TRƯỜNG ĐẠI HỌC KỸ THUẬT – CÔNG NGHỆ CẦN THƠ

AN TOÀN CÁC HỆ THỐNG THÔNG TIN

ThS. Nguyễn Văn Kha

dzokha1010@gmail.com

Chương 5
BẢO MẬT HỆ THỐNG THÔNG TIN

5.1. Xác thực

5.2. Điều khiển truy cập

5.3. Các giao thức truyền thông an toàn

5.1. Xác thực
5.1.1. Khái niệm

Xác định danh tính (ID - Identification) là một cơ chế mà theo đó các thực thể chưa được xác minh hoặc chưa được xác thực tìm kiếm quyền truy cập vào tài nguyên của hệ thống, cung cấp một định danh (Identifier) duy nhất để hệ thống nhận diện. Việc cấp định danh có thể diễn ra theo hai cách là sử dụng thông tin của thực thể để làm định danh hoặc do hệ thống tự động gán một định danh cho thực thể.

Xác thực (Authentication) là quá trình xác định danh tính cho một thực thể chưa được xác thực.

5.1. Xác thực
5.1.1. Khái niệm (tt)

Ủy quyền (Authorization) là quá trình xác nhận một thực thể có quyền để sử dụng một tài sản thông tin hay không bằng cách so sánh với danh sách các tài sản mà thực thể đó được phép truy cập, được gọi là Danh sách điều khiển truy cập (ACL - Access Control List). Có ba cách xử lý uỷ quyền:

- Ủy quyền cho mỗi người dùng đã xác thực: tốn nhiều tài nguyên
- Ủy quyền cho các thành viên của một nhóm: cấp quyền truy cập vào tài nguyên dựa trên quyền truy cập của nhóm. Đây là phương pháp ủy quyền phổ biến nhất.
- Ủy quyền trên nhiều hệ thống: cấp cho thực thể xác thực một vé uỷ quyền được tất cả các hệ thống trong miền xác thực chấp nhận. Đôi khi được gọi là đăng nhập một lần (SSO – Single Sign-On).

5.1. Xác thực
5.1.1. Khái niệm (tt)

Trách nhiệm giải trình (Accountability), còn được gọi là khả năng kiểm toán (Auditability), đảm bảo rằng mọi hành động được thực hiện trên hệ thống máy tính hoặc tài sản thông tin đều có thể được liên kết với người dùng hoặc hệ thống có quyền truy cập.

Trách nhiệm giải trình thường được thực hiện thông qua nhật ký hệ thống, nhật ký cơ sở dữ liệu. Nhật ký hệ thống ghi lại thông tin cụ thể, chẳng hạn như các nỗ lực truy cập không thành công và các sửa đổi hệ thống.

5.1. Xác thực
5.1.1. Phân loại các xác thực thực thể

Có ba loại xác thực thực thể được sử dụng rộng rãi:

- Những gì bạn biết: mật khẩu, mã xác thực duy nhất, số định danh cá nhân (PIN).
- Những gì bạn có hoặc sở hữu: thẻ ID, ATM, Token.
- Những gì bạn là hoặc đặc điểm cá nhân: dấu vân tay, quét võng mạc và mống mắt.

5.2. Điều khiển truy cập
5.2.1. Khái niệm

Điều khiển truy cập (Access Control) là phương pháp mà hệ thống xác định xem có cho phép người dùng vào khu vực đáng tin cậy của tổ chức hay không, như hệ thống thông tin, khu vực hạn chế như phòng máy tính và cả những khu vực vật lý của tổ chức.

Điều khiển truy cập được thực hiện thông qua sự kết hợp của các chính sách, chương trình và công nghệ. Điều khiển truy cập tập trung vào các quyền hoặc đặc quyền mà chủ thể (người dùng hoặc hệ thống) có đối với một đối tượng (tài nguyên), bao gồm:

- Ai được phép truy cập tài nguyên
- Khi nào và từ đâu họ có thể truy cập tài nguyên
- Cách thức sử dụng tài nguyên phù hợp và an toàn

5.2. Điều khiển truy cập
5.2.2. Cơ chế điều khiển truy cập

Nhìn chung, tất cả các phương pháp điều khiển truy cập đều dựa trên bốn cơ chế sau, đại diện cho bốn chức năng cơ bản của hệ thống điều khiển truy cập:

- Xác định danh tính (Identification)
- Xác thực (Authentication)
- Ủy quyền (Authorization)
- Trách nhiệm giải trình (Accountability)

5.2. Điều khiển truy cập
5.2.3. Điều khiển truy cập tùy quyền

Điều khiển truy cập tùy quyền (DAC - Discretionary Access Control) cung cấp khả năng chia sẻ tài nguyên trong cấu hình ngang hàng (Peer-To-Peer), cho phép người dùng có thể điều khiển và cung cấp quyền truy cập vào thông tin hoặc tài nguyên mà họ sở hữu.

Người dùng có thể cho phép truy cập chung, không hạn chế hoặc họ có thể cho phép những người hoặc nhóm cụ thể truy cập vào các tài nguyên này, thường là với các điều khiển về khả năng đọc, chỉnh sửa hoặc xóa của những người dùng khác.

Ví dụ, một người dùng có thể có một ổ cứng chứa thông tin cần chia sẻ với đồng nghiệp trong văn phòng. Người dùng này có thể chọn cho phép quyền truy cập cho các đồng nghiệp cụ thể bằng cách cung cấp tên của họ trong chức năng điều khiển chia sẻ.

5.2. Điều khiển truy cập
5.2.4. Điều khiển truy cập không tùy quyền

Điều khiển truy cập không tuỳ quyền (NDAC - Nondiscretionary Access Control) được quản lý bởi một cơ quan trung ương trong tổ chức. Một dạng điều khiển truy cập không tuỳ quyền được gọi là kiểm soát truy cập dựa trên mạng lưới (LBAC - lattice-based access control), trong đó người dùng được chỉ định một ma trận các quyền cho các khu vực truy cập cụ thể. Cấu trúc mạng lưới chứa các chủ thể và đối tượng, và các ranh giới liên quan đến từng cặp được phân định. Kiểm soát dựa trên mạng lưới chỉ định mức độ truy cập mà mỗi chủ thể có đối với từng đối tượng, như được triển khai trong danh sách kiểm soát truy cập (ACL).

5.2. Điều khiển truy cập
5.2.4. Điều khiển truy cập không tùy quyền

- Điều khiển truy cập theo vai trò (RBAC – Role-based Access Control): liên kết với vai trò của một vị trí công tác của người dùng trong tổ chức.
- Điều khiển truy cập theo nhiệm vụ (TBAC – Task-based Access Control): liên kết với công việc hoặc nhiệm vụ cụ thể.
- Điều khiển truy cập bắt buộc (MAC - Mandatory Access Control): sử dụng lượt đồ phân loại dữ liệu (ví dụ: tối mật, tuyệt mật, mật), cung cấp quyền điều khiển hạn chế đối với việc truy cập vào tài nguyên thông tin.
- Điều khiển truy cập dựa trên thuộc tính (ABAC - Attribute-based Access Control): sử dụng riêng lẻ hoặc kết hợp các thuộc tính (tên, ngày sinh) của một chủ thể tạo định danh phân biệt với các thực thể khác.

