1. Đặc điểm chữ kí số

* Khả năng xác định nguồn gốc: Chữ ký số có thể xác thực danh tính chủ nhân của chữ ký số thông qua chứng thư số của cá nhân, tổ chức, DN.
* Tính bảo mật cao: Chữ ký số có 2 lớp mã khóa, đảm bảo tính bảo mật và không bị đánh cắp thông tin bởi hacker.
* Tính toàn vẹn: Chữ ký số đảm bảo chỉ có người nhận văn bản/tài liệu đã ký số mới có thể mở văn bản/tài liệu đó. Từ đó, đảm bảo tính toàn vẹn của văn bản/tài liệu điện tử trong môi trường điện tử.
* Tính không thể phủ nhận: Chữ ký số không thể xóa bỏ và thay thế.

1. Vai trò của chữ kí số

* Chữ ký số đóng một vai trò quan trọng trong việc xác nhận, đảm bảo về trách nhiệm, quyền và nghĩa vụ của các chủ thể tham gia ký kết văn bản hay giao dịch điện tử.
* Đặc biệt, chữ ký số có vai trò đảm bảo an toàn cho các giao dịch điện tử. Đây là yếu tố quan trọng nhất, là điều kiện tiên quyết khi chuyển các giao dịch có giá trị lớn trên giấy tờ sang giao dịch trên mạng, đem lại lợi thế cạnh tranh cho các DN trong bối cảnh hội nhập kinh tế quốc tế. Với các giao dịch thương mại điện tử B2C, giá trị các giao dịch nhỏ, các cá nhân thường sử dụng các thông tin trên thẻ tín dụng để xác thực sự đồng ý của mình và dùng các thông tin này tương đương với “chữ ký” khi thực hiện các giao dịch này. Với các giao dịch thương mại điện tử B2B có giá trị lớn, việc sử dụng chữ ký số là cần thiết vì tầm quan trọng của giao dịch và đòi hỏi về mức độ bảo mật cũng cao hơn.

1. Cấu tạo của chữ kí số

* -**- *Khóa công khai*** (**Public key**): được công bố rộng rãi cho mọi người và được dùng để mã hóa
* **-** ***Khóa bí mật*** (**Private key**): Những thông tin được mã hóa bằng khóa công khai chỉ có thể được giải mã bằng khóa bí mật tương ứng

RSA là một thuật toán mã hóa khóa công khai được sử dụng rộng rãi trong thương mại điện tử, là thuật toán đầu tiên phù hợp tạo ra chữ ký điện tử đồng thời với việc mã hóa. RSA đánh dấu sự tiến bộ vượt bậc của lĩnh vực mật mã trong sử dụng khóa công cộng, RSA đảm bảo an toàn với điều kiện độ dài khóa đủ lớn.

Có thể coi bài toán xác thực là bài toán "đối ngẫu" với bài toán bảo mật. Vì vậy, sử dụng ngược thuật toán RSA ta có thể có được một sơ đồ chữ ký số RSA như sau:

Giả sử n = pq, trong đó p và q là các số nguyên tố có kích thước tương đương.

CT1

Với K = (n, e, d), ta có D = d là khóa bí mật,

E = (n, e) là khóa công khai, m là bản tin cần ký.

Tạo chữ ký:  S = SigD(m) = mdmod n.

Kiểm tra chữ ký: VerE (m, S) = TRUE ↔ m = Semod n.

