Electronic signature

(امضاء الکترونیکی)

نرگس اکبری نسب

مهندسی تکنولوژی نرم افزار کامپیوتر

کارشناس نرم افزار و امنیت اطلاعات اداره کل زندانهای استان سمنان

چکیده:

امضای الکترونیکی عبارت از داده ای الکترونیکی است که به یک داده پیام ضمیمه می گردد و موجب شناسایی امضا کننده و مبین رضایت او نسبت به مندرجات و محتویات داده پیام است. این امضا به لحاظ ارزش اثباتی، به دو نوع امضای الکترونیکی ساده و امضای الکترونیکی مطمئن تقسیم می شود. امضای دیجیتال نوعی از امضای الکترونیکی است که در آن از فناوری رمزنگاری برای تولید امضا استفاده می شود و از سطح بالایی از امنیت نسبت به سایر انواع امضای الکترونیکی برخوردار است. دفاتر خدمات صدور گواهی الکترونیکی واحدهایی هستند که برای ارائه‌ی خدمات صدور امضای الکترونیکی در کشور تأسیس می‌شوند. این خدمات شامل تولید، صدور، ذخیره، ارسال، تأیید، ابطال و به روز نگهداری گواهی‌های اصالت (امضای) الکترونیکی می‌باشد. بعبارتی دفاتر مزبور بعنوان مرجع ثالثی، اعتبار پیام را از طریق تعیین هویت امضا کننده دیجیتال تضمین می کند. قانون تجارت الکترونیکی ایران مصوب ۱۳۸۲، قانون نمونه امضای الکترونیکی آنسیترال مصوب ۲۰۰۱، دستورالعمل اتحادیه اروپا در زمینه امضای الکترونیکی مصوب ۱۹۹۹ و قانون شماره ۲۳۰ – ۲۰۰۰ مورخ ۱۳ مارس ۲۰۰۰ فرانسه و آئین نامه های شماره ۲۷۲ – ۲۰۰۱ مورخ ۳۰ مارس ۲۰۰۱ و شماره ۹۷۳ – ۲۰۰۵ مورخ ۱۰ اوت ۲۰۰۵ دولت فرانسه از مهمترین قوانین ملی و بین المللی در زمینه حقوق امضای الکترونیکی می باشند.

کلید واژه:

امضای الکترونیکی، امضای دیجیتال، امضای الکترونیکی ساده، امضای الکترونیکی مطمئن

تاریخچه امضای الکترونیکی

گسترش تجارت الکترونیکی و رشد روزافزون آن مستلزم ایجاد اطمینان و اعتماد در افکار عمومی نسبت به این نوع از تجارت می باشد و این اطمینان بایستی از طریق تضمین امنیت و اعتبار تبادل الکترونیکی داده ها صورت گیرد، تبعاً در این میان آنچه بعنوان عاملی اصلی درخصوص صحت انتساب سند به صادر کنندهٔ آن نقش مهمی را ایفا می نماید به طور معمول امضاء و مهر درج شده در ذیل سند است، در این قسمت لازم است ابتدا در خصوص تاریخچه ی امضای الکترونیکی توضیحاتی بیان گردند:

در سال ۱۹۹۶میلادی کمیسیون حقوق تجارت بین الملل سازمان ملل متحد (آنسیترال) قانون نمونه ای در باب تجارت الکترونیکی تدوین کرد، در ماده ۷ این قانون نمونه، امضای واجد شرایط الکترونیکی دارای همان آثار و ارزش اثباتی امضای سنتی شناخته شد.

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.

مقدمه

امضاء بخش مهمی از شخصیت و اعتبار حقوقی، تجاری و حتی هنری اشخاص است و برای اعتبار بخشیدن به مهمترین اسناد بین المللی تا یک کارت تبریک وجود آن ضروری است. امضای یک سند مهمترین دلیل انتساب مفاد سند به ممضی و نشان دهنده پذیرش و قبول محتویات و مندرجات سند توسط متعاملینی است که ذیل آن را با رضایت امضاء کرده اند. بنابراین وجه مشترک اسناد اعم از رسمی یا عادی، تجاری یا غیرتجاری، عقود یا ایقاع و حتی نامه های دوستانه، وجود امضاء است. همچنین به فراخور پیشرفت علم و بهره مندی از تکنولوژی و تحولات ناشی از ظهور پدیده های نوین الکترونیکی، امضاء نیز دستخوش تحول گردید و امروزه به اشکال نوین و الکترونیکی قابل صدور است. با اینحال هرچند بهره مندی از دستاوردهای امضای الکترونیکی، مرهون زحمات متخصصین علوم کامپیوتری، فناوری اطلاعات و ارتباطات است، ولی مطابق هرپدیده نوظهور اجتماعی آثار حقوقی آن دخالت و حضور حقوقدانان را اجتناب ناپذیر می سازد. به همین دلیل است که توجه روز افزون به مفهوم این نوع از امضاء به حدی رسیده است که تمامی قانونگذاران ملی و بین المللی را وادار ساخته حساسیتی ویژه به آن داشته باشند و در کنار تصویب مقررات تجارت الکترونیکی، به وضع قوانین ویژه ای برای امضای الکترونیکی مبادرت ورزند.

به طور کلی آنچه در هر شاخه ای از علوم مهمتر از فرضیه بنظر می رسد، طرح پرسش هایی است که با پاسخگویی به آنها بستر مطالعه و تحقیقات بعدی فراهم شده و برای ذهن پرسشگر هر محققّی، دریچه ای جدید رو به افق تحقیقاتی در آن حوزه می گشاید. پاره ای از سوالات مطرح در زمینه حقوق امضای الکترونیکی به شرح ذیل می باشد:

- ماهیت امضای الکترونیکی چیست ؟
- انواع امضای الکترونیکی کدامند؟ وجوه افتراقی بین آنها چیست؟ و بنا به تفکیک میزان اعتباردهی هریک از انواع امضای الکترونیکی، به اسناد تنظیمی، چه میزان است؟
- وجوه افتراقی در تعاریف امضای الکترونیکی در حقوق ایران و سایر نظامهای حقوقی چیست ؟
- قوانین ناظر بر موضوع امضای الکترونیکی در حال حاضر کدامند؟
- نقش و جایگاه دفاتر صدور گواهی امضای الکترونیکی در تثبیت امضای مطمئن یا پیشرفته چیست ؟

کلیات امضاء

مطابق لغتنامه دهخدا امضاء واژه ای عربی است از ریشه «مضی» به معنای روان کردن، فرمان، اجرا کردن، عمل کردن است فرهنگ معین نیز امضاء را به معنای گذرانیدن، جایز داشتن، نام خود را در زیر نوشته ای نوشتن و دستینه تعریف نموده است. وجه مشترک تعاریف لغوی ذکر شده، ریشه در ابراز رضایت شخص صاحب امضاء در انجام امری دارد. از نظر لغوی در متون خارجی امضاء نام، علامت یا نوشته ای است که با قصد تایید یک سند مورد استفاده قرار می گیرد. مطابق منابع فرانسوی از نظر مفهوم کلی امضاء علامتی شخصی است که در پای یک نوشته یا یک اثر می گذاریم، برای تایید و تصدیق اینکه ما بطور حتم، ایجاد کننده و خالق آن هستیم یا اینکه محتویات و مندرجات آن را تصدیق می کنیم.

