AN TOÀN & BẢO MẬT THÔNG TIN

Giảng viên: Ths Phạm Thanh Bình

Bộ môn Kỹ thuật máy tính & mạng

http://dhthuyloi.blogspot.com

Chương 4:

CÁC ỨNG DỤNG TRONG AN NINH MẠNG

- Các ứng dụng chứng thực
- An ninh Web
- An ninh giao dịch điện tử

Bài 4.3 An ninh giao dịch điện tử

- Giao dịch điện tử là một trong những mục tiêu chủ yếu của hacker, do đó nó đòi hỏi độ an toàn bảo mật rất cao.
- SET (Secure Electronic Transaction – Giao dịch điện tử an toàn) được thiết kế để bảo vệ các giao dịch bằng thẻ tín dụng qua Internet.
- SET ra đời vào tháng 2/1996 do sự đòi hỏi của các chuẩn an ninh cho MasterCard và Visa.

- SET là một tập các giao thức an ninh và các dạng thức cho phép người dùng thanh toán bằng thẻ tín dụng trong một mạng mở (như Internet) một cách an toàn.
- Nhiều công ty lớn đã sớm bắt tay vào phát triển các chỉ định kỹ thuật ban đầu cho SET, gồm IBM, Microsoft, Netscape, RSA, Terisa, và Verisign.
- Năm 1998, SET được công bố rông rãi.

SET cung cấp ba dịch vụ:

- Cung cấp kênh liên lạc an toàn giữa các thực thể góp mặt trong một giao dịch.
- Cung cấp tính tin cậy bằng cách dùng các chứng chỉ số X.509v3.
- Bảo đảm tính riêng tư, do các thông tin chỉ được cung cấp cho các thực thể khi tham gia giao dịch và vào lúc cần thiết.

Các đặc điểm chính của SET

- Tính tin cậy của thông tin
- Tính toàn vẹn dữ liệu
- Chứng thực tài khoản của người dùng thẻ
- Chứng thực nhà bán hàng

Tính tin cậy của thông tin

- Các thông tin về người dùng thẻ và tài khoản tương ứng được bảo vệ an toàn khi lưu thông trên mạng
- Ngay cả người bán cũng không thể nắm giữ được số thẻ tín dụng của người sở hữu, số hiệu này chỉ được cung cấp cho ngân hàng phát hành thẻ
- Mã hóa DES được sử dụng để cung cấp tính tin cậy

Tính toàn vẹn dữ liệu

- Thông tin thanh toán được gửi từ một người dùng thẻ tới nhà bán hàng bao gồm các thông tin đặt hàng, dữ liệu cá nhân, và các lệnh chi trả.
- SET đảm bảo rằng nội dung các thông điệp này không bị biến đổi trên đường đi.
- Chữ ký số RSA dùng mã hash SHA-1 được sử dụng để đảm bảo tính toàn vẹn của thông điệp. Ngoài ra có thể bảo vệ các thông điệp khác bằng HMAC dùng SHA-1

