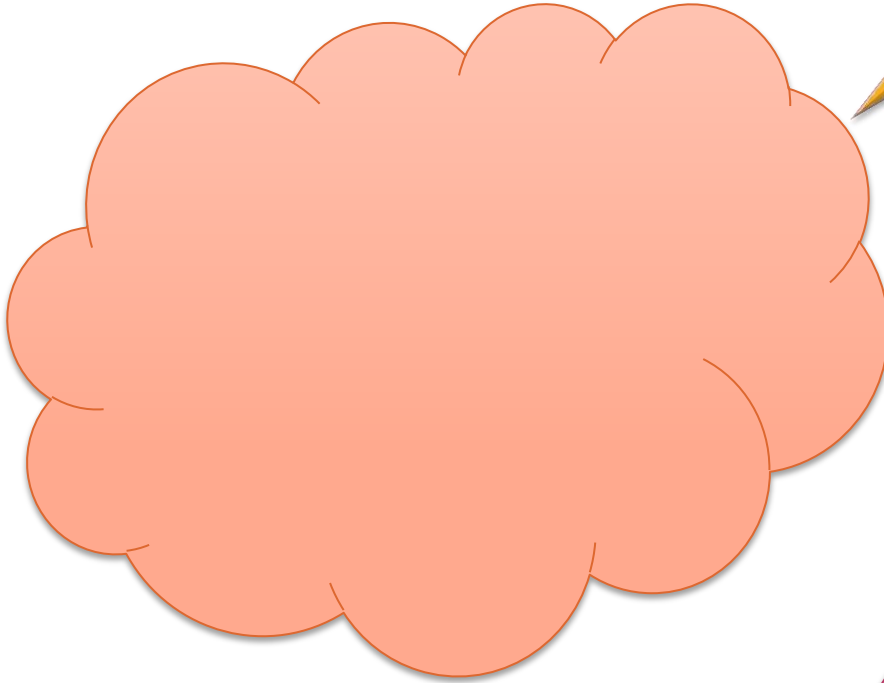
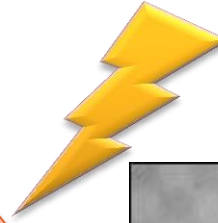




امضای الکترونیکی



استاد مربوطه:



گردآورنده



عناوین

I. مقدمه

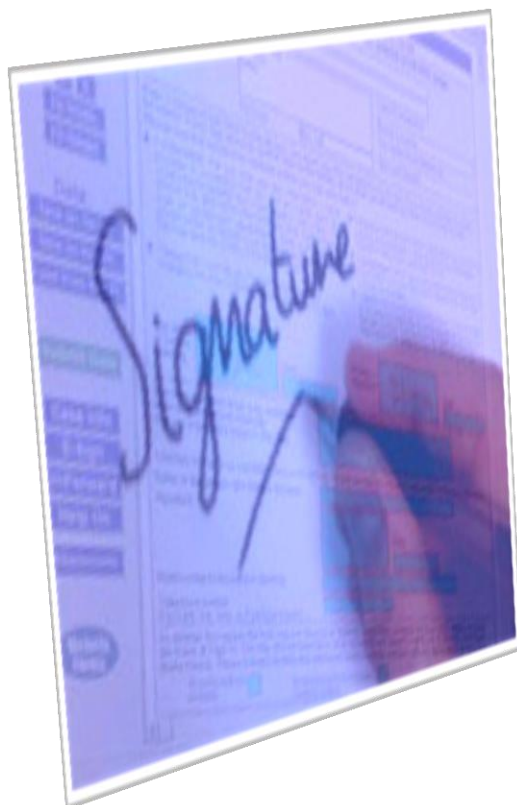
II. معرفی امضای دیجیتال

III. دلایل استفاده از امضای دیجیتال

IV. فرق امضای دیجیتال با دستی

V. پیاده سازی یک امضای دیجیتالی

VI. نتیجه گیری



مقدمه

- کاغذ به عنوان حامل اطلاعات مهم جای خود را کم کم به دیگر راههای تبادل اطلاعات می دهد. در واقع کاغذ دارای معایبی از قبیل انتقال آهسته و پرهزینه اسناد می باشد. همچنین شیوه های ذخیره سازی اطلاعات نیز بسرعت در حال تغییر است و بجای بایگانی انبوه دسته های کاغذ از روشهای الکترونیکی استفاده می شود.