با بررسی و کنکاش در منابع حقوقی ایران به این نتیجه خواهیم رسید که تعریف دقیقی از امضاء ارائه نگردیده است و شاید علت آن باشد که قانونگذار تعریف امضاء را از بدیهیات دانسته است. همین امر باعث گردیده تعریف حقوقی امضاء منبعث از منابع عرفی و با الهام گرفتن از عرف و رویه قضایی باشد. در بیان تعریف حقوقی امضاء، استاد فرهیخته دکتر جعفری لنگرودی معتقدند امضاء عبارت است از «نوشتن نام و یا نام خانوادگی یا هردو، یا رسم علامت به عنوان بیان هویت صاحب علامت در ذیل اوراق و اسناد برای تایید متن سند که نوشته شده است و یا بعد از امضاء نوشته خواهد شد» همچنین امضاء «نوشتن اسم یا اسم خانوادگی (یا هردو) یا رسم علامت خاص، که نشانه هویت صاحب علامت است در ذیل اوراق و اسناد (عادی یا رسمی) که متضمن وقوع معامله یا تعهد یا اقرار یا شهادت و مانند اینها است یا بعدا باید روی آن اوراق تعهد یا معامله ای ثبت شود» تعریف گردیده است.

استاد فقید دکتر ناصر کاتوزیان درجایی دیگر امضا را اینگونه تعریف می نماید «امضا عبارت از ترسیمی شخصی است که به طور معمول حاوی نام شخص است و دلالت بر تصمیم نهایی و رضای او می کند. به همین جهت امضاء باید در محلی قرار گیرد که در نظر عرف نشان رضایت باشد».

مطابق قانون فرانسه و تا قبل از تصویب قانون مورخ ۱۳ مارس ۲۰۰۰ از نظر حقوق این کشور، امضا نوشته ای محسوب می شد که آن با دست کسی که خود را متعهد می گرداند، صورت میگرفت.

به موجب ماده ۱۲۹۳ قانون مدنی «رکن مشترک و اساسی و پایه اعتبار اسناد عادی امضایی است که انتساب مفاد سند به امضا کننده و اراده قاطع او به صدور سند را نشان می دهد» و مستفاد از ماده ۱۲۹۱ همان قانون «نوشته وقتی علیه شخص سندیت دارد که امضاء یا اثر انگشت او ذیل سند باشد». بنابراین اعتبار اسناد ناشی از امضا و تصدیقی است که در آن درج شده است. نوشته منتسب به اشخاص در صورتی قابل استناد است که امضاء شده باشد. سند امضا نشده، ناقص بوده و فاقد مهترین رکن اعتبار می باشد، و این حقیقت مستنبط از اصول کلی حقوق و عرف مسلم است.

تعریف امضاء و جایگاه حقوقی آن

«امضاء عبارتست از نوشتن اسم یا اسم خانوادگی (یا هر دو) یا رسم علامت خاصی که نشانه هویت صاحب علامت است، در ذیل اوراق و اسناد عادی یا رسمی که متضمن وقوع معامله یا تعهد یا قرار یا شهادت و مانند آنها است یا بعداً باید روی آن اوراق تعهد یا معامله‌ای ثبت شود (سفید مهر)» قانون مدنی 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 جنبه‌های سند یا قراردادی است که امضاء شده باشد.

به طور کلی، نوشته منتسب به اشخاص در صورتی قابل استناد است که امضاء شده باشد. امضاء نشان تأیید اعلام‌های مندرج 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 درباره آن گرفته نشده است. بنابراین، هر سندی که امضاء می‌شود در واقع اعتبار می‌یابد و می‌توان آن را به شخصی منتسب نمود و وی را به مندرجات آن ملتزم ساخت.

امضای الکترونیکی

برای تعریف امضاء الکترونیکی لازم است که منابع حقوقی و مواد قانونی مصوب در ایران، کمیسیون حقوق تجارت بین الملل سازمان ملل متحد (آنسیترال)، مصوبات اتحادیه اروپا و سایر نظامات حقوقی ملی همچون فرانسه را بررسی کرده و از گذر مطالعه تطبیقی منابع مذکور به تعریفی جامع از امضای الکترونیکی دست یابیم.

قانونگذار ایران در بند «ی» ماده ۲ قانون تجارت الکترونیکی مصوب ۱۳۸۲ امضای الکترونیکی را هر نوع علامت منضم شده یا به نحو منطقی متصل شده به «داده پیام» (Data message) تعریف می کند که برای شناسائی امضاء کننده «داده پیام» مورد استفاده قرار می‌گیرد.

نقد و بررسی این تعریف از امضای الکترونیکی نیازمند بررسی مفاهیم مزبور در علوم کامپیوتر می باشد. ماده ۲ قانون مذکور امضای الکترونیکی را نوعی علامت منضم شده یا متصل شده به داده پیام می داند که کاربرد آن شناسایی امضاء کننده داده پیام می باشد. بسط این موضوع، نیازمند تبیین مفاهیمی چون داده پیام، علامت، انضمام و اتصال و کاربردهای امضاء می باشد.

در تعریف داده پیام قانونگذار در بند الف ماده مذکور بیان می دارد که «داده پیام هر نمادی از واقعه، اطلاعات یا مفهوم است که با وسایل الکترونیکی، نوری و یا فناوری‌های جدید اطلاعات تولید، ارسال، دریافت، ذخیره یا پردازش می‌شود». بنابراین مطابق تعریف ارائه شده، جنس داده پیام یکی از سه حالت زیر خواهد بود: الف–نمادی از واقعه، ب–اطلاعات، ج–مفهوم. با بررسی مبانی فناوری اطلاعات و مباحث مدیریت دانش در می یابیم که سه عبارت «نمادی از واقعه»، «اطلاعات» و «مفهوم» مندرج در قانون تجارت الکترونیکی، مطابقت معنایی با سه عبارت داده، اطلاعات، دانش در علوم مرتبط با فناوری اطلاعات، دارند، به نحوی که در چارچوب فناوری اطلاعات مفهوم واژه دانش، با واژه های داده و اطلاعات بسیار متفاوت است. در حالی که داده مجموعه ای از دانسته ها، محاسبات و آمار است و فرهنگ رایانه مایکروسافت، «داده» را یک جزء اطلاعاتی می داند. اطلاعات، داده سازمان یافته یا پردازش شده ای است که به هنگام (update) و صحیح می باشد. و واژه دانش، اطلاعاتی است که مفهومی، مرتبط و قابل اجراست .

