریتم این متن بی معنی را به پیام مورد نظر خویش باز می‌گرداند. امضای الکترونیکی از نوع خاصی از علم رمزگذاری استفاده می‌کند و دو الگوریتم متفاوت که هر دو مشتق از روش‌های ریاضی هستند را به کار می‌برد، یکی از الگوریتم‌ها برای ایجاد امضای الکترونیکی و تبدیل آن به یک متن بی معنی یا به عبارتی دیگر برای کد گذاری امضاء و دیگری برای حصول اطمینان از صحیح بودن امضاء و تبدیل پیام به شکل اولیه به کار می‌رود، به این نوع الگوریتم[۶۱] به اصطلاح کلید گفته می‌شود. الگوریتم اول مخصوص شخص امضاء کننده بوده و کلید خصوصی نامیده می‌شود و دومی حالت عمومی داشته و برای حصول اطمینان از صحت امضاء به کار می‌رود و به آن کلید عمومی گفته می‌شود، چون همه افراد باید از درستی امضای شخص مورد نظر اطمینان یابند، کلید عمومی باید در اختیار همه افراد قرار گیرد.[۶۲]



در تعریف رمزگذاری به عبارتی می‌توان گفت فرایند کدگذاری داده‌ها جهت جلوگیری از دستیابی غیر مجاز، به ویژه در طی انتقال رمزگذاری معمولاً براساس یک یا چند کلید انجام می‌شود که برای رمزگشایی، یا بازگرداندن داده‌ها به فرم نخست، ضروری هستند، اداره ملی استانداردهای ایالات متحده، استاندارد رمزگذاری بسیار پیچیده‌ای به نام Data Encryption Standard) DES استاندارد رمزگذاری داده‌ها) ایجاد نموده که براساس یک متغیر ۵۶ بیتی آماده شده و متجاوز از ۷×۱۰^{۱۵} کلید منحصر به فرد برای رمزگذاری سندها فراهم می‌کنند.(۶۳)

صرف نظر از رمز گذاری، روش دیگر مورد استفاده، تابع هش(۶۴) می‌باشد که در هر دو کلید عمومی و خصوصی بکار می‌رود. هش (Hash) که به اصطلاح «عمل خرد کردن» نامیده می‌شود، (۶۵) نام تابعی است که در موارد بسیار زیادی کاربرد دارد، کار این تابع این است که هر ورودی را که دریافت می‌کند، به وسیله تبدیلی، به یک مقدار عددی می‌نگارد، پس به هر تابعی که این کار را انجام دهد، عنوان هش (Hash) اطلاق می‌شود. این مقدار عددی معمولاً از پیام کوتاهتر بوده و منحصر به آن می‌باشد. هرگونه تغییری که در پیام اتفاق افتد، مقدار عددی متفاوتی را ایجاد می‌نماید.

برای مثال تابع مزبور وقتی که سندی را دریافت می‌کند آن را از همان الگوریتم هش که ما استفاده کرده‌ایم عبور می‌دهد و یک هش جدید می‌سازد در عین حال به کمک کلید عمومی، امضاء را رمزگشایی می‌کند و آن را به هش اولیه‌اش تبدیل می‌کند، سپس هش جدید را با هش اصلی مقایسه می‌کند، اگر آن‌ها همسان باشند می‌توان مطمئن شد که سندی که دریافت شده واقعاً از جانب فرستنده اصلی می‌باشد و کسی در آن دست کاری نکرده است و اگر آن‌ها تطبیق نداشته باشند فهمیده می‌شود که در محتویات سند به نحوی، در حین انتقال دست کاری شده است.(۶۶)

این سیستم دارای چند خصوصیت است که ایمنی حاصل از بکارگیری آن را افزایش می‌دهد. اول آنکه احتمال ایجاد دو خلاصه پیام یکسان از دو متن مختلف، بسیار اندک است؛ بطوری که اختلاف جزئی در متن، موجب اختلاف کلی دو «خلاصه پیام» می‌شود. دوم آنکه عملکرد این سیستم یکطرفه می‌باشد؛ یعنی پیام اصلی قابلیت تبدیل به « خلاصه پیام » را دارد، اما با در اختیار داشتن «خلاصه پیام» نمی‌توان به متن اصلی دست یافت. بنابراین استفاده از دو فرآیند در امضای الکترونیکی ضروری است که یکی توسط امضاء کننده و دیگری توسط گیرنده امضای

الکترونیکی به کار رود، امضاء کننده از یک الگوریتم هش که در امضای موردنظر جوابی واحد دارد، استفاده می‌کند بنابراین در کلید خصوصی از همین الگوریتم استفاده می‌شود.
برای حصول اطمینان از صحت امضای الکترونیکی از یک کلید عمومی استفاده می‌شود که این خروجی، الگورتیم هش را که به گیرنده ارسال شده به شکل امضای معمولی تبدیل می‌کند. برای امضاء کردن یک متن یا هر چیز دیگری ابتدا باید امضاء کننده محدوده صحت امضاء، یعنی اینکه چه چیزی را می‌خواهد امضاء نماید تعیین کند. سپس تابع هش در نرم‌افزار امضاء کننده یک خروجی هش را به امضای الکترونیکی تبدیل می‌کند؛ بنابراین امضای مورد نظر منحصر به فرد خواهد بود. برای رمز گشایی امضای الکترونیکی باید از الگوریتم هش دیگری همانند الگوریتمی که برای ایجاد امضاء به کار رفته استفاده شود، با استفاده از کلید عمومی و یک خروجی هش جدید، معین می گردد که این امضاء توسط کلید خصوصی موردنظر ایجاد شده است یا خیر؟
در واقع سیستم هش قابلیت ترکیب با سیستم رمزنگاری کلید عمومی و سایمتریک را داراست، از آنجا که رمز نگاری یک متن طولانی با استفاده از روش کلید عمومی بسیار کند و وقت‌گیر است، ارسال کننده می‌تواند پیام اصلی را با بکارگیری این سیستم، به متنی کوتاه تبدیل کند و سپس آن را با کلید خصوصی خود بصورت رمز درآورده، همراه با پیام اصلی ارسال دارد. در مقصد، مخاطب با استفاده از کلید عمومی ارسال کننده، رمز پیام را می‌گشاید؛ سپس متن اصلی را نیز تبدیل به « خلاصه پیام » کرده، دو « خلاصه پیام » را با یکدیگر مقایسه می‌کند.

۱ – ۳ – امضای مبتنی بر رمز نگاری متقارن[۶۷]

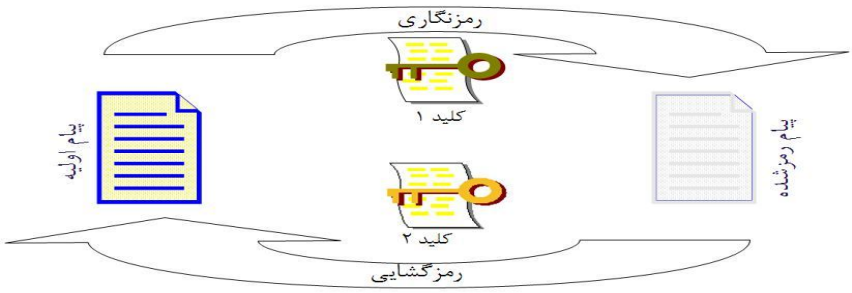
الگوریتم رمزنگاری متقارن که به آن کلید خصوصی و سری نیز گفته می‌شود. عبارت است از الگوریتم‌های رمزنگاری که در آن دو شریک تجاری برای امضاء، رمزنگاری، و رمزگشایی مبادله الکترونیکی داده‌ها باید از کلید واحد و یکسانی استفاده کنند، به عبارتی، چنانچه داده پیام با یک کلید رمزنگاری شده باشد، نمی‌توان آن را با کلید متفاوتی رمزگشایی کرد، استفاده از روش‌های متقارن، کار رمزنگاری را آسان می‌کند و نیازی نیست که هریک از طرفین تجاری الگوریتم محرمانه‌ای تولید و با طرف دیگر مبادله کند، بلکه هر شریک تجاری می‌تواند از همان الگوریتم رمزنگاری استفاده کرده و فقط کلید مشترک محرمانه را مبادله کنند، امنیت این رمزنگاری بستگی به آن دارد که کلید ارسالی تا چه حد امن نگاه داشته شود، طرفین باید در مورد کلید مشترک محرمانه توافق کنند. باید به تعداد روابط تجاری یک شریک تجاری، کلید

