1. Chữ ký số

1.1 Một số khái niệm

Chữ ký số (Digital signature) là một chuỗi dữ liệu liên kết với một thông điệp (message) và thực thể tạo ra thông điệp. Chữ ký số thường được sử dụng để đảm bảo tính toàn vẹn của thông điệp.

Giải thuật tạo chữ ký số (Digital signature generation algorithm) là một phương pháp sinh chữ ký số;

Giải thuật kiểm tra chữ ký số (Digital signature verification algorithm) là một phương pháp xác minh tính xác thực của chữ ký số, có nghĩa là nó thực sự được tạo ra bởi 1 bên chỉ định;

Một hệ chữ ký số (Digital signature scheme) bao gồm giải thuật tạo chữ ký số và giải thuật kiểm tra chữ ký số.

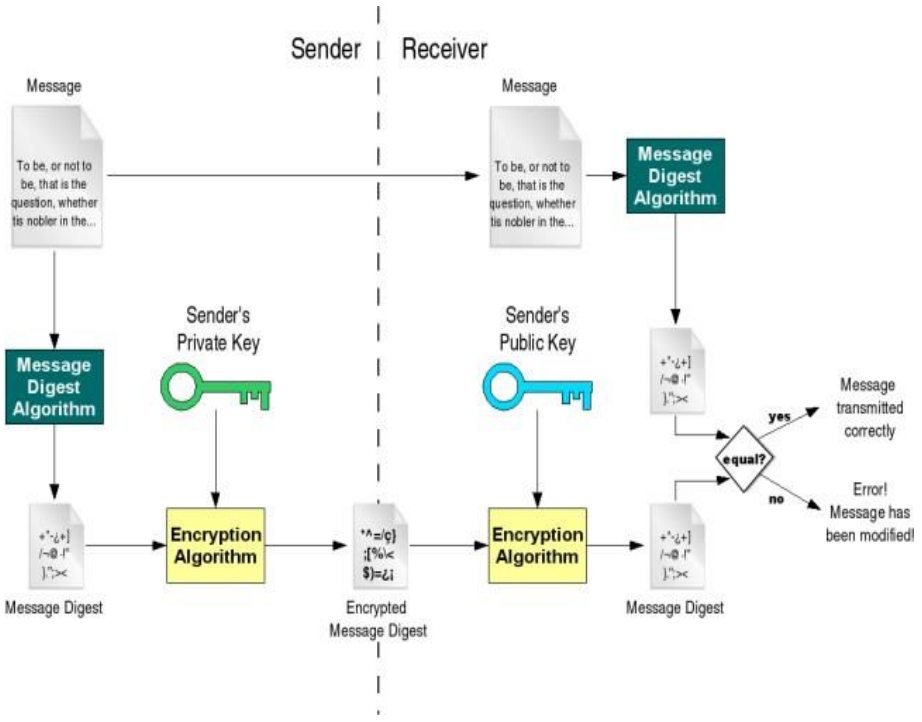
Quá trình tạo chữ ký số (Digital signature signing process) bao gồm:

- Giải thuật tạo chữ ký số, và
- Phương pháp chuyển dữ liệu thông điệp thành dạng có thể ký được.

Quá trình kiểm tra chữ ký số (Digital signature verification process) bao gồm:

- Giải thuật kiểm tra chữ ký số, và
- Phương pháp khôi phục dữ liệu từ thông điệp.

1.2 Quá trình ký và kiểm tra



Hình 3.34. Quá trình tạo chữ ký số và kiểm tra chữ ký số

Hình 3.34 biểu diễn quá trình tạo chữ ký số và kiểm tra chữ ký số cho một thông điệp (Message). Trong khi quá trình tạo chữ ký số cho thông điệp được thực hiện ở bên người gửi (Sender) thì quá trình kiểm tra chữ ký số của thông điệp được thực hiện ở bên người nhận (Receiver). Để có thể tạo và kiểm tra chữ ký số cho thông điệp, người gửi phải sở hữu cặp khóa công khai (Public key) và khóa riêng (Private key). Khóa riêng dùng để tạo chữ ký số và khóa công khai dùng để kiểm tra chữ ký số.

