TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI TP. HỒ CHÍ MINH

KHOA CÔNG NGHỆ THÔNG TIN

AN TOÀN THÔNG TIN- INFORMATION SECURITY

CHƯƠNG 4
CHỮ KÝ SỐ VÀ CHỨNG CHỈ SỐ

Giảng viên: TS. Trần Thế Vinh

CHỮ KÝ SỐ

Khái niệm:

Ý tưởng về mô phỏng chữ ký tay trên văn bản trong đời thường đã có từ lâu, nhưng thực sự chỉ có thể thực hiện được cùng với sự ra đời của hệ mật mã khóa công khai.

Như đã biết, hệ thống mật mã đối xứng đã được sử dụng phổ biến trước đó không có tính chất đại diện duy nhất cho một cá nhân. Trong khi đó, một hệ mã hóa khóa công khai (hay còn gọi là bất đối xứng) có thể được xem là được tạo lập để giúp bảo mật truyền tin trong liên lạc giữa 1 cá nhân và phần còn lại của xã hội. Nhờ có mật mã khóa công khai, khái niệm chữ ký điện tử mới được hiện thực hóa và giúp cho giao dịch kinh tế thương mại trong đời sống có thể đi vào số hóa hoàn toàn, qua đó thúc đẩy hoạt động dịch vụ trực tuyến trên Internet phát triển như ngày này.

Chữ ký điện tử hay chữ ký số có thể so sánh tương tự hoàn toàn với chữ ký tay hay không? Thực ra không phải hoàn toàn tương tự. Chữ ký tay là dấu vết của con người tác động lên cùng bản giấy đã mang chứa văn bản (in/viết sẵn). Phần chữ ký tay và phần văn bản có sẵn là độc lập, không có quan hệ ràng buộc nào. Do các qui luật của thế giới vật lý, người ta không thể đánh tráo chữ ký theo kiểu đơn giản là xé bỏ phần tờ giấy chứa chữ ký và ghép nối vào một phần giấy mang chữ ký tạo mới khác. Tuy nhiên trong thế giới số hóa, các qui luật vật lý này không có mặt, và bất cứ lập trình viên nào cũng có thể tha hồ cắt ghép văn bản số hóa mà không bị phát hiện.

CHỮ KÝ SỐ

CÁC LOẠI CHỮ KÝ VÀ THỜI ĐIỂM SỬ DỤNG

Chữ ký thêm thẩm quyền pháp lý cho tất cả các loại thỏa thuận – nhưng không phải tất cả các chữ ký đều được tạo ra như nhau. Hiện nay chữ ký được phân làm 4 loại:

- Chữ ký ướt
- Chữ ký điện tử
- Chữ ký số
- Chữ ký Click-wrap

Tùy theo hoàn cảnh, bạn có thể cần sử dụng một hoặc nhiều phương pháp này khi đồng ý ký hợp đồng hoặc ký các tài liệu quan trọng khác.

CHỮ KÝ SỐ

CÁC LOẠI CHỮ KÝ VÀ THỜI ĐIỂM SỬ DỤNG

Chữ ký ướt:

Chúng ta đã sử dụng chữ ký ướt trong nhiều thế kỷ. Một trong những chữ ký ướt nổi tiếng nhất là chữ ký tay trong bản Tuyên ngôn độc lập (hầu hết các quốc gia thành lập đều chưa có các loại chữ ký khác). Thuật ngữ chữ ký "ướt" đề cập đến mực ướt được sử dụng để tạo chữ ký viết tay trên một mảnh giấy vật lý. Đó là cách truyền thống mà ta trực tiếp ký vào các tài liệu. Ngoài việc ký tên của mình bằng chữ thảo hoặc chữ in, các kỹ thuật chữ ký ướt hợp lệ khác bao gồm sử dụng một dấu riêng biệt, chẳng hạn như con dấu.

Khi nào nên sử dụng chữ ký ướt:

Mặc dù ngày càng có nhiều doanh nghiệp sử dụng chữ ký điện tử trong vài thập kỷ qua, nhưng vẫn có nhiều trường hợp bạn sử dụng bút mực đáng tin cậy để ký tên của mình:

- Khi ký các văn bản cho vay và các thỏa thuận tài chính khác
- Trên phiếu in thẻ tín dụng
- Để nhanh chóng đồng ý với các thủ tục y tế khẩn cấp
- Khi kiểm tra thể chất

Trong một số trường hợp, một tổ chức có thể thích chữ ký ướt hơn vì họ muốn giữ lại một bản sao vật lý của thỏa thuận.

CHỮ KÝ SỐ

CÁC LOẠI CHỮ KÝ VÀ THỜI ĐIỂM SỬ DỤNG

Chữ ký ướt:

Ưu và nhược điểm của việc sử dụng chữ ký ướt

Mặc dù bạn không thường xuyên phải lựa chọn giữa việc sử dụng chữ ký ướt hoặc chữ ký điện tử, nhưng đôi khi đó là một khả năng. Vì vậy, tại sao lại chọn chữ ký ướt thay vì chữ ký điện tử? Có một vài ưu và nhược điểm cần ghi nhớ.

Chữ ký ướt

Một trong những lý do chính khiến chữ ký ướt có thể được ưa chuộng hơn là cả hai bên thường phải có mặt tại thời điểm ký kết. Điều này tạo cơ hội để xác nhận chi tiết và cơ sở liên lạc trước khi chính thức hóa thỏa thuận. Đó là một phần lý do tại sao một số công ty và doanh nhân thích chữ ký ướt.

Khi bạn trực tiếp ký một tài liệu, bạn có thể bổ sung hiệu lực bổ sung cho quy trình bằng cách thuê Công chứng. Các chuyên gia được nhà nước ủy quyền này chứng kiến chữ ký trên các tài liệu như quyền sở hữu phương tiện và chứng thư nhà ở. Tài liệu được công chứng cung cấp thêm một lớp hiệu lực và đôi khi được yêu cầu, đặc biệt là khi xử lý các tài liệu chính thức của chính phủ.

