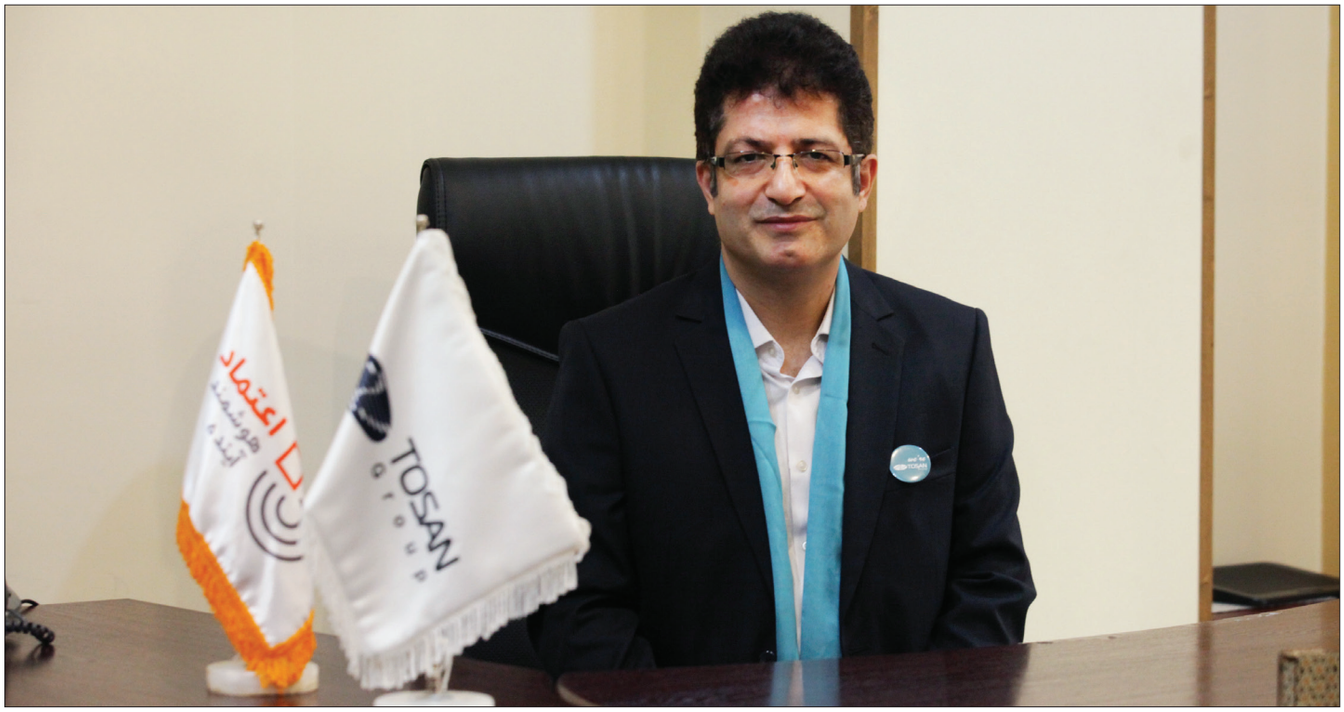

گفت‌وگو با محمدرضا پورحسن، مدیرعامل شرکت اعتماد هوشمند آینده، درباره پیشینه این شرکت و محصولاتش

در دنیای امروز داده‌ها، امنیت باید اولویت اول تمام کسب‌وکارها باشد

شرکت اعتماد هوشمند آینده از هلدینگ تک‌وست به‌دنبال افزایش امنیت اطلاعات و داده‌ها در سازمان‌ها و کسب‌وکارهاست