به نظر می رسد که استفاده از عبارت «علامت» توسط قانونگذار در تعریف امضاء الکترونیکی بدلیل ذهنیتی است که در کتب حقوقدانان از تعریف کهن امضاء، که به هر نوع «علامت یا نوشته» اطلاق می شد، باشد (مظاهری کوهانستانی ۱۳۹۳، ۱۰). در صورتی که در قالب سیستم های فناوری اطلاعات، عبارت علامت یا نوشته به نظر، تعبیر صحیحی نیست، زیرا وقتی داده پیام از جنس داده و اطلاعات است و در قالب دیجیتال ارائه می شود، جنس امضای متصل و منضم به آن نیز باید در قالب دیجیتال و به صورت داده باشد. لذا به نظر می رسد که بهتر بود قانونگذار امضاء را نوعی داده متصل به داده پیام می دانست که وظیفه آن شناسایی امضاء کننده و .... می باشد. عبارت فراداده (Metadata) نیز از جمله عبارات موجود در علوم فناوری اطلاعات است. آنها داده‌هایی هستند درباره ی داده‌های دیگر که جهت توصیف آن داده ها به آن، ضمیمه می شوند.

از جمله نکات لازم به تفسیر در مورد تعریف امضاء الکترونیکی، نحوه انضمام یا اتصال منطقی امضاء به داده پیام و تفاوت این دو پدیده (اتصال و انضمام) با یکدیگر می باشد. در هیچ یک از متون حقوقی به تعریفی برای این عبارت دست نمی یابیم و باید به دنبال تعریفی از آن در علوم کامپیوتر و فناوری اطلاعات باشیم. در علوم کامپیوتر برای محاوره بین سیستم ها از وضع قراردادها و پروتکل ها و سپس ارسال داده های متصل به داده اصلی استفاده می شود. هدرها (Header) از جمله اتصالات منطقی در پایگاه های داده می باشند که در ابتدای داده اصلی قرار گرفته و حاوی مطالب تفسیری برای دریافت کننده و پایگاه داده هستند. این اتصالات را از آن رو منطقی می گویند که در سطح منطقی بر روی داده ها اعمال می شوند و در ساختار فیزیکی ذخیره سازی داده ها تغییری ایجاد نمی کنند. نکته دیگر آن که تعریف امضاء در قانون تجارت الکترونیکی ایران، صرفا به یک جنبه از آثار امضاء یعنی شناسایی امضاء کننده عنایت دارد حال آنکه اثر مهم دیگر امضاء اعلام رضایت و التزام به مفاد سند است که متاسفانه در این ماده مورد غفلت قرار گرفته است.

تعریف امضای الکترونیکی در سایر نظامات حقوقی بین المللی و ملی

از مهمترین منابع حقوقی خارجی در سطح بین المللی در مورد امضای الکترونیکی و به طور کلی حقوق اسناد الکترونیکی می توان به قانون نمونه آنسیترال راجع به تجارت الکترونیکی[۱]، قانون نمونه آنسیترال راجع به امضای الکترونیکی[۲]، کنوانسیون سازمان ملل متحد راجع به استفاده از ارتباطات الکترونیکی در قراردادهای بین المللی[۳]، دستورالعمل اتحادیه ی اروپا راجع به تجارت الکترونیکی[۴]، دستور العمل اتحادیه ی اروپا راجع به امضای الکترونیکی[۵] و قانون ۲۰۳ مورخ ۱۳ مارس ۲۰۰۰ فرانسه و آئین نامه های بعدی آن اشاره کرد.

آنسیترال

مطابق بند الف ماده ۲ قانون نمونه ی امضای الکترونیکی ۲۰۰۱ آنسیترال «امضای الکترونیکی به معنای داده ای در شکل الکترونیکی است که چسبیده یا به طور منطقی به یک داده پیام متصل شده است و می تواند برای شناسایی هویت امضاء کننده در ارتباط با داده پیام و یا نشان دادن رضایت امضاءکننده نسبت به اطلاعات موجود در داده پیام مورد استفاده قرار گیرد»

همین قانون در تعریف داده پیام در بند ج ماده ۲ مقرر می دارد «داده پیام عبارت است از اطلاعاتی که با وسایل الکترونیکی، نوری یا مشابه از جمله مبادله الکترونیکی داده ها، پست الکترونیکی، تلگراف، تلکس، تلکوپی، تولید، ارسال یا دریافت و یا ذخیره می شود و از طرف خود یا کسی که از جانب او نمایندگی دارد عمل می کند»

مهمترین نکته در تعریف مزبور، این است که امضای الکترونیکی به عنوان «داده» مطرح می شود و این تعریف مبین ماهیت فنی و جنس حقیقی و منطقی امضاست. ضمنا برخلاف تعریف امضاء الکترونیکی در حقوق ایران که در آن صرفا به جنبه شناسایی هویت امضاء کننده از طریق صدور امضای الکترونیکی به عنوان تنها آثار و کاربرد امضا اشاره شده است، در مصوبه آنسیترال دو کارکرد شناسایی هویت امضاءکننده و نشان دادن رضایت شخص ممضی نسبت به اطلاعات موجود در داده پیام (سند الکترونیکی یا قرارداد الکترونیکی) برای امضای الکترونیکی احصا شده است.

از نکات مهم مرتبط با حقوق امضای الکترونیکی از منظر مصوبات آنسیترال، می توان گفت که مطابق قانون نمونه تجارت الکترونیکی مصوب ۱۹۹۶، آن دسته از اسناد و مدارک الکترونیکی که کارکردهای اسناد کاغذی را احراز می کنند، از نظر حقوقی معتبرند. عمده این کارکردها عبارتند از : شناسایی شخص امضاء کننده، ایجاد قطعیت در دخالت شخص مذکور در تولید امضاء، ایجاد ارتباط بین شخص مذکور و محتوای سند، نشان دهنده رضایت فرد امضاء کننده نسبت به محتوای سند است.

بررسی تطبیقی حقوق ایـران، فرانسـه، دسـتورالعمل اتحادیـه حقـوق اروپـا مقـررات آنسـیترال در مورد امضای الکترونیکی

قـانون نمونـه آنسـیترال، فرانسـه و دسـتورالعمل اتحادیـه اروپـا بـا معرفـی امضـای الکترونیکـی بـه عنـوان «داده»، مناسـب تـر از قوانین داخلی عمل نموده اسـت. زیـرا همـانطور کـه اشـاره شـد، نظـر بـه تعریـف امضـای الکترونیکـی، واژه علامـت بکـار رفتـه در قانون تجارت الکترونیکی ایران چندان صحیح به نظر نمی رسد.