5.3. Các giao thức truyền thông an toàn
5.3.1. Giao thức an ninh Email

- S/MIME cung cấp một phương tiện nhất quán để gửi và nhận dữ liệu MIME an toàn. S/MIME, dựa trên tiêu chuẩn Internet MIME, là một cải tiến bảo mật cho tin nhắn điện tử mã hóa.
- Hơn nữa, S/MIME không chỉ giới hạn ở email mà còn có thể được sử dụng với bất kỳ cơ chế vận chuyển nào mang dữ liệu MIME, chẳng hạn như HTTP.
- Do đó, S/MIME tận dụng lợi thế cho phép trao đổi tin nhắn an toàn trong các hệ thống truyền tải hỗn hợp. S/MIME sẽ nổi lên như một tiêu chuẩn công nghiệp cho mục đích sử dụng thương mại và tổ chức.

5.3.1. Giao thức an ninh Email
a) Giao thức SMTP

SMTP (Simple Mail Transfer Protocol) là giao thức cơ bản để gửi thư điện tử qua Internet, trong đó các tin nhắn chỉ có thể truyền đi dưới dạng ký tự ASCII 7-bit.

Để làm được điều này, SMTP sử dụng định dạng ASCII của Network Virtual Terminal (NVT). Cụ thể, NVT sử dụng mã NVT ASCII, là một bộ ký tự 8 bit với 7 bit đầu giống chuẩn ASCII và bit thứ 8 luôn có giá trị là 0.

5.3.1. Giao thức an ninh Email
b) Giao thức MIME

MIME (Multipurpose Internet Mail Extensions) được bổ sung để cho phép SMTP truyền tải dữ liệu không phải ASCII, chẳng hạn như hình ảnh hoặc tệp đính kèm. MIME mã hóa các loại dữ liệu này dưới dạng ASCII để SMTP có thể xử lý và gửi đi. Lưu ý rằng MIME không thay thế SMTP hay POP3; nó chỉ mở rộng khả năng của SMTP để gửi dữ liệu phi ASCII.

Tiêu chuẩn MIME cung cấp một cấu trúc chung cho loại nội dung của các thông điệp Internet và cho phép mở rộng cho các ứng dụng loại nội dung mới. Để phù hợp với các loại dữ liệu và biểu diễn tùy ý, mỗi thông điệp MIME bao gồm thông tin cho người nhận biết loại dữ liệu và mã hóa được sử dụng.

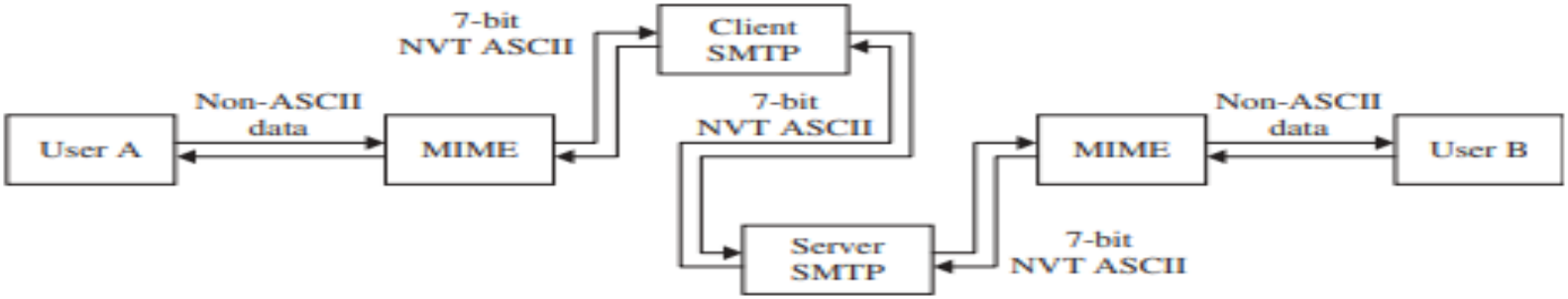
Tiêu chuẩn MIME chỉ định rằng một khai báo loại nội dung phải chứa hai mã định danh, một loại nội dung và một loại phụ, được phân tách bằng dấu gạch chéo. Ví dụ: image/jpeg cho hình ảnh JPEG.

5.3.1. Giao thức an ninh Email
b) Giao thức MIME (tt)

Mô tả MIME
MIME chuyển đổi dữ liệu không phải ASCII tại trang web của người gửi thành dữ liệu NVT ASCII và chuyển đến máy khách SMTP để gửi qua Internet. Máy chủ SMTP tại trang web của người nhận nhận dữ liệu NVT ASCII và chuyển đến MIME để chuyển đổi trở lại thành dữ liệu không phải ASCII ban đầu.

Tiêu đề MIME MIME định nghĩa năm tiêu đề có thể được thêm vào phần tiêu đề SMTP ban đầu:

- MIME_Version
- Content_Type
- Content_Transfer_Encoding
- Content_Id
- Content_Description.



Các hàm chuyển đổi trong MIME

5.3.1. Giao thức an ninh Email
c) Giao thức S/MIME

- S/MIME (Secure/Multipurpose Internet Mail Extensions) là một phương pháp bảo mật cho email giúp mã hóa và xác thực các thông điệp MIME 7-bit. Với S/MIME, bất kỳ hệ thống nào hỗ trợ MIME đều có thể gửi và nhận dữ liệu một cách an toàn. Cụ thể, S/MIME hoạt động với các tác nhân người dùng mail (MUA - Mail User Agents) để bổ sung các dịch vụ bảo mật mã hóa cho email gửi đi và xử lý bảo mật cho email nhận về.
- Để tạo một tin nhắn S/MIME, tác nhân S/MIME cần tuân thủ các tiêu chuẩn bảo mật của S/MIME và các yêu cầu của CMS (Cryptographic Message Syntax), giúp đảm bảo dữ liệu được mã hóa và xác thực đúng quy chuẩn an toàn.
- Tác nhân S/MIME đại diện cho phần mềm người dùng là tác nhân nhận, tác nhân gửi hoặc cả hai. Các tác nhân S/MIME phiên bản 3 nên cố gắng có khả năng tương tác lớn nhất có thể với các tác nhân S/MIME phiên bản 2. S/MIME phiên bản 2 được mô tả trong RFC 2311 đến RFC 2315
- Trước khi sử dụng khóa công khai để cung cấp dịch vụ bảo mật, tác nhân S/MIME phải chứng nhận khóa công khai là hợp lệ. Tác nhân S/MIME phải sử dụng chứng chỉ Cơ sở hạ tầng khóa công khai (PKIX) Internet X.509 để xác thực khóa công khai như được mô tả trong chứng chỉ PKIX và hồ sơ CRL.

