CHƯƠNG VI

AN TOÀN THƯ ĐIỆN TỬ VÀ HỆ THỐNG WEB

ThS. Nguyễn Cao Đạt

E-mail: dat@hcmut.edu.vn

Tham khảo

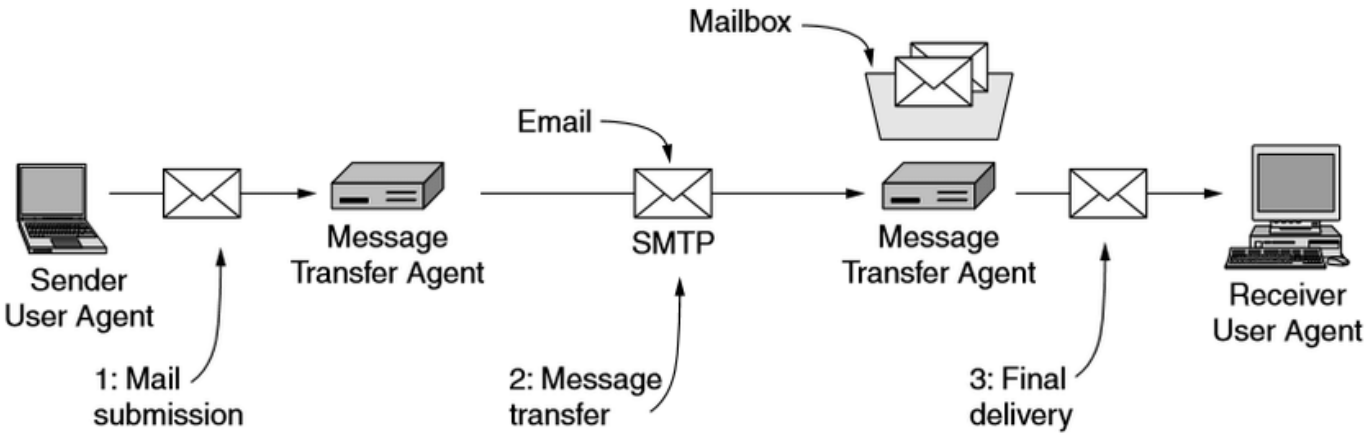
[1]. Cryptography and Network Security: chương 15
[1]. Cryptography and Network Security: chương 17

NỘI DUNG TRÌNH BÀY

- An toàn thư điện tử
- An toàn hệ thống Web
- Giao dịch điện tử an toàn

AN TOÀN THƯ ĐIỆN TỬ

- **Thư điện tử là một trong những dịch vụ được sử dụng rộng rãi trên Internet.**
- **Tuy nhiên nó không an toàn**
  - Nội dung thông điệp có thể xem xét/sửa đổi khi truyền đi
  - Được xem bởi người có quyền cao hơn trên hệ thống đích đến
  - Dễ dàng giả mạo người gửi

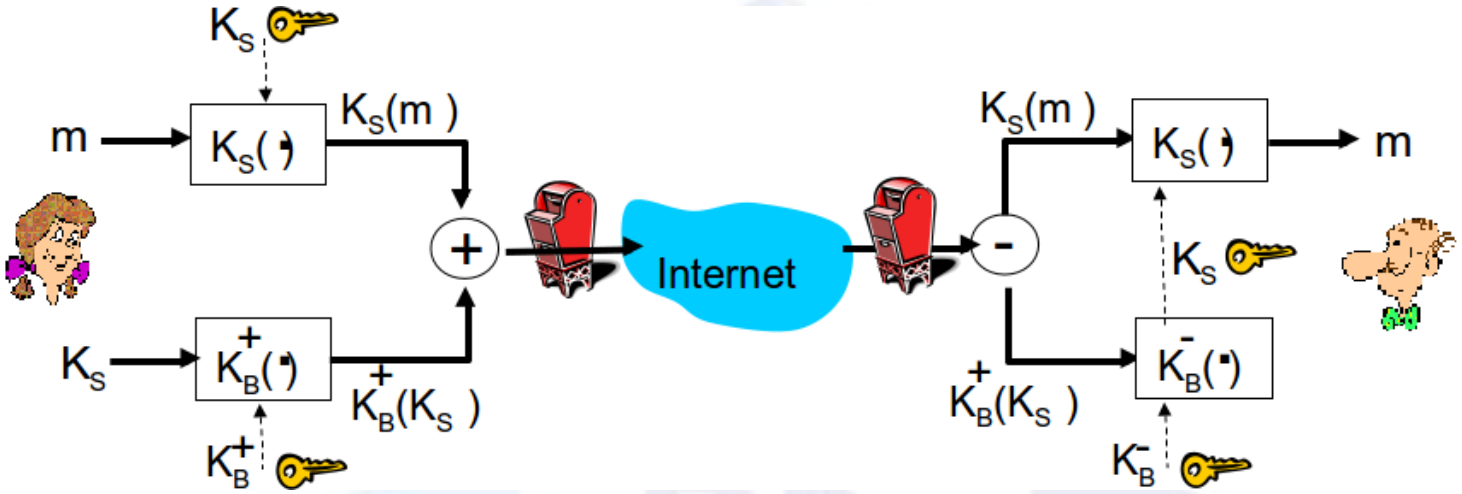


AN TOÀN THƯ ĐIỆN TỬ

- **Các cải tiến cần thiết**
  - Bí mật - Không tiết lộ nội dung thông điệp
  - Toàn vẹn thông điệp - chống sửa đổi nội dung thông điệp
  - Xác thực – Xác thực người gửi, chống thoái thác về nguồn gốc

ĐẢM BẢO TÍNH BÍ MẬT

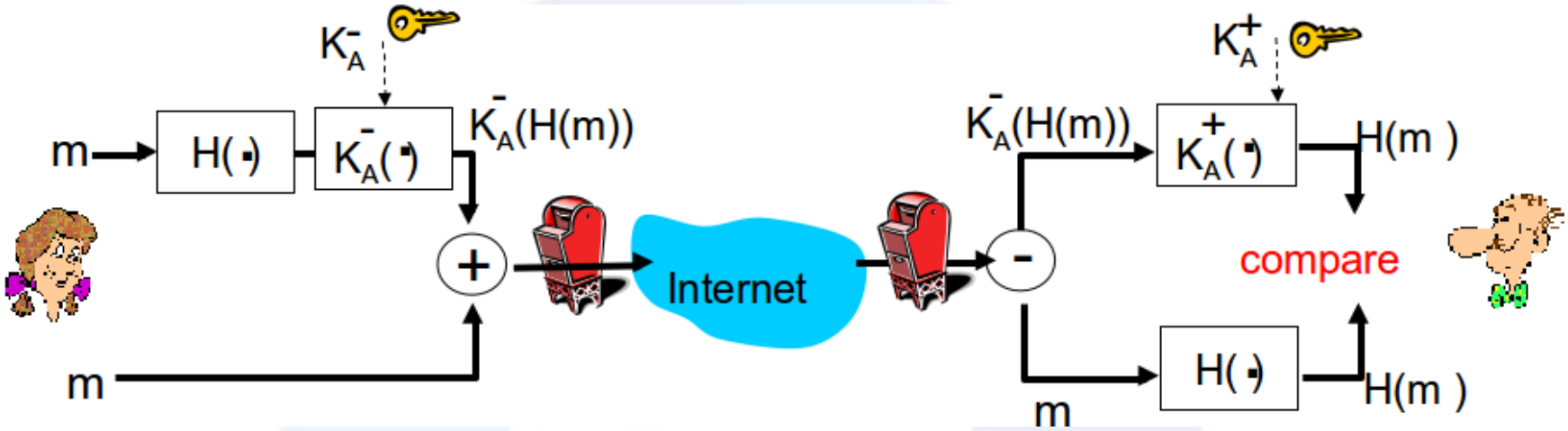
- **Alice muốn gởi thư bí mật với nội dung m đến Bob**



- **Alice**
  - Tạo ngẫu nhiên một khóa bí mật dùng cho mã hóa đối xứng **K_S**
  - Mã hóa đối xứng thông điệp với **K_S**
  - Cũng mã hóa khóa công khai **K_S** với khóa công khai của Bob
  - Gửi cả **$K_S(m)$** và **$K_B(K_S)$** đến Bob