Nhược điểm chữ ký ướt

Có một số hạn chế quan trọng cần lưu ý khi sử dụng chữ ký ướt:

- Đắt tiền (lưu trữ tài liệu giấy có thể tốn kém)
- Chậm hơn (xử lý có thể phải trải qua một số bộ phận và quy trình công việc)
- Khó xác minh hơn sau này (nhân viên phải theo dõi tệp từ bộ nhớ vật lý)

Khi bạn là người ký một tài liệu, bạn có thể thích chữ ký điện tử hơn để không phải giữ một bản sao của tài liệu gốc.

CHỮ KÝ SỐ

CÁC LOẠI CHỮ KÝ VÀ THỜI ĐIỂM SỬ DỤNG

Chữ ký điện tử:

Chữ ký điện tử về cơ bản là một phiên bản kỹ thuật số của chữ ký ướt. Sử dụng chữ ký điện tử là cách phổ biến nhất để đồng ý với một thỏa thuận hoặc đồng ý với các điều khoản được nêu trong hợp đồng điện tử.

Khi nào nên sử dụng chữ ký điện tử

Rất có thể bạn thường xuyên sử dụng chữ ký điện tử vì chúng là phương thức chữ ký ưa thích cho nhiều mục đích. Một số ví dụ về chữ ký điện tử phổ biến bao gồm:

- Đồng ý với các điều khoản của đăng ký trực tuyến
- Ký tờ khai thuế điện tử của bạn
- Bao gồm tên đã nhập của bạn ở cuối email
- Sử dụng mã PIN của bạn tại máy ATM
- Ký các khoản phí trên màn hình tại một sổ đăng ký
- Quét và gửi hình ảnh chữ ký viết tay ướt của bạn

Thường không cần thiết phải in một bản sao của thỏa thuận mà bạn đã sử dụng chữ ký điện tử. Tuy nhiên, bạn có thể muốn lưu file trên máy tính của mình hoặc trên đám mây để làm hồ sơ cá nhân.

CHỮ KÝ SỐ

CÁC LOẠI CHỮ KÝ VÀ THỜI ĐIỂM SỬ DỤNG

Chữ ký điện tử:

Ưu điểm chữ ký điện tử:

Lợi ích chính của việc sử dụng chữ ký điện tử là sự tiện lợi. Bạn không cần phải gặp mặt trực tiếp để ký thỏa thuận, điều đó có nghĩa là bạn có thể dễ dàng tiến hành công việc kinh doanh ở những khoảng cách xa hoặc khi làm việc tại nhà.
Chữ ký điện tử giúp các công ty có thể cung cấp các sản phẩm và dịch vụ mà chúng ta thường sử dụng trực tuyến. Hãy tưởng tượng nếu bạn phải đợi một hợp đồng qua thư mỗi khi bạn muốn đăng ký một nền tảng phát nhạc hoặc phim trực tuyến. Bạn sẽ phải ký tên, gửi lại và sau đó đợi nó được xử lý. Internet sẽ không bao giờ trở thành như ngày nay nếu không có khả năng chữ ký điện tử.

Nhược điểm chữ ký điện tử

Đôi khi bạn có thể thích chữ ký ướt hơn chữ ký điện tử. Như đã đề cập ở trên, có thể có lợi khi các bên cùng nhau ký kết một số thỏa thuận. Nếu bạn vẫn có thông tin chi tiết cần tìm hiểu hoặc nếu bạn muốn trực tiếp tiến hành công việc kinh doanh của mình để đạt được các mục tiêu kết nối mối quan hệ của mình, thì gặp trực tiếp có thể là lựa chọn tốt hơn.
Bạn cũng có thể muốn có được chữ ký ướt trong các tình huống mà bạn cần phải rất cẩn thận trong việc xác minh danh tính của bên kia. Việc ký thỏa thuận trực tiếp làm giảm khả năng gian lận.

CHỮ KÝ SỐ

CÁC LOẠI CHỮ KÝ VÀ THỜI ĐIỂM SỬ DỤNG

Chữ ký số:

Thuật ngữ "chữ ký số" là một chút sai lệch. Bạn có thể cho rằng chữ ký điện tử và chữ ký số là giống nhau, nhưng chúng khác nhau ở một số điểm quan trọng.
Chữ ký số là một phương thức xác thực cho phép mã được đính kèm dưới dạng chữ ký. Các cơ quan chứng nhận bên thứ ba cấp chữ ký số và các khóa liên quan.
Bạn có thể coi chữ ký số giống như dấu vân tay số hóa được nhúng trong file tài liệu. Nó vượt xa chữ ký điện tử bằng cách thực sự xác nhận tính xác thực của tài liệu. Nó tương tự như cách một dịch vụ công chứng thêm tính hợp lệ cho chữ ký ướt.

Khi nào nên sử dụng chữ ký số

Trong nhiều trường hợp, chữ ký số là một phần của quy trình ẩn bên trong mà bạn thậm chí không nhận thấy. Ví dụ: nếu bạn sử dụng Microsoft Outlook để xử lý email của mình, thì bạn đang sử dụng chữ ký điện tử mỗi khi gửi email. Microsoft đặt chữ ký điện tử trên mọi email được gửi từ máy chủ của mình.
Thông thường, ta sử dụng chữ ký số bên cạnh chữ ký điện tử. Đây là trường hợp khi một tài liệu điện tử nhắc bạn thêm chữ ký số tùy chọn để tăng cường bảo mật. Không ai khác ngoài người nhận được ủy quyền có thể xem tài liệu.

CHỮ KÝ SỐ

CÁC LOẠI CHỮ KÝ VÀ THỜI ĐIỂM SỬ DỤNG

Chữ ký số:

Có một số yếu tố cần xem xét khi quyết định có nên sử dụng quy trình chứng nhận chữ ký số hay không.