5.3. Các giao thức truyền thông an toàn
5.3.2. Giao thức bảo mật mạng

- IPsec là giao thức được thiết kế để bảo vệ thông tin liên lạc theo cách an toàn qua TCP/IP. Giao thức IPsec là một tập hợp các tiện ích mở rộng bảo mật do IETF phát triển và cung cấp các dịch vụ xác thực và riêng tư tại tầng mạng bằng cách sử dụng mật mã hiện đại.
- Để bảo vệ nội dung của một Datagram, dữ liệu được chuyển đổi bằng các thuật toán mã hóa. Có hai loại chuyển đổi chính tạo nên cơ sở của IPsec, Tiêu đề xác thực (AH - Authentication Header) và Tải trọng bảo mật đóng gói (ESP - Encapsulating Security Payload). Cả AH và ESP đều là hai giao thức cung cấp tính toàn vẹn không kết nối, xác thực nguồn gốc dữ liệu, tính bảo mật và dịch vụ chống phát lại. Các giao thức này có thể được áp dụng riêng lẻ hoặc kết hợp để cung cấp một tập hợp các dịch vụ bảo mật mong muốn cho tầng IP. Chúng được cấu hình trong một cấu trúc dữ liệu gọi là Hiệp hội bảo mật (SA - Security Association).

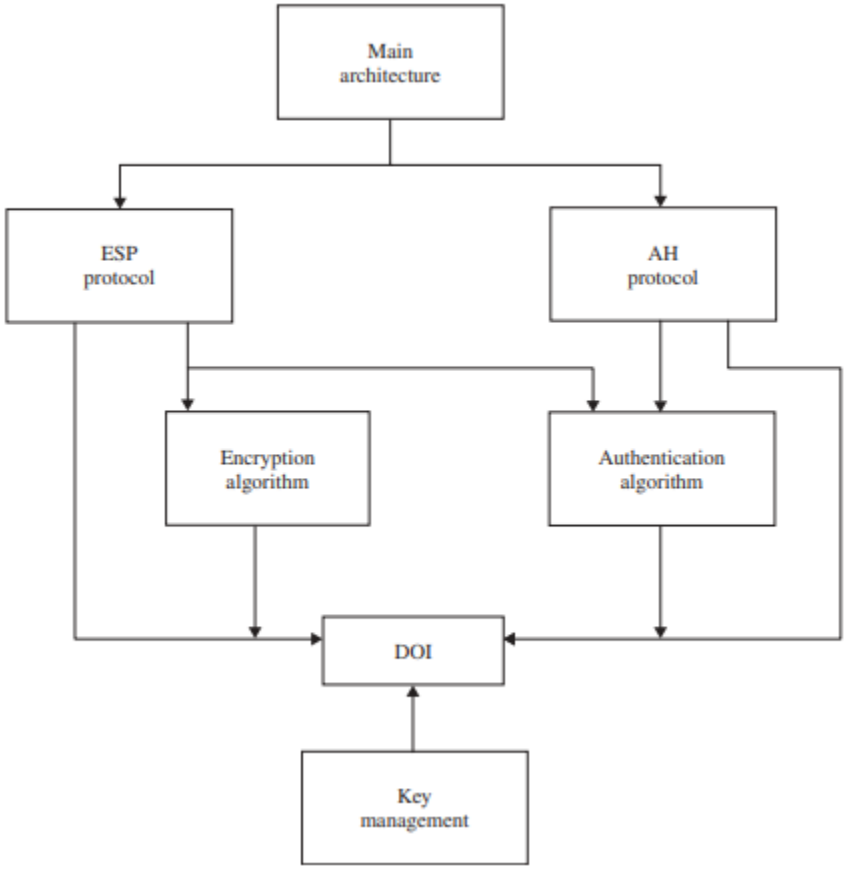
Các thành phần cơ bản của kiến trúc IPsec được giải thích theo các chức năng sau:

- Giao thức bảo mật cho AH và ESP.
- SA để quản lý chính sách và xử lý lưu lượng.
- Quản lý khóa thủ công và tự động cho Internet Key Exchange (IKE), giao thức xác định khóa Oakley và Internet Security Association and Key Management Protocol (ISAKMP).
- Thuật toán để xác thực và mã hóa.

5.3.2. Giao thức bảo mật mạng
a) Tài liệu giao thức IPsec

Bộ giao thức IPsec được chia thành bảy nhóm chính, mỗi nhóm mô tả các tiêu chuẩn và giao thức liên quan đến bảo mật mạng. Vào tháng 11/1998, Nhóm mạng IETF phát hành RFC 2411 làm tài liệu hướng dẫn phát triển IPsec, trong đó nêu cách dùng các thuật toán mã hóa và xác thực với các giao thức AH và ESP của IPsec. Bảy nhóm này làm rõ các phần của IPsec để đảm bảo bảo mật trong giao tiếp IP.

- Kiến trúc (Architecture): Tài liệu kiến trúc chính bao gồm các khái niệm chung, yêu cầu bảo mật, định nghĩa và cơ chế xác định công nghệ IPsec.
- ESP: Tài liệu này bao gồm định dạng gói và các vấn đề chung liên quan đến việc sử dụng ESP để mã hóa gói và xác thực tùy chọn. Tài liệu giao thức này cũng chứa các giá trị mặc định, nếu phù hợp, và chỉ định một số giá trị trong Miền diễn giải (DOI - Domain of Interpretation).



5.3.2. Giao thức bảo mật mạng
a) Tài liệu giao thức IPsec (tt)

- AH: Tài liệu này bao gồm định dạng gói và các vấn đề chung liên quan đến việc sử dụng AH để xác thực gói. Tài liệu này cũng chứa các giá trị mặc định, chẳng hạn như nội dung đệm mặc định và chỉ định một số giá trị trong tài liệu DOI.
- Thuật toán mã hóa (Encryption algorithm): Đây là một tập hợp các tài liệu mô tả cách sử dụng các thuật toán mã hóa khác nhau cho ESP. Cụ thể,

  + Chỉ định kích thước và độ mạnh của khóa cho từng thuật toán;

  + Bất kỳ ước tính nào có sẵn về hiệu suất của từng thuật toán;

  + Thông tin chung về cách thuật toán mã hóa này được sử dụng trong ESP; các tính năng của thuật toán mã hóa này được ESP sử dụng, bao gồm mã hóa và/hoặc xác thực.

- Thuật toán xác thực (Authentication algorithm): Đây là một tập hợp các tài liệu mô tả cách các thuật toán xác thực khác nhau được sử dụng cho AH và cho tùy chọn xác thực của ESP. Cụ thể,

  + Chỉ định các tham số hoạt động như số vòng và định dạng khối đầu vào hoặc đầu ra;

  + Các yêu cầu đệm ngầm định và rõ ràng của thuật toán này;

  + Xác định các tham số/phương pháp hoạt động tùy chọn;

  + Các phạm vi mặc định và bắt buộc của thuật toán;

  + Tiêu chí so sánh dữ liệu xác thực cho thuật toán.