ĐẢM BẢO TÍNH TOÀN VẸN VÀ XÁC THỰC

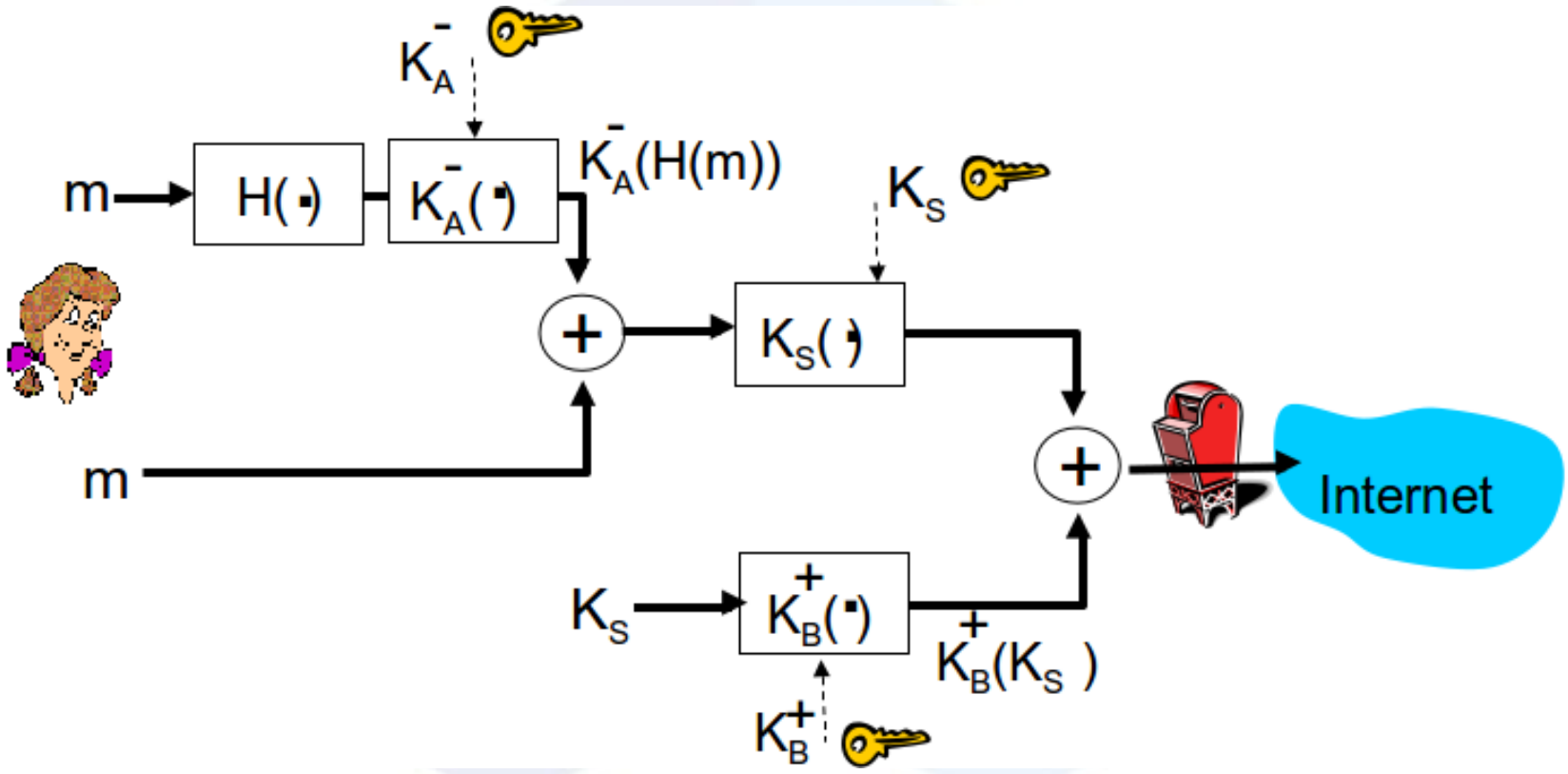
- **Alice muốn gởi thư có xác thực người gửi và toàn vẹn thông điệp m đến Bob**



- **Alice**
  - Tạo chữ ký số trên thông điệp **m**
  - Gửi cả thông điệp **m** (bản rõ) và chữ ký số đến Bob

ĐẢM BẢO CẢ BA MỤC TIÊU

- **Alice muốn gởi thư bí mật có xác thực người gửi và toàn vẹn thông điệp m đến Bob**



Pretty Good Privacy (PGP)

- Được sử dụng rộng rãi để **an toàn thư điện tử**.
- Được Phil Zimmermann phát triển.
- Chọn những thuật toán mã hóa sẵn có tốt nhất và tích hợp vào thành một chương trình và thực thi được trên nhiều hệ thống.
- Gồm cả hai phiên bản miễn phí và thương mại.
- Cung cấp hai dịch vụ chính bí mật và xác thực.
- Có thể dùng cho E-mail và các ứng dụng lưu trữ tập tin.

Dịch vụ xác thực trong PGP

1. Bên gửi tạo thông điệp
2. Dùng SHA-1 để tạo giá trị băm 160 bits của thông điệp
3. Ký trên giá trị băm với RSA dùng khóa riêng của bên gửi và đính kèm nó với thông điệp
4. Bên nhận dùng RSA và khóa công khai của bên gửi để giải mã chữ ký và phục hồi mã băm tương ứng
5. Bên nhận xác minh giá trị băm trên thông điệp nhận được và so sánh với mã băm đã giải mã

Dịch vụ bí mật trong PGP

1. Bên gửi tạo thông điệp và một số 128 bits ngẫu nhiên như khóa phiên
2. Mã hóa thông điệp dùng CAST-128 / IDEA / 3DES trong chế độ CBC/CFB với khóa phiên
3. Khóa phiên được mã hóa dùng RSA với khóa công khai của người nhận và đính kèm đến thông điệp đã mã hóa
4. Bên nhận dùng RSA với khóa riêng để giải mã và khôi phục khóa phiên
5. Khóa phiên sẽ được dùng để giải mã thông điệp

Bí mật kết hợp với xác thực trong PGP

- **Có thể dùng cả hai dịch vụ trên cùng một thông điệp**
  - Tạo chữ ký và đính kèm vào thông điệp
  - Mã hóa cả thông điệp và chữ ký dùng khóa phiên
  - Đính kèm khóa phiên đã được mã hóa bằng RSA/ElGamal dùng khóa công khai của người nhận

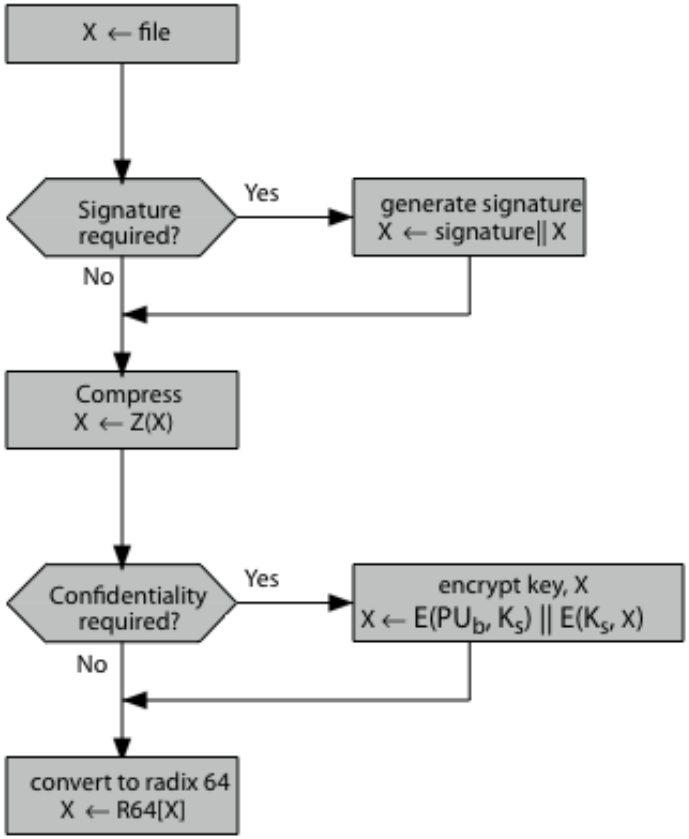
Dịch vụ nén trong PGP

- **Mặc định PGP nén thông điệp sau khi ký nhưng trước khi mã hóa**
  - Tiết kiệm không gian cho cả việc truyền e-mail hay lưu trữ tập tin.
  - Lưu trữ thông điệp chưa nén và chữ ký cho việc xác minh sau này.
- **Dùng thuật toán nén ZIP**