محرمانه نگهداری شود، یعنی یک کلید برای هریک از شرکای تجاری، بعلاوه باید متذکر شد که در این روش اصالت منشأ یا مقصد (عدم انکار اصل، تحویل و دریافت) قابل اثبات نمی‌باشد، از آنجا که دو طرف دارای کلید محرمانه رمزنگاری مشترکی هستند، بنابراین هر داده پیام الکترونیکی که با یک کلید رمزنگاری شده باشد، می‌تواند به وسیله هریک از طرفین تجاری فرستاده شده باشد. با استفاده از آنچه که رمزنگاری کلید عمومی نامیده می‌شود و در الگوریتم غیرمتقارن به کارمی‌رود، مسائل مربوط به انکار اصل و تحویل و عدم انکار دریافت را می‌توان حل کرد.(۶۸)

۲ – ۳ – امضای مبتنی بر رمز نگاری نامتقارن(۶۹)

در رمز نگاری نامتقارن که به آن کلید عمومی نیز گفته می‌شود، یکی از دو کلید رمزگذاری، کلید عمومی است. هرکاربر این کلید را در اختیار دیگران قرارمی‌دهد تا برای رمزگذاری پیام‌های ارسالی وی و همچنین رمزگشایی امضای الکترونیکی وی از آن استفاده کنند. رمزگذاری کلید عمومی عبارت است از یک طرح متقارن که از یک جفت کلید برای رمزگذاری استفاده می‌کند: کلید عمومی داده‌ها را رمزگذاری می‌کند و کلید خصوصی در هماهنگی با کلید عمومی داده‌ها را رمزگشایی می‌کند، فرآیند بالا برای امضای الکترونیکی به صورت معکوس است؛ فرستنده از کلید خصوصی برای ایجاد شماره الکترونیکی منحصر به فردی استفاده می‌کند و اشخاص دیگر کلید عمومی مربوطه را پردازش کرده و می‌توانند از آن برای خواندن شماره استفاده کنند.(۷۰)

بنابراین سیستم‌های رمزنگاری نامتقارن مبتنی بر دو کلید هستند. یک کلید عمومی و یک کلید خصوصی که هرچند متفاوت هستند اما از نظر محاسباتی با یکدیگر مرتبط هستند. با استفاده از کلید خصوصی، شخص می‌تواند پیام را رمزنگاری و ارسال کند و این پیام فقط با استفاده از کلید عمومی فرستنده قابل رمزگشایی است و به این صورت تمامیت پیام و هویت فرستنده آن تضمین می‌شود.



از طرفی دیگر امضاءکننده با استفاده از کلید عمومی گیرنده، پیام را امضاء می‌نماید و دریافت کننده با استفاده از کلیدخصوصی خود پیام را رمزگشایی می‌نماید. این عمل امضاءکننده را مطمئن می‌سازد که فقط گیرنده مورد نظر می‌تواند پیام را بخواند. در این شیوه امضای الکترونیکی تضمین می‌کند که محتوای سند تغییرنیافته است و همچنین احتمال هرگونه انکار بعدی برای ارسال کننده پیام را منتفی می‌سازد.(۷۱)

۴ – مفاهیم موجود در ساختار امضای الکترونیکی مطمئن

۱ – ۴ – زیرساخت کلید عمومی

با توجه به آنچه گفته شد مشخص است که مهمترین موضوع در امضاء الکترونیکی، قابلیت انتساب آن به اصل ساز یا ارسال کننده داده پیام می‌باشد به عبارت دیگر ارسال کننده و دریافت کننده یعنی طرفین یک رابطه حقوقی بایستی نسبت به اصالت و امنیت داده پیام ارسالی و همچنین تمامیت آن بطور نسبی و به تناسب ارزش و موضوع رابطه تجاری مورد نظر از اطمینان لازم برخوردار باشند.

امنیت اطلاعات الکترونیکی به وسیله تأسیس مراجع گواهی الکترونیکی انجام می‌شود و مهمترین ابزار فنی که به وسیله این نهاد جدید برای تأمین امنیت به خدمت گرفته می‌شود زیرساخت کلید عمومی(۷۲) (PKI) و تشکیل مرجع گواهی(۷۳) (CA) است.(۷۴) زیرساخت کلید عمومی در واقع مهندسی امنیت مبادله اطلاعات در محیط غیرایمن اینترنت است تا سطح بالایی از اعتماد و اطمینان را برای کاربران فراهم نماید، طرف های روابط تجاری در سراسر جهان با مساله ایمن نبودن مبادله اطلاعات در اینترنت مواجه هستند، این امر و ضرورت استفاده از اینترنت این نیاز را نشان می‌دهد که بایستی راهکاری برای حل این مشکل ارائه گردد، اینترنت اصولاً یک دسترسی باز به اطلاعات را اقتضاء نموده و دارای سطح پائینی 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.

رمزگذاری اطلاعات، نقصی را که اینترنت در این زمینه دارد جبران خواهدکرد، طرفین یک رابطه تجاری می‌توانند با استفاده از این پدیده، پیام خود را مبادله کرده و مطمئن باشند که: ۱ـ ارسال کننده حقیقی آن را ارسال کرده است.(۷۵) ۲ـ محتوای پیام به طور عمد یا سهو تغییر نکرده است.(۷۶) ۳ـ در موقع لزوم به مدرک پیام و زمان ارسال و دریافت دسترسی مطمئن و غیرقابل انکار وجود دارد.(۷۷) در تعریف زیرساخت کلید عمومی می‌توان گفت که زیرساخت

کلید عمومی مجموعه‌ای از سازمان‌ها، سیاست‌ها،[۷۸] مأموران، سیستم ها (نرم افزاری و سخت افزار) و قراردادها است که برای صدور، توزیع و مدیریت گواهی کلید عمومی مورد استفاده قرارمی‌گیرد. در بستر تجارت الکترونیکی چون طرفین حضور فیزیکی ندارند انجام معامله و مبادله اطلاعات ممکن است با این خطرات همراه باشد؛ کاربران غیرمجاز خود را به عنوان کاربران مجاز جلوه دهند، مشارکت در مبادله یا معامله برخط توسط یک طرف تکذیب شود، داده جعل شود و یا اینکه دسترسی غیرمجاز صورت گیرد. زیرساخت کلید عمومی نوعی مدیریت ارتباطات و ایجاد سطحی قابل قبول از اطمینان را به وجود می‌آورد. این کار از طریق مدیریت و کنترل استفاده از کلیدها و گواهی‌های رمزنگاری انجام می‌شود. بدون مدیریت و ایجاد سطوح ایمنی توسط PKI، امنیت مبتنی بر رمزنگاری دراکثر روابط تجاری غیرممکن خواهد شد.

