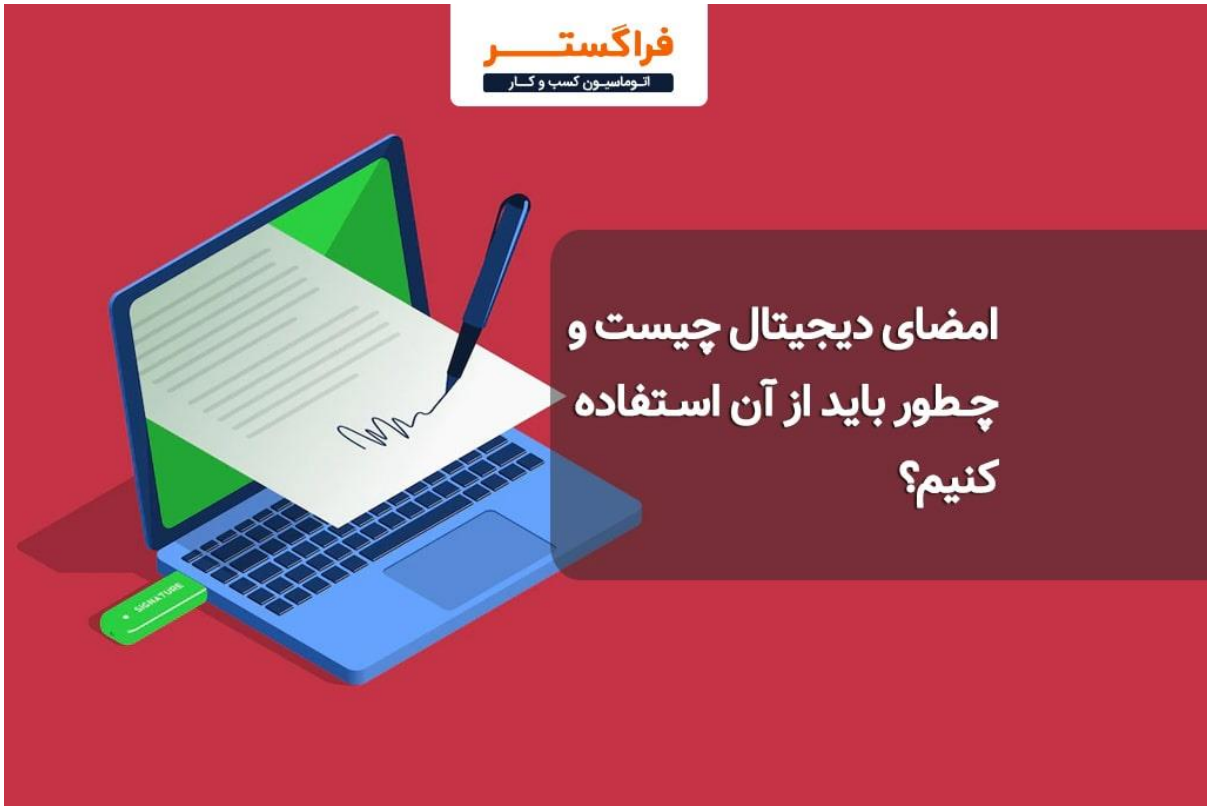
فراگستر

اتوماسیون کسب و کار

امضای دیجیتال چیست و چطور باید از آن استفاده کنیم؟

زمان تقریبی مطالعه: ۱۰ دقیقه

با رواج بیشتر تجارت الکترونیک به صورت آنلاین، بسیاری از قراردادها و تراکنش‌هایی که قبلاً روی کاغذ امضاء و به صورت فیزیکی تحویل داده می‌شدند، حالا با اسناد و گردش کارهای کاملاً دیجیتال جایگزین شده‌اند. با این حال، اسناد دیجیتال نیز از خطر دزدی یا دستکاری اطلاعات در امان نیستند. برای کاهش خطر این نوع سوءاستفاده‌ها، کسب‌وکارها به ابزارهایی نیاز دارند که بتواند اصالت و ایمنی اسناد، داده‌ها و ارتباطات حیاتی خود را تأیید و فرستنده آنها را احراز هویت کنند. ابزار رایجی که برای این منظور استفاده می‌شود، امضای دیجیتال است. در این مقاله با تعریف امضای دیجیتال و کاربردهای آن آشنا خواهید شد.