Ưu điểm chữ ký số:

Chữ ký điện tử có thể làm cho hợp đồng trở nên ràng buộc về mặt pháp lý hơn. Quy trình chứng nhận chữ ký số bổ sung tính bảo mật cho tài liệu và cho phép tài liệu được giữ riêng tư giữa các bên.

Nhược điểm chữ ký số:

Trải qua quá trình lấy chữ ký số có thể tốn thời gian và có thể không lý tưởng cho các thỏa thuận nhạy cảm về thời gian. Nó cũng có thể trở nên đắt đỏ nếu bạn cần sử dụng dịch vụ chữ ký số thường xuyên.

CHỮ KÝ SỐ

CÁC LOẠI CHỮ KÝ VÀ THỜI ĐIỂM SỬ DỤNG

Chữ ký click-wrap:

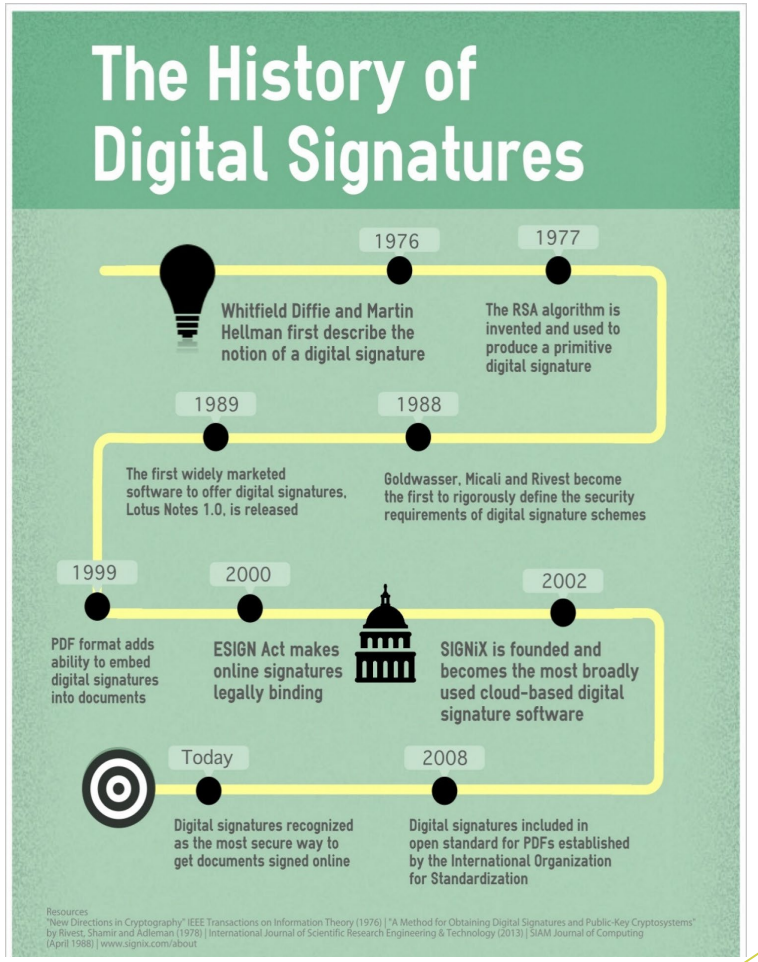
Chữ ký clickwrap không phải là chữ ký theo nghĩa thông thường, nhưng kết quả tương tự như các phương pháp khác. Clickwrap, hoặc "thỏa thuận nhấp qua", đề cập đến quá trình đánh dấu vào ô để chấp nhận các điều khoản và điều kiện. Bạn chắc chắn đã sử dụng clickwrap để đồng ý với các điều khoản của trang web, cho phép cài đặt ứng dụng trên điện thoại của mình hoặc đăng ký bảo hành khi mua hàng lớn.

Là chủ sở hữu doanh nghiệp, bạn có thể bao gồm khả năng clickwrap trên trang web của mình trong một số trường hợp nhất định. Ví dụ: nếu trang web của bạn cung cấp chat room hoặc forum, bạn có thể muốn những người đóng góp đồng ý tuân thủ các quy tắc cụ thể khi họ đóng góp. Đây cũng có thể là một cách đơn giản, an toàn để người dùng xác minh rằng họ đồng ý với các điều khoản và điều kiện của bạn trước khi đăng ký dịch vụ của bạn.

CHỮ KÝ SỐ

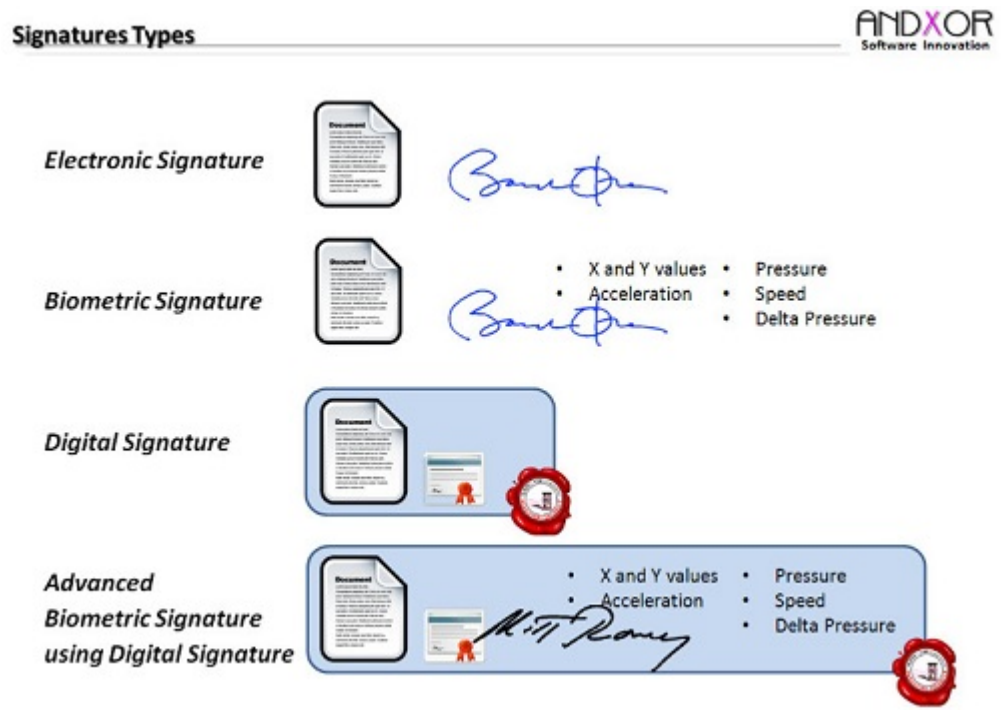
Lịch sử hình thành chữ ký số:

- **1976:** Whitfield Diffie và Martin Hellman lần đầu tiên mô tả ý tưởng về lược đồ chữ ký số, nhưng họ chỉ đưa ra giả thiết rằng các lược đồ đó tồn tại
- **1977:** Ronald Rivest, Adi Shamir và Len Adleman đã phát minh ra thuật toán RSA, thuật toán này có thể được sử dụng để tạo ra một chữ ký số nguyên thủy.
- **1988:** Lotus Notes 1.0 sử dụng thuật toán RSA, trở thành gói phần mềm tiếp thị rộng rãi đầu tiên cung cấp chữ ký số.
- **1999:** Khả năng nhúng chữ ký số vào tài liệu được thêm vào định dạng PDF
- **2000:** Đạo luật ESIGN làm cho chữ ký điện tử có tính ràng buộc về mặt pháp lý
- **2002:** SIGNiX được thành lập và trở thành phần mềm chữ ký số dựa trên đám mây được sử dụng rộng rãi nhất.
- **2008**: Định dạng file PDF trở thành tiêu chuẩn mở của Tổ chức Tiêu chuẩn hóa Quốc tế (ISO) với tên gọi ISO 32000. Bao gồm chữ ký số như một phần không thể thiếu của định dạng.
- **Ngày nay** chữ ký số được công nhận là cách an toàn nhất để ký tài liệu trực tuyến



CHỮ KÝ SỐ

Phân biệt giữa chữ ký điện tử(Electronic Signature) và chữ ký số (Digital Signature)



Giống nhau: Tính duy nhất của cả hai loại chữ ký này đó là đều **thay thế cho chữ ký viết tay truyền thống** và được sử dụng trong các giao dịch trực tuyến.

CHỮ KÝ SỐ

Phân biệt giữa chữ ký điện tử(Electronic Signature) và chữ ký số (Digital Signature)

Yếu tố so sánh	Chữ ký điện tử (Electronic Signature)	Chữ ký số (Digital Signature)
Tính chất	**Chữ ký điện tử** có thể là bất kỳ biểu tượng, hình ảnh, quy trình nào được đính kèm với tin nhắn hoặc tài liệu biểu thị danh tính của người ký và hành động đồng ý với nó.	**Chữ ký số** có thể được hình dung như một "dấu vân tay" điện tử, được mã hóa và xác định danh tính người thực sự ký nó.
Tiêu chuẩn	Không phụ thuộc vào các tiêu chuẩn. Không sử dụng mã hóa.	Sử dụng các phương thức **mã hóa mật mã**.
Cơ chế xác thực	Xác minh danh tính người ký thông qua email, mã PIN điện thoại, v.v.	ID kỹ thuật số dựa trên **chứng chỉ – Digital Signature Certificate (DSC)**.
Tính năng	**Xác minh** một tài liệu.	**Bảo mật** một tài liệu.
Xác nhận	Không có quá trình xác nhận cụ thể.	Được thực hiện bởi các **cơ quan chứng nhận tin cậy** hoặc **nhà cung cấp dịch vụ ủy thác**.
Bảo mật	Dễ bị giả mạo.	**Độ an toàn cao**.
Phần mềm độc quyền	Có thể được xác nhận bởi bất cứ ai mà không cần phần mềm xác minh độc quyền	Trong nhiều trường hợp, chữ ký số không được ràng buộc về mặt pháp lý và sẽ yêu cầu phần mềm độc quyền để xác nhận chữ ký số.

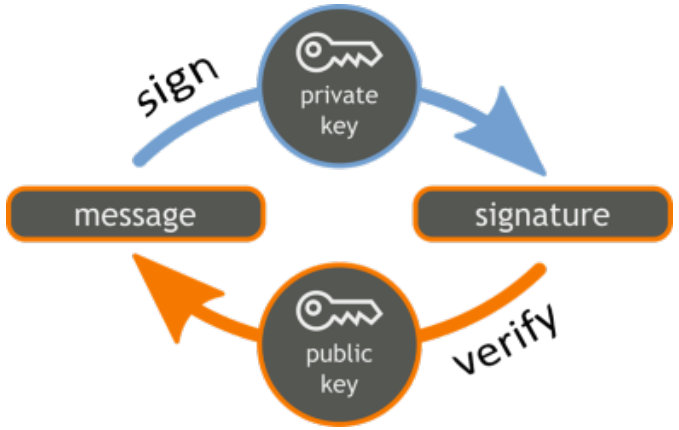
CHỮ KÝ SỐ

Định nghĩa:

Chữ ký số là một kỹ thuật toán học được sử dụng để xác nhận tính xác thực, tính toàn vẹn và tính không thoái thác của một thông điệp, phần mềm hoặc tài liệu kỹ thuật số.

