امضای دیجیتال

• امضای دیجیتال به اندازه امضای دستی قابل اطمینان است. برای ساخت امضای دیجیتال نیاز به یک کلید خصوصی است که فقط خود فرد مجاز آن را می داند. نشانه‌ها با انجام عملیات تولید مطمئن و ذخیره کلید خصوصی امضای دیجیتال را امن می‌کنند. به این ترتیب برای احراز هویت قابل استفاده‌است. چون همانطور که گفته شد کلید خصوصی نشانه‌ای بر شخصیت فرد و یگانه بودن آن است. نشانه‌هایی که برای احراز هویت استفاده می‌شوند باید یک شماره خاص و یکتا داشته باشند. تمام روش‌های نشانه برای امضای دیجیتال به مسائل و قوانین ملیتی مناسب نیستند. نشانه‌هایی کهصفحه کلید ندارند یا از **اینترفیس‌های**)به انگلیسی (Interface :دیگری استفاده می‌کنند برای سناریو امضا مناسب نیستند.

انواع نشانه‌های سخت افزاری و نرم‌افزاری

- بعضی از نشانه‌های امنیتی هم به صورت سخت افزاری و هم به صورت نرم‌افزاری در دسترس هستند. اگر فردی به این دو نوع نشانه امنیتی نگاه کند، از لحاظ ساختاری یکسان به نظر می‌رسند ولی در توابع یک سری تفاوت‌هایی با هم دارند.

انواع نشانه‌های سخت افزاری و نرم‌افزاری

- **نشانه غیرمتصل(Disconnected)**
- نشانه مورد نظر هیچ گونه اتصال فیزیکی و منطقی با کامپیوتر مشتری ندارد. به طور معمول به دستگاه ورودی خاصی نیاز ندارند. در عوض یک صفحه نمایش داخل خود دارند که داده‌های احراز هویت به وسیله آن نمایش داده می‌شود و کاربر به صورت دستی اطلاعات را با صفحه کلید وارد می‌کند. این نوع نشانه (معمولاً همراه یک رمز عبور) برای احراز هویت در تشخیص افراد به صورت بر خط بیشتر مورد استفاده قرار می‌گیرد.

یک نشانه غیر متصل

انواع نشانه‌های سخت افزاری و نرم‌افزاری

- **نشانه متصل(Connected)**

  - این نوع نشانه باید حتماً به صورت فیزیکی به کامپیوتر مشتری متصل گردد. نشانه‌ها در این دسته به طور اتوماتیک اطلاعات احراز هویت را به کامپیوتر مشتری در همان اولین ارتباط منتقل می‌کند، به جز اطلاعاتی که باید به طور دستی توسط کاربر داده شود. برای استفاده از این نوع نشانه باید دستگاه ورودی مناسبی روی سیستم نصب شود. معمول ترین نوع از نشانه‌های متصل، کارت‌های هوشمند و نشانه USB است که به ترتیب نیاز به دستگاه کارت خوانکارت هوشمند و پورت USB دارند.

انواع نشانه‌های سخت افزاری و نرم‌افزاری

- **کارت هوشمند**

- بسیاری از نشانه‌های متصل از تکنولوژی کارت هوشمند استفاده می‌کنند. کارت هوشمند می‌تواند خیلی ارزان و شامل مکانیزم‌های امنیتی مطمئن باشد. (همانند آن‌هایی که توسط مؤسسه‌های مالی استفاده می‌گردد، مثل دسته چک) عملکرد محاسباتی کارت هوشمند اغغلب محدود است و آن به دلیل توان مصرفی بسیار کم آن هاست.

ضرورت استفاده از پروتکل SSL

- بسیاری از افراد اطلاعات مورد نیاز خود را در طول روز از طریق اینترنت دریافت و ارسال می نمایند. برخی از این اطلاعات محرمانه نبوده و اهمیت چندانی ندارد.

به عنوان مثال: آگهی فروش سهام یک شرکت مطلب محرمانه ای نیست.

- اما برخلاف این اطلاعات، اطلاعاتی وجود دارند که بسیار قابل اهمیت و محرمانه هستند.

به عنوان مثال رمز حسابهای بانکی از این قبیل اطلاعات است.

ضرورت استفاده از پروتکل SSL

- درصورتیکه در هنگام انتقال چنین اطلاعاتی از پروتکل امنیتی استفاده ننمائیم، این احتمال وجـود دارد کـه اطلاعـات بدون آگاهی خودمان به سرقت رفته و مورد سوء استفاده قرار گیرند.

- اینجاست که بحث امنیت اطلاعات انتقالی و پروتکل های امنیتی مثل SSL مطرح می‌شود.

پروتکل SSL

- SSL یا Secure Socket Layer ،یکی از پروتکل‌های انتقال اطلاعات در وب و بین یک مرورگر و یک سرور است و انتقال اطلاعات را به صورت امن تضمین می نماید.
- این پروتکل که رایجترین پروتکل انتقال امن اطلاعات در وب است، توسط کمپانی Netscape تهیه شد و پس از مدتی علاوه بر مرورگر Netscape، توسط مرورگرIE نیز مورد استفاده قرار گرفت.
- اکنون تقریباً تمام مرورگرهای استاندارد از جمله فایر فاکس، اینترنت اکسپلورر، اپرا، گوگل کروم و سافاری آن را پشتیبانی می کنند.

عملکرد پروتکل SSL

- هنگام استفاده از SSL، مرورگر از public key موجود در خود استفاده کرده و اطلاعات را کد می نماید و سپس به سرور می فرستد. آنگاه سرور با استفاده از private key خود، اطلاعاتی را که دریافت نموده است رمز گشائی (Decode) می نماید.
- از آنجا که کلید خصوصی تنها در سرور نصب شده است، تقریباً غیر ممکن است که در بین راه اطلاعات انتقالی رمزگشائی و مشاهده شوند.

مکانیزم‌های تشکیل دهنده پروتکل SSL

- مکانیزم های تشکیل دهنده SSL عبارتند از:

1. تایید هویت سرویس دهنده
2. تایید هویت سرویس گیرنده
3. ارتباطات رمز شده