5.3.2. Giao thức bảo mật mạng
a) Tài liệu giao thức IPsec (tt)

- Quản lý khóa (Key management): Đây là một tập hợp các tài liệu mô tả các lược đồ quản lý khóa. Các tài liệu này cũng cung cấp một số giá trị nhất định cho DOI. Hiện tại, quản lý khóa đại diện cho các giao thức Oakley, ISAKMP và Resolution.
- DOI: Tài liệu này chứa các giá trị cần thiết để các tài liệu khác liên kết với nhau. Chúng bao gồm các mã định danh cho các thuật toán mã hóa và xác thực đã được phê duyệt, cũng như các tham số hoạt động như thời gian tồn tại của khóa.

5.3.2. Giao thức bảo mật mạng
b) Hiệp hội an ninh (SA- Security Association)

SA là nền tảng của IPsec. Cả AH và ESP đều sử dụng SA. Do đó, SA là khái niệm chính xuất hiện trong cả cơ chế xác thực và bảo mật cho IPsec. SA là kết nối đơn giữa người gửi và người nhận, cung cấp các dịch vụ bảo mật cho lưu lượng được truyền trên đó. Nếu cả bảo vệ AH và ESP đều được áp dụng cho luồng lưu lượng, thì cần có hai SA để trao đổi an toàn hai chiều.

Một SA được xác định duy nhất bằng ba tham số như sau:

- Chỉ số tham số bảo mật (SPI - Security Parameter Index): Chỉ số này được gán cho mỗi SA và mỗi SA được xác định thông qua SPI. Người nhận sử dụng SPI để xác định SA cho một gói tin. Trước khi người gửi sử dụng IPsec để giao tiếp với người nhận, người gửi phải biết giá trị chỉ mục cho một SA cụ thể. Sau đó, người gửi đặt giá trị vào trường SPI của mỗi datagram gửi đi. SPI được mang trong tiêu đề AH và ESP để cho phép người nhận chọn SA mà gói tin đã nhận được được xử lý. Tuy nhiên, giá trị chỉ mục không được chỉ định toàn cục. Cần có sự kết hợp giữa địa chỉ đích và SPI để xác định SA.

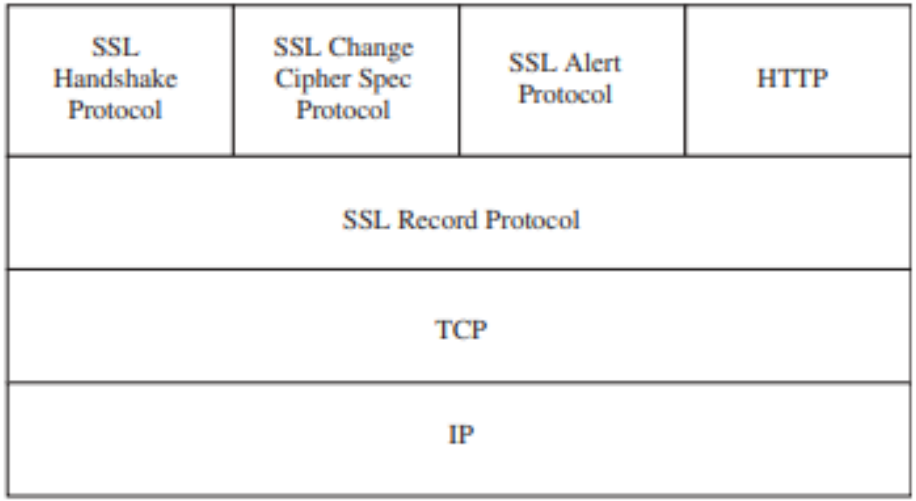
5.3.2. Giao thức bảo mật mạng
b) Hiệp hội an ninh (SA- Security Association)

Một SA được xác định duy nhất bằng ba tham số như sau (tt):

- Địa chỉ đích IP (IP destination address): Bởi vì hiện tại, các địa chỉ đơn hướng chỉ được phép bởi các cơ chế quản lý IPsec SA, đây là địa chỉ của điểm cuối đích của SA. Điểm cuối đích có thể là hệ thống người dùng cuối hoặc hệ thống mạng như tường lửa hoặc bộ định tuyến.
- Mã định danh giao thức bảo mật (Security protocol identifier): Mã định danh này cho biết liên kết là AH hay ESP SA.

5.3. Các giao thức truyền thông an toàn
5.3.3. Giao thức SSL

- SSL là một giao thức hai tầng. Ở cấp độ thấp hơn, Giao thức SSL Record được xếp tầng trên giao thức vận chuyển đáng tin cậy như TCP. Giao thức SSL Record cũng được sử dụng để đóng gói nhiều giao thức cấp cao hơn. Một giao thức cấp cao hơn có thể xếp tầng trên giao thức SSL.
- Giao thức SSL Record tiếp nhận thông điệp từ tầng ứng dụng cần truyền, phân mảnh dữ liệu thành các khối có thể quản lý được, tùy chọn nén dữ liệu, áp dụng MAC, mã hóa, thêm tiêu đề và truyền kết quả đến TCP. Dữ liệu nhận được sẽ được giải mã, xác minh, giải nén, lắp ráp lại và sau đó chuyển đến các Client cấp cao hơn.



Hai tầng của giao thức SSL

5.3.3. Giao thức SSL
a) Trạng thái phiên và kết nối

Phiên SSL (SSL Session) là sự kết hợp giữa Client và Server, được thiết lập bởi giao thức bắt tay (Handshake). Chúng định nghĩa một tập hợp các tham số mật mã được chia sẻ giữa các kết nối để tránh việc đàm phán tốn kém cho mỗi kết nối.

Phiên SSL duy trì trạng thái của Client và Server thông qua trạng thái hiện tại và trạng thái chờ xử lý. Khi nhận được thông báo thay đổi thông số mật mã, nó sẽ sao chép trạng thái đọc đang chờ xử lý vào trạng thái đọc hiện tại. Khi gửi thông báo thay đổi thông số mật mã, nó sẽ sao chép trạng thái ghi đang chờ xử lý vào trạng thái ghi hiện tại. Sau khi hoàn tất bắt tay, Client và Server giao tiếp bằng thông số mật mã mới được thỏa thuận.

5.3.3. Giao thức SSL
a) Trạng thái phiên và kết nối

Trạng thái phiên được định nghĩa bởi các thành phần sau:

- Định danh phiên (Session identifier): là giá trị do Server tạo ra, xác định trạng thái phiên đang hoạt động hoặc có thể tái sử dụng nếu cần.