Đặc điểm chữ ký số:

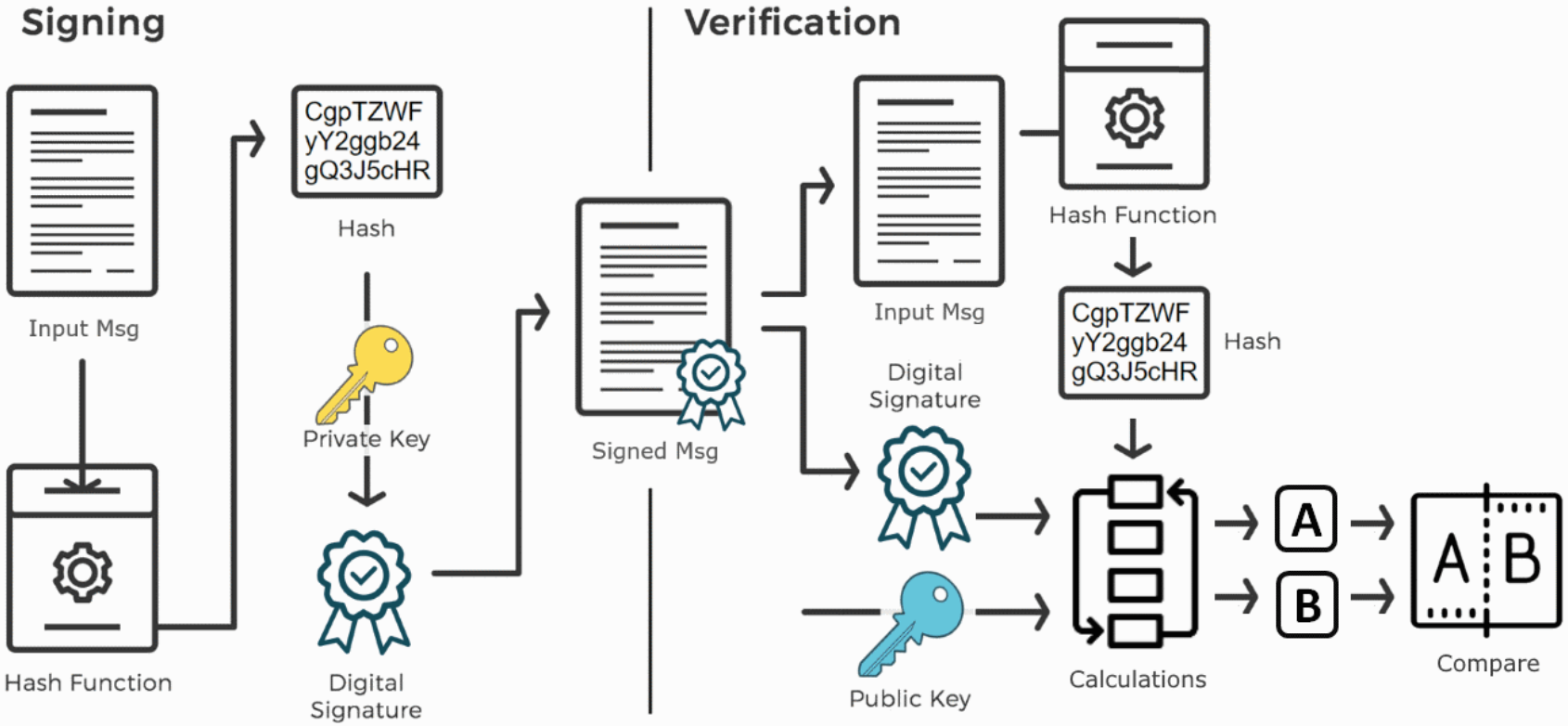
- Một kỹ thuật liên kết một người/thực thể với dữ liệu số. Sự ràng buộc này có thể được xác minh độc lập bởi người nhận cũng như bất kỳ bên thứ ba nào.
- Một giá trị mật mã được tính toán từ dữ liệu và khóa bí mật chỉ người ký mới biết.
- Trong thế giới thực, người nhận tin nhắn cần đảm bảo rằng tin nhắn đó thuộc về người gửi. Người gửi không thể thoái thác nguồn gốc của tin nhắn đó. Yêu cầu này rất quan trọng trong các ứng dụng kinh doanh, vì khả năng xảy ra tranh chấp về dữ liệu được trao đổi là rất cao



CHỮ KÝ SỐ

Mô hình chữ ký số:

Sơ đồ chữ ký số dựa trên mật mã khóa công khai. Mô hình sơ đồ chữ ký số được mô tả trong hình dưới:



CHỮ KÝ SỐ

Các bước thuật toán tạo chữ ký số:

1. **Thuật toán tạo khóa (key)**: Chữ ký số là chữ ký điện tử, đảm bảo rằng thông điệp được gửi bởi một người gửi cụ thể. Trong khi thực hiện các giao dịch kỹ thuật số, tính xác thực và tính toàn vẹn phải được đảm bảo, nếu không, dữ liệu có thể bị thay đổi hoặc ai đó cũng có thể hành động như thể anh ta là người sở hữu.

2. **Thuật toán ký:** Để tạo chữ ký số, các thuật toán ký giống như chương trình email tạo ra một hàm băm một chiều của dữ liệu điện tử sẽ được ký. Sau đó, thuật toán ký sẽ mã hóa giá trị băm bằng khóa riêng (khóa chữ ký). Hàm băm được mã hóa này cùng với các thông tin khác như thuật toán băm là chữ ký số. Chữ ký số này được nối với dữ liệu và được gửi đến người xác minh. Lý do mã hóa hàm băm thay vì toàn bộ tin nhắn hoặc tài liệu là hàm băm chuyển đổi bất kỳ đầu vào tùy ý nào thành giá trị có độ dài cố định ngắn hơn nhiều. Điều này giúp tiết kiệm thời gian và hơn nữa băm nhanh hơn nhiều so với ký.