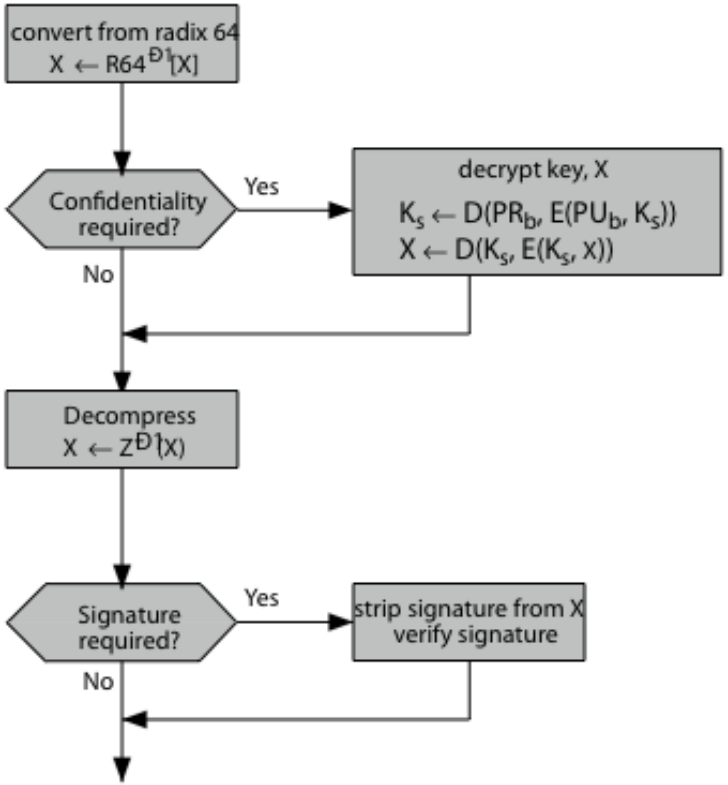
Dịch vụ tương thích E-mail trong PGP

- Do các hệ thống E-mail chỉ chấp nhận dùng các ký tự in được trong bảng mã ASCII.
- Cần phải chuyển đổi dữ liệu khi cần gửi dữ liệu nhị phân.
- PGP chuyển dữ liệu nhị phân thành các ký tự in được trong bảng mã ASCII dùng thuật toán radix-64
  - Ánh xạ 3 bytes thành 4 ký tự in được
  - Cũng nối thêm CRC để phát hiện lỗi khi truyền
- PGP cũng tự động chia nhỏ thông điệp nếu thông điệp quá lớn

Các dịch vụ trong PGP



(a) Generic Transmission Diagram (from A)



(b) Generic Reception Diagram (to B)

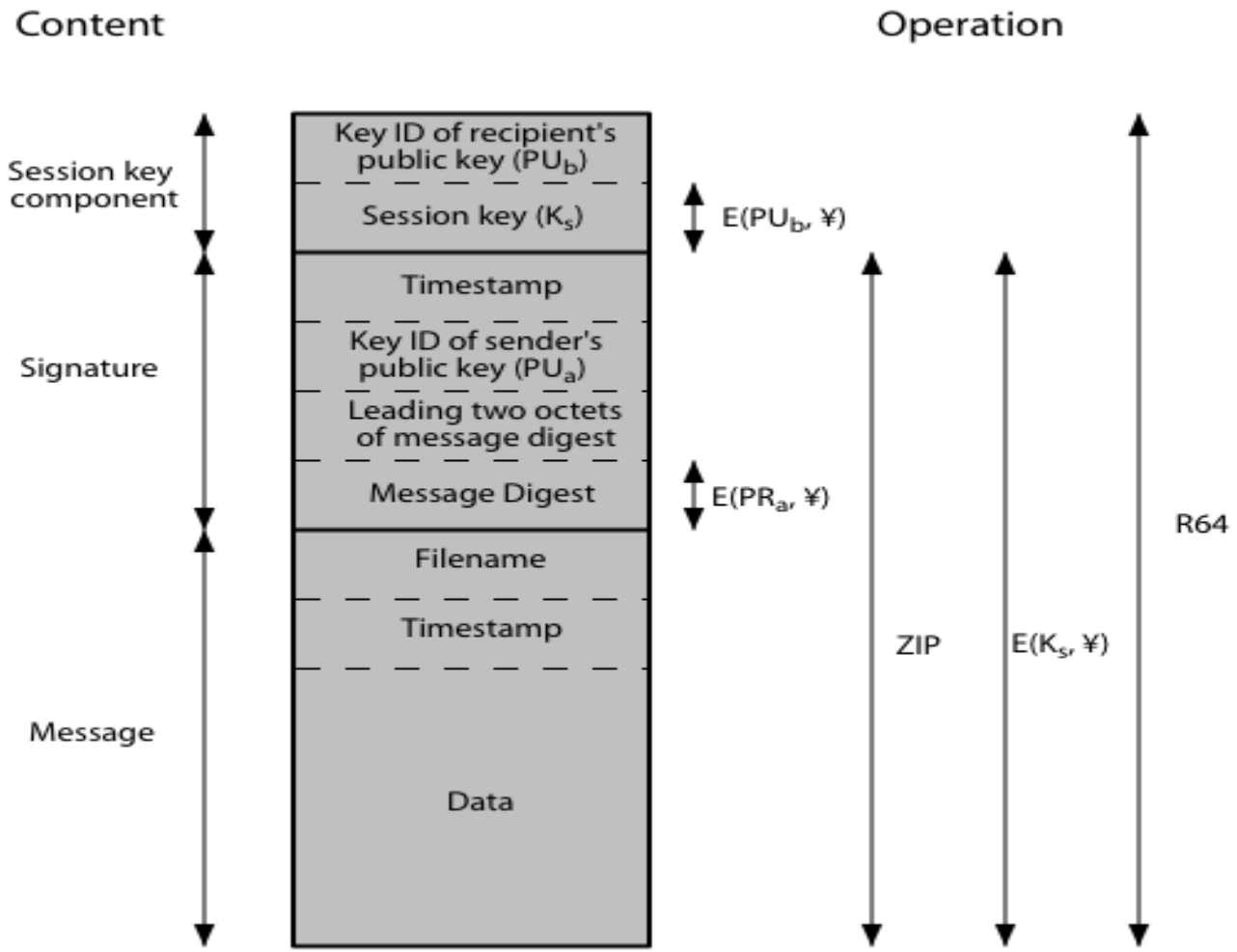
Khóa phiên PGP

- Cần khóa phiên mới cho mỗi thông điệp
  - Với kích thước khác nhau:56-bit với DES, 128-bit với CAST hay IDEA, 168-bit với Triple-DES
- Tạo dựa trên bộ tạo ANSI X12.17
- Dùng các đầu vào ngẫu nhiên được lấy từ các lần sử dụng trước đó và thời điểm gõ trên bàn phím của người dùng

Định danh khóa trong PGP

- **Nhiều cặp khóa có thể được dùng vì vậy cần xác định cặp khóa thực sự được dùng để mã hóa/giải mã khóa phiên**
  - Có thể gởi khóa công khai với mỗi thông điệp
  - Phương pháp này không hiệu quả
- **Dùng định danh khóa dựa trên khóa**
  - Định danh khóa(key ID) nhỏ hơn nhiều so với khóa
  - Ảnh hưởng ít nhất 64-bits của khóa
  - Khả năng định danh khóa duy nhất rất cao
  - Gởi đính kèm định danh khóa với mỗi thông điệp
- **Cũng có thể dùng định danh khóa cho chữ ký số trong PGP**