1. Ưu điểm của chữ kí số

* **a. Đảm bảo tính pháp lý trong giao dịch điện tử:** Chữ ký số có khả năng đảm bảo tính toàn vẹn của tài liệu điện tử cũng như xác định danh tính của người ký, là bằng chứng chống chối bỏ trách nhiệm trên các văn bản và nội dung đã ký. Đây được đánh giá là phương thức duy nhất để xác định tính pháp lý của văn bản điện tử hiện nay.
* **b. Đảm bảo an toàn, bảo mật thông tin:**Quá trình ký số được thực hiện dựa trên công nghệ mã hóa công khai có tính bảo mật cao, chỉ người có mật khẩu mới có khả năng ký. Việc giả mạo chữ ký số gần như là bất khả thi, trong khi khả năng giả mạo chữ ký tay có thể lên đến 55-70%. Chữ ký số còn có thể sử dụng hàm đặc biệt, đảm bảo chỉ người nhận mới có khả năng mở đọc văn bản đã ký số.
* **c. Tiết kiệm thời gian, công sức và chi phí cho doanh nghiệp:** Chữ ký số giúp giảm thời gian và công sức xử lý giấy tờ cho tất cả nhân sự trong doanh nghiệp. Thay vì phải in tài liệu, lưu trữ và ký tay từng văn bản, người dùng hoàn toàn có thể ký từ xa hàng loạt văn bản điện tử và gửi trực tiếp cho lãnh đạo, đối tác, khách hàng,… Thế mạnh của ký số được phát huy tối đa trong bối cảnh làm việc từ xa (remote work) như hiện nay.

* **d. Tiện lợi cho lịch trình làm việc của CEO và các cấp quản lý:** Nhờ có chữ ký số, việc ký kết có thể diễn ra ở bất kỳ đâu trong bất kỳ thời gian nào, trên cả PC và các thiết bị di động như laptop, máy tính bảng hoặc điện thoại. Yếu tố này đặc biệt hữu ích với các CEO, lãnh đạo doanh nghiệp - những người cần ký duyệt nhiều nhưng thường xuyên bận việc hoặc làm việc ngoài văn phòng.

1. Hàm băm
   1. Hàm băm (Hash Funtion) làm hàm toán học chuyển đổi thông điệp (message) có độ dài bất kỳ (hữu hạn) thành một dãy bít có độ dài cố định (tùy thuộc vào thuật toán băm). Dãy bít này được gọi là thông điệp rút gọn.(message disgest) hay giá trị băm (hash value), đại diện cho thông điệp ban đầu.
      1. Hàm băm SHA-1: Thuật toán SHA-1 nhận thông điệp ở đầu vào có chiều dài k<264 bit, thực hiện xử lý và đưa ra thông điệp thu gọn (message digest) có chiều dài cố định 160 bits. Quá trình tính toán cũng thực hiện theo từng khối 512bits, nhưng bộ đệm xử lý dùng 5 thanh ghi 32-bits. Thuật toán này chạy tốt với các bộ vi xử lý có cấu trúc 32 bits.
2. Quá trình bên gửi

* Tính toán chuỗi đại diện (message digest/ hash value) của thông điệp sử dụng một giải thuật băm (Hashing algorithm)
* Chuỗi đại diện được ký sử dụng khóa riêng (Private key) của người gửi và 1 giải thuật tạo chữ ký (Signature/ Encryption algorithm). Kết quả chữ ký số (Digital signature) của thông điệp hay còn gọi là chuỗi đại diện được mã hóa (Encryted message digest)
* Thông điệp ban đầu (message) được ghép với chữ ký số( Digital signature) tạo thành thông điệp đã được ký (Signed message)
* Thông điệp đã được ký (Signed message) được gửi cho người nhận

1. Quá trình bên nhận

* Tách chữ ký số và thông điệp gốc khỏi thông điệp đã ký để xử lý riêng;
* Tính toán chuỗi đại diện MD1 (message digest) của thông điệp gốc sử dụng giải thuật băm (là giải thuật sử dụng trong quá trình ký)
* Sử dụng khóa công khai (Public key) của người gửi để giải mã chữ ký số -> chuỗi đại diện thông điệp MD2
* So sánh MD1 và MD2:
  + Nếu MD1 =MD2 -> chữ ký kiểm tra thành công. Thông điệp đảm bảo tính toàn vẹn và thực sự xuất phát từ người gửi (do khóa công khai được chứng thực).
  + Nếu MD1 <>MD2 -> chữ ký không hợp lệ. Thông điệp có thể đã bị sửa đổi hoặc không thực sự xuất phát từ người gửi.