- Chứng chỉ ngang hàng (Peer Certificate): là chứng chỉ X.509 v3 của ngang hàng. Phần tử này của trạng thái có thể là NULL.

- Phương pháp nén (Compression Method): thuật toán được sử dụng để nén dữ liệu trước khi mã hóa.

- Xác định mật mã (Cipher Spec): Định rõ thuật toán mã hóa dữ liệu (như NULL và DES) và thuật toán băm (như MD5 hoặc SHA-1) được sử dụng để tính toán MAC. Nó cũng định nghĩa các thuộc tính mật mã như kích thước băm.

- Bí mật chính (Master secret): Chuỗi bí mật 48 byte được chia sẻ giữa Client và Server, sử dụng để tạo khóa mã hóa và các tham số an toàn khác.

- Có thể tiếp tục (Is resumable): Cờ xác định liệu phiên này có thể được dùng để mở lại các kết nối mới mà không cần đàm phán lại không.

5.3.3. Giao thức SSL
a) Trạng thái phiên và kết nối

Kết nối (Connection) là một kỹ thuật vận chuyển (trong định nghĩa mô hình phân tầng của OSI) cung cấp một loại dịch vụ phù hợp. Đối với SSL, các kết nối như vậy là các mối quan hệ ngang hàng (Peer-To-Peer). Các kết nối là tạm thời. Mỗi kết nối được liên kết với một phiên.

Trạng thái kết nối được xác định bởi các yếu tố sau:

- Máy chủ và máy khách ngẫu nhiên (Server and Client Random): Đây là chuỗi byte được máy chủ và máy khách chọn ngẫu nhiên cho mỗi kết nối.

- Bí mật MAC ghi Server (Server write MAC secret): Điều này cho biết khóa bí mật được sử dụng trong các hoạt động MAC (Mã xác thực thông điệp) trên dữ liệu gửi bởi Server.

- Bí mật MAC ghi Client (Client write MAC secret): Điều này biểu thị khóa bí mật được sử dụng trong các hoạt động MAC trên dữ liệu gửi bởi Client.

5.3.3. Giao thức SSL
a) Trạng thái phiên và kết nối

Trạng thái kết nối được xác định bởi các yếu tố sau (tt):

- Khóa ghi Server (Server write key): Đây là khóa mã hóa thông thường cho dữ liệu được Server mã hóa và Client giải mã.

- Khóa ghi Client (Client write key): Đây là khóa mã hóa thông thường cho dữ liệu được Client mã hóa và Server giải mã.

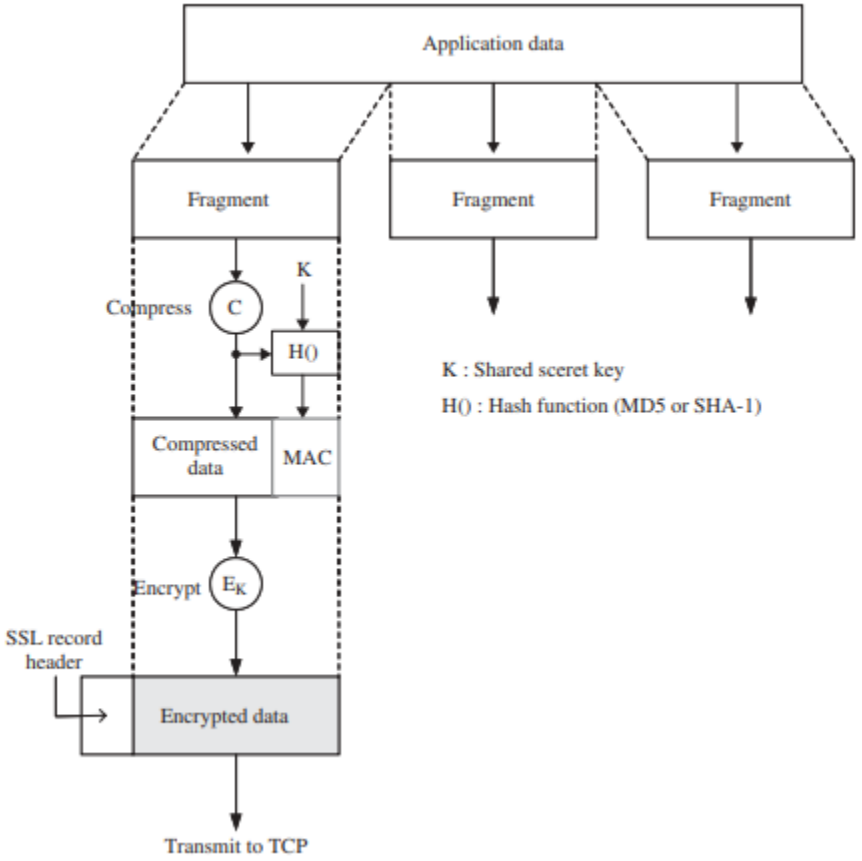
- Các vectơ khởi tạo (IV - Initialization Vector): Khi sử dụng mã hóa khối ở chế độ chuỗi khối mã hóa (CBC - cipher block chaining), IV được duy trì cho mỗi khóa. Trường này đầu tiên được khởi tạo bởi Giao thức bắt tay SSL. Sau đó, khối văn bản mã hóa cuối cùng từ mỗi bản ghi được lưu giữ để sử dụng làm IV với bản ghi tiếp theo. IV được XOR với khối văn bản thuần túy đầu tiên trước khi mã hóa.

- Số thứ tự (Sequence Number): Mỗi bên duy trì số thứ tự riêng cho các tin nhắn được truyền và nhận cho mỗi kết nối. Khi một bên gửi hoặc nhận tin nhắn thay đổi thông số mã hóa, số thứ tự thích hợp được đặt thành không. Số thứ tự không được vượt quá 2^{64}- 1.