در اکثر نظام های حقوقی دنیا، برای امضـاء دو کـارکرد اساسـی مطـرح شـده اسـت: اول اینکـه هویـت کسـی کـه سـند از طـرف او صادر شده است را مشخص مـی نمایـد و دوم آنکـه اصـالت محتـوای سـند و آثـار حقـوقی آن را ثابـت مـی کنـد. قـانون آنسـیترال نیز به دو کارکرد امضاء یعنی؛ شناسایی هویـت امضـاء کننـده و رضـایت وی بـه مفـاد سـند توجـه کـرده اسـت امـا در قـانون ایـران به رضایت امضاءکننده نسبت به مفاد سـند توجـه نشـده و تنهـا بـه شناسـایی امضـاءکننده اشـاره شـده اسـت. بنـابراین شایسـته تـر این بود که قانونگذار ایران برای تکمیل تعریف خود، قصد التزام امضاء کننده به مفاد سند را متذکر می شد.

متون قانون فرانسه ساختاری را می سازند که مبتنـی بـر فـرض صـحت بـوده و پـیش بینـی ایـن فـرض خـود متفـاوت بـا سیسـتم اتحادیه اروپا می باشد و به نوعی امتیازی برای قانونگذار فرانسه محسوب می گردد.

برخلاف دسـتورالعمل اروپـا، کـه مسـائل فنـی امضـای الکترونیکـی را نیـز بیـان نمـوده، قـانون ۱۳ مـارس ۲۰۰۰ فرانسـه در مـورد تطبیق حقوق ادله با فنـاوری هـای اطلاعـات و مـرتبط بـا امضـای الکترونیکـی – کـه قـانون مـدنی فرانسـه را کامـل نمـود – وارد هیچ ملاحظه فنی نشده است.

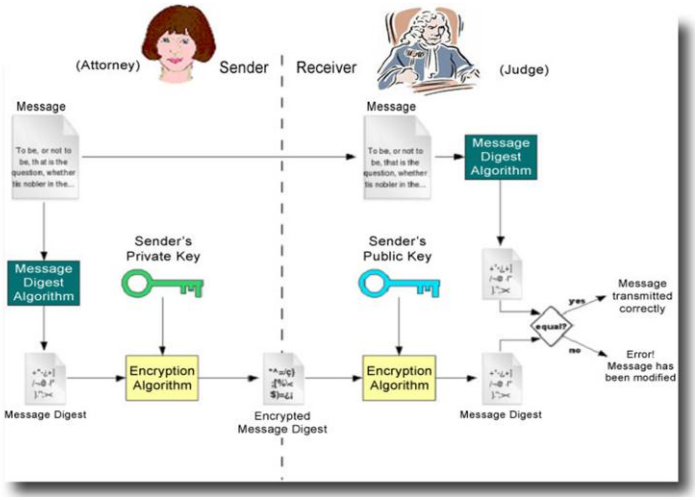
از برآیند همه تعاریف ذکرشـده مـی تـوان نکـات ذیـل را اسـتنباط نمـوده و در تعریـف امضـای الکترونیکـی بایـد مـورد توجـه قـرار داد:

اولا امضـای الکترونیکـی یـک داده الکترونیکـی اسـت کـه بـه یـک داده الکترونیکـی دیگـر (سـند یـا قـرارداد) متصـل مـی شـود. ثانیا؛ امضای ذیل سند توسط خود شخص و یـا بـه دسـتور او انجـام مـی گیـرد، بـرای شناسـایی شـخص امضـا کننـده بـه کـار مـی رود. ثالثـا؛ تصـدیق محتـوای سـند و اعطـای اثـر حقـوقی بـه آن یکـی دیگـر از کارکردهـای امضـای الکترونیکـی اسـت کـه بایـد مورد توجه قرار گیرد.

رابعا؛ امضا اعم از الکترونیکی یا دستی واجـد یـک عنصـر معنـوی بنـام قصـد التـزام بـه مفـاد سـند بایـد باشـد. ایـن همـان چیـزی است که در واقع به یک امضاء اثر حقوقی می بخشد.

با توجه به مطالب بیان شده به نظر می رسد می توان امضای الکترونیکی را چنین تعریف نمود:

«امضای الکترونیکی عبـارت از داده ای اسـت کـه در بسـتر الکترونیکـی و بـه قصـد التـزام بـه منـدرجات و مفـاد داده پیـام، بـه آن منضـم یـا متصـل مـی شـود و بیـانگر رضـایت ممضـی بـه مفـاد و منـدرجات آن داده پیـام بـوده و موجبـات شناسـایی ایشـان را فراهم می کند».



بررسی امضای الکترونیکی و امضای دیجیتال

امضـای دیجیتـال نـوعی از امضـای الکترونیکـی کـه از سـطح بـالایی از امنیـت نسـبت بـه سـایر انـواع امضـای الکترونیکـی برخوردار است و به عنوان موثرترین و کـاربردی تـرین وسـیله برقـراری ارتبـاط ایمـن بـین طـرفین تبـادل پیـام در محـیط مجـازی تلقی مـی گـردد. علـت ایـن اسـت کـه، در ایـن روش از فنـاوری «رمزنگـاری» (Cyptography) بـرای تولیـد امضـاء اسـتفاده مـی شـود. امضـای دیجیتـال پیشـرفته‌تـرین و پرکـاربردترین نـوع از امضـاهای الکترونیکـی اسـت و بـه دلیـل امنیـت بـالای آن جـایگزین سـایر روش‌هـای موجـود شـده و بیشـتر قانونگـذاران ـ از جملـه قانونگـذار ایـران ـ ایـن شـیوه از امضـاء را پذیرفتـه‌انـد. همـانطور کـه گفتـه شـد، امضـای دیجیتـال مبتنـی بـر علـم رمزنگـاری اسـت و از دو نـوع الگـوریتم بـه نـام‌هـای کلیـد عمـومی (public key) و کلیـد خصوصـی (private key) اسـتفاده مـی‌کنـد. رمزگـذاری یعنـی تبـدیل اطلاعـات بـه یـک شـکل غیـر قابل فهم جهت انتقـال آن بـه مقصـد و رمزگشـایی بـه معنـای برگردانـدن اطلاعـات رمـز شـده بـه حالـت اولیـه و قابـل خوانـدن. رمـز نگـاری بـه دو شـیوه متقـارن (symmetric) و نامتقـارن (asymmetric) وجـود دارد. رمزنگـاری متقـارن عبـارت است از الگـوریتم هـای رمزنگـاری کـه در آن دو شـریک تجـارتی، بـرای امضـاء و رمزنگـاری و رمزگشـایی مبادلـه ی الکترونیکـی داده ها باید از کلید واحد و یکسـانی اسـتفاده کننـد کـه الگـوریتم هـای رمزنگـاری متقـارن نامیـده مـی شـود. در ایـن روش هـر دو طرفـی کـه قصـد رد و بـدل اطلاعـات را دارنـد از یـک کلیـد مشـترک بـرای رمزگـذاری و نیـز بازگشـایی رمـز اسـتفاده مـی‌کننـد. دراین حالـت، بازگشـایی و رمزگـذاری اطلاعـات دو فرآینـد معکـوس یکـدیگر مـی‌باشـند. بنـابراین یـک الگـوریتم متقـارن از یـک کلید هم برای رمزنگاری و هم بـرای رمزگشـایی اسـتفاده مـی‌کنـد. در رمزنگـاری نامتقـارن بـه جـای یـک کلیـد مشـترک، از یـک زوج کلیـد بـه نـام‌هـای کلیـد عمـومی و کلیـد خصوصـی اسـتفاده مـی‌شـود. کلیـد عمـومی مشـترک بـین طـرفین اسـت و کلیـد خصوصی به صورت محرمانه توسط هر یک از طرفین حفظ می شود. معروف ترین نوع این الگوریتم RSA می باشد.