- فن‌آوریهای جدید انتقال اطلاعات، مانند: پست الکترونیک، ارسال و ذخیره اطلاعات را ساده‌تر، سریع‌تر و حتی ایمن‌تر ساخته است.



معرفی امضای دیجیتالی

- یکی از تکنولوژی‌هایی که موجب افزایش اعتماد گردیده، امضای دیجیتالی می‌باشد. این تکنیک مبتنی بر رمزنگاری باعث به رسمیت شناسی اطلاعات الکترونیکی شده به طوریکه هویت پدیدآورنده سند و جامعیت اطلاعات آن، قابل بازبینی و کنترل می‌باشد و بخاطر ساختار غیرفیزیکی واسطه (وسیله حامل داده)، روشهای سنتی علامتگذاری فیزیکی واسطه توسط مهر یا امضاء (برای مقاصد تجاری و حقوقی) غیرقابل استفاده می‌باشند



- برای اینکه هویت فرستنده سند تایید شود و نیز برای اطمینان از اینکه سند در طول مدت انتقال به گیرنده دستکاری نشده است از امضای دیجیتالی استفاده می شود . میتوان كل يك سند و یا قسمتی از آن را امضا کرد .



دلایل استفاده از امضای دیجیتال

◦ به طور کلی سه دلیل برای استفاده از امضای دیجیتالی وجود دارد که شامل:

1- استفاده از کلید عمومی این اجازه را به هر شخصی می دهد که کلید خود را به سمت فرستنده اطلاعات بفرستد و سپس گیرنده پس از دریافت اطلاعات، آن را توسط کلید خصوصی خود بازگشایی میکند، بنابراین امضای دیجیتالی این امکان را می دهد که فرستنده یا گیرنده مطمئن شوند که اطلاعات از محل یا شخص مورد نظر دریافت میشود .

2- اطلاعات در طول مدت انتقال ممکن است توسط دیگران دستکاری شود . برای اینکه از صحت اطلاعات رسیده مطمئن شویم نیاز به يك امضاي دیجیتالي در این حالت احساس مي شود.

3- رد کردن اطلاعات فرستاده شده . گیرنده اطلاعات برای اینکه مطمئن شود فرستنده بعدا از اطلاعاتي که فرستاده اعلام بي خبري نکند و آنها را رد نکند از فرستنده يك امضا درخواست میکند تا شاهدي بر این ادعا باشد .



فرق امضای دیجیتالی با دستی

- (1) امضای دیجیتال نوعی رمزنگاری نامتقارن است که خصوصیات امضای دستی را در فضای مجازی فراهم می کند.
- (2) هر فرد در فضای مجازی دارای امضای دیجیتالی خاص خود است و تنها این فرد قادر به تولید این امضا است.