۲ – ۴ – الزامات زیرساخت کلید عمومی

زیرساخت کلید عمومی برای شکل گیری تجارت در اینترنت به الزامات زیر نیاز دارد: **تصدیق:** باید هویت اشخاص قبل از هرگونه مبادله و معامله مشخص شود، برای این منظور از گواهی دیجیتال که توسط مراجع گواهی صادر می‌شود استفاده خواهد شد. **اجازه:** برای اجتناب از فعالیت‌های غیرمجاز، حدود تصرف اشخاص برای مشارکت در مبادله، معامله یا اجازه دسترسی به منابع باید مشخص شود. **محرمانه بودن:** با رمزکردن اطلاعات می‌توان از دسترسی غیرمجاز ممانعت کرد، مدیریت و مبادله داده‌های رمزنگاری شده ازطریق PKI صورت می‌گیرد. **تمامیت اطلاعات:** باید از تحریف و تغییر عامدانه یا سهوی اطلاعات، درهنگام ارسال و یا ذخیره‌کردن آن جلوگیری شود. **غیرقابل انکار بودن:** روشی که برمبنای آن به سادگی بتوان مشارکت طرفین را در انجام معامله ثابت کرد، در سیستم مبتنی بر PKI نحوه عمل به گونه‌ای است که زمان دقیق وقایع ثبت می‌شود و می‌توان از طریق ممیزی امضای دیجیتال و گواهی کلید عمومی به سابقه یک معامله دسترسی پیدا کرد.

۳ – ۴ – فنّاوری زیرساخت کلید عمومی

در ارتباط با فنّاوری زیر ساخت کلید عمومی، ارائه توضیحاتی در ارتباط با اجزاء تشکیل دهنده آن که در روند ایجاد کلید عمومی و دسترسی بدان ایفاء نقش می‌نمایند، ضروری است، از جمله عوامل مؤثر در این روند مراجع ثبت و گواهی می‌باشند. مرجع ثبت، اطلاعاتی را که یک

درخواست کننده هنگام ثبت نام ارائه می‌دهد بررسی نموده و تأیید می‌نماید. باتوجه به اینکه تعداد افرادی که می‌خواهند هویت خود را به عنوان موضوع گواهی به ثبت برسانند زیاد و ازنظر جغرافیایی پراکنده هستند باید مراجع ثبت متعدد در کشور وجود داشته باشند تا با مراجعه به این مراجع، ثبت نام افراد با اعمال دقّت‌های لازم امکان پذیر گردد و اتلاف وقت و هزینه و تجمع در یک مرجع گواهی خودداری گردد. کارکرد مرجع ثبت در یک فضای نیمه کاغذی، نیمه الکترونیکی معنا می‌یابد، مرجع ثبت یک تأسیس تعاملی و کاملاً سازگار با مرجع گواهی می‌باشد که می‌تواند پشتیبانی فعالیت‌های اولیه و اصلی را برای تولید کلید، ذخیره سازی و دسترسی به اطلاعات انجام دهد، هر مرجع ثبت معمولاً می‌تواند مرجع گواهی‌های مختلف را پشتیبانی کند وظایف اولیه مرجع ثبت از قرار زیر است:

۱- **نام نویسی(ثبت) کاربر** : فرایندی که به موجب آن کاربر به عنوان یک طرف بالقوه زیرساخت عمومی ثبت می‌شود، این فرآیند فیزیکی است و فقط برای یک بار انجام می‌شود، متقاضی با در دست داشتن مدرک شناسایی، به یکی از این مراکز مراجعه کرده و نام نویسی می‌کند، مرجع ثبت مشخصات کاربر را در یک پایگاه داده ویژه به وجود آورده و به عبارتی برای وی شناسنامه دیجیتال صادر می‌کند، اطلاعات این شناسنامه کاملاً معادل شناسنامه مرسوم است.

۲- **مدارک** : فرآیندی که براساس آن مرجع ثبت به خوبی می‌تواند هویت متقاضی را برای بار اول احراز کرده و تأیید کند که کلید عمومی حقیقتاً متعلق به متقاضی است.

۳- **تأیید درخواست‌های کاربر نهایی** : مرجع ثبت وظیفه تأیید یا رد درخواست‌های کاربر نهایی را چه برای اخذ گواهی برای اولین بار یا تجدید یا انقضای گواهی دارد.

۴- **لغو گواهی** : اقدامی که براساس آن مرجع ثبت به مرجع گواهی دستور می‌دهد تا گواهی کاربر را لغو کند. مرجع ثبت ممکن است براساس سیاستی که در قانون معین شده مجبور به اعلام دلیل باشد.

در مورد نقش مرجع گواهی(CA) نیز بایستی متذکر شد که طرفین رابطه تجاری بایستی 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 اینترنت انجام می‌شود. برای تصدیق یک امضای دیجیتال، شخصی که می‌خواهد از هویّت طرف دیگر اطمینان یابد، باید به کلیدعمومی امضاء کننده دسترسی و اطمینان داشته باشد که کلید عمومی موردنظر با کلید خصوصی امضاء کننده

مطابقت می‌کند، از آنجا که کلیدهای عمومی و خصوصی هیچ ارتباط و همراهی ذاتی با شخص ندارند، لازم است مکانیزمی پیش‌بینی شود تا چنین همراهی و ارتباطی ایجاد گردد.
برای اینکه استفاده از کلید عمومی و خصوصی نتیجه بخش باشد لازم است کلید عمومی به نحوی شایسته در دسترس اشخاص که خواهان استفاده از آن هستند قرارگیرد، از طرفی بسیاری از این افراد امضاء کننده را نمی‌شناسند و فقط از طریق اینترنت با او آشنا شده‌اند، بنابراین لازم است یک سیستم قابل اعتماد بین آن دو قرارگیرد تا ضمن پخش کلید عمومی به نحو مقتضی، صحّت کلیدهای عمومی و خصوصی را تضمین و اطمینان لازم را درجهت شناسایی هویّت و انجام معاملات مورد نظر جلب نماید. بنابراین مرجع ثبت براساس یک مدیریت از پیش تعیین شده شکل می‌گیرد، مسؤلیت مرجع ثبت در یک جمع بندی کلی عبارت است از:

۱- **گواهی کلید** : مرجع ثبت، کلید عمومی طرف را امضاء و گواهی صادر می‌کند.
۲- **تجدیدکلید** : تجدید گواهی طرف، در زمانی که گواهی منقضی شده است.
۳- **لغو گواهی** :گواهی کاربر را به فهرست لغو شدگان می‌افزاید و بدین ترتیب گواهی را ازآن تاریخ به بعد بی‌اعتبار می‌سازد.
۴- **ارسال گواهی** : گواهی را در فهرست PKI قرارمی‌دهد تا امکان بازیافت آن توسط طرف اعتمادکننده ممکن شود.
۵- **نگهداری فهرست لغوشدگان** : فهرست لغو گواهی را روزآمد نگه‌می‌دارد.
۶- **ارسال فهرست لغوشدگان** : اسامی گواهی‌های لغوشده را به فهرست PKI ارسال می‌کند تا کاربران PKI بتوانند آن را جست‌وجو و بازیافت کنند.

براساس بند ۱۱ ماده ۲ دستورالعمل اتحادیه اروپا، تأمین کننده خدمات گواهی، واحد یا شخص حقیقی یا حقوقی است که گواهی‌نامه‌ها را صادر نموده یا سایر خدمات مرتبط با امضای الکترونیکی را فراهم می‌سازد.
بند۹ ماده۲ دستورالعمل اتحادیه اروپا بیان می‌دارد «گواهی‌نامه، گواهی الکترونیکی است که داده تصدیق امضاء را به شخص مرتبط می‌سازد و هویّت وی را تأیید می‌نماید.» منظور از داده تصدیق امضاء در این ماده همان کلید عمومی است.