انواع امضای الکترونیک:

تاکنون، روش‌های متفاوتی در خصوص چگونگی انجام امضای الکترونیک معرفی و به کار گرفته شده که هر کدام ضریب امنیت و موارد کاربرد مخصوص به خود را دارند که به آن اشاره می‌کنیم:

گذرواژه‌ها :در این روش ساده و رایج، از یک گذر واژهٔ منحصر به فرد با استفاده از یک شماره هویت شخصی در انتهای اسناد استفاده می‌شود که امنیت آن بسیار پایین است و به راحتی توسط نفوذگرها شناسایی شده و به سرقت می‌رود.

امضای بیت مپ :این نوع امضاء با استفاده از اسکن امضای دست‌نویس افراد که شخص روی کاغذ امضا می‌کند، بدست می‌آید و سپس شخص این اسکن را به‌عنوان امضاء به هر داده پیامی ضمیمه می‌کند.

قلم نوری :در این نوع فناوری، فرد با این قلم بر روی صفحهٔ مخصوص دیجیتالی امضا می‌کند و همان امضاء روی نمایشگر رایانه پدیدار می‌شود؛ درواقع چیزی شبیه اینکه فرد در صفحهٔ مانیتور امضاء می‌کند اتفاق می‌افتد. این روش ساده نیز امنیت بالایی ندارد و امکان جعل آن زیاد است.

امضای بیومتریک :در این روش با استفاده از مؤلفه‌های فردی از قبیل خصوصیات رفتاری همانند نحوهٔ انجام امضای دست‌نویس و خصوصیات فیزیولوژیک همانند اثرانگشت، امضای بیومتریک حاصل می‌شود. مشکل اساسی این روش در این است که علی‌رغم منحصر به فرد بودن، با افزایش سن افراد، بیماری و ... امضای بیومتریک افراد ممکن است تغییر کند و می‌توان گفت این امضا نیز مصون از اشتباه نیست.

امضای دیجیتال :امضای دیجیتال بهترین و پیشرفته‌ترین و پرکاربردترین نوع از امضاهای الکترونیک است که به دلیل امنیت بالای آن، جایگزین سایر روش‌های موجود شده و اکثر قانون‌گذاران از جمله قانونگذاران تجارت الکترونیک ایران که مرکز توسعه تجارت الکترونیک می‌باشد، این شیوه امضا را پذیرفته است

امضای الکترونیکی ساده و امضای الکترونیکی مطمئن

با بررسی تطبیقی ماهیت فنی و حقوقی امضای الکترونیکی به دو سطح مختلف از امضای الکترونیکی رسیده و در می یابیم که این پدیده حقوقی به دو دسته امضای الکترونیکی ساده و امضای الکترونیکی مطمئن تقسیم شده است. در حقوق اروپا امضای الکترونیکی به دو دسته امضای الکترونیکی ساده و امضای الکترونیکی پیشرفته تقسیم می شود. قانون مدنی فرانسه تفاوتی بین امضای الکترونیکی ساده و مطمئن قائل نشده است، ولی شورای دولتی فرانسه که ماموریت نحوه تعیین هویت امضا کننده و نیز تضمین سند به آن واگذار شده (ماده ۴-۱۳۱۶) در آئین نامه ۲۷۲-۲۰۰۱، بین امضای الکترونیکی ساده و امضای الکترونیکی مطمئن تفاوت قائل شد

در ماده ۲-۲ دستورالعمل اروپا، امضای الکترونیکی پیشرفته دارای شرایط و ویژگی های ذیل است؛ باید:

- منحصرا متعلق به امضاء کننده باشد.
- امکان شناسایی و تشخیص هویت امضاء کننده را فراهم سازد.
- به وسیله ابزاری ایجاد شود که منحصرا تحت کنترل امضاء کننده باشد.
- به گونه ای به داده های مربوطه متصل و منضم شود که هر نوع تغییر بعدی در داده پیام، قابل شناسایی و ردیابی باشد.

در حقوق فرانسه، فراز دوم از ماده یک آئین نامه ۳۰ مارس ۲۰۰۱ در خصوص امضای الکترونیکی مطمئن بیان می دارد:

«...۲ـ "امضای الکترونیکی مطمئن": امضایی الکترونیکی است که علاوه بر (تعریف فوق‌الذکر) الزامات و شرایط ذیل را نیز دربرمی‌گیرد. این الزامات و شرایط عبارتند از اینکه امضای الکترونیکی باید:

الف – مختص به امضاء کننده باشد؛

ب– امکان شناسایی و تشخیص هویت امضاء کننده را فراهم آورد؛

ج– به وسیله ابزاری ایجاد شود که امضاء کننده بتواند آن را در کنترل انحصاری خود داشته باشد؛

دـ رابطه‌اش را با سندی که به آن منضم می‌شود تضمین کند، به نحوی که هر تغییر بعدی (بعد از امضای سند و انضمام امضای الکترونیکی) (کی نیا ۱۳۸۸: ۶۰) در سند قابل تشخیص باشد»

بنابراین مطابق حقوق فرانسه و برابر ماده ۱ آئین نامه شورای دولتی فرانسه امضای الکترونیکی ساده عبارت است از به کارگیری رویه قابل اعتماد در تعیین هویت است که رابطه اش را با سندی که به آن منظم است تضمین می کند. در مقابل امضای الکترونیکی مطمئن، امضایی است که علاوه بر دارا بودن شرایط امضای الکترونیکی(ساده)، باید اولا توسط روشهایی ایجاد شود که در کنترل انحصاری امضا کننده باشد و ثانیا رابطه امضا را با سندی که منضم به آن است تضمین کند، به نحوی که هرگونه تغییر بعدی در سند قابل کشف باشد. در حقوق ایران، ماده ۱۰ قانون تجارت الکترونیکی ایران که ناظر به بند ک ماده ی ۲ همان قانون است، در تعریف امضای الکترونیکی مطمئن مقرر می دارد: «امضای الکترونیکی مطمئن باید دارای شرایط زیر باشد:

الف- نسبت به امضا کننده منحصر به فرد باشد. ب- هویت امضا کننده داده پیام را معلوم کند. ج- به وسیله ی امضاءکننده و یا تحت اراده ی 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».