با گسترش استفاده از اینترنت و فضای مجازی در سال‌های اخیر؛ نیاز به افزایش امنیت اطلاعات، افزایش دانش بومی و بهبود زیرساخت‌های لازم برای ایجاد امنیت و اطمینان خاطر در محیط سایبری روزبه‌روز بیشتر احساس می‌شود و در حوزه تجارت الکترونیک اهمیت می‌یابد. شرکت اعتماد هوشمند آینده با اعتماد و سرمایه گروه توسن، در راستای تحقق این اهداف شروع به فعالیت کرده و با بسترسازی و ایجاد قابلیت‌های رمزنگاری، امنیت داده، صدور گواهی الکترونیکی و امضای دیجیتال؛ خدمات نوینی مانند امضای همراه و چک الکترونیک را عرضه می‌کند. با محمدرضا پورحسن، مدیرعامل شرکت اعتماد هوشمند آینده درباره این شرکت و خدماتی که ارائه می‌دهند، گفت‌وگو کردیم.

لطفا برایمان کمی در خصوص پیشینه شرکت اعتماد هوشمند و اینکه چرا گروه تک‌وست به سراغ تاسیس این شرکت رفت، توضیح دهید.

گروه سرمایه‌گذاران فناوری تک‌وست در راستای افزایش امنیت اطلاعات در فضای مجازی و ایجاد پشتوانه قانونی برای معاملات مالی و تبادل اطلاعات، از حدود چهار سال پیش تصمیم به استفاده از زیرساخت‌های تکنولوژیک مانند امضای الکترونیکی گرفت، چراکه پایه و اساس تجارت الکترونیک در جهان، استفاده از امضای الکترونیکی است. به همین خاطر نیز شرکت اعتماد هوشمند آینده در بهمن‌ماه ۱۳۹۴ با هدف اصلی راه‌اندازی مرکز میانی خصوصی صدور گواهی الکترونیکی تاسیس شد و کسب مجوز مرکز میانی خصوصی از مرکز دولتی صدور گواهی الکترونیکی ریشه (وزارت صنعت، معدن و تجارت) را در دستور کار خود قرار داد.

این شرکت در تیرماه ۱۳۹۶ موفق به اخذ مجوز اولیه راه‌اندازی مرکز میانی از مرکز ریشه دولتی شد و سپس طی سال‌های ۱۳۹۶ و ۱۳۹۷ تامین تجهیزات زیرساختی و سخت‌افزاری و فرایند طراحی و تولید نرم‌افزار صدور گواهی الکترونیکی را دنبال کرد و پس از انجام بازرسی‌های نهایی، سرانجام در دی‌ماه ۱۳۹۷ موفق به اخذ پروانه بهره‌برداری شد که امیدواریم گام‌های مثبتی را در

تخصص اعتماد هوشمند آینده

- راه‌اندازی سرویس امضای همراه برای اپراتورهای تلفن همراه؛
- قابلیت ارائه خدمات مشاوره در حوزه گواهی الکترونیکی، ایجاد مراکز میانی و تامین و تجهیز مراکز؛
- انجام مشاوره و ایجاد قابلیت PKI enabling سیستم‌های اطلاعاتی و نرم‌افزارهای کاربردی سازمان‌ها؛
- قابلیت ارائه مهر زمانی برای افراد حقیقی و حقوقی؛
- قابلیت ارائه سرویس ایمن‌سازی سیستم‌های تحت وب با سرویس SSL.

خدمات گواهی الکترونیک

- گواهی امضای اشخاص حقیقی
- گواهی احراز هویت اشخاص حقیقی و حقوقی
- امنیت در تبادلات مالی
- گواهی Code Signing حقیقی و حقوقی
- گواهی سرور SSL\TLS
- گواهی مهر سازمانی
- گواهی مراکز مهر زمانی
- گواهی پاسخگوی OCSP Signing

جهت ارتقای امنیت فضای مجازی و تبادلات تجاری و مالی طی کند.