۱- امضای دیجیتال چیست؟

امضای دیجیتال دقیقاً همان چیزی است که بنظر می‌رسد و معادل مدرن و دیجیتالی امضای دست‌نویس یا مهر و موم نامه‌ها محسوب می‌شود. این نوع امضاها که مبتنی بر استانداردهای PKI هستند، از یک تکنیک ریاضی پیشرفته برای احراز هویت امضاءکننده استفاده می‌کند و تضمین می‌کنند که اسناد و پیام‌های دیجیتالی ارسال شده به صورت الکترونیکی در حین انتقال تغییر نکرده و دستکاری نشده است.

همچنین امضاءکنندگان می‌توانند از این نوع امضاء برای تأیید اسناد دیگر استفاده کنند.

امضای دیجیتال از یک نظر به نوعی شبیه به امضای فیزیکی است، زیرا هر ۲ منحصر به امضاءکننده هستند. اما تفاوت آنها این است که امضای دیجیتال امنیت بسیار بیشتری داشته و اطلاعات دیگری مانند مبدا پیام و وضعیت آن را نیز ارائه می‌دهند. امضای دیجیتال بر اساس بالاترین استانداردهای امنیتی طراحی می‌شود و در ایران و بسیاری از کشورهای دیگر از نظر قانونی الزام‌آور هستند.

۲- طرز کار امضای دیجیتال چگونه است؟

امضای دیجیتال مبتنی بر "رمزنگاری کلید عمومی" است که با عنوان رمزنگاری نامتقارن نیز شناخته می‌شود. در این نوع امضاء، با استفاده از یک الگوریتم کلید عمومی، ۲ کلید (یکی خصوصی و دیگری عمومی) تولید می‌شود که از نظر ریاضی با هم مرتبط هستند.

امضای دیجیتال از طریق ۲ کلید رمزنگاری که دارای اعتبار متقابل هستند کار می‌کنند. فردی که امضای دیجیتال را ایجاد می‌کند از یک کلید خصوصی برای رمزگذاری داده‌های مربوط به امضا استفاده می‌کند، در حالی که تنها راه برای رمزگشایی آن داده‌ها با کلید عمومی امضاءکننده است. اگر گیرنده نتواند سند را با کلید عمومی امضاءکننده باز کند، این نشانه وجود مشکلی در سند یا امضاء است. اینگونه است که امضای دیجیتال احراز هویت می‌شود.

البته فناوری امضای دیجیتال مستلزم این است که تمامی طرفین اطمینان داشته باشند که فردی که امضاء را ایجاد می‌کند، کلید خصوصی را مخفی نگه داشته است. اگر شخص دیگری به کلید امضای خصوصی دسترسی داشته باشد، می‌تواند امضاهای دیجیتالی تقلبی را به نام دارنده کلید خصوصی ایجاد کند.

۳- چگونه یک امضای دیجیتال بسازیم؟

برای ایجاد یک امضای دیجیتال، از نرم افزاری که قابلیت امضای دیجیتال دارد مانند نرم افزارهای ایمیل استفاده می‌شود. این نرم‌افزارها با استفاده از یک الگوریتم، یک هش (مجموعه‌ای از حروف و اعداد) از داده‌های الکترونیکی به عنوان یک امضاء ایجاد می‌کنند. سپس از کلید خصوصی خالق امضای دیجیتال برای رمزگذاری هش استفاده

می‌شود. این هش رمزگذاری شده – همراه با اطلاعات دیگر، مانند الگوریتم هش‌کردن – امضای دیجیتال محسوب می‌شود.

از مزایای استفاده از هش این است که هر هش منحصر به اطلاعاتی است که برای آن ساخته شده است. بنابراین کوچکترین تغییری در داده ها، حتی تغییر در یک کاراکتر، باعث ایجاد یک هش متفاوت می‌شود. این ویژگی دیگران را قادر می‌سازد تا از کلید عمومی امضاءکننده برای رمزگشایی هش و تأیید صحت داده‌ها استفاده کنند.

نحوه کار اینگونه است که کامپیوتر بر مبنای همان الگوریتم یک هش دوم برای داده ها ایجاد می‌کند. پس از رمزگشایی از هش اول، این ۲ هش با یکدیگر مقایسه می‌شوند. اگر با هم مطابقت داشته باشند، ثابت می‌کند که داده‌ها از زمان امضای آن تغییر نکرده‌اند. اگر ۲ هش مطابقت نداشته باشند، داده‌ها یا به نوعی دستکاری شده‌اند و کلید خصوصی و عمومی مربوط به امضاء با یکدیگر مطابقت ندارند.