3. **Thuật toán xác minh chữ ký:** Người xác minh nhận Chữ ký số cùng với dữ liệu. Sau đó, nó sử dụng thuật toán Xác minh để xử lý trên chữ ký số và khóa công khai (khóa xác minh), sau đó tạo ra một số giá trị. Nó cũng áp dụng cùng một hàm băm trên dữ liệu nhận được và tạo ra một giá trị băm. Sau đó, giá trị băm và đầu ra của thuật toán xác minh được so sánh. Nếu cả hai đều bằng nhau, thì chữ ký điện tử là hợp lệ, nếu không thì chữ ký điện tử đó không hợp lệ.

CHỮ KÝ SỐ

Tầm quan trọng của chữ ký số:

Trong số tất cả các nguyên tắc mật mã, chữ ký số sử dụng mật mã khóa công khai được coi là công cụ rất quan trọng và hữu ích để đạt được an toàn thông tin.

Ngoài khả năng cung cấp tính năng chống từ chối thông điệp, chữ ký số còn cung cấp khả năng xác thực thông điệp và tính toàn vẹn của dữ liệu.

Xác thực tin nhắn: Khi người xác minh xác thực chữ ký số bằng khóa chung (public key) của người gửi. Họ được đảm bảo rằng chữ ký chỉ được tạo bởi người gửi sở hữu khóa bí mật (private key) tương ứng chứ không phải ai khác.

Tính toàn vẹn của dữ liệu: Trong trường hợp kẻ tấn công có quyền truy cập vào dữ liệu và sửa đổi dữ liệu đóm, thì việc xác minh chữ ký số ở đầu nhận không thành công. Hàm băm của dữ liệu đã sửa đổi và đầu ra do thuật toán xác minh cung cấp sẽ không khớp. Do đó, người nhận có thể từ chối thông báo một cách an toàn với giả định rằng tính toàn vẹn của dữ liệu đã bị vi phạm

Không thoái thác: Vì người ta cho rằng chỉ người ký mới biết về khóa chữ ký, nên anh ta chỉ có thể tạo chữ ký duy nhất trên một dữ liệu nhất định. Do đó, người nhận có thể giải trình dữ liệu vàc chữ ký số với bên thứ ba làm bằng chứng nếu có bất kỳ tranh chấp nào phát sinh trong tương lai.

Bằng cách thêm mã hóa khóa công khai vào sơ đồ chữ ký số, chúng ta có thể tạo một hệ thống mật mã cung cấp 4 yếu tố bảo mật thiếu yếu là – Quyền riêng tư, Xác thực, Tính toàn vẹn và không thoái thác

CHỮ KÝ SỐ

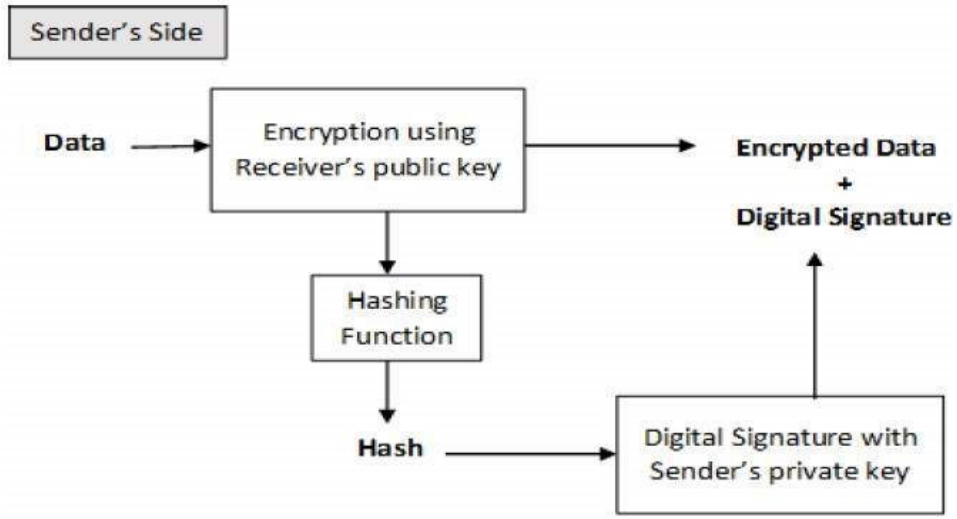
Các yêu cầu khi tạo chữ ký số:

CHỮ KÝ SỐ

Mã hóa chữ ký số:

Trong nhiều giao tiếp kỹ thuật số, mong muốn trao đổi một tin nhắn được mã hóa hơn là văn bản gốc để đạt được tính bảo mật. Trong sơ đồ mã hóa khóa công khai, khóa (mã hóa) công khai của người gửi có sẵn trong miền mở(internet) và do đó, bất kỳ ai cũng có thể giả mạo danh tính của anh ta và gửi bất kỳ tin nhắn được mã hóa nào đến người nhận.

Điều này khiến người dùng sử dụng mật mã khóa công khai để mã hóa cần tìm kiếm chữ ký số cùng với dữ liệu được mã hóa để đảm bảo xác thực thông báo và không thoái thác.
Điều này có thể được lưu trữ bằng cách kết hợp chữ ký số với sơ đồ mã hóa. Có **hai khả năng, ký rồi mã hóa** và **mã hóa rồi ký** .
Tuy nhiên, hệ thống mật mã dựa trên ký rồi mã hóa có thể bị người nhận khai thác để giả mạo danh tính của người gửi và gửi dữ liệu đó cho bên thứ ba. Do đó, phương pháp này không được ưa thích. Quá trình mã hóa-rồi-ký đáng tin cậy hơn và được áp dụng rộng rãi. Điều này được mô tả trong hình minh họa sau:



Người nhận sau khi nhận được dữ liệu được mã hóa và chữ ký trên đó, trước tiên sẽ xác minh chữ ký bằng khóa chung của người gửi. Sau khi đảm bảo tính hợp lệ của chữ ký, anh ta sẽ truy xuất dữ liệu thông qua giải mã bằng khóa riêng của mình.