۷ – طرف اعتمادکننده[۷۹]

طرف اعتمادکننده کسی است که از اطلاعات موجود در گواهی یک ثبت نام کننده استفاده

کرده و به رابطه معتبر بین هویت ثبت نام کننده و کلید عمومی وی اعتماد می‌کند تا با تطبیق کلیدعمومی فهرست شده با اطلاعات فرد مورد ادعا از هویت فرستنده پیام، صحت، تمامیت و محرمانگی پیام اطمینان حاصل کند. براساس بند۵ ماده۲ قانون نمونه آنستیرال درمورد امضای الکترونیکی، طرف اعتمادکننده شخصی است که برمبنای یک گواهی یا یک امضای الکترونیکی عمل می‌کند. در پیش نویس قانون تجارت الکترونیک نیز به تبعیت از این تعریف طرف اعتمادکننده به عنوان شخصی که براساس گواهی یا امضای الکترونیکی اقدام می‌کند معرفی شده بود، اما این بند در متن نهایی قانون حذف شد.

۴ – ۴ – فهرست زیرساخت کلید عمومی

فهرست زیر ساخت کلید عمومی یک بانک اطلاعاتی بر خط است که به همه اطراف مبادله این امکان را می‌دهد که لیست گواهی‌ها، اطلاعات مربوط به لغو (گواهی‌های لغوشده)[۸۰] و سیاست‌های مرتبط به یک مرجع گواهی را جست و جو و بازیافت کند.[۸۱] طبق مقررات، افراد خاصی در افزودن یا کاستن اطلاعات این فهرست صلاحیت دارند. خدمات فهرست زیر ساخت شامل تهیه و مدیریت کامل داده‌های مربوط به ثبت نام کننده است، این داده‌ها تنها گواهی را دربرنمی‌گیرد، بلکه اطلاعات دیگری از جمله آدرس پست الکترونیکی، شماره تلفن و.... را نیز شامل می‌شود. هنگامی که مرجع گواهی، گواهی را صادرنمود، گواهی وارد فهرست PKI مربوط به گواهی‌های معتبر می‌شود تا اشخاص ثالث بتوانند به آن دسترسی داشته باشند، ممکن است برای دسترسی به فهرست مزبور محدودیت‌هایی وجود داشته باشد تا افراد غیر مجاز نتوانند به اطلاعات دست یابند.[۸۲]

فهرست دیگر موجود در فهرست PKI، لیست گواهی‌های رجوع شده است. این گواهی‌ها پیش از آنکه تاریخ انقضای اعتبار آن‌ها فرارسد به دلیلی بی‌اعتبار شده‌اند، با دسترسی به این فهرست می‌توان با اطلاعات دقیق‌تری راجع به هویت طرف معامله تصمیم‌گیری نمود[۸۳] 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، نشانی، شماره حساب بانکی یا هرمشخصه مؤثر دیگری تغییر نموده باشد.[۸۴]

۵ – ۴ – پاکت دیجیتالی

زمانی که داده پیام از حساسیت ویژه‌ای برخوردار بوده و لازم است محتوای آن از دسترس

دیگران پوشیده بماند از پاکت دیجیتالی استفاده می‌شود، این پاکت‌ها برای منظورهای متفاوتی طراحی شده اند، به عنوان مثال دارندگان کارت‌های اعتباری که از استاندارد SET [۸۵] استفاده می‌کنند، شماره کارت خود را در داخل پاکت دیجیتال می‌گذارند، این پاکت را فقط مرکز پردازش کارت (صادرکننده کارت) می‌تواند بازکند چون پاکت دیجیتال یک سیستم رمزنگاری متقارن است. البته پاکت‌های دیجیتال این قابلیت را دارند که از هر دو سیستم رمز نگاری متقارن و نامتقارن بهره ببرند، پاکت‌های دیجیتالی که از سیستم رمزنگاری متقارن استفاده می‌کنند معمولاً از کلید رمزنگاری داده متقارن یک زمانه به نام DEK (Data Encryption KEY) یا کلید فصلی جهت رمزنگاری داده به نحو انبوه بهره می‌برند، DEK باید از طریق سیم به دریافت کننده ارسال تا وی بتواند « داده » رمزشده را رمزگشایی کند. DEK پس از آنکه با کلید عمومی دریافت کننده رمز شد به وی ارسال خواهد شد، DEK فقط برای یک بار و نسبت به آن پیام خاص کاربرد دارد. برای ایجاد پاکت دیجیتال، ارسال کننده فقط باید به کلید عمومی دریافت کننده دسترسی داشته باشد. هر نوع الگوریتم متقارن را می‌توان برای این منظور استفاده کرد. اما دریافت کننده حتماً باید به همان الگوریتم مشابه دسترسی داشته باشد. در نهایت، دریافت کننده با کلید اختصاصی خود پیام را رمزگشایی می‌کند، این امر سبب می‌شود تا شخص مجاز پاکت نامه را باز کند.

با این روش الگوریتم مورد استفاده به طور خودکار شناسایی نمی‌شود، بنابراین ارسال کننده باید تاحدی اطلاعات مربوط به روش مورد استفاده خود را برای دریافت کننده ارسال کند، این پاکت‌های دیجیتال، محرمانگی پیام را تضمین می‌کنند، اما هویت طرفین را تصدیق نمی‌کنند. بنابراین پیام امضای دیجیتال شده را داخل این پاکت‌های دیجیتال قرارداده شده و ارسال می‌گردند، از طرف دریافت‌کننده، امضاء فقط توسط شخص مجاز قابل تطبیق است، چون فقط وی به کلید اختصاصی جدید برای بازکردنDEK دسترسی دارد.

یکی از مزایای استفاده از پاکت دیجیتال این است که دریافت کننده و ارسال کننده لازم نیست که به طور همزمان بر خط باشند. بنابراین پاکت‌های دیجیتال برای سیستم‌های غیر هم‌زمان بسیار ایده‌آل هستند، حسن دیگر آنها اجرای خوب و مؤثر است، زمان قطعی ارسال آن وقتی خواهد بود که پاکت دیجیتال به طور کامل و صحیح ایجاد شده و در غیر اینصورت ارسال نخواهد شد. پاکت‌های دیجیتال می‌تواند با استفاده از پروتکل‌های انتقال داده مثل http ارسال شود.

گفتار هشتم : مزایا و معایب امضای الکترونیکی

الف) مزایای امضای الکترونیکی

۱- تسریع در امضای قرارداد و اسناد در هر نقطه‌ای از جهان بدون حضور فیزیکی و امکان پردازش مبادلات مالی بیشتر در تمامی کشورها.

۲- کاهش هزینه‌های ایاب و ذهاب و مبادله از طریق امضای الکترونیکی اسناد در هر نقطه از جهان.

۳- تسریع در امضای الکترونیکی قراردادها و اسناد تجاری و اعتباری در معاملات الکترونیکی به علت نوسانات سریع و لحظه‌ای قیمت‌ها.

۴- مدیریت دریافت و جابجایی پول یا ارز در بانک‌های داخلی و خارجی.

۵- امضای الکترونیکی بیمه‌نامه‌ها با شرایط مطمئن خودش در خصوص حمل و نقل کالا و خدمات.

۶- داشتن ضریب ایمنی مطمئن و بالاتر از امضای دستی به جهت داشتن رمز و کلید خصوصی.

۷- ذخیره، ارسال و دریافت داده‌ها بدون تغییر به جهت داشتن امضای الکترونیکی مطمئن.

۸- فایل امضای الکترونیکی حاوی اطلاعاتی مانند: نام، نام خانوادگی، پست سازمانی و پست فرستنده نامه یا اسناد، نشانی پستی سازمان، شماره تلفن، فاکس، وب سایت و پست الکترونیکی است که در انتها نامه یا سند الکترونیکی اضافه و ارسال می‌گردد.

۹- امضای هر سند متفاوت با مفاد اسناد دیگر است.