5.3.3. Giao thức SSL
b) Giao thức SSL Record

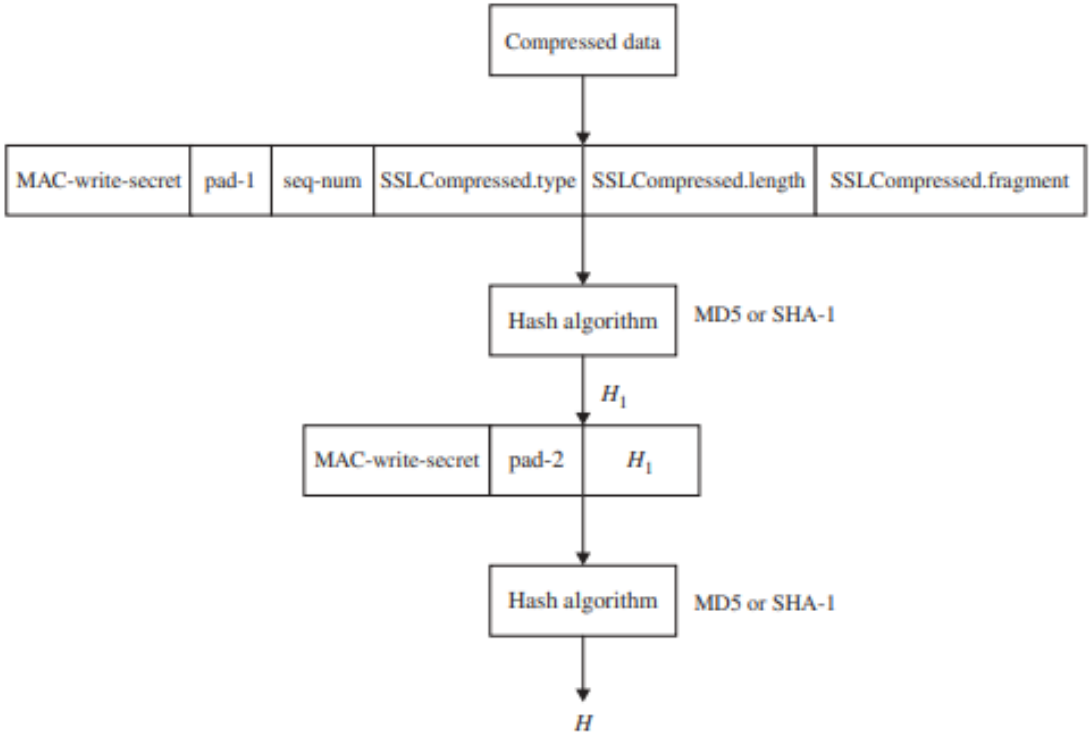
Giao thức Bản ghi SSL lấy một thông điệp ứng dụng để truyền đi, phân mảnh dữ liệu thành các khối có thể quản lý được, tùy chọn nén dữ liệu, áp dụng MAC, mã hóa, thêm tiêu đề và truyền kết quả trong một phân đoạn TCP.

Dữ liệu nhận được được giải mã, xác minh, giải nén, lắp ráp lại và sau đó chuyển đến các máy khách cấp cao hơn.



Hoạt động của giao thức SSL Record

5.3.3. Giao thức SSL
b) Giao thức SSL Record

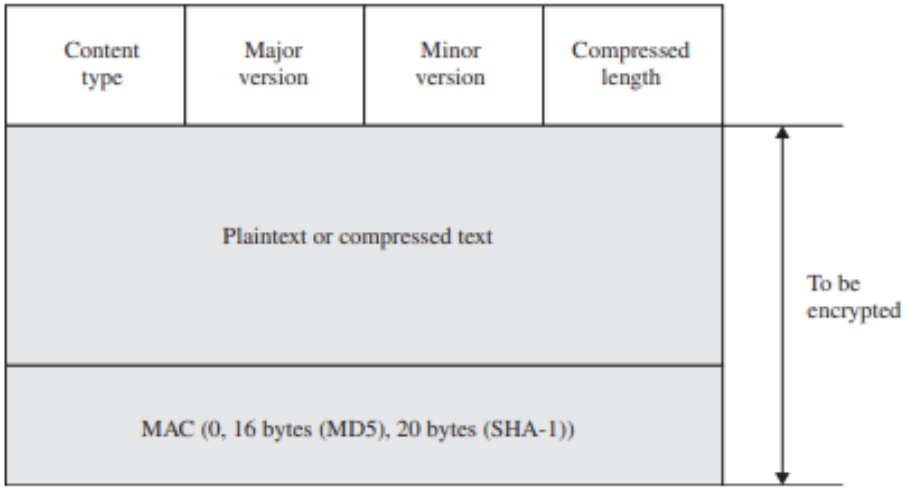


Tính toán MAC trên dữ liệu nén

MAC được tính toán trước khi mã hóa:
H1 = hash(MAC-write-secret || pad-1 || seq-num || SSLCompressed.type || SSLCompressed.length || SSLCompressed.fragment)
H = hash(MAC-write-secret|| pad-2||H1)
Trong đó:

- ||: ký hiệu nối
- Hash: có thể là MD5 hoặc SHA-1
- Pad-1: Byte 0x36 (0011 0110) lập 48 lần (384 bit) với MD5 và 40 lần (320 bit) với SHA-1
- Pad-2: Byte 0x5C (0101 1100) lập 48 lần với MD5 và 40 lần với SHA-1

5.3.3. Giao thức SSL
b) Giao thức SSL Record



Định dạng giao thức SSL Record

Quá trình xử lý cuối cùng của Giao thức SSL Record là thêm tiêu đề SSL Record:

- Kiểu nội dung (Content type) - 8 bit: Trường này là giao thức lớp cao hơn được sử dụng để xử lý đoạn mã được đính kèm.
- Phiên bản chính (Major Version - 8 bit: phiên bản chính của SSL đang được sử dụng. Đối với SSLv3, giá trị là 3.
- Phiên bản phụ (Minor Version) - 8 bit: Trường này chỉ ra phiên bản phụ của SSL đang được sử dụng. Đối với SSLv3, giá trị là 0.
- Độ dài nén (Compressed length) - 16 bit: Chỉ ra độ dài tính bằng byte của đoạn bản rõ hoặc đoạn đã nén nếu cần nén. Giá trị tối đa là $2^{14} + 2048$.

5.3.3. Giao thức SSL
c) Giao thức thay đổi thông số mật mã SSL

- Giao thức thay đổi thông số mật mã SSL (SSL Change Cipher Spec) là giao thức đơn giản nhất trong ba giao thức dành riêng cho SSL. Giao thức này bao gồm một thông báo duy nhất, được nén và mã hóa theo CipherSpec hiện tại. Thông báo bao gồm một byte duy nhất có giá trị 1. Thông báo change cipher spec được cả Client và Server gửi để thông báo cho bên nhận rằng các bản ghi tiếp theo sẽ được bảo vệ theo CipherSpec và các khóa vừa được thương lượng.
- Việc tiếp nhận thông báo này khiến trạng thái đang chờ được sao chép vào trạng thái hiện tại, trạng thái này cập nhật bộ mật mã sẽ được sử dụng trên kết nối này. Client gửi thông báo change cipher spec sau khi trao đổi khóa bắt tay và thông báo xác minh chứng chỉ (nếu có) và Server gửi một thông báo sau khi xử lý thành công thông báo trao đổi khóa mà Client nhận được.

5.3.3. Giao thức SSL
d) Giao thức cảnh báo SSL

Một trong những kiểu nội dung được SSL Record Layer hỗ trợ là kiểu cảnh báo. Tin nhắn cảnh báo truyền tải mức độ nghiêm trọng của tin nhắn và mô tả về cảnh báo.
Tin nhắn cảnh báo bao gồm 2 byte.

