Digital Signature – Chữ ký số là gì ?

**Chữ ký số (digital signature)** là một kĩ thuật xác thực cho phép người chủ nội dung của 1 thông điệp được quyền đính kèm 1 đoạn dữ liệu số như là chữ kí đánh dấu của người chủ đối với nội dung đã tạo ra. Về cơ bản, chữ kí số sẽ được tạo ra bằng cách hash nội dung thông điệp sau đấy mã hoá chuỗi hash bằng khoá bí mật (**private key**) của người chủ nội dung.

**Chữ ký số**, digital signature, giúp ta đạt được những mục đích sau :

– **Non-repudiation** : có thể hiểu là giúp cho người nhận khi kiểm tra nội dung đã được ký chữ ký số kèm theo sẽ biết chắc người ký không thể chối cãi về những gì đã tạo ra ở thời điểm bắt đầu tạo chữ kí số.

– **Integrity** : chữ ký số giúp kiểm tra tính toàn vẹn dữ liệu của nội dung được gửi đi là không bị thay đổi hay chỉnh sửa kể từ lúc khởi tạo chữ ký số và ký vào văn bản gửi đi.

– **Authenticity** : chữ ký số cũng dùng để chứng thực nguồn gửi nội dung thông điệp đi. Thường thì thông tin về người chủ của chữ ký sẽ được thêm vào kèm với nội dung chữ ký số để giúp người nhận chứng thực được ai đã gửi thông điệp đi.

**Chữ ký số** ứng dụng nhiều trong các hoạt động cấp chứng chỉ Certificate SSL,… Chữ ký số cũng có có thể sử dụng trong các giao dịch thư điện tử, để mua bán hàng trực tuyến, đầu tư chứng khoán trực tuyến, chuyển tiền ngân hàng, thanh toán trực tuyến mà không sợ bị đánh cắp tiền như với các tài khoản Visa, Master.

**I. Các yêu cầu thành phần để tạo ra được chữ ký số**

– Chữ ký số dựa trên công nghệ mã hoá khóa công khai (RSA): mỗi người dùng phải có 1 cặp khóa (key pair) bao gồm khóa công khai (public key) và khóa bí mật (private key).

+ **Private key** : là một khóa trong cặp khóa thuộc hệ thống mật mã không đối xứng, được dùng để tạo chữ ký số.

+ **Public key** : là một khóa trong cặp khóa thuộc hệ thống mật mã không đối xứng, được sử dụng để giả mã kiểm tra chữ ký số được tạo bởi khóa bí mật tương ứng trong cặp khóa.

+ **Digital Sign** (ký số) : là việc đưa khóa bí mật vào một chương trình phần mềm để tự động tạo và gắn chữ ký số vào thông điệp dữ liệu. Khi đọc các tài liệu chuyên ngành, bạn sẽ gặp nhiều cụm từ “**sign**” hoặc “**signed <object>**“, thì bạn phải hiểu là liên quan đến hoạt động của chữ kí số.

+ **Signer** (người ký) : là đối tượng dùng đúng khóa bí mật của mình để tạo chữ ký số và ký vào một thông điệp dữ liệu dưới tên của mình.

+ **Recipient** (người nhận) : là tổ chức, cá nhân nhận được thông điệp dữ liệu được ký số bởi người ký, sử dụng chứng thư số (digital certificate) của người ký đó để kiểm tra chữ ký số trong thông điệp dữ liệu nhận được và tiến hành các hoạt động, giao dịch có liên quan.

**II. Thế Digital Signature hoạt động như thế nào ?**

Hoạt động tạo ra chữ ký số Digital Signature yêu cầu phải có 1 cặp key **public & private**. Người kí sẽ giữ **private key** và dùng để **mã hoá thông tin tạo ra chữ kí số**, người nhận phải có**public key** của người kí tương ứng cặp với private key để **giải mã chữ kí số** nhằm đối chiếu thông tin.

Vậy ta có thể hình dung như thế này, bạn có 1 văn bản word hợp đồng và bạn cần gửi cho luật sư của bạn. Điều quan trọng là làm sao để luật sư biết chắc chắn văn bản word hợp đồng này được soạn thảo bởi chính bạn hay đã được xét duyệt bởi bạn.