منظور از مرکز میانی چیست؟

مرکز میانی به موجودیتی گفته می‌شود که با مجوز شورای سیاست‌گذاری گواهی الکترونیکی کشور، مجوز صدور گواهی الکترونیکی برای متقاضیان را دریافت کرده است. گواهی الکترونیکی ضمانتی است که به افراد، سازمان‌ها و حتی مولفه‌های سخت‌افزاری و نرم‌افزاری برای حضور، فعالیت و احراز هویت در جهت اطمینان‌سازی و اعتمادسازی اعطا می‌شود.

هم‌اکنون مرکز میانی شرکت اعتماد هوشمند با فراهم کردن زیرساخت‌های فنی و با اخذ مجوزهای مورد نیاز، امکان صدور گواهی امضای الکترونیکی را برای متقاضیان، در سراسر کشور مهیا کرده است.

مرکز میانی اعتماد هوشمند چه خدماتی را به متقاضیان ارائه می‌دهد؟

مرکز میانی اعتماد هوشمند، چند سرفصل مهم برای خدمات خود تعریف کرده که گواهی امضای الکترونیکی، گواهی SSL، گواهی پست الکترونیکی امن و سرویس مهر زمانی جزء مهم‌ترین سرفصل‌های خدمات ما هستند. علاوه بر اینها سرویس زیرساخت کلید عمومی (PKI) نیز یکی از سرویس‌های اصلی ما به‌شمار می‌رود. این زیرساخت به مجموعه‌ای از خدمات، محصولات، سیاست‌ها، فرایندها و سیستم‌های نرم‌افزاری و سخت‌افزاری گفته می‌شود که جهت مدیریت و به‌کارگیری گواهی‌های الکترونیکی و به‌منظور ارائه سرویس‌های امنیتی مختلف مبتنی بر رمزنگاری کلید عمومی مورد استفاده قرار می‌گیرد.

درباره گواهی امضای الکترونیکی کمی بیشتر برایمان توضیح دهید. این گواهی چه مزایایی را به وجود می‌آورد؟

بدون تردید، امنیت یکی از مهم‌ترین مسائل در حوزه فناوری اطلاعات و ارتباطات است. جعل را باید موضوعی جدا از هک دانست، اما نتیجه هر دو؛ نفوذ، از دست دادن اطلاعات و کاهش امنیت است. برای جلوگیری از نفوذ به سامانه‌ها و پیشگیری از جعل هویت، اسناد و مدارک در فضای مجازی، امضای الکترونیکی یکی از بهترین راهکارها به‌شمار می‌رود.

امضای الکترونیکی مفهومی شبیه امضای دستی و اثرانگشت اما با امنیتی بسیار بالا در فضای مجازی دارد. وقتی یک سند الکترونیکی مانند یک قرارداد، نامه‌های اداری و فرم‌های الکترونیکی، امضای الکترونیکی شود، چند مزیت مهم اتفاق می‌افتد؛ اول اینکه دریافت‌کننده سند یا پیام الکترونیکی می‌تواند هویت صاحب سند را به‌درستی تشخیص دهد و از جعلی‌نبودن آن اطمینان حاصل کند؛ چراکه گواهی الکترونیکی هر فرد شناسه اوست. دوم اینکه امکان جعل یا تغییر اسناد غیرممکن می‌شود و هر تغییری در محتوای سند امضاشده قابل تشخیص است و موجب نامعتبر شدن امضای الکترونیکی آن می‌شود و سوم اینکه هیچ‌کس نمی‌تواند امضای خود روی سند را انکار کند؛ چراکه با استفاده از امضای الکترونیکی روی سند و «گواهی الکترونیکی» فرد، می‌توان به هویت امضاکننده آن پی برد و در نهایت، برخلاف امضای دستی که همیشه ثابت است، امضای الکترونیکی هر سند برای آن سند منحصربه‌فرد است. در واقع، امضای الکترونیکی هر سند مرتبط با محتوای آن سند است و امکان جداسازی امضای الکترونیکی از سند به‌منظور استفاده مجدد روی سندی دیگر، یا جایگزین کردن آن با امضایی دیگر وجود ندارد.