Các bước của quá trình tạo chữ ký số cho thông điệp (bên người gửi - Sender):

- 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 một giải thuật tạo chữ ký (Signature/Encryption algorithm). Kết quả là chữ ký số (Digital signature) của thông điệp hay còn gọi là chuỗi đại diện được mã hóa (Encrypted 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.

Các bước của quá trình kiểm tra chữ ký số của thông điệp (bên người nhận - Receiver):

- 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 để khôi phục chuỗi đại diện thông điệp MD2. Trên thực tế, người gửi thường chuyển chứng chỉ số khóa công khai của mình cho người nhận và người nhận thực hiện việc kiểm tra chứng chỉ số của người gửi và tách lấy khóa công khai nếu việc kiểm tra thành công.
- So sánh hai chuỗi đại diện 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.

1.3 Các giải thuật chữ ký số

Mục này trình bày 2 giải thuật chữ ký số thông dụng là RSA và DSA. RSA được sử dụng rộng rãi do RSA có thể được sử dụng để mã hóa thông điệp và tạo chữ ký số cho thông điệp. DSA là thuật toán chữ ký chuẩn được Viện NIST (Hoa Kỳ) phát triển.

1.3.1 Giải thuật chữ ký số RSA

Giải thuật RSA đề cập ở mục 3.3.2.2 có thể được sử dụng với hai mục đích để mã hóa - giải mã thông điệp và tạo chữ ký số - kiểm tra chữ ký số cho thông điệp. Điểm khác biệt giữa việc sử dụng RSA cho mã hóa và chữ ký số là bên sở hữu các cặp khóa và việc sử dụng các khóa trong quá trình mã hóa và giải mã. Cụ thể:

- RSA sử dụng cho mã hóa thông điệp:

+ Người nhận phải sở hữu cặp khóa công khai (Public key) và khóa riêng (Private key). Người nhận chuyển khóa công khai của mình cho người gửi;

+ Người gửi mã hóa thông điệp sử dụng khóa công khai của người nhận và chuyển bản mã cho người nhận;

+ Người nhận giải mã thông điệp sử dụng khóa riêng của mình để khôi phục bản rõ của thông điệp.

- RSA sử dụng cho tạo chữ ký số thông điệp:

+ Người gửi phải sở hữu cặp khóa công khai (Public key) và khóa riêng (Private key). Người gửi chuyển khóa công khai của mình cho người nhận;

+ Người gửi sử dụng khóa riêng để tạo chữ ký số cho thông điệp (bản chất là sử dụng khóa riêng để mã hóa chuỗi đại diện cho thông điệp);

+ Người nhận sử dụng khóa công khai của người gửi để kiểm tra chữ ký số của thông điệp (bản chất là sử dụng khóa công khai để giải mã khôi phục chuỗi đại diện cho thông điệp).

Quá trình ký và kiểm tra chữ ký số sử dụng giải thuật RSA tương tự như quá trình ký và kiểm tra chữ ký số tổng quát đã trình bày ở mục 3.4.1.2 và Hình 3.34, trong đó quá trình ký sử dụng giải thuật mã hóa RSA với khóa riêng của người gửi và quá trình kiểm tra sử dụng giải thuật giải mã RSA với khóa công khai của người gửi.

1.3.2 Giải thuật chữ ký số DSA

DSA (Digital Signature Algorithm) là thuật toán chữ ký số được phát triển từ giải thuật ElGamal Signature Algorithm và được công nhận là chuẩn chữ ký số sử dụng trong các cơ quan chính phủ bởi Viện NIST (Hoa Kỳ) vào năm 1991. DSA gồm 3 gồm 3 khâu:
(1) sinh cặp khóa, (2) quá trình ký thông điệp và (3) quá trình kiểm tra chữ ký của thông điệp.

* Sinh khóa cho một người dùng:

- Chọn số ngẫu nhiên x sao cho $0 < x < q$;
- Tính $y = g^x \bmod p$;
- Khóa công khai là (q, p, g, y);

- Khóa riêng là x.