در بند ۳ ماده ی ۶ قانون نمونه آنسیترال (۲۰۰۱) نیز آمده است:

«امضای الکترونیکی قابل اعتماد باید دارای شرایط زیر باشد:

الف- داده ی ایجاد امضاء به همراه مطلبی که در آن امضا مورد استفاده قرار می گیرد، مرتبط با شخص امضاء کننده باشد و نه فرد دیگری؛ ب- داده ی ایجاد امضاء، تحت کنترل امضاء کننده باشد و نه فرد دیگری؛ ج- هرگونه تغییری در امضاء، بعد از زمان امضاء، قابل کشف باشد؛ د- در جایی که هدف از امضاء حصول اطمینان در خصوص اصالت اطلاعات مرتبط با امضاء است، هرگونه تغییری در اطلاعات بعد از امضاء، قابل کشف باشد»

در بررسی فنی میان انواع مختلف امضای الکترونیکی، می توان گفت که تنها امضای دیجیتال است که در دسته امضای الکترونیکی مطمئن قرار گرفته و مابقی را می توان امضای الکترونیکی ساده دانست. منحصر به فرد بودن و تحت کنترل انحصاری بودن کلید خصوصی، امکان بررسی تغییرات بعدی در امضاء و اطلاعات مندرج در داده پیام با کمک کلید عمومی، که همگی از شرایط تحقق امضای الکترونیکی مطمئن است، از طریق امضای دیجیتال امکان پذیر است. بنابراین به عنوان نتیجه کلی می توان گفت: امضای دیجیتال در میان انواع دیگر امضای الکترونیکی (گذر واژه، بیومتریک، قلم نوری و ....) از شرایط امضای الکترونیکی مطمئن برخوردار است. و آثار حقوقی از جمله برابری کارکرد با امضا دست نویس بر آن مترتب می شود.

مراجع گواهی امضاء الکترونیکی

با استفاده از روش امضای دیجیتال یا امضای مبتنی بر رمزنگاری نامتقارن تمامیت سند، محرمانه بودن اطلاعات(در صورت لزوم) و امنیت داده ها تضمین می شود؛ اما یک مساله مهم حل نشده باقی می ماند و آن، تضمین هویت امضا کننده است. در واقع به لحاظ حقوقی، مهمترین اثر امضاء اثبات رابطه سند با کسی است که امضاء به او نسبت داده شده است. (زرکلام ۴۰:۱۳۸۲) امضای الکترونیکی مطمئن یا دیجیتال به تنهایی قادر به تضمین هویت امضا کننده نیست. بنابراین مرجع ثالثی باید اعتبار پیام را از طریق تعیین هویت امضا کننده دیجیتال تضمین کند. در همین راستا و در تایید ضرورت تضمین هویت امضاکنندگان ماده ۱۶ قانون تجارت الکترونیکی کشورمان مقرر می دارد: «هر داده پیامی که توسط شخص ثالث مطابق ماده (۱۱) این قانون ثبت و نگهداری می شود، مقرون به صحت است». بنابراین صحت انتساب داده پیام مطمئن و امضای الکترونیکی مطمئن به فرد صادر کننده آن و لزوم تصدیق آن از سوی مرجع ثالث و صالح رسمی، امری است که اهمیت آن غیرقابل انکار است.

ایـن مرجـع ثالـث در قـانون تجـارت الکترونیکـی و قـانون نمونـه امضـای الکترونیکـی آنسـیترال (۲۰۰۱) اصـطلاحا «دفـاتر خـدمات صـدور گـواهی الکترونیکـی» یـا «دفـاتر خـدمات الکترونیکـی» یـا «مراجـع گـواهی» نامیـده مـی شـود. مطـابق مـاده ۳۱ قانون تجارت الکترونیکی ایران: «دفـاتر خـدمات صـدور گـواهی الکترونیکـی واحـدهایی هسـتند کـه بـرای ارائـه‌ی خـدمات صـدور امضـای الکترونیکـی در کشـور تأسـیس مـی‌شـوند. ایـن خـدمات شـامل تولیـد، صـدور، ذخیـره، ارسـال، تأییـد، ابطـال و بـه روز نگهـداری گـواهی‌هـای اصـالت (امضـای) الکترونیکـی مـی‌باشـد.» مـاده ۲ (هـــ) قـانون نمونـه امضـای الکترونیکـی آنسـیترال (۲۰۰۱) در تعریـف ایـن دفـاتر آورده اسـت: «دفتـر خـدمات صـدور گـواهی الکترونیکـی عبـارت از شخصـی اسـت کـه اقـدام بـه صدور گواهی می کند و امکان دارد خـدمات دیگـری در ارتبـاط بـا امضـای الکترونیکـی ارائـه دهـد.» در حقـوق فرانسـه نیـز دفـاتر خدمات الکترونیکی بعنوان تضمین کننـده هویـت امضـاءکننده پـیش بینـی شـده اسـت بنـابراین وظیفـه دفـاتر گـواهی الکترونیکـی تعیـین هویـت امضـاءکننده و نتیجتـا سـندیت بخشـیدن بـه اطلاعـات الکترونیکـی اسـت. در واقـع، گـواهی دیجیتـال کـه توسـط دفـاتر خـدمات الکترونیکـی صـادر مـی شـود، هویـت امضـا کننـده را از طریـق کنتـرل رابطـه بـین کلیـد عمـومی و دارنـده کلیـد خصوصی مربوط تضمین مـی کنـد. همـانطور کـه مـی دانیـد امضـای دیجیتـال دارای دو جـز متفـاوت، امـا از نظـر ریاضـی مـرتبط است. کلیـد خصوصـی کـه در اختیـار صـاحب امضـا اسـت و کلیـد عمـومی کـه در فهرسـت مرجـع گـواهی قـرار دارد. ایـن مرجـع تضمین می کند که کلید عمومی مسـتقر در فهرسـت بـه درسـتی اعـلام و ایجـاد شـده اسـت؛ زیـرا هویـت دارنـده کلیـد خصوصـی که منطبق با کلید عمومی اسـت نـزد مرجـع گـواهی وجـود دارد. بـرای اطمینـان از اینکـه داده پیـام از سـوی کسـی کـه ادعـا مـی کنـد صـادر شـده، وجـود کلیـد عمـومی ضـروری اسـت. در واقـع، مرجـع گـواهی دو وظیفـه مهـم دارد: اول تخصـیص یـک کلیـد خصوصی به دارنـده و ثبـت آن بـه عنـوان یـک مسـتند اطلاعـاتی؛ دوم نگهـداری کلیـد مکمـل آن بـه عنـوان کلیـد عمـومی و در دسترس قرار دادن فهرست نام دارندگان کلید عمومی از طریق سیستم درون خطی و بانکهای اطلاعاتی ویژه.