- Byte đầu tiên lấy giá trị cảnh báo hoặc nghiêm trọng để truyền tải mức độ nghiêm trọng của tin nhắn. Nếu mức độ nghiêm trọng, SSL sẽ ngay lập tức chấm dứt kết nối. Trong trường hợp này, các kết nối khác trên cùng một phiên có thể tiếp tục, nhưng các mã định danh phiên phải bị vô hiệu hóa, ngăn không cho phiên bị lỗi được sử dụng để thiết lập các kết nối mới.
- Byte thứ hai chứa mã chỉ ra cảnh báo cụ thể. Cũng giống như các ứng dụng khác sử dụng SSL, tin nhắn cảnh báo được nén và mã hóa, theo chỉ định của trạng thái kết nối hiện tại.

5.3.3. Giao thức SSL
d) Giao thức cảnh báo SSL

Một thông số kỹ thuật của các cảnh báo liên quan đến SSL luôn nghiêm trọng:

- unexpected-message. Đã nhận được một thông báo không phù hợp.
- bad-record-mac. Cảnh báo này được trả về nếu nhận được một bản ghi có MAC không chính xác.
- Decompression-failure: Chức năng giải nén đã nhận được đầu vào không phù hợp (tức là dữ liệu sẽ mở rộng đến độ dài lớn hơn độ dài tối đa cho phép).
- No-certificate: Thông báo cảnh báo này có thể được gửi để phản hồi yêu cầu chứng chỉ nếu không có chứng chỉ phù hợp nào khả dụng.
- Bad-certificate: Chứng chỉ đã nhận bị hỏng, nghĩa là chứa chữ ký không xác minh chính xác.

5.3.3. Giao thức SSL
d) Giao thức cảnh báo SSL

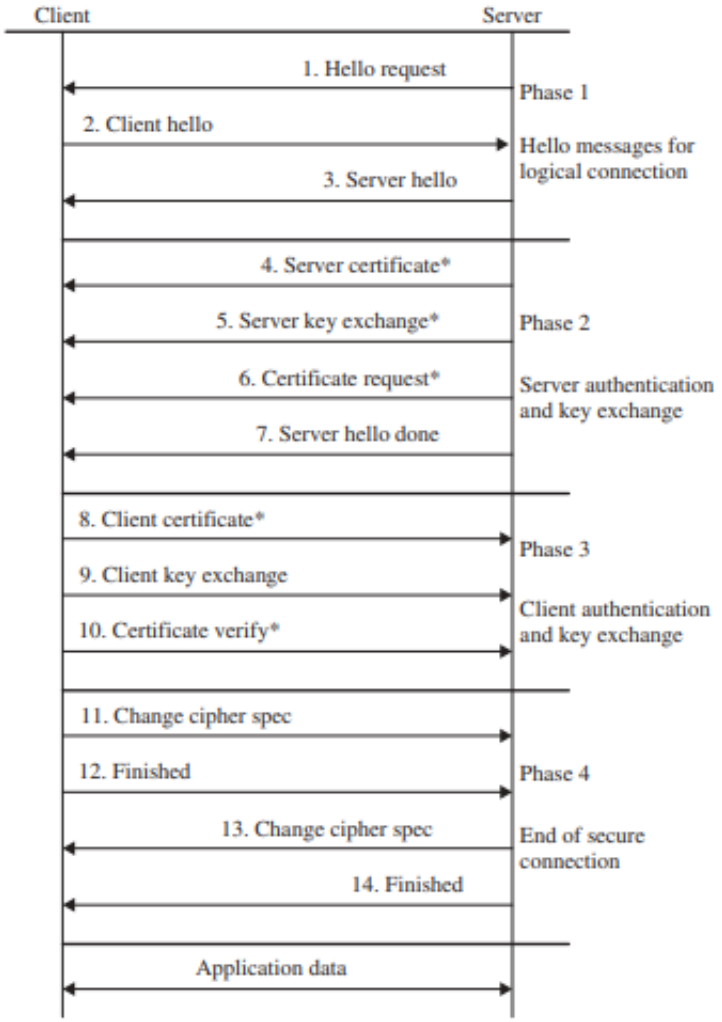
Một thông số kỹ thuật của các cảnh báo liên quan đến SSL luôn nghiêm trọng (tt):

- unsupported certificate: Loại chứng chỉ đã nhận không được hỗ trợ.
- Certificate-revoked: Người ký đã thu hồi chứng chỉ.
- Certificate-expired: Chứng chỉ đã hết hạn hoặc hiện không hợp lệ.
- Certificate-unknown: Một số vấn đề không xác định khác đã phát sinh trong quá trình xử lý chứng chỉ, khiến chứng chỉ không được chấp nhận.
- illegal-parameter. Một trường trong quá trình bắt tay nằm ngoài phạm vi hoặc không nhất quán với các trường khác.
- Close-notify: Thông báo này thông báo cho người nhận rằng người gửi sẽ không gửi thêm bất kỳ thông báo nào trên kết nối này. Phiên sẽ không thể tiếp tục nếu bất kỳ kết nối nào bị chấm dứt mà không có thông báo close-notify phù hợp với mức độ bằng cảnh báo. Mỗi bên được yêu cầu gửi cảnh báo close-notify trước khi đóng phía ghi của kết nối. Bất kỳ bên nào cũng có thể khởi tạo cảnh báo close-notify. Bất kỳ dữ liệu nào nhận được sau cảnh báo đóng đều bị bỏ qua.

5.3.3. Giao thức SSL
e) Giao thức bắt tay SSL (SSL Handshake)

Giao thức bắt tay SSL được vận hành trên tầng SSL Record là phần quan trọng nhất của SSL. Giao thức này cung cấp ba dịch vụ cho các kết nối SSL giữa Server và Client để bảo vệ dữ liệu được gửi trong SSL Record trước khi giao thức ứng dụng truyền hoặc nhận byte dữ liệu đầu tiên.

- Giao thức bắt tay cho phép Client/Server đồng ý về phiên bản giao thức
- Xác thực lẫn nhau bằng MAC
- Thương lượng thuật toán mã hóa và khóa mật mã