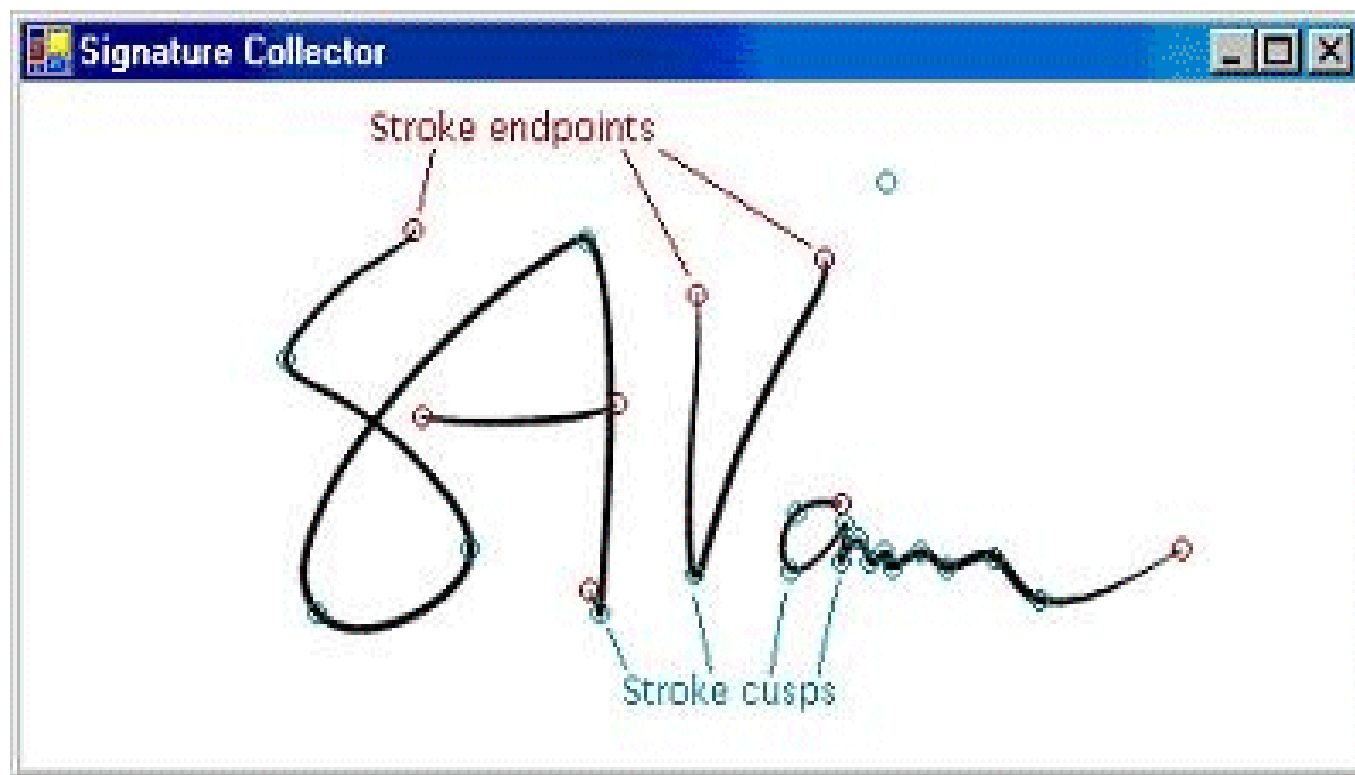
3) اما امضای دیجیتال دارای خصوصیات دیگری نیز هست که امضای دستی فاقد آن است. بوسیله امضای دیجیتال می توان مطمئن بود که محتوای سند یا پیغام تغییر نکرده و افراد غیر مجاز سند الکترونیکی مربوطه را مخدوش نکرده اند. این بدان دلیل است که امضای دیجیتال به ازای هر سند یا پیام وابسته به متن، تولید می شود و امضای تولید شده برای هر سند، منحصر به فرد می باشد.



The image shows a digital signature form and a signature window. The form is titled "Forms" and contains several sections. The first section is a list of declarations: "Even if someone else has filled in the claim form for you, you must sign this declaration." followed by five bullet points: "I understand that you may use the information I have provided in court that I have made or may make, and may give some information to other authorities and providers for companies such as banks and engineers", "I know that I must let you know in writing about any change in my data", "I declare that the information I have given on this form is correct and is", "I understand that if I give information that is incorrect or incomplete, you", and "I agree that you will use the information I have provided to process my". Below this is a section for "Signature of person claiming" with a text box containing "John Smith" and a "Date" field. The second section is "If this form has been filled in by someone other than the person claiming" with a text box for "Please tell us why you are filling in this form for the person claiming". The third section is "Name of the person who filled in the form" with a "Signature" field and a "Relationship to the person claiming" field. The signature window is titled "Signature" and shows a stylized signature "John Smith" in a box. Below the signature are three buttons: "Enter" - Accept signature, "Del" - Clear signature, and "Esc" - Cancel. At the bottom of the window is a "Tab" button labeled "Switch to Tablet PC".