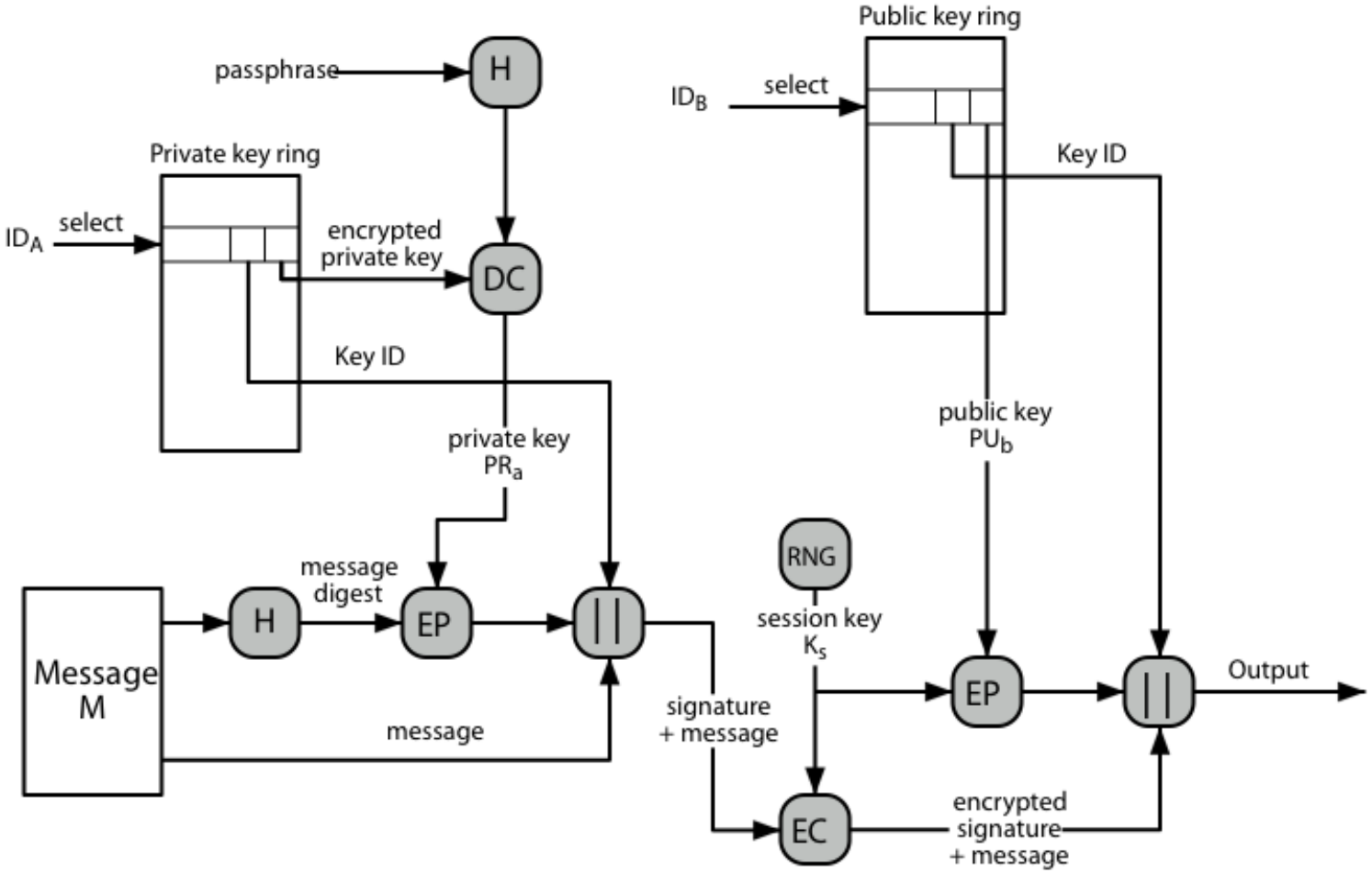
Định dạng thông điệp với PGP



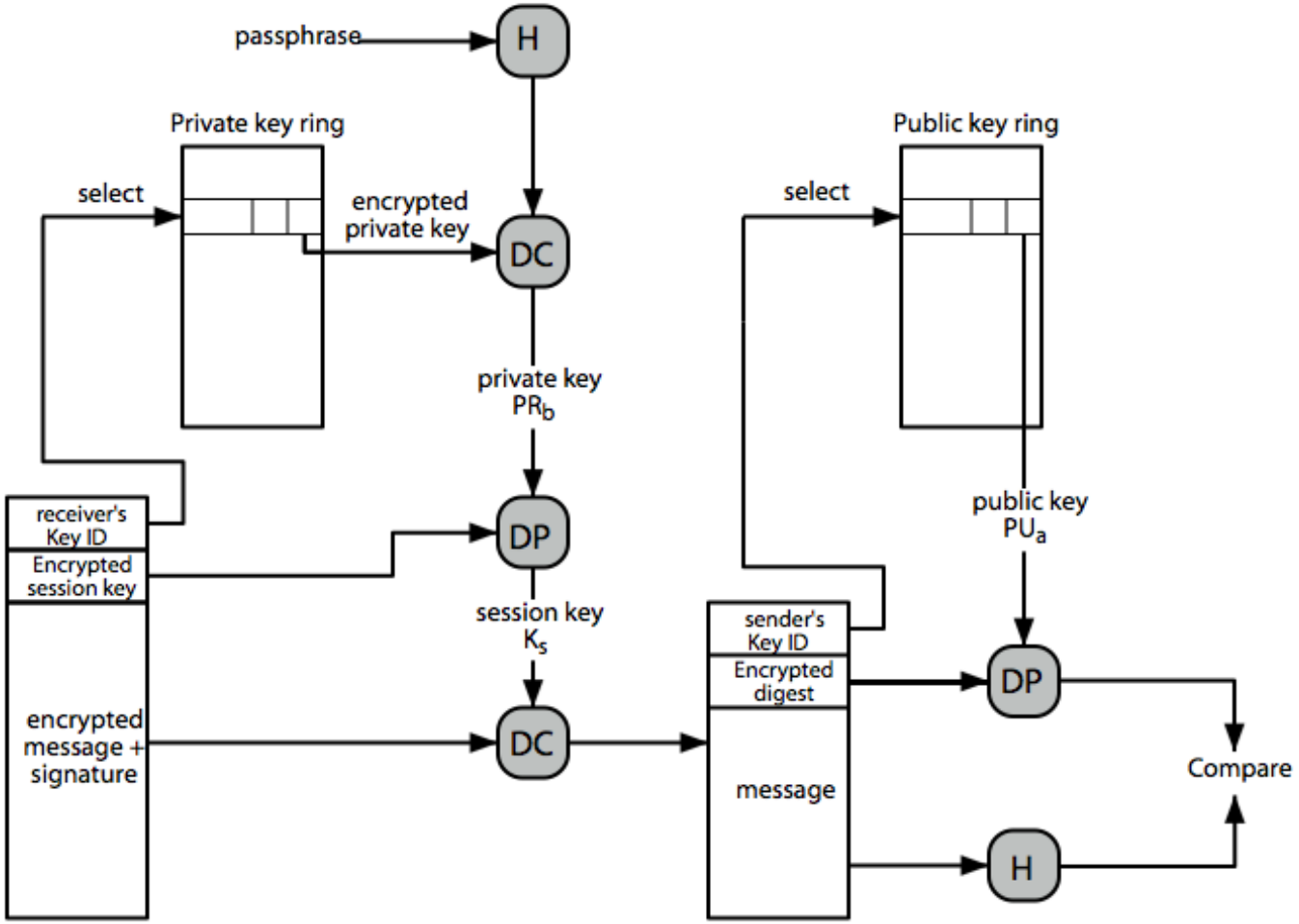
Chùm khóa PGP

- **Mỗi người dùng PGP có hai chùm khóa**
  - Chùm khóa công khai chứa tất cả các khóa công khai của các người dùng PGP mà người dùng biết và được đánh chỉ số dùng định danh khóa.
  - Chùm khóa riêng chứa cặp khóa công khai/riêng của người dùng. Chúng được đánh chỉ số dùng định danh khóa và được mã hóa bởi một mật khẩu gọi là pass-phrase. Pass-phrase sẽ được người dùng cung cấp mỗi khi yêu cầu dùng một cặp khóa.
- **An toàn của các khóa riêng phụ thuộc vào độ an toàn của pass-phrase**

Tạo thông điệp với PGP



Xử lý khi tiếp nhận thông điệp



Quản lý khóa PGP

- **Trong PGP mỗi người dùng có thể hành động như CA**
  - Có thể ký các khóa cho những người dùng mà họ biết trực tiếp
  - Giới thiệu tin tưởng đến những người dùng khác như hình thức "web of trust"
- **Hình thức "web of trust"**
  - Các khóa tin tưởng được ký
  - Có thể tin tưởng các khóa khác đã được ký nếu có một chuỗi các chữ ký đến chúng
- Chùm khóa sẽ bao gồm cả các chỉ số tin tưởng
- Người dùng cũng có thể thu hồi khóa nếu nghi ngờ bị thỏa hiệp hay đã sử dụng 1 thời gian dài

NỘI DUNG TRÌNH BÀY

- An toàn thư điện tử
- An toàn hệ thống Web
- Giao dịch điện tử an toàn

AN TOÀN HỆ THỐNG WEB

- **Web được sử dụng rộng rãi trong doanh nghiệp, chính phủ, các cá nhân.**
- **Nhưng Web dễ bị thương tổn với nhiều loại hình tấn công**
  - Bí mật
  - Toàn vẹn
  - Từ chối dịch vụ
  - Xác thực
- **Cần thêm các cơ chế an ninh bổ sung**