امضای دیجیتال را می‌توان با هر نوع پیامی، خواه اصل پیام رمزگذاری شده باشد یا نه، استفاده کرد تا گیرنده بتواند از هویت فرستنده و دست نخورده ماندن پیام مطمئن شود. از سوی دیگر، امضای دیجیتال انکار امضاء را برای امضاءکننده دشوار می‌کند، زیرا امضای دیجیتال هم برای سند و هم برای امضاءکننده منحصر به فرد است و آنها را به هم پیوند می‌دهد. به این ویژگی قابلیت عدم انکار می‌گویند.

اکثر نرم افزارهای مدرن ایمیل مدرن از استفاده از امضای دیجیتال پشتیبانی می‌کنند. امضای دیجیتال همچنین به طور گسترده برای اثبات صحت، یکپارچگی داده‌ها، ارتباطات و تراکنش‌های انجام شده از طریق اینترنت استفاده می‌شود.

۴- مزایای امضای دیجیتال چیست؟

امضای دیجیتال مزایای زیادی دارد. در ادامه برخی از این مزایا آورده شده‌اند:

- امنیت: این ویژگی را می‌توان مزیت اصلی امضای دیجیتال دانست. زیرا برخلاف امضای کاغذی، قابلیت تغییر یک امضای دیجیتال ایمن وجود ندارد. در امضاهای دیجیتال از روش‌های متعددی برای حفظ امنیت استفاده می‌شود از جمله رمزهای شخصی، الگوریتم‌های رمزگذاری کلید عمومی، و روش‌های متعدد دیگر.

- اعتبار قانونی: از مزیت‌های دیگر امضای دیجیتال اعتبار قانونی است. یعنی شما می‌توانید در همه جای دنیا به آن استناد کنید. در کشور ما نیز بر اساس قانون تجارت الکترونیکی مصوب سال ۱۳۸۲، امضاء الکترونیک در نظام حقوقی ایران به رسمیت شناخته شده است و تردیدی در اعتبار آن وجود ندارد.
- صرفه جویی در هزینه‌ها: با حذف امضای کاغذی و دیجیتالی شدن آن، دیگر نیازی به هزینه برای کاغذ و همینطور حمل و نقل آنها نخواهد بود. شما می‌توانید به سادگی با استفاده از یک کامپیوتر، اسناد خود را امضاء، ارسال و در صورت ضرورت با کمترین هزینه آنها را بایگانی کنید.
- صرفه‌جویی در زمان: مزیت دیگر امضای دیجیتال، صرفه‌جویی در زمان است. با امضای دیجیتال دیگر لازم نیست منتظر رسیدن پست یا پیک نامه‌رسان باشید. تنها با یک کلیک، سند دیجیتالی امضاءشده توسط شما به سرعت ارسال می‌گردد. همچنین، زمان کمتری برای تهیه پیش‌نویس اسناد برای امضاء، دخیره‌سازی اسناد و جستجوی آنها صرف خواهد شد.
- ثبت مشخصات زمانی: در هر امضای دیجیتال، داده‌های مربوط به امضاء همراه با مشخصات زمانی آن ثبت می‌شود که می‌تواند در بسیاری موارد از جمله در اختلافات حقوقی مورد استفاده قرار بگیرد.
- کمک به حفظ محیط زیست: استفاده از امضای دیجیتال باعث کاهش مصرف کاغذ و در نتیجه کاهش قطع درختان می‌شود. همچنین بدون ایجاد ضایعات فیزیکی، به حفظ محیط زیست کمک می‌کند.
- امکان نظارت بهتر: هر امضای دیجیتال یک ردپای دیجیتال نیز ایجاد می‌کند. این ردپای دیجیتالی باعث کاهش خطا در هنگام بررسی آنها می‌شود و نظارت بر فعالیت‌های سازمان و ثبت سوابق آنها را آسان‌تر می‌کند.
- تسهیل گردش کار دیجیتال: وجود امضای دیجیتال، فرآیند گردش‌کار دیجیتالی را در سازمان‌ها آسان‌تر می‌کند. زیرا با امضای دیجیتالی نیازی به اعتبارسنجی دستی آنها نخواهید داشت و امضاء دیجیتالی و به گردش انداختن اسناد قابلیتی است که در بسیاری از نرم‌افزارهای BPMS نیز مانند اتوماسیون کسب و کار فراگستر ارائه می‌شود.