به‌طور خلاصه می‌توانم بگویم به‌کارگیری گواهی امضای الکترونیکی در سامانه‌ها، امضای اسناد و تراکنش‌های الکترونیکی چندین ویژگی مهم دارند؛ احراز هویت و اطمینان از اینکه پیام دریافتی واقعا از منبع مورد انتظار باشد، یعنی اصالت فرستنده و پیام برای گیرنده احراز شود. محرمانگی که در آن گیرنده می‌تواند مطمئن باشد افراد غیرمجاز نمی‌توانند به محتوای داده دست پیدا کنند. تمامیت یا اطمینان از اینکه در متن ارسالی هیچ‌گونه تغییری رخ نداده و انکارناپذیری به این مفهوم که فرستنده نمی‌تواند امضای خود را انکار کند.

امضای الکترونیکی از نظر پشتوانه حقوقی و قانونی چه وضعیتی دارد و اساسا چه اسنادی را می‌توان با آن امضا کرد؟

به استناد ماده ۷ قانون تجارت الکترونیکی مصوب سال ۱۳۸۲ مجلس شورای اسلامی «هرگاه قانون، وجود امضا را لازم بداند، امضای الکترونیکی مکفی است.» بر اساس این ماده، امضای الکترونیکی به‌تنهایی و بدون نیاز به امضای دستی برای قانون کفایت می‌کند؛ بنابراین در کاربردهای مختلف می‌توان از گواهی امضای الکترونیکی استفاده کرد و از مزایای متعدد آن بهره برد.

با استفاده از گواهی امضای الکترونیکی می‌توان اسناد در فرمت‌هایی مانند پی‌دی‌اف، ورد و اکسل را امضا کرد. نرم‌افزارهای متداول برای امضای الکترونیکی اسناد، نرم‌افزارهای ادوبی و مایکروسافت آفیس هستند. علاوه بر این، یکی از مهم‌ترین کاربردهای امضای الکترونیکی، امن‌سازی ورود به سامانه‌ها با استفاده از امضای الکترونیکی است. در این صورت کاربران برای ورود به حساب کاربری علاوه بر دانستن رمز عبور، نیازمند اتصال توکن به سیستم و به‌کارگیری امضای الکترونیکی هستند. این امر امنیت سامانه را در بالاترین سطح قرار می‌دهد.

درباره بحث امنیت سامانه‌ها صحبت کردید، لطفا در خصوص گواهی SSL هم کمی توضیح دهید.

همان‌طور که حتما می‌دانید Secure Socket Layer یا همان SSL، پروتکلی برای ایجاد ارتباط امن بین وب‌سایت و کاربر است. این ارتباط امن از تمامی اطلاعاتی که بین وب‌سایت و کاربر انتقال می‌یابد، محافظت می‌کند تا این داده‌ها به‌صورت محرمانه و دست‌نخورده باقی بمانند. SSL یک استاندارد فنی است و توسط میلیون‌ها وب‌سایت در سراسر جهان برای برقراری امنیت انتقال اطلاعات استفاده می‌شود. برای اینکه یک وب‌سایت بتواند ارتباطی امن داشته باشد نیاز به یک گواهی SSL دارد.

با استفاده از گواهی SSL، امکان رمزگذاری بسته‌های اطلاعاتی در هنگام تبادل فراهم می‌شود و این امکان را به سرویس‌دهنده و کاربر آن می‌دهد که ارتباط خود را در بستری امن و به دور از مداخله دیگران به‌صورت رمزگذاری‌شده برقرار کنند و از صحت اطلاعات مبادله‌شده اطمینان یابند. بدون وجود این پروتکل، تمامی اطلاعات مبادله‌شده به‌سادگی در کانال ارتباطی قابل رویت، تغییر و سوءاستفاده هستند. همچنین بدین‌وسیله تایید هویت وب‌سایت یا سرویس‌های نرم‌افزاری ممکن می‌شود و مراجعه‌کننده به سایتی که دارای گواهی معتبر است، می‌تواند از جعلی‌نبودن سایت و صحت هویت آن اطمینان حاصل کند.

