# امضای دیجیتالی و گواهینامه‌ی دیجیتالی

همانطور که می‌دانیم درتجارت سنتی، برای احراز هویت افراد مشکلی نداریم و افراد به‌طور فیزیکی وجود دارند و اسناد مستقیماً به شخص داده می‌شود ولی درتجارت الکترونیکی، ما در یک بستر اینترنتی و دیجیتالی هستیم و دیگر احراز هویت اینگونه نخواهد بود. همچنین در خصوص داده‌ها واطلاعات در حالت سنتی، ما می‌توانیم اصل و کپی یک سند را با هم تشخیص دهیم و کسی نمی‌تواند خودش را جای دیگری معرفی کند، در حالی که در داده‌های الکترونیکی اصل و کپی فرقی با هم ندارند و شخص نیز می‌تواند خودش را به جای دیگری معرفی نماید.

زیرساخت کلید عمومی یا PKI مجموعه سخت‌افزار و نرم‌افزار و آیین‌نامه‌های اجرایی است که بتوان یک زیرساخت امن برای شبکه و تجارت ایجاد نمود. لازمه‌ی تجارت امن، جلوگیری از حملات امنیتی و تأمین سرویس و راهکارهای امنیتی است و برای این منظور مراکز استاندارد سنجی امنیت بر اساس CPT ، CPS (آئین‌نامه‌های اجرایی و محیط فیزیکی) نظر می‌دهند. حال اگر مسئله امنیت را حل کنیم و شخص مطمئن باشد که طرف حساب او، همان فردی است که قبلاً عنوان کرده است و همچنین اطلاعات به طور امن رد و بدل شود، مشکل مبادله‌ی دیجیتالی اطلاعات حل می‌شود. برای احراز هویت در حالت سنتی، به گواهینامه، پاسپورت و یا شناسنامه نیاز است ولی در حالت الکترونیکی، ما به گواهینامه‌ی دیجیتالی نیاز داریم. قبل از بحث در خصوص امضا و گواهی دیجیتالی بایستی موضوع رمزنگاری بررسی گردد.

رمزنگاری یک متن، علمی است که با یک سری الگوریتم‌های پیچیده‌ی ریاضی روی متن تغییراتی می‌دهد و متن به هم ریخته‌ای به ما می‌دهد که بدون داشتن کلید رمز، قابل استفاده نیست. رمزنگاری، از زمان سزار شروع گردید؛ به طوری که او یک سری کلید تعریف می‌کرد. به‌عنوان مثال هر حرف را با چند حرف جلوتر از خودش عوض می‌کرد و به این ترتیب متن به صورت به‌هم ریخته در آمده که بدون داشتن کلید رمز، قابل خواندن نبود. در جنگ جهانی دوم، آلمان‌ها از روش ماشین انیگما (Enigma) برای رمزنگاری استفاده می‌کردند، به صورتی که یک چرخ دنده برای رمزکردن بود که اگر آنرا از روی ماشین بر می‌داشتند دیگر کسی قادر به خواندن مطلب نبود.

با تبادل پیشرفت فناوری اطلاعات و موضوع امنیت اطلاعات. آقایان هلمن و دیفل، رمزنگاری عمومی را مطرح نمودند که با روش‌های ریاضی کار می‌کرد و شامل الگوریتم‌های متقارن و نامتقارن بود. در الگوریتم متقارن، یک کلید داریم که با آن، داده رمزنگاری شده و با همان نیز کلید داده رمزگشایی می‌شود. استاندارد DES که برای آن استفاده می‌شود (data encryption standard)، حجم داده را کوچک می‌کند و در واقع یک کلید مشترک بین طرفین می‌باشد. مشکلی که در این شیوه موجود است موضوع ارسال کلید برای کاربران و تعداد کلیدهای رمزنگاری است که مدیریت کلید را مشکل می‌سازد. مثلاً برای ۴ نفر ما ۶ کلید می‌خواهیم. ولی مزیت آن سرعت بالا هنگام رمزنگاری است و هر چه طول کلید بیشتر باشد مدت زمان شکستن و سرعت کمتر می‌شود.

در الگوریتم نامتقارن، دو کلید داریم. یکی عمومی برای رمزنگاری و یکی برای رمزگشایی یا decryption. لذا مرکز CA، به هر شخص، دو کلید می‌دهد، یعنی Privacy را مؤسسه می‌دهد و کلید عمومی در اختیار همه است. کلید خصوصی می‌تواند بر روی Smart Card باشد و به‌وسیله قوه‌ی قضاییه قابل نظارت و پیگیری است.

همچنین شرکت بیمه می‌تواند گواهی‌های ارایه شده از مرکز صدور گواهی (CA) را بیمه نماید. مزیت این روش عدم نیاز به توزیع و ارسال (بر روی اینترنت قرار می‌گیرد) و قابلیت رد انکار طرفین است ولی سرعت پائین به لحاظ حجم بالای اطلاعات و پیچیدگی تولید را می‌توان از معایب آن دانست. به‌هر حال امضای دیجیتالی به لحاظ ویژگی رد انکار دارای کاربردهای متنوعی است.

علاوه بر ویژگی‌های فوق، بایستی به این نکته اذعان داشت که امضای سنتی همیشه شکل ثابتی دارد، لذا می‌تواند جعل شود، در حالی که امضای دیجیتال قابل جعل نیست، متفاوت است و هیچکس کلید خصوصی شخص را در اختیار ندارد. همچنین موارد عدم انکار (Non-repudiation)، جامعیت داده‌ها (Integration) و تأییدهویت (Authentication) از طریق امضای دیجیتالی تحقق می‌یابد.

تفاوت گواهینامه‌ی دیجیتالی با امضای دیجیتالی در این است که گواهی دیجیتالی یک کلید عمومی را به اطلاعات شناسایی فرد پیوند می‌زند. گواهی دیجیتالی باید از استاندارد خاصی مثل X.۵۰۹ پیروی کند. اگر روی آیکون قفل زرد کوچک هر سایت در سمت چپ پائین، راست کلیک کنیم، گواهی دیجیتالی سایت قابل مشاهده است. مرکز صدور گواهی الکترونیکی زیر نظر وزارت بازرگانی بوده و هماهنگ با یک سری شرکت‌های خارجی (مالزی) فعالیت می‌نماید و وظایف آن عبارت است از: تولید، ابطال و سیاست گذاری. این مرکز دارای تعدادی دفاتر ثبت نام یا RA می‌باشد که امضاء یا گواهی دیجیتالی را بر روی CD، کارت هوشمند و توکن ارایه می‌دهند. بدیهی است ارایه آن بر روی سی‌دی ارزان‌تر و برای محیط‌های آموزشی مناسب است ولی ارایه آن بر روی کارت هوشمند گران‌تر و نیاز به Card Reader دارد. در حالی که توکن گران قیمت و امن است و دارای pass word نیز می‌باشد. اکنون مرکز صدور گواهی دیجیتالی چهار مدل گواهی ارایه می‌دهد که عبارتنداز:

۱ـ SE-Secure Email

۲ـ SSL-Secure Socket Layer (URL)

۳ـ گواهی ثبت سفارش برای بازرگانان

۴ـ امضای دیجیتال

**علی ثاقب موفق**
**رییس گروه امنیت شبکه**
**اداره‌ی کل رایانه و فناوری اطلاعات**