انواع امضای دیجیتال

۵- انواع امضای دیجیتال کدام است؟

سه نوع مختلف از گواهی امضای دیجیتال (DSC) وجود دارد:

- کلاس ۱: که نمی‌توان از آنها در اسناد تجاری قانونی استفاده کرد، زیرا تنها با استفاده از شناسه ایمیل و نام کاربری تأیید می‌شوند. امضاهای دیجیتال کلاس ۱ سطحی ابتدایی از امنیت را فراهم می‌کنند و در محیط‌هایی استفاده می‌شوند که خطر کمی برای آسیب دیدن داده‌ها وجود دارد.
- کلاس ۲: اغلب برای پر کردن فرم های الکترونیکی اسناد مالیاتی، از جمله اظهارنامه مالیات بر درآمد و اظهارنامه مالیات کالا و خدمات (GST) استفاده می‌شود. امضاهای دیجیتال کلاس ۲ هویت امضاءکننده را با استفاده از یک پایگاه داده از پیش تأیید شده احراز هویت می‌کنند. امضای دیجیتال کلاس ۲ در محیط‌هایی استفاده می‌شود که خطرات و پیامدهای آسیب به داده‌ها متوسط است.

- کلاس ۳: امضاهای کلاس ۳، بالاترین سطح امضای دیجیتال هستند که برای انجام آنها، شخص یا سازمان باید برای اثبات هویت خود قبل از امضاء در مقابل مرجع صدور گواهی حاضر شوند. از امضای دیجیتال کلاس ۳ برای مزایده‌های الکترونیکی، مناقصه‌های الکترونیکی، بلیط‌های الکترونیکی، امضای اسناد دادگاه و در سایر محیط‌هایی که عواقب و پیامدهای نقص امنیت داده‌ها زیاد است، استفاده می‌شود.

۶- موارد استفاده از امضای دیجیتال کدام است؟

امروزه از امضای دیجیتال در انواع مختلفی از اسناد الکترونیکی به منظور بهبود کارایی و امنیت تراکنش‌های تجاری آنلاین، استفاده می‌شود، از جمله:

قراردادها و اسناد حقوقی :امضای دیجیتال از نظر قانونی الزام آور است. بنابراین، استفاده از آن برای هر سند قانونی که نیاز به امضاء و تأیید یک یا چند طرف برای اطمینان از عدم تغییر سند دارد، ایده‌آل است.

تفاهم‌نامه‌های فروش :با امضای دیجیتالی قراردادها و توافق‌نامه‌های فروش، هویت فروشنده و خریدار احراز می‌شود و هر ۲ طرف خیالشان از بابت الزام‌آور بودن امضاها و عدم دستکاری در شرایط و ضوابط قرارداد راحت می‌شود.

اسناد مالی :واحدهای مالی سازمان‌ها می‌توانند صورت‌حساب‌های خرید را با استفاده از امضاء دیجیتالی صادر و برای مشتریان ارسال کنند تا آنها از اصالت درخواست پرداخت از طرف فروشنده، نه فردی که قصد سوءاستفاده دارد، اطمینان ارسال کنند.

داده‌های بهداشت و درمان :در حوزه بهداشت و درمان، حفظ حریم خصوصی داده‌ها هم برای سوابق بیماران و هم در ارتباط با داده‌های تحقیقاتی بسیار مهم است. امضای دیجیتال تضمین می‌کند که این اطلاعات حساس در هنگام اشتراک گذاری بین طرفین دستکاری نشوند.

فرم‌های اداری دولتی :سازمان‌های دولتی در مقایسه با بسیاری از کسب و کارهای بخش خصوصی، دستورالعمل‌ها و مقررات سخت‌گیرانه‌تری دارند. با استفاده از امضای دیجیتال در ادارات دولتی می‌توان از تأیید مجوزها گرفته تا امضاهای ساده اداری را با اطمینان از صحت و اصالت آنها انجام داد و بهره وری این فرآیندها را بهبود بخشید.

اسناد حمل و نقل :برای تولیدکنندگان، اطمینان از صحت مندرجات بارنامه‌ها باعث کاهش خطاهای پرهزینه حمل و نقل می‌شود. با این حال، احراز اصالت بارنامه‌ها به صورت کاغذی، امری زمان‌بر است و اسناد کاغذی ممکن است همیشه قابل دسترسی نبوده و یا گم شوند. اما با امضای دیجیتالی اسناد حمل و نقل، فرستنده‌ها و گیرندگان می‌توانند به سرعت به آنها دسترسی پیدا کرده و تأیید کنند که امضاها به‌روز بوده و هیچ دستکاری صورت نگرفته است.