۱۰- در امضای الکترونیکی ارسال کننده و دریافت کننده نمی‌توانند منکر ارسال (دریافت) پیام یا تبادل مالی شوند.

۱۱- امضای الکترونیکی، اصالت و تصدیق هویّت یک پیغام یا سند و یا فایل اطلاعاتی را تضمین می‌کند.

۱۲- امضای الکترونیکی منحصر به فرد بودن و تمامیت امنیت و هویّت داده‌ها برای مراجع قضایی با اطمینان قابل پذیرش است.

۱۳- امضای الکترونیکی به راحتی قابل جابجایی است و شخص دیگری نمی‌تواند آن را محدود کند.

۱۴- امضای الکترونیکی دارای آثار حقوی همسان با امضای دستی است.

۱۵- گیرنده امضای الکترونیکی می‌تواند مطمئن باشد که اطلاعات حین انتقال تغییر پیدا نکرده است.

ب) معایب امضای الکترونیکی

۱- امضای الکترونیکی ممکن است به صورت خودکار و پس از طی زمان مشخص نابود شود.
۲- شبکه اینترنتی یک شبکه جهانی و بدون مسئول یا سیاست گذاری خاصی است.
۳- امضای الکترونیکی غیر مطمئن می‌تواند جعل شود.
۴- امکان سوء استفاده از طریق دسترسی به کلید عمومی وجود دارد.
۵- دسترسی غیرمجاز از طریق هکرها، به داده پیام امضاء شده قبل از رسیدن به مقصدوجود دارد.

گفتار نهم : قابلیّت استناد به امضای الکترونیکی

همان طور که گفته شد، امضای الکترونیکی برخلاف امضای دستی یا مندرج در اسناد کاغذی، در یک محیط الکترونیکی و با استفاده ازروش‌ها و فناوری‌های الکترونیکی ایجاد می‌شود، برای اینکه چنین امضایی در مقام دعوی یا دفاع قابل استناد باشد ضروری است که برخی از ویژگی‌های مهم امضای دستی، یعنی تک (منحصر به فرد) بودن، تعیین هویّت، تحت کنترل داشتن و امکان ممیزی را حائز باشد. بدین منظور هر روزه بر کیفیت استانداردهای فنی که چنین خصوصیاتی را تضمین کنند افزوده می‌شود. با این حال، تفاوت‌های زیادی بین نوشته‌های الکترونیک و اسناد کاغذی وجود دارند که باعث تفاوت در آثار حقوقی هر یک از این دو نوشته می‌شود، از جمله تفاوت‌ها این است که اسناد کاغذی در اصل، نمونه‌های فیزیکی بی‌مانند هستند، حال آنکه داده الکترونیکی نامحسوس بوده و به سادگی قابل تغییر است و سرانجام اینکه دستکاری یک سند کاغذی باید فیزیکی باشد وروی کاغذ قابل تشخیص است، در حالی که دست کاری الکترونیکی را به کمک چشم نمی‌توان کشف کرد.

برای بررسی موضوع، ضرورت دارد مواردی که طرفین مبادله الکترونیکی در خصوص نحوه این مبادله و ارزش اثباتی آن توافق کرده‌اند و اصطلاحاً به آن سامانه بسته می‌گویند از مواردی که چنین توافقی بین طرفین مبادله الکترونیکی وجود ندارد و از آن به سامانه باز تعبیر می‌شود تفکیک گردند.

منظور از سامانه بسته این است که طرفین از پیش در خصوص ارزش اثباتی امضای الکترونیکی و عنداللّزوم بار اثبات دلیل توافق کرده باشند، در مقابل، سامانه باز، سامانه ای است که در آن

هیچ‌گونه توافق قبلی راجع به امضای الکترونیکی، نحوه ایجاد و میزان دلالت آن وجود ندارد، در چارچوب این سامانه اصولاً طرفین همدیگر را نمی‌شناسند و از موقعیت اقتصادی یکدیگر با خبر نیستند، رابطه حقوقی بین ارائه کنندگان کالا و خدمات و مصرف کنندگان اغلب در چنین محیطی شکل می‌گیرد، بدیهی است طرفین رابطه حقوقی که ازطریق اینترنت یا شاهراه‌های اطلاعاتی با هم مرتبط می‌شوند، برای هر گونه مبادله کالا و خدمات با پول باید از هویّت یکدیگر آگاهی یابند، از درستی و دقت اطلاعاتی که ردّ و بدل می‌شود و نیز تمامیت این اطلاعات اطمینان حاصل کنند.(۸۶)

چنانچه امضای الکترونیکی بخواهد همانند امضای دست نویس در مقام دعوی یا دفاع قابل استناد باشد باید از یکسری شرایط امضای دستی مثل منحصر به فرد بودن، قدرت تعیین هویّت و عدم امکان جعل توسط دیگران برخوردار باشد، البته در صورتیکه شرایط مذکور برای امضای الکترونیکی تحقق یافته باشد، همانند امضاهای دستی دارای ارزش اثباتی است و از این حیث هیچ تفاوتی با آن ندارد. امضای الکترونیکی یک داده است و همان طور که بیان شد « داده پیامها » نیز دارای ارزش اثباتی هستند. اما با توجه به ماده ۱۳ قانون تجارت الکترونیکی ایران، باید گفت که به طور کلی ارزش اثباتی داده پیام‌ها، با توجه به عوامل مطمئنه از جمله تناسب روش‌های ایمنی به کار گرفته شده تعیین می‌شود.حال چنانچه داده پیام‌های تشکیل دهنده امضاء، از تمام شرایط فنی لازم برخوردار باشند اعتبار حقوقی و جایگاه آنها در ادله اثبات دعوی همانند جایگاه امضاهای دست نویس است و می‌تواند به عنوان دلیل در مقام دعوی یا دفاع در محاکم مورد پذیرش قرار گیرد، به همین دلیل در قانون تجارت الکترونیکی ایران از امضایی که تمام شرایط فنی را برخوردار است تحت عنوان «امضای الکترونیکی مطمئن» نام برده شده است.

طبق ماده ۲ قانون مذکور امضای الکترونیکی مطمئن، امضایی است که شرایط مندرج در ماده ۱۰ آن قانون را داشته باشد، همچنین طبق ماده ۱۵ قانون مذکور نسبت به امضایی که با شرایط فوق ایجاد شده است نمی‌توان ادعای انکار و تردید کرد و تنها می‌توان نسبت به آن ادعای جعل نمود، بنابراین، به نظر می‌رسد که در عرصه تجارت الکترونیکی می‌توان در مقام تنظیم قراردادها، با منضم نمودن امضای الکترونیکی، داده های مزبور را از اعتبار قابل قبولی برخوردار داشت. در خصوص ارزش اثباتی امضاء موارد ذیل قابل طرح است:

۱- آنجا که هر امضایی می‌تواند تعهدآور باشد، بنابراین امضاءکننده در هنگام امضاء بایستی واجد قصد، رضا و اهلیت بوده و امضای الکترونیکی از این قاعده مستثنی نخواهد بود.

۲- هر امضایی که واجد شرایط فوق باشد، اعم از دستی یا الکترونیکی به نفع یا علیه امضاء کننده قابل استناد خواهد بود، درنتیجه اگر امضاءکننده الکترونیکی امضای خویش را انکار نماید، درآن صورت به وسیله کارشناسی، معرفی شهود و یا سایر ادله اثبات دعوا می‌توان صدور امضاء از سوی وی را اثبات نمود، همچنین در مورد امضاء الکترونیکی نیز کارشناس فنی رایانه می‌تواند از طریق بررسی کلید خصوصی که بیان شد، صدور امضاء از سوی شخص منتسب به وی را اثبات نماید.