AN TOÀN HỆ THỐNG WEB

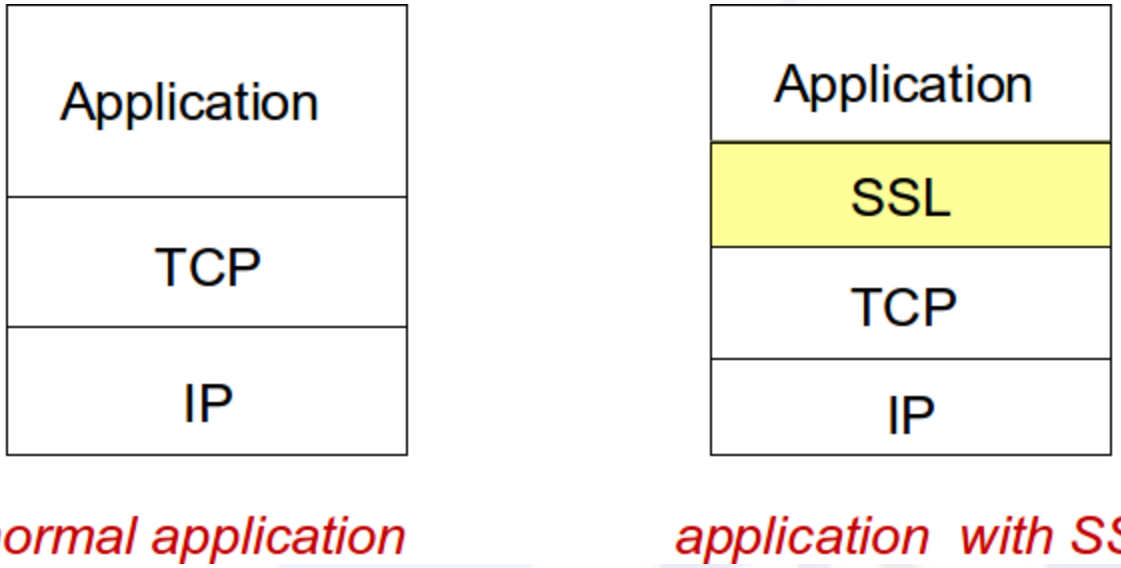
- **SSL(Secure Sockets Layer)**
  - Giao thức an toàn triển khai rộng rãi
  - Được hỗ trợ trên hầu hết trình duyệt, máy chủ Web (https)
  - Nhiều tỉ đô la Mỹ$/năm trên SSL
  - Được Netscape đề xuất vào 1994
  - Biến thể là TLS(transport layer security)
- **Cung cấp**
  - Tính bí mật
  - Toàn vẹn
  - Xác thực

SSL(Secure Sockets Layer)

- **Mục tiêu ban đầu**
  - Giao dịch thương mại điện tử trên Web
  - Mã hóa (Đặc biệt là số credit-card)
  - Xác thực Web
  - Xác thực khách là tùy chọn

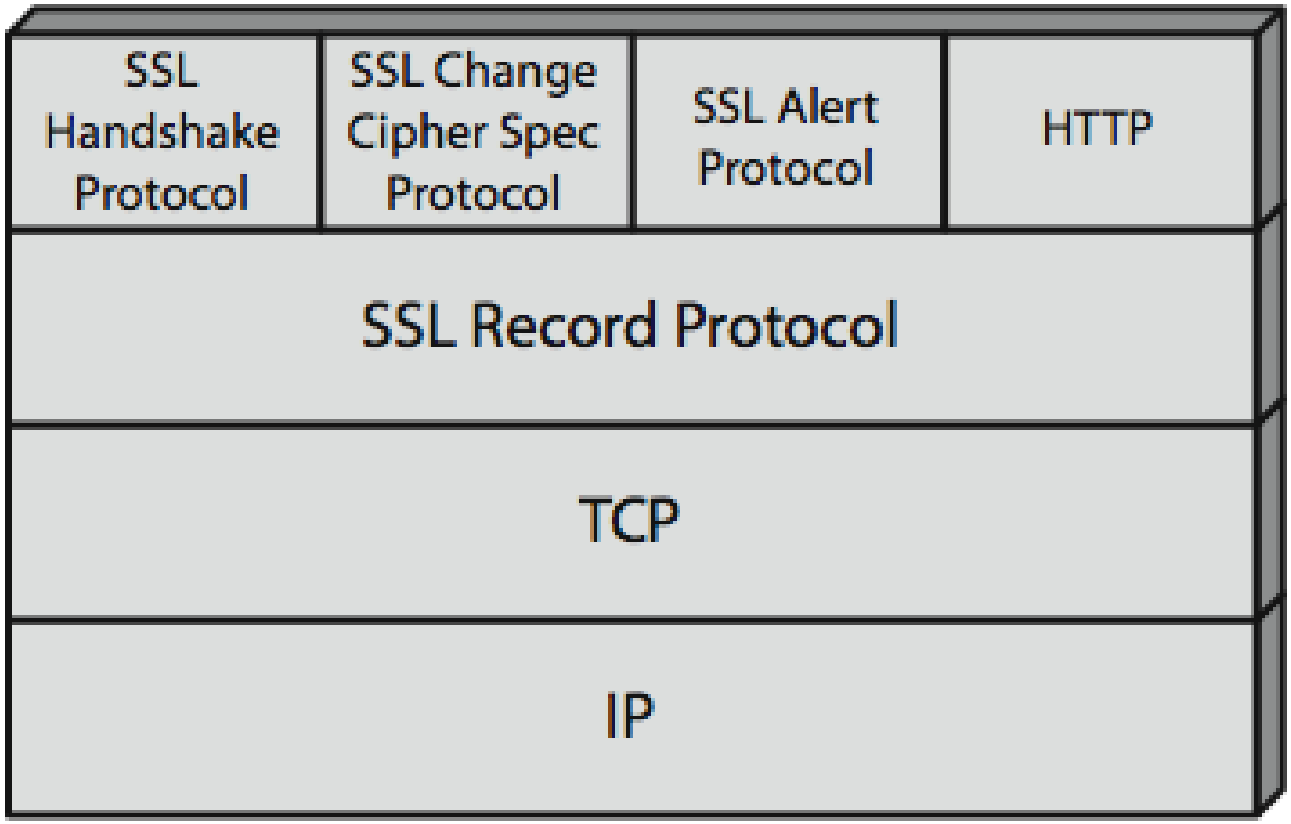
SSL(Secure Sockets Layer)

- **Chuyển đổi ứng dụng TCP**



  - SSL cung cấp giao diện lập trình (API - application programming interface) đến các ứng dụng.
  - Nhiều ngôn ngữ lập trình như C/C++/C#/Java có thư viện lập trình với SSL

KIẾN TRÚC SSL

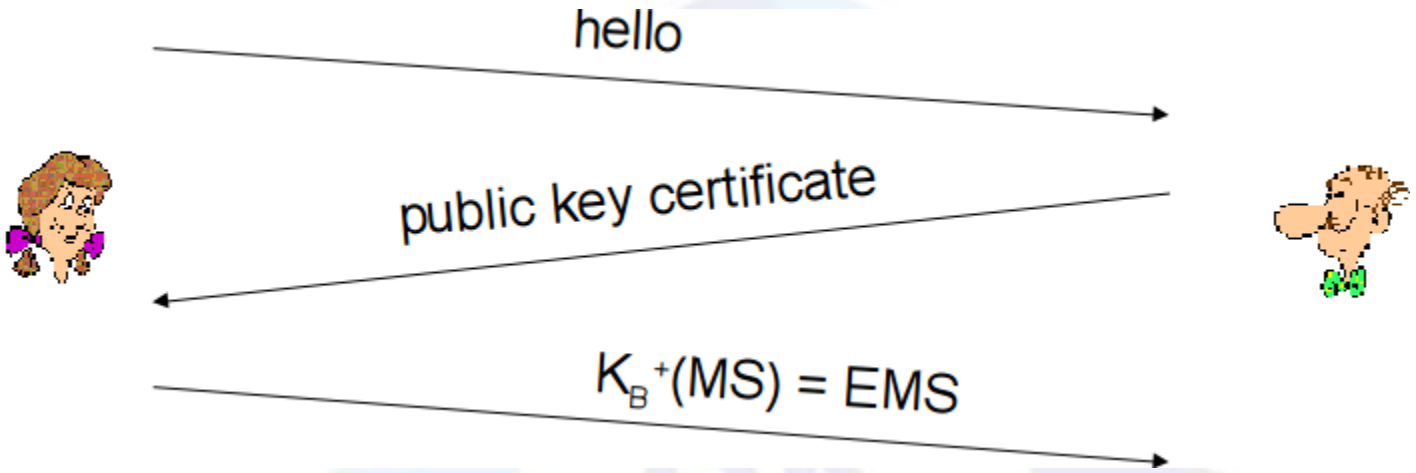


KIẾN TRÚC SSL

- **Hai khái niệm quan trọng trong SSL**
  - **Kết nối SSL**
    - Một liên kết truyền thông ngang hàng, ngắn hạn
    - Kết hợp với một phiên SSL
  - **Phiên SSL**
    - Một sự kết hợp giữa client và server
    - Được tạo dùng giao thức bắt tay(Handshake Protocol)
    - Định nghĩa một tập các tham số liên quan đến mật mã
    - Có thể được chia sẻ bởi nhiều kết nối SSL

SSL(Secure Sockets Layer)

- **Bắt tay an toàn đơn giản**



  - MS(Master key): Khóa chủ
  - EMS(Encrypted master key): Khóa chủ đã được mã hóa

SSL(Secure Sockets Layer)