**Quá trình kí (Signing)**

Lúc này **quá trình kí (Signing)** sẽ diễn ra như sau :

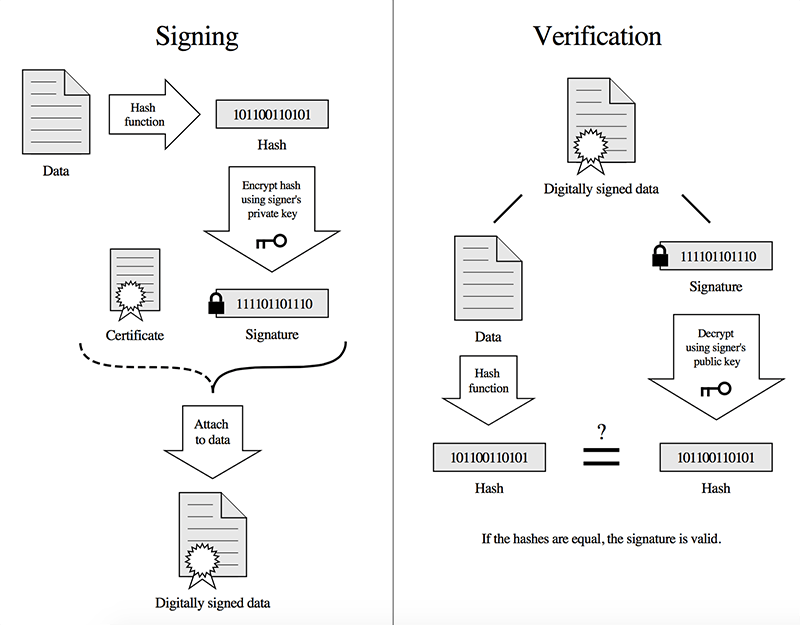
**1.** Ta có văn bản word hợp đồng .word (data).

**2.** Ta sử dụng chương trình**thuật toán băm** (MD5 hoặc SHA), băm văn bản word ra sẽ được 1 chuỗi kí tự duy nhất với độ dài cố định. Ta gọi là chuỗi H : (software) -> hash + word file -> string H .

– Thuật toán băm phải được thống nhất giữa 2 bên để có được kết quả chính xác giống nhau khi kiểm tra.

**3.** Sau đấy bạn sử dụng private key của bạn để mã hoá chuỗi băm từ văn bản word. Ta sẽ được 1 chuỗi ký tự hash đã được mã hoá gọi là cipher hash. Ta có thể gọi là chuỗi C : string H + private key người kí -> **cipher hash A**.

**4.** Lúc này “**cipher hash A”** chính là chữ kí số của người kí tạo ra là bạn (cipher hash A = digital signature). Nhiệm vụ lúc này của ta là thêm nó vào nội dung file word vào cuối văn bản, để bên kia nhận được nội dung văn bản và các chữ kí số.



*Hình trích nguồn từ Internet*

**Quá trình kiểm tra thông tin chữ kí số (Verification)**

Quá trình kiểm tra thông tin chữ ký số (Verification) sẽ diễn ra như sau :

**1.** Người nhận sẽ nhận được văn bản hợp đồng bao gồm nội dung chính + chữ kí số “**cipher hash A**” . Lúc này người nhận sẽ tách riêng nội dung văn bản hợp đồng và chữ kí số ra xử lý độc lập.

**2.** Ở phần nội dung văn bản hợp đồng, người nhận làm công việc giống người kí đó là ta sử dụng chương trình thuật toán băm (MD5 hoặc SHA) giống bên kí, băm văn bản word ra sẽ được 1 chuỗi kí tự duy nhất với độ dài cố định. Ta gọi là chuỗi H2 chẳng hạn sẽ đại diện cho chuỗi string hash của người nhận đã hash ra : (software) -> hash + word file -> **string H2**

**3.** Người nhận sử dụng public key của người kí (**signer’s public key**) để giải mã chuỗi “cipher hash A” đính kèm trong văn bản hợp đồng ra được chuỗi “**string H**” : cipher hash A + public key người kí -> **string H.**

**4.** Đối chiếu thông tin trùng khớp giữa string H và string H2 . Nếu khớp nhau tức nội dung chính xác, không bị thay đổi nội dung, chính xác của người đã tạo ra văn bản và hoàn tất quá trình kiểm tra thông tin chữ ký số (**verification**).

**Lưu ý :**

– Bất cứ thay đổi dù là nhỏ nhất vào nội dung thông điệp gửi đi (data) hay nôm na là văn bản hợp đồng sau khi đã khởi tạo chữ kí số cũng sẽ tạo ra kết quả hoàn toàn khác ở phía người nhận khi họ hash băm văn bản ra và đối chiếu với thông tin hash ở chữ kí số của bạn.