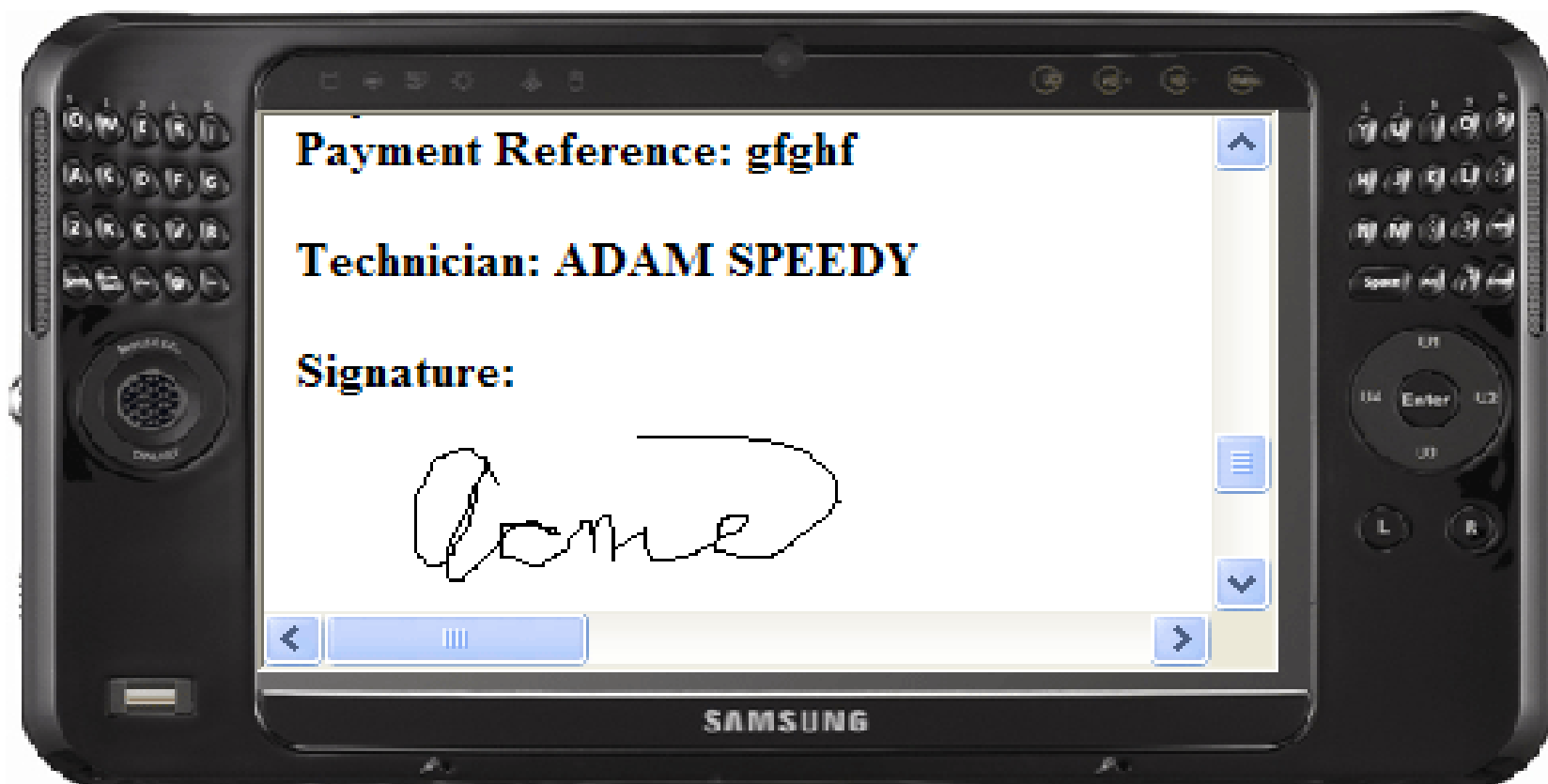
4) امضای دیجیتال برای هر مستند یا پیغام بوسیله کلید خصوصی فرد تولید میشود و در واقع یک عدد با طول بلند است. کلید خصوصی فرد به صورت امن در وسیله ای مانند کارت هوشمند نگهداری می شود. بدین ترتیب جعل امضای دیجیتال بسیار مشکل تر از امضای دستی است.