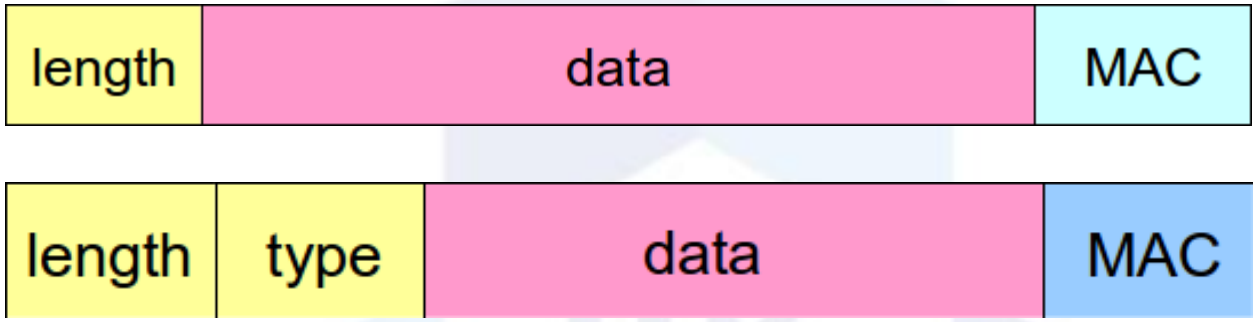
- **Phát sinh khóa**
  - Dùng các khóa khác nhau cho MAC và mã hóa
  - Các khóa được tạo ra từ khóa chủ
  - Bốn khóa
    - $\mathbf{K_c}$ = Khóa mã hóa cho dữ liệu gửi từ client đến server
    - $\mathbf{M_c}$ = Khóa MAC cho dữ liệu gửi từ client đến server
    - $\mathbf{K_s}$ = Khóa mã hóa cho dữ liệu gửi từ server đến client
    - $\mathbf{M_s}$ = Khóa MAC cho dữ liệu gửi từ server đến client

SSL(Secure Sockets Layer)

- **Giao thức bắt tay trong SSL**
  - Cho phép client và server
    - Xác thực lẫn nhau
    - Đàm phán các thuật toán mã hóa và MAC
    - Đàm phán các khóa mật mã được dùng
  - Bao gồm các giai đoạn
    1. Thiết lập các khả năng an ninh
    2. Xác thực Server và trao đổi khóa
    3. Xác thực Client và trao đổi khóa
    4. Kết thúc

SSL(Secure Sockets Layer)

- **Xử lý dữ liệu**
  - Chuyển luồng dữ liệu thành một loạt record

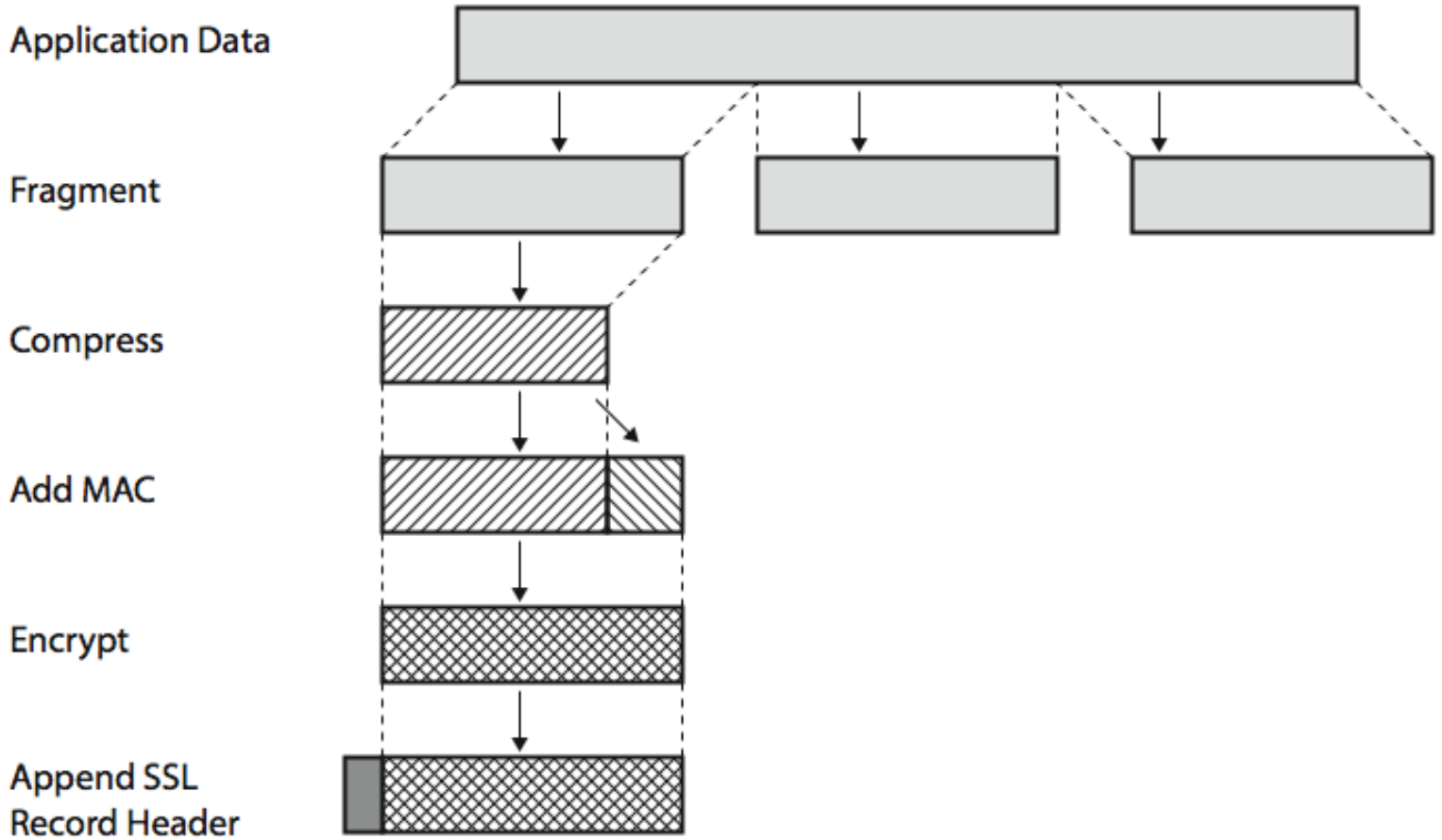


- **Tính toán MAC**
  - MAC = MAC(M_x, sequence || data)
  - Nhằm chống tấn công phát lại

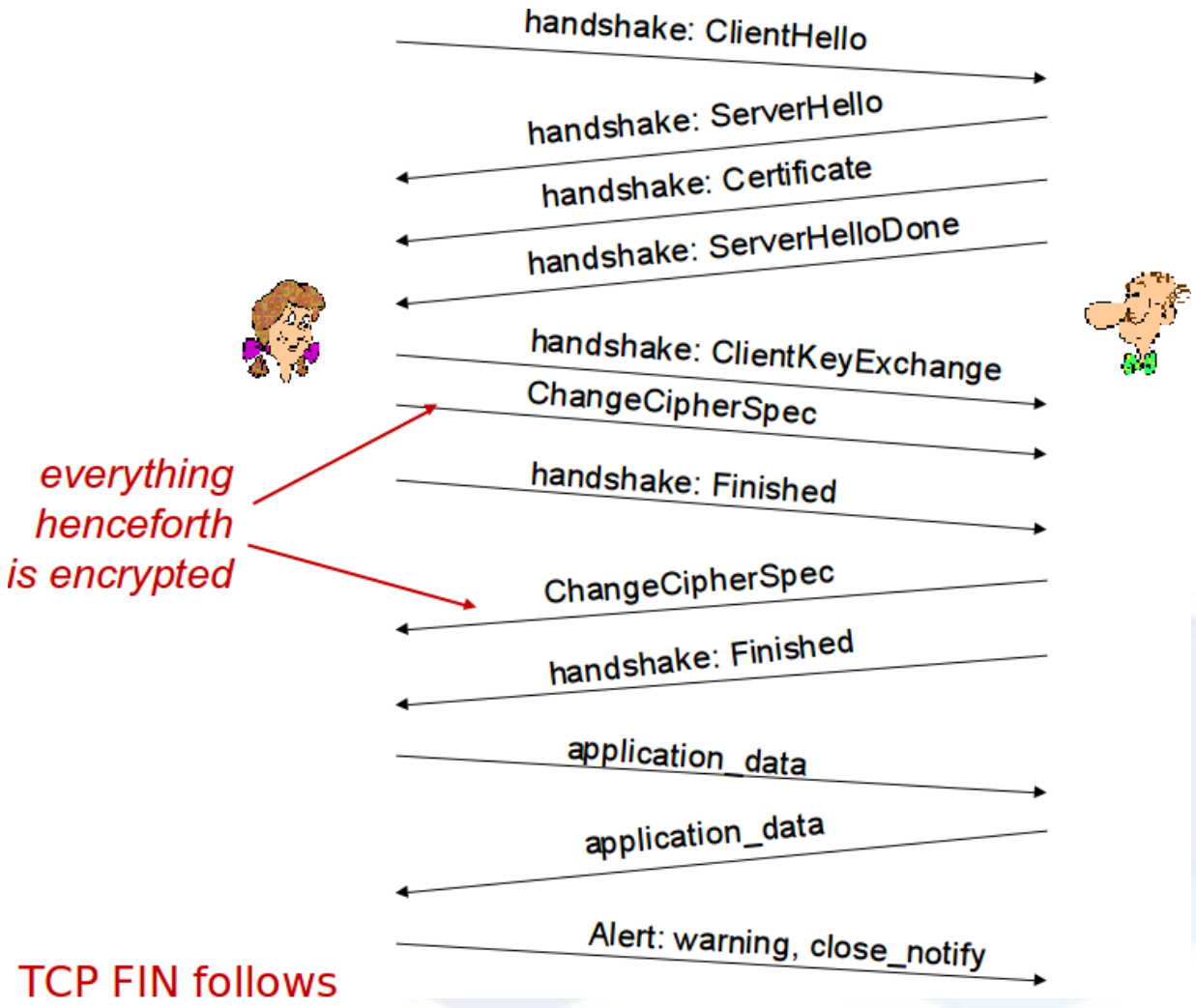
SSL(Secure Sockets Layer)