۳- همان‌طور که گفته شد، بنظر می رسد که اسناد الکترونیکی مطمئن و امضای الکترونیکی مطمئن اسناد عادی در حکم اسناد رسمی هستند که نسبت به آن‌ها انکار و تردید مسموع نیست و تنها می‌توان ادعای جعلیت نمود. از این رو درصورت اثبات جعلیت دلایل رایانه‌ای مزبور، محکوم علیه می‌تواند در اجرای بند ۶ ماده ۴۲۶ قانون آئین دادرسی مدنی[۸۷] از مجرای اعاده دادرسی به منظور نقض حکم از مرجع صالح اقدام نماید.[۸۸] مقنن در ماده ۱۴ ق.ت.ا.ا همسو با قانون نمونه آنسیترال، هرگونه داده پیامی را که به طریق مطمئن ایجاد و نگهداری شده باشد را از حیث محتویات و همچنین امضاء مندرج در آن، تعهدات یا طرفی که تعهد کرده و کلیهٔ اشخاصی که قائم مقام قانونی آنان محسوب می‌شوند، اجرای مفاد آن و سایر آثار در حکم اسناد معتبر و قابل استناد در مراجع قضائی و حقوقی دانسته، بعلاوه مطابق ماده ۱۵ همان قانون تصریح گردیده است که نسبت به داده پیام مطمئن، سوابق الکترونیکی مطمئن و امضای الکترونیکی مطمئن، انکار و تردید مسموع نیست و تنها ادعای جعلیت نسبت به داده پیام مزبور قابل طرح بوده و یا اینکه مدعی می تواند ثابت نماید که چنین داده پیامی به جهتی از جهات قانونی از اعتبار ساقط شده است.

ماده ۹ قانون نمونه آنسیترال مصوب ۱۹۹۶ میلادی از یک سو مقرر می‌دارد که امضای الکترونیکی به این دلیل که به صورت داده پیام است و یا به دلیل اینکه داده پیام فاقد اصل است نباید مردود اعلام شود و از سوی دیگر، برای امضای الکترونیکی قائل به قدرت اثباتی است که بر اساس قابلیت اطمینان، روش ایجاد امضاء، نگهداری و ارسال پیام، حفظ تمامیت اطلاعات، هویّت ارسال کننده و سایر ملاحظات ارزیابی می‌شود.

دستورالعمل مورخ ۱۳ دسامبر ۱۹۹۹ اتحادیه اروپا نیز در ماده پنج خود تحت عنوان «آثار حقوقی امضای الکترونیکی» دولتهای عضو را موظّف می‌سازد که اولاً برای امضای الکترونیکی پیشرفته (مطمئن) همان آثاری را بشناسند که برای امضای دستی قائل هستند و ثانیاً آن‌را به عنوان دلیل در دادگاه مورد پذیرش قرار دهند، بند ۲ این ماده برای امضای ساده نیز ارزش

اثباتی قائل شده و دولت‌های عضو را از اینکه چنین امضایی را به دلیل قالب الکترونیکی آن یا فقدان گواهی تأئید شده و مردود اعلام کنند، منع می‌کند.
قانون مورخ ۱۳ مارس ۲۰۰۰ فرانسه راجع به انطباق دلایل با فناوری اطلاعاتی که به تبعیت از دستورالعمل اروپا مورخ ۱۳ دسامبر سال ۱۹۹۹ تدوین شده است به شکل روشن‌تر ارزش اثباتی امضای الکترونیکی را تبیین نموده است، براساس ماده ۱ـ۱۳۱۶ قانون مدنی فرانسه «نوشته‌ی الکترونیک» نیز همانند نوشته کاغذی به عنوان دلیل پذیرفته می‌شود، به این شرط که هویّت شخص صادر کننده آن را مشخص سازد و تمامیت آن را تضمین کند.
همچنین ماده ۳ـ۱۳۱۶ در تکمیل ماده ۱ـ۱۳۱۶ همان قانون مقرر می‌دارد: « نوشته‌های الکترونیکی از همان قدرت اثباتی برخوردار هستند که نوشته‌های مضبوط بر روی کاغذ برخوردارند.» فایده اصلی این تشبیه، وارد کردن دلیل انفورماتیکی در سامانه اثباتی سنتی است، بدون اینکه جایگاه خاصی برای آن در نظر گرفته شود. به موجب ماده ۶ ق.ت.ا.ا، هرگاه وجود یک نوشته از نظر قانون لازم باشد، « داده پیام » در حکم نوشته است مگر در موارد زیر:

- ❖ اسناد مالکیت اموال غیرمنقول
- ❖ فروش مواد دارویی به مصرف کنندگان نهایی.
- ❖ اعلام، اخطار، هشدار و یا عبارات مشابهی که دستور خاصی برای استفاده کالا صادر می‌کند و یا از بکارگیری روش‌های خاصی به صورت فعل یا ترک فعل منع می‌کند.

نتیجه گیری

بنظر می‌رسد که تمامی اعتبار تجارت الکترونیکی بر قابلیّت استناد به داده پیام و امکان اتّکاء به مفاد توافقات و قراردادهای تشکیل شده در محیط سایبر و با استفاده از وسائط الکترونیکی مبتنی است. اگر اشخاص حقیقی و یا حقوقی اعتماد کافی به آثار حقوقی مقصود از توافقات فیمابین نداشته باشند؛ بی‌گمان با احتیاط بیشتری از آن استفاده کرده و در موارد مهم که ضریب اطمینان بیشتری مورد نظر است، متمایل به امضاء سنّتی خواهند شد.
اهداف کلّی حاکم بر عرصه تجارت الکترونیکی کاملاً در جهت تأمین مقصود فوق طرّاحی شده‌اند و در این میان امضاء الکترونیکی بخش قابل توجّهی از متون قانونی را چه در بعد ملّی و چه در بعد بین‌المللی به خود اختصاص داده است. ایده امضاء الکترونیکی مطمئن، بر نگرانی‌های ناشی از عدم امکان اتّکاء بر درستی اظهارات طرفین در محیط الکترونیکی و موضوع قابلیّت استناد به این اظهارات استوار است. در حقوق سنّتی، تصدیق یا گواهی امضاء، هیچ

امتیازی به مندرجات سند نداده و درواقع بر اعتبار مفاد آن نمی‌افزاید؛ ولی امضاء کننده را در حد اعتبار سندی رسمی، به امضاء خویش پایبند ساخته و صرفاً امکان طرح ادّعای جعل را مقدور می‌سازد، نقش دفاتر گواهی و تصدیق امضاء در تجارت الکترونیکی از نقشی که دفاتر اسناد رسمی در این زمینه ایفاء می‌کنند؛ پررنگ‌تر است.

دفاتر صدور گواهی در تجارت الکترونیکی با احراز هویّت طرف متقاضی و در اختیار قراردادن کلیدهای خصوصی و عمومی، علاوه بر اینکه خود، اهلیّت و هویّت متقاضی را احراز می‌نمایند، با دردسترس دیگران قراردادن کلید عمومی، این امر را برای طرفهای رابطه حقوقی و قراردادی با متقاضی مزبور فراهم می‌سازند که با رجوع به فهرست دارندگان کلید، از اطّلاعات موجود در آن برای اطمینان بیشتر بهره مند شوند و مسلّماً در این مسیر مسئولیّت دفاتر مزبور در برابر اثبات نادرستی اظهارت راجع به هویّت به معنای عام و یا سایر مندرجات این فهرست، به طور خاص، غیرقابل انکار است. از سوی دیگر «ضرورت الصاق امضای الکترونیکی مطمئن به داده پیام، به نحوی که هر تغییری در داده پیام قابل کشف باشد» مذکور در بند د مادّه ۱۰ ق ت ا ا نیز مقرّه‌ای است که در همین راستا و به منظور اختصاص جایگاه و اثر بخشی ویژه به امضای الکترونیکی مطمئن، به گسترش اطمینان هرچه بیشتر در عرصه تجارت الکترونیکی کمک می‌نماید.