- 5) توسط امضای دیجیتال سندیت خاصی به اسناد الکترونیکی داده می شود. بدین ترتیب می توان بصورت قابل اعتماد و مطمئن ارسال کننده سند را شناسایی کرد. در نتیجه اسناد الکترونیکی قابل پیگیری بوده و به کمک آن فعالیت افراد در فضای مجازی جنبه حقوقی پیدا می کند و قوانین حقوقی اسناد کاغذی در مورد اسناد الکترونیکی قابل اجرا می شود.



6) از طرف دیگر با توجه به عدم امکان جعل امضای دیجیتال، اسناد یا پیام های امضا شده قابل انکار از طرف امضا کننده نیست. بدین وسیله مراجع قضایی می توانند از این خصوصیت جهت استناد قانونی به سند الکترونیکی استفاده کنند.



برای پیاده سازی يك امضای دیجیتالی نیاز به سه الگوریتم داریم :



A. يك الگوریتم برای ایجاد کلید

B. الگوریتم برای ایجاد امضا

C. الگوریتم برای تایید امضا

برای ایجاد يك امضای دیجیتالی باید يك عدد
checksum برای سند مورد نظر محاسبه
شود.

برای مثال

فرض کنید مینا قصد ارسال يك پیام به سارا را دارد
مینا پیام خود را همراه با امضای دیجیتالی برای سارا می فرستد.
این امضای دیجیتالی توسط کلید خصوصی که مالک آن مینا
می باشد ایجاد شده است . در سمت دیگر سارا با استفاده از
الگوریتم تایید امضا و کلید عمومی که از مینا دریافت کرده
صحت امضا و اینکه امضا از طرف مینا می باشد را تایید
Security with Digital Signatures
میکند.



جمع بندی

- در جهان امروز مدیریت اسناد الکترونیکی و ارسال و دریافت اطلاعات الکترونیکی بخش بزرگی از تبلیغات و فعالیت‌های اجرایی را شامل می‌شود. استفاده از اطلاعات مبتنی بر کامپیوتر در سطح جهان به طرز قابل توجهی در حال گسترش می‌باشد. یکی از تکنولوژی‌هایی که موجب افزایش اعتماد گردیده، امضای دیجیتالی می‌باشد. این تکنیک مبتنی بر رمزنگاری باعث به رسمیت شناسی اطلاعات الکترونیکی شده به طوریکه هویت پدیدآورنده سند و جامعیت اطلاعات آن، قابل بازبینی و کنترل می‌باشد.

- در نتیجه می توان مستندات، پیغام ها و داده های الکترونیکی را توسط امضای دیجیتال تایید کرده و سندیت بخشید، به شکلی که مطمئن بود که تولید کننده امضا چه کسی است و متن پیغام امضا شده، پس از امضا تغییر نکرده است. بدین وسیله متن سند یا پیغام امضا شده قابل استناد و پیگیری بوده و غیر قابل انکار است.



پایان