بـرای ثبـت امضـای الکترونیکـی در ایـران، شـخص امضـاء کننـده بایـد بـرای شناسـایی هـویتش بـه صـورت حضـوری بـه دفـاتر گواهی امضای الکترونیکی مراجعـه نمایـد، البتـه ایـن شـرط در قـانون ذکـر نشـده اسـت و علـت آن نیـز شـاید بـدیهی بـودن ایـن امر بوده اسـت، چـون در صـورتی کـه شـخص نـزد دفـاتر بـرای ثبـت امضـای الکترونیکـی حاضـر نشـود، امضـایش نیـز از اعتبـار برخـوردار نخواهـد بـود، همـانطور کـه ذکـر شـد، علـت مراجعـه حضـوری شـخص، صـرفا بـرای تشـخیص هویـت مـی باشـد نـه امضای اسناد و مدارک خاصی کـه تـا امکـان صـدور امضـای الکترونیکـی را امکـان پـذیر نمایـد، چـون فـرد، قبـل از ثبـت امضـاء، اسناد و مدارک لازم را در دفتر صدور امضای الکترونیکی تکمیل کرده است.

مزایای امضای الکترونیکی

۱- تسریع در امضای قرارداد و اسناد در هر نقطه ای از جهان بدون حضور فیزیکی و امکان پردازش مبادلات مالی بیشتر در تمامی کشورها.
۲- کاهش هزینه های 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 لحظه ای قیمت ها.
۴- مدیریت دریافت و جابجایی پول یا ارز در بانکهای داخلی و خارجی.
۵- امضای الکترونیکی بیمه نامه ها 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 داده ها 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 هویت یک پیغام یا سند و یا فایل اطلاعاتی را تضمین میکند.
۱۲- امضای الکترونیکی منحصر به فرد بودن و تمامیت امنیت و هویت داده ها برای مراجع قضایی با اطمینان قابل پذیرش است.
۱۳- امضای الکترونیکی به راحتی قابل جابجایی است و شخص دیگری نمی تواند آن را محدود کند.
۱۴- امضای الکترونیکی دارای آثار حقوقی همسان با امضای دستی است.

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 می تواند 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 مقصد وجود دارد.

در اتوماسیون اداری امضای نامه‌ها چگونه انجام می‌شود؟

در تعریف یک نامه اداری چند پارامتر اساسی وجود دارد که شاید مهم‌ترین آن‌ها وجود امضا بر روی نامه باشد بطوریکه اگر نامه‌ای بدون امضا باشد به هیچ عنوان در گردش مستندات و نامه‌های اداری سندیت نداشته و از اعتبار لازم برخوردار نخواهد بود. لازم است به این نکته اشاره کنیم که در مسیر ایجاد یک نامه از مرحله پیش‌نویس تا ثبت نامه و دریافت شماره اندیکاتور بنا به سیاست سازمان، نامه می‌تواند بیش از یک امضاکننده هم داشته باشد. در سازمان‌هایی مانند بانک‌ها مرسوم است که یک نامه را دو یا حتی سه امضاکننده، امضا کنند.

درصورتیکه بنا به سیاست سازمان، برای صدور نامه، بیش از یک امضا لازم باشد، امضای هرکدام از امضاکنندگان نسبت به یکدیگر تقدم و تأخر دارد. یعنی ابتدا باید امضاکننده اول نامه را امضا نموده و سپس امضاکنندگان بعدی نسبت به امضای نامه اقدام نمایند.

در نرم‌افزارهای اتوماسیون اداری استاندارد، باید قابلیت تعریف امضاکننده یا امضاکنندگان و تعیین سطوح پیش‌نیاز برای امضای نامه‌ها فراهم باشد.

با ذکر این مقدمه به روش‌های امضای نامه‌ها در سیستم‌های اتوماسیون اداری می‌پردازیم.

معمولاً در نرم‌افزارهای اتوماسیون اداری دو مفهوم برای امضای یک نامه در نظر گرفته می‌شود که به شرح هر دوی آنها می‌پردازیم.

امضای تصویری

امضای دیجیتال

امضای تصویری در اتوماسیون اداری

برای هر کاربرِ صاحب امضا در نرم‌افزار اتوماسیون اداری، ضروری است یک تصویر امضا در هنگام «تعریف مشخصات کاربر» تعریف شود. این تصویر امضا معمولاً در قالب فرمت‌هایی مانند png یا jpg به همراه سایز مشخصی است که پس از ثبت نهایی نامه، با درج خودکار در محل مشخص‌شده در متن نامه، با بهترین کیفیت و گرافیک در هنگام چاپ قابل مشاهده است.

استفاده از این امکان در سیستم‌های اتوماسیون اداری فرآیند امضای نامه را سرعت خواهد بخشید. البته ممکن است در سازمان یا اداره‌ای با توجه به این مهم که حتماً باید امضای اصل بر روی نامه درج گردد، یا با توجه به شرایط ویژه یک نامه، از امکان درج تصویر امضا توسط نرم‌افزار استفاده نشود و نامه‌های ایجاد شده در سیستم، برای درج امضای واقعی نزد صاحب امضا برده شود.

امضای دیجیتال در اتوماسیون اداری

و اما مفهوم دوم که درواقع همان امضای دیجیتال بوده هنوز هم در بعضی موارد با مفهوم اول یعنی تصویر امضا تداخل معنی پیدا می‌کند درصورتی‌که کاملاً با آن متفاوت است.

در سیستمهای اتوماسیون اداری برای احراز و اطمینان از اصل بودن هویت امضاکننده نامه، امکاناتی وجود دارد که معمول‌ترین آن پشتیبانی از توکن سخت‌افزاری است.

توکن سخت‌افزاری مانند یک USB عمل می‌کند بطوریکه قابلیت ذخیره‌سازی اطلاعات را دارد و دقیقاً مشابه همان به پورت کامپیوتر یا لپ تاپ کاربر متصل میشود.

در نرم‌افزارهای اتوماسیون اداری، کاربرِ دارای مجوز امضای دیجیتال، یک توکن سخت‌افزاری حاوی کلید خصوصی دارد که صرفاً مختص به خود اوست. به هنگام امضای سند، کاربر توکن سخت‌افزاری خود را به پورت USB کامپیوتر خود متصل می‌کند و سند مذکور با استفاده از کلید خصوصی کاربر که در توکن ذخیره‌شده است، امضاء خواهد شد.

قبل از امضاء کردن، نرم‌افزار با مکانیزم خاصی مانند بررسی کدملی و یا شماره سریال توکن، از تعلق توکن به کاربر موردنظر اطمینان حاصل می‌کند و سپس به وی اجازه امضاء کردن را می‌دهد. در این حالت کاربر بعد از اتصال توکن شخصی خود صرفاً می‌تواند تصویر امضای خود را در زیر نامه درج نماید و بدیهی است که اگر امضاکننده، این توکن را در اختیار نداشته باشد، نرم‌افزار امکان درج تصویر امضای او را نمیدهد.