- **Toàn vẹn thông điệp**
  - Dùng MAC với một khóa bí mật được thống nhất giữa hai bên
  - Tương tự như HMAC
- **Bí mật**
  - Dùng mã hóa đối xứng với khóa bí mật được định nghĩa bởi giao thức bắt tay
  - Dùng các thuật toán AES, IDEA, RC2-40, DES-40, DES, 3DES, Fortezza, RC4-40, RC4-128
  - Các thông điệp được nén trước khi mã hóa

SSL(Secure Sockets Layer)



SSL(Secure Sockets Layer)



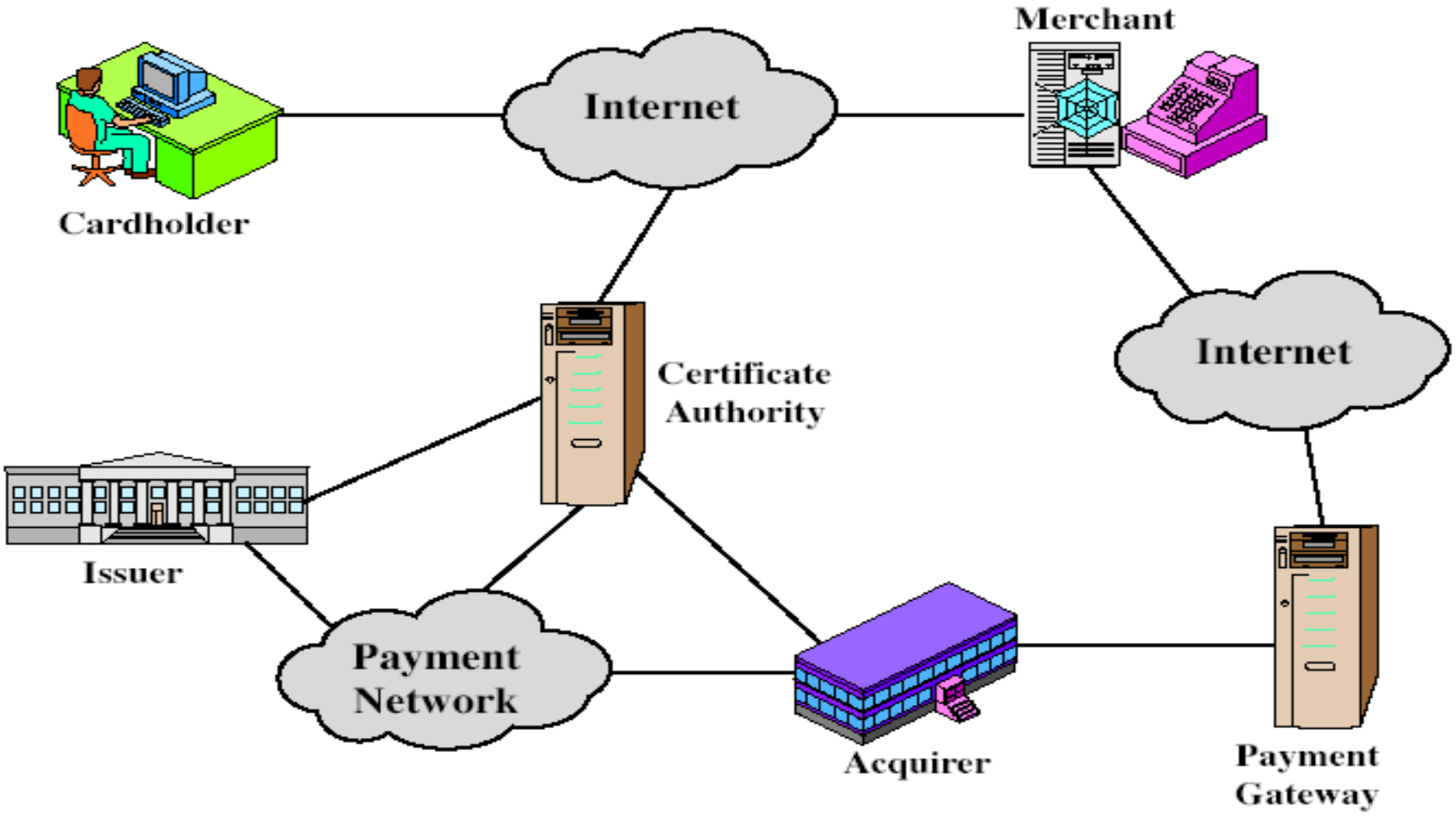
NỘI DUNG TRÌNH BÀY

- An toàn thư điện tử
- An toàn hệ thống Web
- Giao dịch điện tử an toàn

GIAO DỊCH ĐIỆN TỬ AN TOÀN

- **SET - Secure Electronic Transaction**
  - Đặc tả an ninh và mã hóa mở
  - Bảo vệ các giao dịch thẻ tín dụng trên Internet
  - Được Mastercard, Visa, .. phát triển vào năm 1996
- **Một tập các giao thức và định dạng**
  - Thông tin liên lạc an toàn giữa các bên
  - Tin tưởng dựa trên việc sử dụng chứng chỉ X.509 v3
  - Riêng tư được hiểu là thông tin được hạn chế cho những ai cần nó

CÁC THÀNH PHẦN CỦA SET



GIAO DỊCH SET

1. Khách hàng mở tài khoản
2. Khách hàng nhận một chứng chỉ
3. Nơi bán hàng mở tài khoản và cũng có một chứng chỉ
4. Khách hàng đặt hàng
5. Nơi bán hàng được xác minh
6. Đơn đặt hàng và thanh toán được gửi
7. Nơi bán hàng yêu cầu ủy quyền thanh toán
8. Nơi bán hàng xác nhận đơn đặt hàng
9. Nơi bán hàng cung cấp hàng hóa hay dịch vụ
10. Nơi bán hàng yêu cầu thanh toán