۷- تفاوت امضای دیجیتال و امضای الکترونیکی چیست؟

امضای الکترونیکی و امضای دیجیتال اصطلاحاتی هستند که اغلب به جای یکدیگر استفاده می‌شوند، اما با یکدیگر تفاوت دارند. امضای دیجیتال برای امضاء و تأیید صحت یک سند به الگوریتم ها و رمزگذاری متکی است. به عبارتی، در حالی که هدف از امضای الکترونیکی (e-Signature) تأیید ساده یک سند است، یک امضای دیجیتال به طور مؤثر سند را با استفاده از ویژگی‌های امنیتی محافظت می‌کند.

امضای الکترونیکی به شخص اجازه می‌دهد تا به صورت الکترونیکی تصویر یک امضاء را به سند یک قرارداد آنلاین اضافه کند. بنابراین امضاهای الکترونیکی نسخه دیجیتالی امضای کاغذی هستند و هدف امضاءکننده الکترونیکی با امضاءکننده کاغذی یکسان است، اما امضاء به‌جای دست‌نویس، به‌صورت الکترونیکی ثبت می‌شود که نیاز به امضاهای کاغذی را از بین می برد. به علاوه، همانند امضای کاغذی، امضای الکترونیکی یک اصطلاح حقوقی با دارای تعریف قانونی نیز است.

تفاوت اصلی بین این ۲ این نوع امضاء این است که یک امضای الکترونیکی می‌تواند تنها نام امضاءکننده در فرمی در یک صفحه وب باشد و اغلب مربوط به قراردادی است که امضاءکننده قصد انجام آن را دارد. اما یک امضای دیجیتال تایید شده، مدرکی رمزنگاری شده است که عمدتاً برای ایمن سازی اسناد استفاده می‌شود و استفاده از آن با اجازه مراجع صدور گواهینامه ممکن است. بنابراین می‌توان گفت که امضای دیجیتال نوعی امضای الکترونیکی است که امنیت بیشتری نسبت به امضای الکترونیکی سنتی ارائه می‌دهد.

۸- کلام آخر

در این مقاله در مورد امضای دیجیتال و تفاوت آن با امضای الکترونیک خواندید. یکی از موارد پرکاربرد امضای دیجیتال در مکاتبات و فرآیندهای سازمانی است. اتوماسیون اداری فراگستر یکی از بهترین نرم افزارهای اتوماسیون در ایران است که یک رابط کاربری ساده و در عین حال قدرتمند برای امضای دیجیتالی اسناد تجاری در اختیار شما قرار می‌دهد. به این ترتیب شما می‌توانید ضمن خودکارسازی گردش کار دیجیتالی سازمان خود، استانداردهای امنیتی داخلی و بین المللی مربوط به امضای الکترونیکی را رعایت کرده و امنیت مکاتبات خود را به حداکثر برسانید.

۹- سوالات متداول مشتریان

۱-امضای دیجیتال چیست؟

امضای دیجیتال معادل کامپیوتری امضای دست‌نویس یا مهر و موم نامه‌هاست. این نوع امضاء از یک تکنیک ریاضی پیشرفته برای احراز هویت امضاءکننده استفاده کرده و تضمین می‌کند که اسناد دیجیتالی دستکاری نشده باشند.

۲-موارد استفاده از امضای دیجیتال کدام است؟

از امضای دیجیتال در انواع مختلفی از اسناد الکترونیکی برای بهبود کارایی و امنیت آنها استفاده می‌شود، از جمله در قراردادها و اسناد حقوقی، تفاهم‌نامه‌های فروش، اسناد مالی، فرم‌های اداری دولتی و اسناد حمل و نقل.

۳-مزایای امضای دیجیتال چیست؟

برخی از مزایای امضای دیجیتال عبارتند از: امنیت بیشتر، اعتبار قانونی، صرفه‌جویی در زمان و هزینه، همراه داشتن مشخصات زمانی، کمک به حفظ محیط زیست، امکان نظارت بهتر و تسهیل گردش کار دیجیتال.

فراگستر

اتوماسیون کسب و کار

@faragostarco | faragostar | www.faragostar.net