CHỮ KÝ SỐ

CÁC LOẠI TẤN CÔNG VÀO CHỮ KÝ SỐ

Có 3 loại tấn công thường nhằm vào chữ ký số:

- Tấn công bằng thông điệp đã chọn (Chosen message attack)
- Tấn công bằng thông điệp đã biết (Known message attack)
- Tấn công chỉ bằng khóa (Key only attack)

CHỮ KÝ SỐ

CÁC LOẠI TẤN CÔNG VÀO CHỮ KÝ SỐ

1. Tấn công bằng thông điệp đã chọn (Chosen message attack):

Phương pháp tấn công được chọn có hai loại:

- **Phương pháp được chọn chung –** Trong phương pháp này, C đánh lừa A để ký điện tử vào các thông báo mà A không có ý định thực hiện và không biết về khóa công khai của A.

- **Phương pháp được chọn trực tiếp –** Trong phương pháp này, C có kiến thức về khóa công khai của A và có được chữ ký của A trên các tin nhắn và thay thế tin nhắn gốc bằng tin nhắn C muốn A ký với chữ ký của A trên chúng không thay đổi.

2. Tấn công bằng thông điệp đã biết:

Trong cuộc tấn công bằng tin nhắn đã biết, C có một vài tin nhắn và chữ ký trước đó của A. Bây giờ C cố gắng giả mạo chữ ký của A trên các tài liệu mà A không có ý định ký bằng cách sử dụng phương pháp vũ phu bằng cách phân tích dữ liệu trước đó để tạo lại chữ ký của A. Cuộc tấn công này tương tự như cuộc tấn công văn bản đơn giản đã biết trong mã hóa.

3. Tấn công chỉ dùng khóa:

Trong tấn công chỉ dùng khóa, khóa công khai của A có sẵn cho mọi người và C tận dụng thực tế này và cố gắng tạo lại chữ ký của A và ký điện tử vào các tài liệu hoặc tin nhắn mà A không có ý định thực hiện. Điều này sẽ gây ra mối đe dọa lớn đối với việc xác thực thông báo không bị từ chối vì A không thể từ chối việc ký vào nó.

CHỮ KÝ SỐ

ỨNG DỤNG CỦA CHỮ KÝ SỐ

Lợi ích của Chữ ký số:

- **Văn bản pháp lý và hợp đồng:** Chữ ký số có tính ràng buộc về mặt pháp lý. Điều này làm cho chúng trở nên lý tưởng cho bất kỳ tài liệu pháp lý nào yêu cầu chữ ký được xác thực bởi một hoặc nhiều bên và đảm bảo rằng hồ sơ không bị thay đổi.
- **Hợp đồng mua bán:** Việc ký điện tử các hợp đồng và hợp đồng mua bán xác thực danh tính của người bán, người mua, và cả hai bên có thể chắc chắn rằng chữ ký có tính ràng buộc về mặt pháp lý cũng như các điều khoản của thỏa thuận không bị thay đổi.
- **Tài liệu tài chính:** Bộ phận tài chính ký điện tử hóa đơn để khách hàng có thể tin tưởng rằng yêu cầu thanh toán là từ đúng người bán chứ không phải từ một kẻ xấu đang cố lừa người mua gửi thanh toán đến tài khoản lừa đảo.
- **Dữ liệu sức khỏe:** Trong ngành chăm sóc sức khỏe, quyền riêng tư là tối quan trọng đối với cả hồ sơ bệnh nhân và dữ liệu nghiên cứu. Chữ ký điện tử đảm bảo rằng thông tin bí mật này không bị sửa đổi khi được truyền giữa các bên xác nhận.
- **Các cơ quan chính quyền trung ương, địa phương** có các chính sách và quy định chặt chẽ hơn so với nhiều công ty thuộc khu vực tư nhân. Từ phê duyệt giấy phép đến đóng dấu chúng trên bảng chấm công, chữ ký điện tử có thể tối ưu hóa năng suất bằng cách đảm bảo đúng người tham gia phê duyệt thích hợp.
- **Chứng từ vận chuyển:** Giúp các nhà sản xuất tránh các lỗi vận chuyển tốn kém bằng cách đảm bảo các bản kê khai hàng hóa hoặc vận đơn luôn chính xác. Tuy nhiên, giấy tờ giấy rất cồng kềnh, không phải lúc nào cũng dễ lấy trong quá trình vận chuyển và có thể bị thất lạc. Bằng cách ký điện tử các tài liệu vận chuyển, người gửi và người nhận có thể nhanh chóng truy cập vào file, kiểm tra xem chữ ký có được cập nhật hay không và đảm bảo rằng không có sự giả mạo nào xảy ra.

CHỮ KÝ SỐ

ỨNG DỤNG CỦA CHỮ KÝ SỐ

Một số loại chữ ký số thông dụng trên thị trường hiện nay:

1. **Chữ ký số USB token**

   Ra đời đầu tiên trên thị trường, **chữ ký số USB Token** là loại chữ ký số truyền thống và hiện nay vẫn đang được phần đông các doanh nghiệp, cá nhân sử dụng để ký số chứng từ, tài liệu. Đặc trưng của chữ ký số USB Token là sử dụng một thiết bị phần cứng có hình dạng USB để lưu trữ khóa bí mật giúp tạo lập chữ ký số.

   Quá trình ký số của chữ ký số USB Token yêu cầu sự kết nối của USB Token và máy tính nên không tránh khỏi một số bất cập như không thể ký số từ xa khi không có Token hay việc ký số bị giới hạn trên máy tính. Ngoài ra, chữ ký số USB Token cũng không đáp ứng được nhu cầu sử dụng nhiều người trên 1 Token. Tuy nhiên, ưu điểm vượt trội của chữ ký số USB Token là dễ sử dụng và có độ bảo mật cao, khó có thể làm giả.