CHỮ KÝ ĐÔI

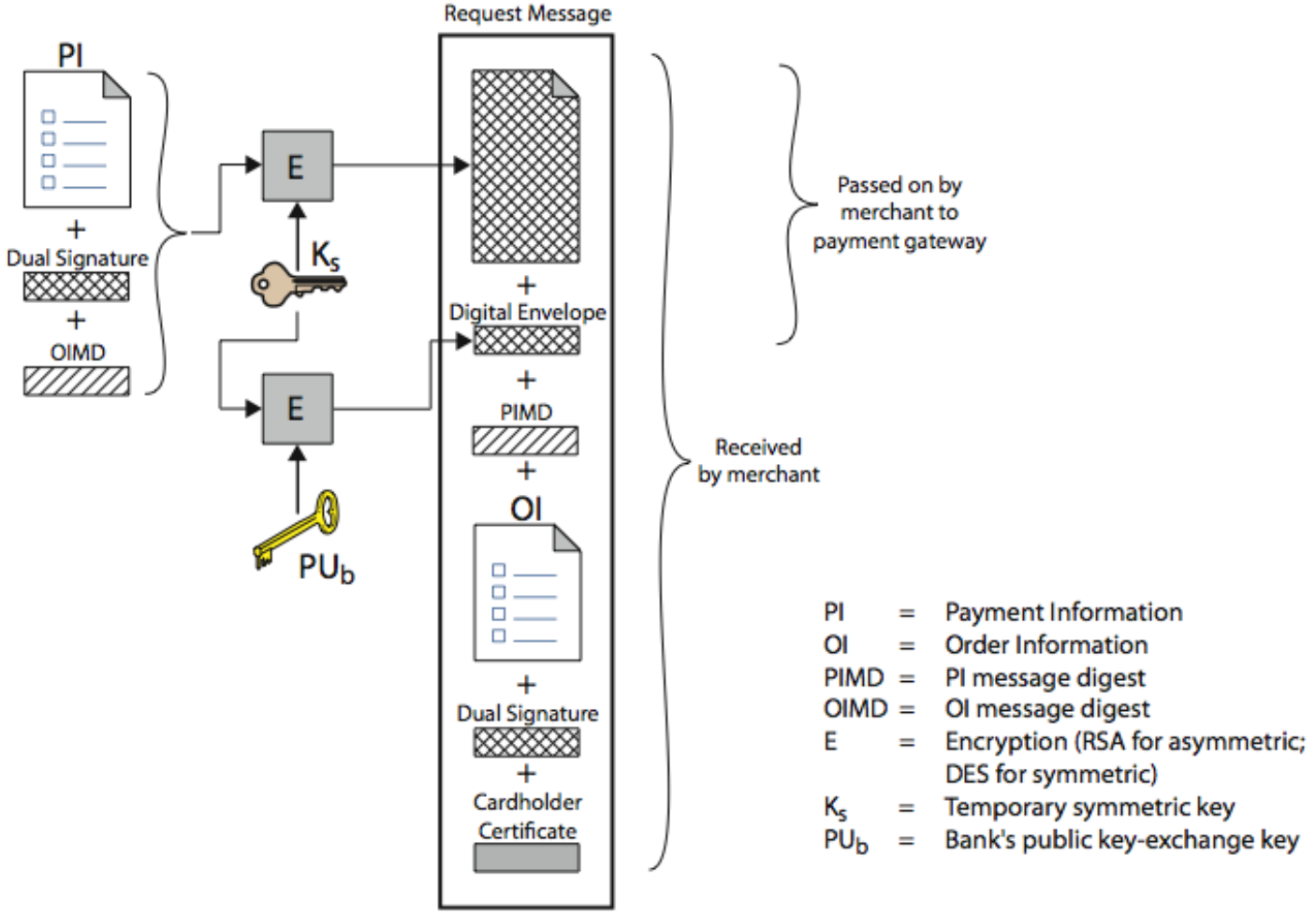
- **DS - Dual Signature**
- **Khách hàng tạo chữ ký đôi nhằm liên kết hai thông điệp được gửi đến hai nơi nhận khác nhau.**
- Các thông điệp cần gửi gồm:
  - Thông tin đặt hàng (order information-OI)
  - Thông tin thanh toán (payment information-PI)
- Tuy nhiên không bên nào cần thông tin chi tiết của bên kia nhưng phải biết chúng được liên kết với nhau vì vậy cần dùng chữ ký đôi.
- **Tạo chữ ký đôi**
  - Ký trên giá trị kết nối của OI & PI

$$DS=E(PR_c, [H(H(PI)||H(OI))])$$

YÊU CẦU MUA HÀNG

- **Gồm 4 thông điệp**
  1. Yêu cầu khởi tạo – lấy chứng chỉ
  2. Đáp ứng khởi tạo – đáp ứng được ký
  3. Yêu cầu mua hàng – OI & PI
  4. Đáp ứng đặt hàng – thừa nhận đặt hàng

YÊU CẦU MUA HÀNG – KHÁCH HÀNG

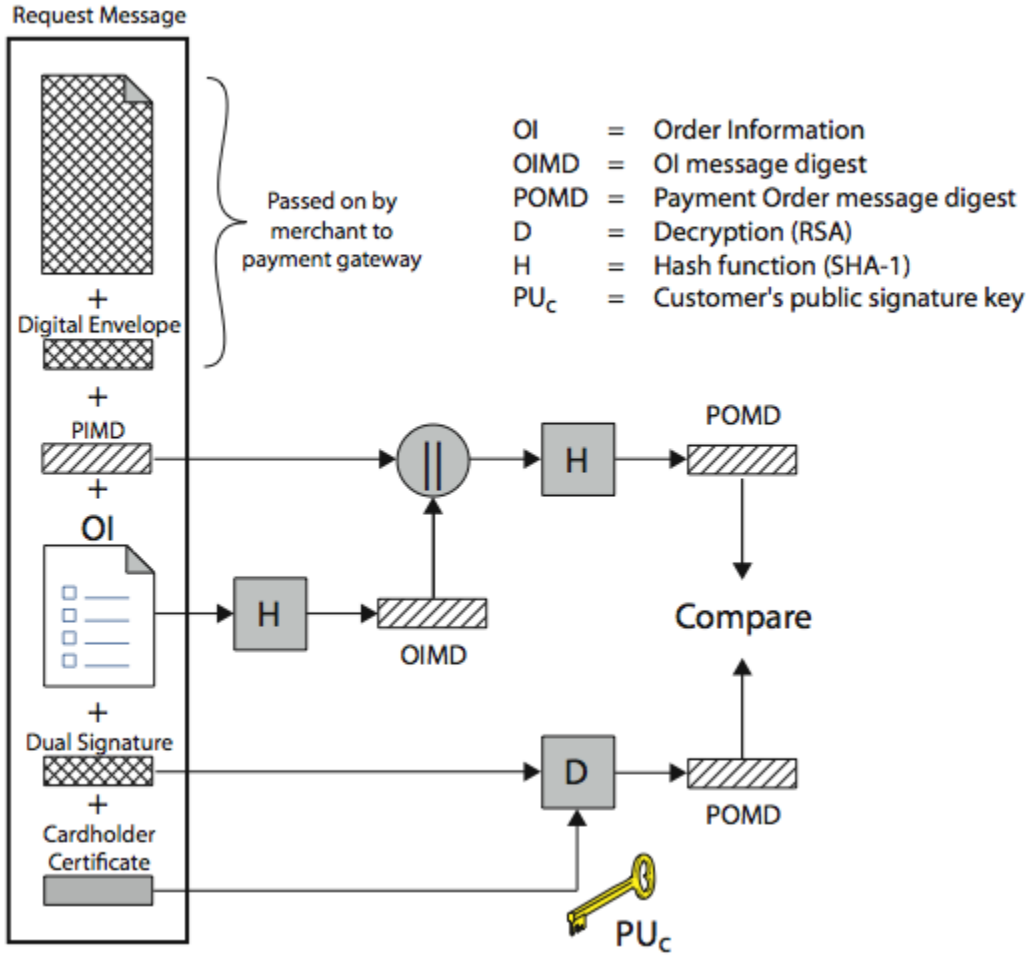


PI = Payment Information
OI = Order Information
PIMD = PI message digest
OIMD = OI message digest
E = Encryption (RSA for asymmetric; DES for symmetric)
K_s = Temporary symmetric key
PU_b = Bank's public key-exchange key

YÊU CẦU MUA HÀNG – NƠI MUA HÀNG

1. Xác minh chứng chỉ của người mua
2. Xác minh chữ ký đôi dùng khóa công khai của người mua để chắc chắn đơn đặt hàng không bị giả mạo khi truyền và nó được ký bởi khóa riêng của người mua
3. Chuyển thông tin thanh toán đến cổng thanh toán cho việc ủy quyền
4. Gửi một đáp ứng mua hàng đến người mua hàng

YÊU CẦU MUA HÀNG – NƠI MUA HÀNG



ỦY QUYỀN TẠI CỔNG THANH TOÁN

1. Xác minh các chứng chỉ
2. Giải mã khối phong bì ủy quyền để lấy khóa đối xứng, giải mã tiếp để có nội dung thông điệp ủy quyền
3. Xác minh chữ ký nơi bán hàng trên khối ủy quyền
4. Giải mã khối phòng bì của khối thanh toán để lấy khóa đối xứng, giải mã tiếp khối thanh toán
5. Xác minh chữ ký đôi trên khối chi trả
6. Xác minh định danh giao dịch nhận được từ nơi ban hàng có khớp với định danh giao dịch trong PI nhận được từ người mua hàng
7. Yêu cầu và nhận một ủy quyền từ nhà phát hành chứng chỉ người mua hàng
8. Gửi đáp ứng ủy quyền về lại nơi bán hàng

TÓM TẮT

- PGP là gói phần mềm cho an toàn hệ thống E-mail. Nó cung cấp xác thực dùng chữ ký số, bí mật dùng mã hóa khối đối xứng. PGP kết hợp các công cụ để xây dựng một mô hình tin cậy khóa công khai và quản lý chứng chỉ khóa công khai.
- SSL cung cấp các dịch vụ bảo mật cho TCP và các ứng dụng sử dụng TCP. Phiên bản chuẩn Internet được gọi là TLS.

TÓM TẮT(T.T)

- SSL/TLS cung cấp dịch vụ bí mật dùng mã hóa đối xứng và dịch vụ toàn vẹn dựa trên MAC.
- SSL/TLS bao gồm các giao thức cho phép hai ứng dụng TCP xác định các cơ chế và các dịch vụ an ninh mà chúng sẽ sử dụng.
- SET là một đặc tả kỹ thuật mở được thiết kế để bảo vệ các giao dịch dùng thẻ tín dụng trên Internet.