در حوزه پست الکترونیکی چه راهکارهایی را برای افزایش امنیت ارائه می‌دهید؟

اگر شما از پست الکترونیک برای ارسال یا دریافت مطالب شخصی و محرمانه یا هر مطلب مهمی استفاده می‌کنید، باید به‌دنبال راه‌حلی برای مخفی کردن مطالب داخل نامه‌های خود باشید. یکی از بهترین راهکارها استفاده از گواهی پست الکترونیک امن است.

با استفاده از این گواهی می‌توانید ایمیل‌ها و پیوست ایمیل‌های خود را رمزگذاری و سپس استفاده کنید. این گواهی از طریق پروتکل S/MIME امکان محرمانگی و امن کردن ایمیل را به‌واسطه رمزگذاری محتوای پیام و همچنین امضای آن فراهم می‌سازد.

یکی از نرم‌افزارهای متداول برای استفاده از گواهی پست الکترونیکی امن Microsoft Outlook است. البته استفاده از گواهی پست الکترونیک امن فقط به این نرم‌افزار محدود نیست و به‌طور کلی در هر نرم‌افزاری با قابلیت پشتیبانی از S/MIME قابل استفاده است. با استفاده از سرویس گواهی پست الکترونیک امن، ارسال و دریافت نامه‌های الکترونیکی با امنیت بسیار بیشتری انجام می‌شود و امکان تامین امنیت پست الکترونیکی با رمزگذاری و امضای محتوای پیام فراهم می‌شود. با این کار امکان رمزگشایی و دسترسی به محتویات پیام و ایمیل رمزنگاری‌شده تنها توسط گیرنده مقدور است و او می‌تواند از هویت ارسال‌کننده نامه اطمینان حاصل کند.

منظور از سرویس مهر زمانی چیست و چه تفاوتی با امضای الکترونیکی دارد؟

مهر زمانی، نوعی امضای الکترونیکی است که دارای تاریخ و ساعت باشد و گواهی می‌کند که محتویات آن در زمان مشخصی امضا شده‌اند. این سرویس جهت ثبت دقیق زمان در هنگام امضای اسناد مختلف؛ از جمله قراردادها یا توافق‌نامه‌ها و بایگانی آنها مورد استفاده قرار می‌گیرد.

با این سرویس می‌توان وجود یک داده در یک زمان خاص را اثبات کرد و امضای یک سند خاص در زمان اعتبار گواهی امضاکننده را تایید کرد. همچنین بعد از ایجاد مهر زمانی می‌توان عدم تغییر داده‌ها را تضمین کرد که انکارناپذیری امضا نیز جزء مزایای مهم آن به شمار می‌رود.

ارزش‌هایی که اعتماد هوشمند ارائه می‌دهد

- عدم انکار شخص حقیقی و حقوقی (اصالت و امکان پیگیری حقوقی)
- امنیت در تبادل اطلاعات و حفظ محرمانگی اسناد
- امنیت در تبادلات مالی
- جلوگیری از هرگونه سوءاستفاده و سودجویی
- ساده‌سازی و آسان کردن کاربرد استفاده از قابلیت زیرساخت کلید عمومی در سامانه‌های نرم‌افزاری

PKI چیست؟

PKI مجموعه‌ای از سخت‌افزارها، نرم‌افزارها، سیاست‌ها و رویه‌های مورد نیاز برای ایجاد، مدیریت، توزیع، استفاده، ذخیره و لغو گواهی‌های دیجیتالی است. PKI با تکیه بر مجموعه‌ای از مکانیسم‌های رمزنگاری کلید عمومی، سرویس‌های امنیتی مورد نیاز در سازمان را فراهم می‌کند.