پی نوشت ها

۱. نوری، محمدعلی و نخجوانی، رضا، حقوق تجارت الکترونیکی، صص ۱۰۶ و ۱۰۷.
۲. البته در مواردی قانونگذار نوشته ی بدون امضاء را نیز مانند سند دانسته است مانند دفاتر تجاری، ماده ۱۴ق ث و ماده ۱۲۹۷ ق م.
۳. شمس، عبدالله، ادلّه اثبات دعوا، نشر دراک، ج اوّل، ۱۳۸۷ ص ۹۰.
۴. کاتوزیان، ناصر، اثبات و دلیل اثبات، بهار ۸۷، ج اوّل ص ۳۱۷.
۵. کاتوزیان، ناصر، همان، ص ۲۷۸.
۶. صدرزاده افشار، محسن، ادلّه اثبات دعوا در حقوق ایران، نشر دانشگاهی، ۱۳۶۹ ، ج اوّل صص ۹۰-۹۱.
۷. کاتوزیان، ناصر، همان منبع، ص ۳۱۷ .
۸. سرشار، محمود، طریقه کشف جعل در عصر حاضر، مجلّه کانون وکلاء، ج ۳۲،خرداد و تیر ۱۳۳۲ ص ۲۳.
۹. صدرزاده افشار، همان ص ۹۱.
۱۰.جعفری لنگرودی، محمدجعفر، مبسوط در ترمینولوژی حقوق، ج اول، ص ۶۲۶.
۱۱.م ۲۲۵ ق آ د م.

12. Certificate Authority.
13. Uncitral Model law on Electronic Commerce.(1996)

۱۴.به هنگام تدوین قانون نمونه، کارکردهای زیر برای امضاء شمرده شده: ۱)تعیین هویّت شخص۲)ایجاد قطعیت راجع به دخالت شخصی که عمل امضاء را انجام داده است۳) اثبات پایبندی شخص به محتویات سند امضاء شده۴) اثبات این موضوع که امضاء کننده هنگام امضاء در چه محلی حضور داشته است و در این باره رجوع کنید به:
http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf

15. Model Law on Electronic Signature 2001 (MLES)
16. The Model Norary Act, September 1, 2002 Published As a Public Service by the Notary Association. available at:www.nationalnotary.org.
17. Uniform Electronic Transactions Act 1999(UETA) Section 8 (2).
18. EU Directive on Electronic Signatures 1999.
19. Law adapting evidence to information technology and relating to electronic signature, March13, 2000.

۲۰.شمس، عبدالله، همان، ص ۹۱

۲۱.هیئت مولفان و ویراستاران شرکت مایکروسافت، فرهنگ تشریحی اصطلاحات کامپیوتری؛مترجم فرهاد قلی زاده نوری ،کانون نشر علوم ،۱۳۸۳ ص ۶۷۷.

22. Todd, Paul, E- Commerce law, London: Cavendish Pub. 2005, p 99.
23. Ralph Bloemers, Electronic and digital signatures, available at: http://www.stoel.com.
24. Electronic Signature.
25. Secure/Enhanced/Advanced Electronic Signature.
26. Signatory.

۲۷.در تعریف اینکه امضاء کننده چه شخصی است بند ل و م ماده ۲ ق.ت.ا.ا آن را تعریف نموده که در بند ل بیان می‌نماید «امضاء کننده (Signatory): هر شخص یا قائم مقام وی که امضای الکترونیکی تولید می‌کند.» بند م ماده مذکور «شخص (Person): اعم است از شخص حقیقی و حقوقی و یا سیستم های رایانه‌ای تحت کنترل آنان.»

28. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for Eelectronic Signatures. Available at:
. http://europa.eu/legislation_summaries/information_society/l24118_en.htm

29. Uncitral Model Law on Electronic Signatures with Guide to Enactment 2001, available at:
http://www.uncitral.org/pdf/english/texts/electcom/ml-elecsig-e.pdf.

30. See: DAUZON, OLIVIER, Le Droit du Commerec Electronice, Hercity – France, Editions Du Decree NO 2001 – 272 Du 20 Mars 2001, Available at: http://playmendroit.free.fr// droit-des-novellas-technologies / decret-du-2003, 2001.
31. Uniform Electronic Transactions Act 1999 (UETA).
32. Electronic Signatures in Global and National Commerce Act, 20 June 2000, Available at:http://www. Cio. Noaa. gov / it management / pllo 6229. pdf.
33. http://www.ida.gov.sg/Policies%20and%20Regulation/20060420164343.aspx .
34. Secure Electronic Signature.
35. E.U: Electronic Signatures Directive, 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for Electronic Signatures.
36. Todd, Paul, Ibid. 157 & Jim Minihan, Digital Signatures, available At: http://www.aiim.org/Resources/Archive/Magazine/2002-May-Jun/24142.
37. http://www.bundesnetzagentur.de/media/archive/3612.pdf.
38. Public Key.
39. Private Key.

۴۰.این دو کلید امضاء از هم مجزّا اما از لحاظ ریاضی منطبق و به هم متّصل هستند و هیچ یک بدون دیگری کامل نیست امضای دیجیتالی دارای مراحلی است. اما در عمل امضاء

کننده با این پیچیدگی روبرو نیست و آنرا بر صفحه نمایش رایانه خود تماشا می کند دستورات ساده و با استفاده از کلیک موس است. زمانی که پیام از حساسیت برخوردار است و لازم است محتوای آن از دید دیگران پنهان بماند از پاکت دیجیتالی استفاده می شود. این پاکتها برای مقاصد متفاوتی مناسب و دارای کاربرد هستند. برای مثال دارندگان کارت های اعتباری که از استاندارد SET استفاده می کنند، شماره کارت خود را در پاکت دیجیتال گذارده و این پاکت را فقط مرکز پردازش صادر کننده کارت می تواند باز کند، به عبارت دیگر پاکت دیجیتالی یک سامانه رمزنگاری متقارن است.

41. Hoop key.

42. Certificate key.

۴۳.هیئت مولفان و ویراستاران شرکت مایکروسافت، پیشین، ص ۲۲۶.

44. See, http://www.reallegal.com/downloads / pdf / E - sigwhite paper. Pdf .

45. Cryptography.

۴۶.آهنی، بتول، برقراری امنیّت در قراردادهای الکترونیکی، فصلنامه فقه و حقوق دانشگاه امام صادق (ع)، واحد خواهران، ش ۳۰ ص ۷۳.

47. Asymmetric Cryptography.

۴۸.زیست سنجی Biometrics. در گذشته به علم اندازه‌گیری و تحلیل ویژگی‌های بیولوژیکی انسان گفته می‌شد. در فنّاوری رایانه، بیومتریک به روش‌های امنیتی و تأیید اعتباری مربوط می‌شود که برای تشخیص یا بررسی صحت هویّت یک شخص، بر نشان‌های بیولوژیکی و قابل اندازه‌گیری اشخاص تکیه دارند. به عنوان مثال، از اثر انگشت، اثر دست یا تشخیص صدا می‌توان برای دستیابی به یک رایانه، یک اتاق یا یک حساب تجاری الکترونیکی استفاده نمود. طرح‌های امنیتی عموماً به سه سطح طبقه‌بندی می‌شوند: سطح اول: بر چیزی که یک شخص با خود دارد تکیه دارد، مثلاً یک کارت شناسایی عکس دار یا یک کارت رایانه‌ای، سطح دوم: بر چیزی که شخص می‌داند تکیه دارد، مثلاً کلمه عبور یا یک کد عددی، سطح سوم یا بالاترین سطح، بر چیزی که بخشی از اعضای بیولوژیکی یا رفتار شخص است تکیه دارد، مثلاً اثر انگشت، ساختار رگ‌ها در شبکیه چشم یا امضاء، ر.ک، هیأت مولفان و ویراستاران انتشارات مایکروسافت ، پیشین، ص ۸۵.