* Quá trình ký thông điệp:

- H là hàm băm sử dụng và m là thông điệp gốc;
- Tính H(m) từ thông điệp gốc;
- Tạo số ngẫu nhiên k cho mỗi thông điệp, $0 < k < q$;
- Tính $r = (g^k \bmod p) \bmod q$;
- Nếu r = 0, chọn một k mới và tính lại r;
- Tính $s = k^{-1}(H(m) + xr) \bmod q$;
- Nếu s = 0, chọn một k mới và tính lại r và s;
- Chữ ký là cặp (r, s).

* Quá trình kiểm tra chữ ký

- Loại bỏ chữ ký nếu r và s không thỏa mãn $0 < r , s < q$;
- Tính H(m) từ thông điệp nhận được;
- Tính $w = s^{-1} \bmod q$;
- Tính u1 = H(m) * w mod q;
- Tính u2 = r * w mod q;
- Tính $v = ((g^{u1} * y^{u2}) \bmod p) \bmod q$;
- Chữ ký là xác thực nếu v = r.

Theo một số nghiên cứu, giải thuật chữ ký số DSA và giải thuật chữ ký số RSA có độ an toàn tương tương. Ưu điểm của giải thuật chữ ký số DSA so với giải thuật chữ ký số RSA là quá trình sinh cặp khóa và quá trình ký nhanh hơn. Tuy nhiên, quá trình kiểm tra chữ ký số bởi DSA thực hiện chậm hơn RSA. Trên thực tế, giải thuật chữ ký số RSA được sử dụng rộng rãi hơn do RSA có thể sử dụng cho cả mục đích mã hóa/giải mã và ký/kiểm tra chữ ký, trong khi DSA chỉ có thể sử dụng để ký/kiểm tra chữ ký.

2. Chứng chỉ số

2.1 Giới thiệu

Chứng chỉ số (Digital certificate), còn gọi là chứng chỉ khóa công khai (Public key certificate), hay chứng chỉ nhận dạng (Identity certificate) là một tài liệu điện tử sử dụng một chữ ký số để liên kết một khóa công khai và thông tin nhận dạng của một thực thể. Ba thành phần cơ bản nhất của một chứng chỉ số gồm:

- Chữ ký số: là chữ ký của một bên thứ 3 tin cậy cung cấp chứng chỉ số, thường gọi là CA – Certificate Authority;
- Khóa công khai: là khóa công khai trong cặp khóa công khai và khóa riêng của thực thể;

- Thông tin nhận dạng: là tên, địa chỉ, tên miền hoặc các thông tin định danh của thực thể.

Chứng chỉ số có thể được sử dụng để xác minh chủ thể thực sự của một khóa công khai. Hình 3.35 là giao diện biểu diễn một chứng chỉ số do bên thứ 3 là một đơn vị của công ty Verisign cấp cho tên miền www.vietcombank.com.vn của ngân hàng TMCP Ngoại thương Việt Nam.

2.2 Nội dung chứng chỉ số

Như biểu diễn trên Hình 3.36, nội dung của một chứng chỉ số gồm nhiều trường thông tin. Các trường thông tin cụ thể theo chuẩn chứng chỉ số X.509 gồm:

- Serial Number: Số nhận dạng của chứng chỉ số;
- Subject: Thông tin nhận dạng một cá nhân hoặc một tổ chức;