5.3. Các giao thức truyền thông an toàn
5.3.4. Giao dịch điện tử an toàn (SET)

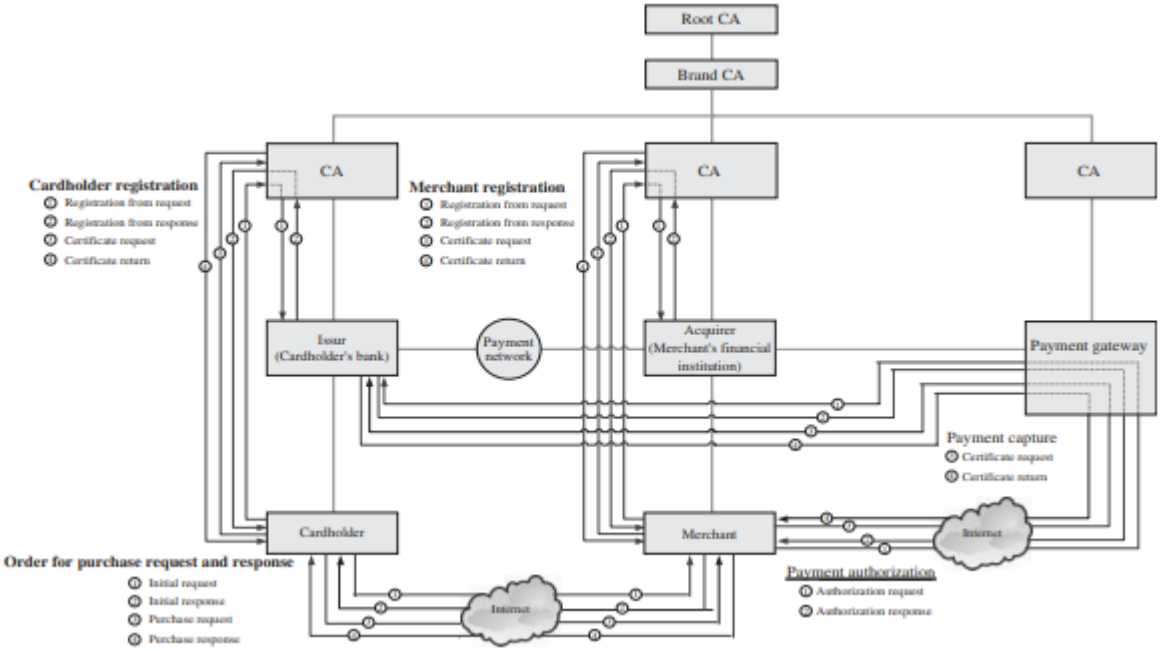
Giao dịch điện tử an toàn (SET - Secure Electronic Transaction) là một giao thức được thiết kế để bảo vệ các giao dịch thẻ tín dụng qua Internet. Đây là một tiêu chuẩn được ngành công nghiệp hỗ trợ, được MasterCard và Visa hình thành vào tháng 2 năm 1996.

SET dựa vào mật mã và chứng chỉ kỹ thuật số X.509 v3 để đảm bảo tính bảo mật và an toàn của tin nhắn. SET là giao thức giao dịch Internet duy nhất cung cấp bảo mật thông qua xác thực. Nó chống lại rủi ro thông tin giao dịch bị thay đổi trong quá trình truyền tải bằng cách giữ thông tin được mã hóa an toàn mọi lúc và bằng cách sử dụng chứng chỉ kỹ thuật số để xác minh danh tính của những người truy cập vào thông tin chi tiết về thanh toán.

5.3.4. Giao dịch điện tử an toàn (SET)
a) Mối quan hệ giữa các thành phần trong SET

Hệ thống SET có các thành phần chính cho giao dịch an toàn trực tuyến:

- Chủ thẻ (Cardholder): Người sở hữu thẻ thanh toán để mua sắm trực tuyến.
- Đơn vị phát hành (Issuer): Ngân hàng phát hành thẻ và đảm bảo thanh toán các giao dịch hợp lệ.
- Thương gia (Merchant): Cá nhân/tổ chức bán hàng hóa/dịch vụ và chấp nhận thanh toán qua thẻ.
- Đơn vị thanh toán (Acquirer): Ngân hàng liên kết với thương gia, xử lý và xác nhận giao dịch thanh toán.
- Cổng thanh toán (Payment gateway): Kết nối thương gia và đơn vị thu mua, thực hiện các dịch vụ thanh toán và xác thực giao dịch.
- Cơ quan cấp chứng chỉ (CA - Certification Authority): Cấp chứng chỉ khóa công khai cho các bên, tạo chuỗi tin cậy và xác thực chữ ký số.

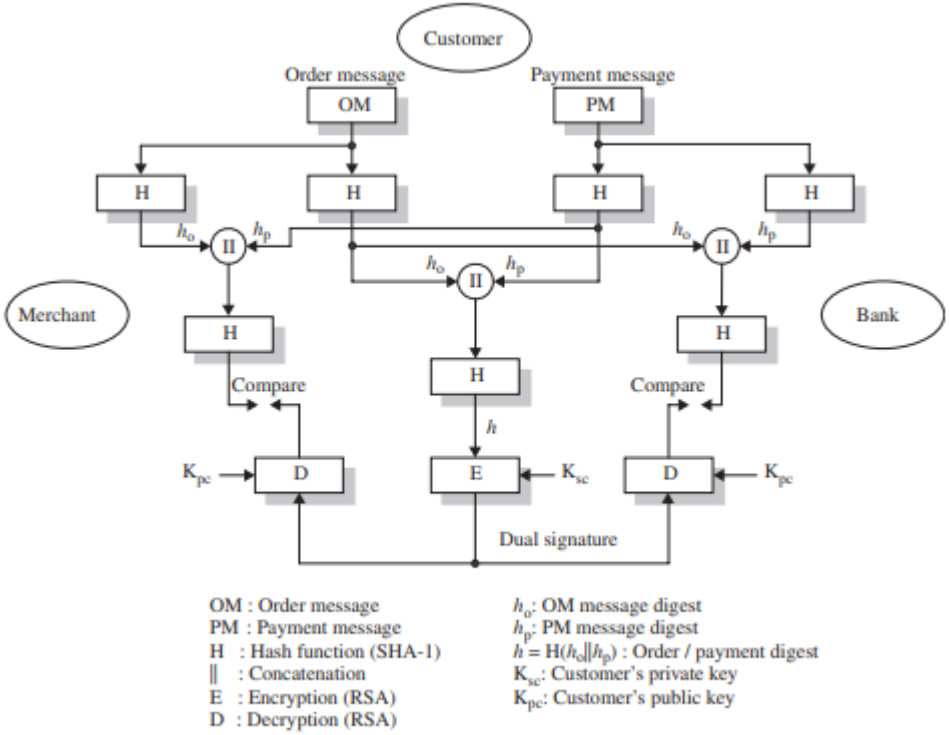


Hệ thống phân cấp giao dịch SET chỉ ra mối quan hệ giữa những người tham gia

5.3.4. Giao dịch điện tử an toàn (SET)
b) Xác thực thông điệp đặt hàng/thanh toán

Chữ ký kép (DS - Dual Signature) được tạo ra bằng cách tạo bản tóm tắt thông điệp của hai thông điệp: bản tóm tắt đơn hàng và bản tóm tắt thanh toán.

- Khách hàng lấy mã băm (bản tóm tắt thông điệp) của cả thông điệp đơn hàng (OM) và PM bằng cách sử dụng thuật toán SHA-1.
- Sau đó, hai bản băm này, ho và hp, được nối lại và lấy mã băm h của kết quả.
- Cuối cùng, khách hàng mã hóa (thông qua RSA) mã băm cuối cùng bằng khóa riêng của mình, Ksc, tạo ra DS.



Chữ ký kép và xác thực thông điệp đặt hàng/thanh toán

Cảm ơn các bạn,

Chúc các bạn thành công!