۴۹.اسکن کردن امضاهای دستی که روی کاغذ انجام می‌شود نیز از این قبیل است.

50. Originator .

۵۱.بند ی ماده ۲ ق.ت.ا.ا بیان می‌دارد « امضای الکترونیکی (Electronic Signature) عبارت است از هر نوع علامت منظم شده یا به نحو منطقی متصل شده به داده پیام است که برای شناسایی امضاء کننده داده پیام مورد استفاده قرار می‌گیرد».

۵۲.امضای الکترونیکی مطمئن (Secure / Enhanced / Advanced Electronic Signature) هر امضاء الکترونیکی است که مطابق با ماده ۱۰ این قانون باشد می توان گفت که امضای الکترونیکی مطمئن معادل امضای دیجیتالی است.

۵۳.ماده ۱۱ ق.ت.ا.ا سابقه الکترونیکی مطمئن را تعریف می‌نماید که اعلام می‌دارد «سابقه الکترونیکی مطمئن عبارت از «داده پیام» ای است که با رعایت شرایط یک سامانه اطلاعاتی مطمئن ذخیره شده و به هنگام لزوم در دسترس و قابل درک است.»

ـ در این مبحث آنچه در خصوص امضای الکترونیکی از حیث آثار حقوقی گفته می‌شود اعم از امضای الکترونیکی ساده و امضاء الکترونیکی مطمئن است و عبارت امضای الکترونیکی که به کار می‌رود به مفهوم وسیع آن است.

54. Article 9 (3): Where the law requires that a communication or a contract should be signed by a party, or provides consequences for the absence of a signature, that requirement is met in relation to an electronic communication if: (a) A method is used to identify the party and to indicate that party's intention in respect of the information contained in the electronic communication ; and (b) the method used is either: (i) As reliable as appropriate for the purpose for which the electronic communication was generated or communicated, in the light of all the circumstances, including any relevant agreement; or (ii) Proven in fact to have fulfilled the functions described in subparagraph (a) above, by itself or together with further evidence.

55. UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001, p40.

56. Ibid.

۵۷.السان، مصطفی، جنبه های حقوقی ثبت الکترونیکی- ماهنامه کانون سردفتران و دفتریاران- دوره دوم بهار ۸۷- ش ۷۹ صص ۱۹و۱۸.

۵۸.زرکلام، ستّار، حقوق تجارت الکترونیک، مؤسسه مطالعات و پژوهشهای حقوقی شهردانش، ۱۳۸۸، ص ۱۹۳.

۵۹.زرکلام، ستّار،امضاء الکترونیکی و جایگاه آن در نظام ادلّه اثبات دعوا، مجله مدرس، دوره ۷، ش ۱، بهار۱۳۸۲، ص ۲۹۷.

60. Encryption.

۶۱.الگوریتم: دستورات ساده و قابل فهم رایانه که اجرای پشت سر هم آنها منجر به هدف معینی (برای مثال حل مساله‌ای) می‌شود. این دستورات گام به گام اجرا می‌شوند و در صورت درست بودن محاسباتی در مرحله‌ای خاص به نتیجه می‌رسد. واژه الگوریتم برگرفته از نام ریاضیدان بزرگ ایرانی خوارزمی است.

۶۲.السان، مصطفی، دوان یامچی، امین، ماهیت رایانه‌ای و جنبه‌های حقوقی امضای دیجیتالی، فصلنامه دیدگاههای حقوقی، ش ۳۱، ۱۳۸۵، ص ۲۷.

۶۳.هیأت مولفان و ویراستاران انتشارات مایکروسافت، پیشین، ص ۲۷۳.

64. Todd, Paul, Ibid, p 103.

۶۵.Hashing algorithm الگوریتم در هم سازی ـ فرمولی که برای تولید مقادیر « درهم » و امضای دیجیتال مورد استفاده قرار می‌گیرد. Hash function = Hashing algorithm الگوریتم در هم سازی ـ فرمولی که برای تولید مقادیر « درهم » و امضاهای دیجیتال مورد استفاده قرار می‌گیرد.

۶۶.هیأت مولفان و ویراستاران انتشارات مایکروسافت، پیشین، صص ۳۵۲، ۳۵۱، ۱۰۵.

67. Asymmetric.

۶۸. K.K Bajaj Debjani، از مبادله الکترونیکی اطلاعات (EDI) تا تجارت الکترونیکی، مترجم، دکتر بهنام مجتهدی، تهران مؤسسه مطالعات و پژوهش‌های بازرگانی، ۱۳۷۶، چاپ اول، صص ۲۸۴-۲۸۹.

69. Symmetric.

۷۰.هیأت مولفان و ویراستاران انتشارات مایکروسافت، پیشین، ص ۶۰۷.

71. Todd, Paul, Ibid, P106.

72. Public Key Infrastructure.

73. Certification Authority .

۷۴.مواد ۱۰ و ۱۱ ق.ت.ا.ا به این موضوع اشاره کرده اند.

75. Authentication .

76. Integrity .

77. Non Repudiation.

78. Policies.

79. Relying Party.

80. Revoked certifications.

۸۱. به عبارتی می‌توان گفت فهرست زیرساخت کلیدعمومی، یک پایگاه اطلاعاتی است که لیست گواهی‌های معتبر و گواهی‌های لغو شده را در اختیار اطراف معامله و سایر اجزاء عملیاتی زیرساخت کلیدعمومی قرارمی‌دهد.

۸۲.هیأت مولفان و ویراستاران انتشارات مایکروسافت، پیشین، ص ۳۰۳.

83. Todd, Paul, Ibid, p103 & http://www.Pki.page.org / http://www.rsa.com.

۸۴.به طور کلی کارکردهای یک فهرست PKI را می‌توان در دو مورد زیر خلاصه نمود:

الف ـ ذخیره نمودن گواهی دیجیتال و لیست گواهی‌های ملحق شده لازم به یادآوری است؛ همانطوری که گواهی‌ها(معتبر) به وسیله مرجع گواهی امضاء می‌شوند، گواهی‌های ملحق شده نیز باید حسب مورد به وسیله مرجع گواهی یا دربرخی موارد مرجع ثبت یا مدیریت فهرست کلید عمومی امضاء شوند تا ضمن رجوع، اعتماد لازم نسبت به آن‌ها در زمان اعتبارشان محفوظ بماند. ب ـ ترتیبی اتخاذ نماید تا اطراف امضاء کننده بتوانند به فهرست مورد دسترسی داشته باشند.

85. Secure Electronics Transactions Protocol (SET).

پروتکلی برای انجام معاملات امن در اینترنت؛ این پروتکل نتیجه تلاش مشترک GTE، IBM، MasterCard، ر، ک، هیأت مولفان و ویراستاران انتشارات مایکروسافت، پیشین، ص۲۴۰.

۸۶.گزارش توجیهی قانون تجارت الکترونیکی، پائیز ۱۳۸۰.

۸۷.م۴۲۶ق.آد.م « نسبت به احکامی که قطعیت یافته ممکن است به جهات زیر درخواست اعاده دادرسی شود:... بند ۶ حکم دادگاه مستند به اسنادی بوده که پس از صدور حکم، جعلی بودن آن‌ها ثبت شده باشد.».

ر، ک، کردنائیج، حسن، ماهیت حقوقی اسناد الکترونیکی و امضای الکترونیکی و تأثیر اثبات جعلیت آن‌ها در اعاده دادرسی، مجله پیام آموزش، شماره۲۴، ۱۳۸۵، ص