Hình 3.35. Giao diện biểu diễn một chứng chỉ số

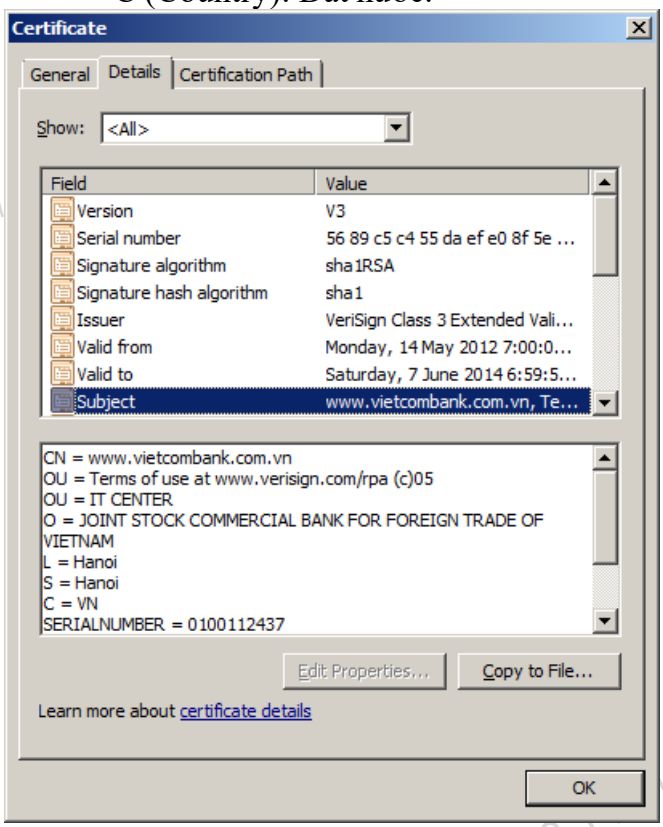
- Signature Algorithm: Giải thuật tạo chữ ký;
- Signature Hash Algorithm: Giải thuật tạo chuỗi băm cho tạo chữ ký;
- Signature: Chữ ký của người/tổ chức cấp chứng chỉ;
- Issuer: Người/tổ chức có thẩm quyền/tin cậy cấp chứng chỉ;
- Valid-From: Ngày bắt đầu có hiệu lực của chứng chỉ;
- Valid-To: Ngày hết hạn sử dụng chứng chỉ;

- Key-Usage: Mục đích sử dụng khóa (chữ ký số, mã hóa,…);
- Public Key: Khóa công khai của chủ thể;
- Thumbprint Algorithm: Giải thuật băm sử dụng để tạo chuỗi băm cho khóa công khai;
- Thumbprint: Chuỗi băm tạo từ khóa

công khai; Các mục thông tin của

trường Subject gồm:

- CN (Common Name): Tên chung, nhưng một tên miền được gán chứng chỉ;
- OU (Organisation Unit): Tên bộ phận/phòng ban;
- O (Organisation): Tổ chức/Cơ quan/công ty;
- L (Location): Địa điểm/Quận huyện;
- S (State/Province): Bang/Tỉnh/Thành phố;
- C (Country): Đất nước.



Hình 3.36. Nội dung chi tiết của một chứng chỉ số

2.3 Ứng dụng của chứng chỉ số

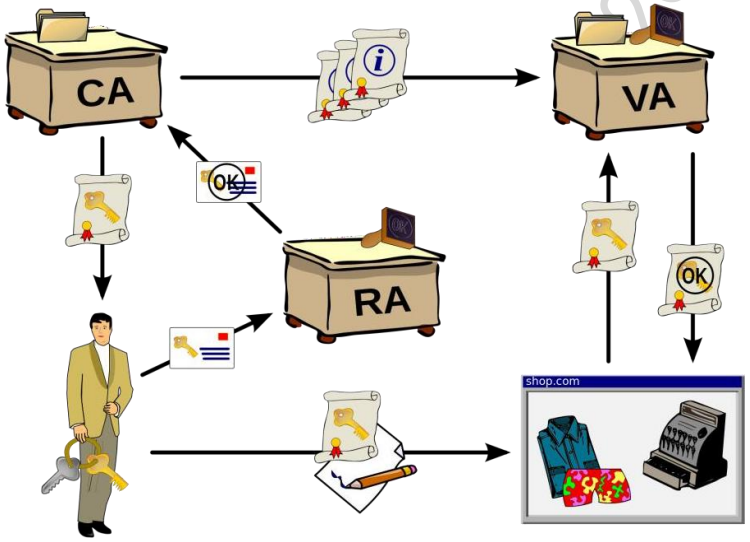
Chứng chỉ số được sử dụng rộng rãi trong bảo mật thông tin truyền và xác thực thông tin nhận dạng của các bên tham gia giao dịch điện tử, trao đổi khóa trong nhiều ứng dụng khác nhau. Cụ thể:

- Sử dụng chứng chỉ số trong đảm bảo an toàn giao dịch trên nền web: với chứng chỉ số, một website có thể được cấu hình để hoạt động theo chế độ "an toàn" (HTTPS), trong đó toàn bộ thông tin trao đổi giữa máy chủ và máy khách được đảm bảo tính bí mật (sử dụng mã hóa khóa đối xứng), tính toàn vẹn và xác thực (sử dụng hàm băm có khóa MAC). Ngoài ra, các máy chủ và máy khách có thể xác thực thông tin nhận dạng của nhau sử dụng chứng chỉ số.
- Chứng chỉ số cũng có thể được sử dụng để bảo mật thông tin truyền trong nhiều ứng dụng khác, như email, truyền file,…
- Sử dụng chứng chỉ số có thể ngăn chặn hiệu quả dạng tấn công người đứng giữa do các bên tham gia giao dịch có thể xác thực thông tin nhận dạng của nhau. Nếu các bên sử dụng thêm chữ ký số thì có thể ngăn chặn việc sửa đổi các thông điệp trao đổi trên đường truyền.
- Chứng chỉ số có thể được sử dụng trong trao đổi khóa.

3. PKI

Hạ tầng khóa công khai (Public-key infrastructure - PKI) là một tập các phần cứng, phần mềm, nhân lực, chính sách và các thủ tục để tạo, quản lý, phân phối, sử dụng, lưu trữ và thu hồi các chứng chỉ số. Một PKI gồm các thành phần sau:

- Certificate Authority (CA): Cơ quan cấp và kiểm tra chứng chỉ số;
- Registration Authority (RA): Bộ phận tiếp nhận, kiểm tra thông tin nhận dạng của người dùng theo yêu cầu của CA;
- Validation Authority (VA): Cơ quan xác nhận thông tin nhận dạng của người dùng thay mặt CA;
- Central Directory (CD): Là nơi lưu danh mục và lập chỉ số các khóa;
- Certificate Management System: Hệ thống quản lý chứng chỉ;
- Certificate Policy: Chính sách về chứng chỉ.



Hình 3.37. Lưu đồ cấp và sử dụng chứng chỉ số trong PKI

Hình 3.37 biểu diễn lưu đồ cấp và sử dụng chứng chỉ số trong PKI, trong đó gồm 2 khâu chính:

- Đăng ký, xét duyệt và cấp chứng chỉ số:

+ Người dùng có yêu cầu cấp chứng chỉ số tạo một cặp khóa, gồm 1 khóa công khai và 1 khóa riêng;

+ Người dùng tạo yêu cầu cấp chứng chỉ số (Certificate request), trong đó tích hợp khóa công khai và thông tin định danh của mình. Yêu cầu cấp chứng chỉ số thường được lưu dưới dạng 1 file văn bản theo định dạng của chuẩn X.509;

+ Người dùng gửi yêu cầu cấp chứng chỉ số đến Bộ phận tiếp nhận (RA). RA kiểm tra các thông tin trong yêu cầu cấp chứng chỉ số, nếu hợp lệ thì chuyển yêu cầu đến Cơ quan cấp chứng chỉ (CA);

+ CA sẽ thực hiện việc xác minh các thông tin nhận dạng của chủ thể và nếu xác minh thành công thì cấp chứng chỉ số cho người yêu cầu. Chứng chỉ số được CA ký bằng khóa riêng của mình để đảm bảo tính xác thực và toàn vẹn và thường được lưu dưới dạng 1 file văn bản theo định dạng của chuẩn X.509;

+ Sau khi phát hành chứng chỉ số cho người dùng, CA chuyển thông tin về chứng chỉ số đã cấp cho thành phần VA để xác nhận thông tin nhận dạng theo yêu cầu;

+ Người dùng cài đặt chứng chỉ số vào hệ thống và có thể bắt đầu sử dụng trong các ứng dụng của mình.

- Sử dụng và kiểm tra chứng chỉ số:

+ Người dùng tạo đơn hàng, ký vào đơn hàng bằng khóa riêng, gửi đơn hàng đã ký và chứng chỉ số cho nhà cung cấp;

+ Nhà cung cấp chuyển chứng chỉ số của người dùng cho VA để kiểm tra, nếu chứng chỉ số hợp lệ thì tiến hành xác thực chữ ký số của người dùng sử dụng khóa công khai của người dùng lấy từ chứng chỉ số. Nếu chữ ký của người dùng xác thực thành công thì đơn hàng được duyệt.