البته به دلیل کاربرد بسیار زیاد توکن‌های سخت‌افزاری صرفاً از آنها برای درج امضا در نامه استفاده نمی‌شود و در سیستم‌های اتوماسیون اداری کاربردهای مختلف و دیگری نیز خواهند داشت .

نتیجه گیری

از مجموع مطالب فوق بدست می آید که، امضای الکترونیکی عبارت از داده ای است که در بستر الکترونیکی و به قصد التزام به مندرجات و مفاد داده پیام، به آن منضم یا متصل می شود و بیانگر رضایت ممضی به مفاد و مندرجات آن داده پیام بوده و موجبات شناسایی ایشان را فراهم می کند. امضاء صرف نظر از شکل و نحوه ایجاد آن (دستی یا الکترونیکی) از کارکرد یکسان و مشابه برخوردار است. و بعبارتی دیگر دارای هم ارزی عملکردی می باشد. ضمنا قانون نمونه آنسیترال، فرانسه و دستورالعمل اتحادیه اروپا با معرفی امضای الکترونیکی به عنوان «داده»، مناسب تر از قوانین داخلی عمل نموده است. زیرا همانطور که اشاره شد، نظر به تعریف امضای الکترونیکی، واژه علامت بکار رفته در قانون تجارت الکترونیکی ایران چندان صحیح به نظر نمی رسد.

همچنین در اکثر نظام های حقوقی دنیا، برای امضاء دو کارکرد اساسی مطرح شده است: اول اینکه هویت کسی که سند از طرف او صادر شده است را مشخص می نماید و دوم آنکه اصالت محتوای سند و آثار حقوقی آن را ثابت می کند. اما در قانون ایران به رضایت امضاءکننده نسبت به مفاد سند توجه نشده و تنها به شناسایی امضاءکننده اشاره شده است. بنابراین شایسته تر این بود که قانونگذار ایران برای تکمیل تعریف خود، قصد التزام امضاء کننده به مفاد سند را متذکر می شد.

دیگر آنکه امضای دیجیتال پیشرفته‌ترین و پرکاربردترین نوع از امضاهای الکترونیکی است و مبتنی بر علم رمزنگاری است و از دو نوع الگوریتم به نام‌های کلید عمومی و کلید خصوصی استفاده می‌کند.

امضای الکترونیکی مطمئن امضایی است که دارای ضریب بالایی از اطمینان بوده و نشانگر متعلق بودن شخص مورد نظر می باشد. امضای الکترونیکی ساده عبارت از هر نوع داده منضم شده یا به نحو منطقی متصل شده به داده پیام است و فاقد شرایط خاص امضای الکترونیکی مطمئن است.

دیگر آنکه، مسئولیت اصلی دفاتر خدمات گواهی الکترونیکی اصالت سنجی هویت اشخاص متقاضی، ارائه کلیدهای امضای الکترونیکی و تصدیق اصالت هویت اشخاص و تصدیق امضای الکترونیکی آن ها می باشد.

منابع

الف – فارسی

۱. اصغرزاده بناب، مصطفی ، ۱۳۹۱، حقوق ثبت کاربردی جلد دوم (دعاوی و اعتراضات ثبتی مربوط به اسناد و آیین رسیدگی به آنها)، تهران، انتشارات مجد

۲. توربان، افرایم و همکاران(نوبسنده)، ریاحی، حمیدرضا و همکاران (مترجم)، ۱۳۸۶، فناوری اطلاعات در مدیریت: دگرگونی سازمان ها در اقتصاد دیجیتالی)جلد دوم)، تهران، انتشارات پیام نور

۳. جعفری لنگرودی، محمد جعفر، ۱۳۷۷، ترمینولوژی حقوق، تهران، نشر گنج دانش

۴. جعفری لنگرودی، محمد جعفر، ۱۳۸۱، مبسوط در ترمینولوژی حقوق (جلد اول)، تهران، نشر گنج دانش

۵. دهخدا، علی اکبر، ۱۳۸۵، فرهنگ متوسط دهخدا، تهران، موسسه انتشارات و چاپ دانشگاه تهران

۶. زرکلام، ستار، ۱۳۸۲، امضای الکترونیکی و جایگاه آن در نظام ادله اثبات دعوی. مجله مدرس، شماره ۱

۷. قانون تجارت الکترونیکی ایران مصوب ۱۳۸۲/۱۰/۲۴

۸. قلی زاده نوری، فرهاد، ۱۳۷۹، فرهنگ تشریحی اصطلاحات کامپیوتری مایکروسافت (ترجمه)، تهران، انتشارات کانون نشر علوم

۹. کاتوزیان، ناصر، ۱۳۸۰، اثبات و دلیل اثبات (جلد اول)، تهرات، نشر میزان

۱۰. کی نیا، محمد، ۱۳۸۸، امضای الکترونیک منطبق با حقوق فرانسه، تهران، انتشارات بنیاد حقوقی میزان

۱۱. مظاهری کوهانستانی، رسول، ناظم، رسول، ۱۳۹۳، مطالعه تطبیقی امضای الکترونیکی در حقوق ایران و مقررات آنسیترال، تهران، انتشارات جنگل

۱۲. معین، محمد، ۱۳۷۵، فرهنگ فارسی معین (جلد دوم)، تهران، انتشارات امیرکبیر

ب – لاتین

۱. DIRECTIVE ۱۹۹۹/۹۳/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of ۱۳ December ۱۹۹۹ on a Community framework for electronic signatures

۲. DIRECTIVE ۲۰۰۰/۳۱/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of ۸ June ۲۰۰۰ on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)

۳. Garner, A, Brayan. (۲۰۰۰). Black's Law Dictionary. Tehran: Dadgostar.

۴. KAINIYA, Mohammad. (۲۰۰۸).LA SIGNATURE ELECTRONIQUE, Mémoire pour le master ۲ de droit notariat. Université Jean-Moulin Lyon III

۵. KAINIYA, Mohammad.(۲۰۱۱). La dématérialisation des actes et conventions (de l'expérience francaise à sa réception par le droit iranien?), Thèse de doctorat. Université Jean-Moulin Lyon۳.

۶. La loi n° ۲۰۰۰-۲۳۰ du ۱۳ mars ۲۰۰۰ Adoptée par le Parlement français

۷. Le décret n۲۰۰۱-۲۷۲ du ۳۰ mars ۲۰۰۱ Le gouvernement français a approuvé

۸. Le décret n° ۲۰۰۵-۹۷۳ du ۱۰ août ۲۰۰۵ Le gouvernement français a approuvé

۹. UNCITRA Model Law on Electronic Commerce Guide to Enactment with ۱۹۹۶

۱۰. UNCITRAL Model Law on Electronic Signatures with Guide to Enactment ۲۰۰۱

۱۱. United Nations Convention on the Use of Electronic Communications in International Contracts