2. **Chữ ký số Smarcard**

   Chữ ký số Smartcard là loại chữ ký số được tích hợp trên sim do một số nhà mạng nghiên cứu và phát triển. Với chữ ký số Smartcard, người dùng có thể ký số nhanh chóng và linh động trên điện thoại di động.

   Mặc dù vậy, loại chữ ký số này còn hạn chế phạm vi người dùng khi người dùng bị phụ thuộc vào loại sim mà nhà cung cấp lựa chọn. Đồng thời, nguy cơ không thể thực hiện ký số nếu sim nằm ngoài vùng phủ sóng cũng là một nhược điểm khác tồn tại ở chữ ký số Smartcard.

CHỮ KÝ SỐ

ỨNG DỤNG CỦA CHỮ KÝ SỐ

Một số loại chữ ký số thông dụng trên thị trường hiện nay:

3. Chữ ký số HSM

Chữ ký số HSM(Hardware security module) là một thiết bị phần cứng dùng để bảo vệ và quản lý các cặp khóa điện tử, giúp tăng tốc độ xác thực và mã hóa dữ liệu. Chữ ký số HSM được đánh giá có nhiều tính năng cao cấp hơn so với USB Token và Smartcard để đáp ứng nhu cầu hoạt động của các hệ thống lớn, có yêu cầu cao về hiệu năng và tính bảo mật.

Nhược điểm của chữ ký số HSM là giá thành khá cao và chỉ phù hợp với những doanh nghiệp lớn, có hệ thống quy mô lớn và cơ sở hạ tầng tốt. Ngoài ra, chữ ký số HSM cho phép nhiều người cùng ký số tại các điểm khác nhau nhưng thường giới hạn dưới 20 điểm truy cập ký số.

4. Chữ ký số từ xa

Đây là loại chữ ký số mới xuất hiện trên thị trường và khác biệt với những loại chữ ký số thông dụng khác bởi thay vì dựa vào thiết bị phần cứng, chữ ký số từ xa (Remote signature) được sử dụng trên nền tảng công nghệ điện toán đám mây. Đặc điểm này giúp người dùng có thể ký số linh động mọi lúc, mọi nơi trên máy tính, điện thoại hay tablet một cách trực tiếp mà không bị phụ thuộc vào thiết bị phần cứng như USB Token hay sim,…

Tuy loại bỏ những bất cập xung quanh việc phụ thuộc vào thiết bị phần cứng nhưng chữ ký số từ xa vẫn chưa được ưu tiên sử dụng do còn vướng mắc một số vấn đề xung quanh việc bảo mật dữ liệu. Để nghiên cứu và phát triển được loại chữ ký số này đòi hỏi nhà cung cấp phải có hạ tầng công nghệ tốt, đặc biệt phải tuân thủ tuyệt đối các tiêu chuẩn về bảo mật theo đúng quy định.

CHỨNG CHỈ SỐ

Giấy chứng nhận điện tử

Chứng chỉ số được cấp bởi một bên thứ ba đáng tin cậy chứng minh danh tính của người gửi đối với người nhận và danh tính của người nhận đối với người gửi.

Chứng chỉ kỹ thuật số là chứng chỉ do Tổ chức phát hành chứng chỉ (CA) cấp để xác minh danh tính của chủ sở hữu chứng chỉ. CA cấp chứng chỉ kỹ thuật số được mã hóa có chứa khóa công khai của người nộp đơn và nhiều thông tin nhận dạng khác. Chứng chỉ số dùng để đính kèm khóa công khai với một cá nhân hoặc một tổ chức cụ thể.

Chứng chỉ số bao gồm: - Tính xác thực

1.Tên người được cấp chứng chỉ.
2.Số sê-ri được sử dụng để xác định duy nhất một chứng chỉ, cá nhân hoặc tổ chức được xác định bởi chứng chỉ
3.Ngày hết hạn.
4.Bản sao khóa công khai của chủ sở hữu chứng chỉ. (được sử dụng để giải mã tin nhắn và chữ ký số)
5.Chữ ký số của cơ quan cấp chứng chỉ.

Chứng chỉ số cũng được gửi cùng với chữ ký số và thông điệp.

Chứng chỉ số so với chữ ký số:

Chữ ký số được sử dụng để xác minh tính xác thực, tính toàn vẹn, không từ chối, tức là đảm bảo rằng tin nhắn được gửi bởi người dùng đã biết và không bị sửa đổi. Trong khi chứng chỉ số được sử dụng để xác minh danh tính của người dùng, có thể là người gửi hoặc người nhận. Do đó, chữ ký số và chứng chỉ là những thứ khác nhau nhưng cả hai đều được sử dụng để bảo mật. Hầu hết các trang web sử dụng chứng chỉ kỹ thuật số để tăng cường sự tin tưởng của người dùng của họ

CHỨNG CHỈ SỐ

Tính năng	Chữ ký số	Giấy chứng nhận điện tử
Khái niệm cơ bản / Định nghĩa	Chữ ký điện tử giống như dấu vân tay hoặc file đính kèm vào tài liệu kỹ thuật số để đảm bảo tính xác thực và tính toàn vẹn của nó.	Chứng chỉ kỹ thuật số là một file đảm bảo danh tính của chủ sở hữu và cung cấp bảo mật.
Quy trình / Các bước	Giá trị băm của tin nhắn gốc được mã hóa bằng khóa bí mật của người gửi để tạo chữ ký số.	Nó được tạo bởi CA (Cơ quan chứng nhận) bao gồm bốn bước: Sinh khóa, Đăng ký, Xác minh, Tạo.
Dịch vụ an ninh	Tính xác thực của Người gửi, tính toàn vẹn của tài liệu và tính chống từ chối .	Nó cung cấp bảo mật và tính xác thực của chủ sở hữu chứng chỉ.
Tiêu chuẩn	Nó tuân theo Tiêu chuẩn Chữ ký Số (Digital Signature Standard - DSS).	Nó tuân theo định dạng chuẩn X.509