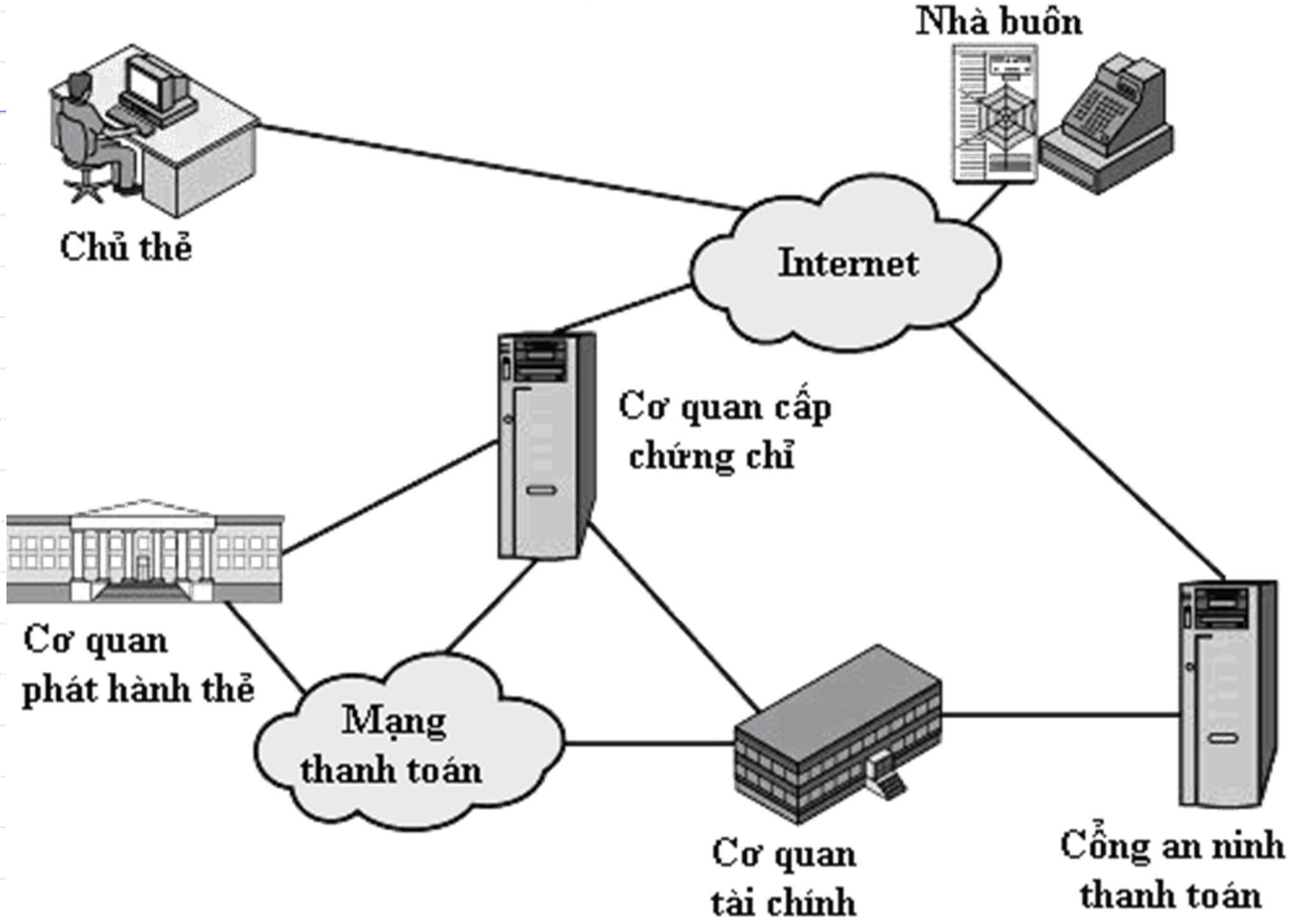
Chứng thực tài khoản của người dùng thẻ

- SET cho phép các nhà bán hàng xác minh một người dùng thẻ là hợp pháp đối với một thẻ tín dụng hợp lệ và tài khoản ứng với thẻ đó.
- Chứng chỉ số X.509v3 chứa các chữ ký RSA được sử dụng cho chức năng này.

Chứng thực nhà bán hàng

- SET cho phép người sở hữu thẻ xác minh được rằng nhà bán hàng đã sẵn có mối quan hệ với cơ quan tài chính hỗ trợ thanh toán bằng thẻ.
- SET dùng các chứng chỉ số X.509v3 với các chữ ký RSA cho chức năng này

Các thành phần tham gia giao dịch điện tử



Người sở hữu thẻ (Cardholder)

- Người mua sắm giao tiếp với nhà bán hàng từ một máy tính cá nhân qua Internet
- Người dùng thẻ là một cá nhân hợp pháp sở hữu thẻ thanh toán (ví dụ: MasterCard, Visa…), thẻ này được cung cấp bởi một nhà phát hành thẻ.

Bên phát hành thẻ (Issuer)

- Đây là một cơ quan tài chính (chẳng hạn một ngân hàng), nó cung cấp thẻ thanh toán cho người sở hữu thẻ
- Một cách tổng quát, bên phát hành thẻ là bên có trách nhiệm trong việc thanh toán nợ của người sở hữu thẻ

Người bán hàng (Merchant)

- Người bán là một cá thể hay tổ chức có hàng hóa hay dịch vụ bán cho người sở hữu thẻ
- Thông thường, các hàng hóa dịch vụ này được mời chào qua trang Web hoặc bằng thư điện tử
- Một nhà bán hàng chấp nhận thanh toán thẻ phải có sẵn một quan hệ hợp pháp với cơ quan tài chính.

Cơ quan tài chính (Acquirer)

- Là cơ quan thiết lập một tài khoản với người bán và xử lý các công việc liên quan tới thanh toán qua thẻ
- Các nhà bán hàng muốn chấp nhận thanh toán nhiều loại thẻ nhưng thường không muốn giao tiếp với nhiều nhà phát hành thẻ
- Cơ quan tài chính sẽ hỗ trợ người bán hàng xử lý mối quan hệ giữa các bên, tiến hành chuyển khoản cho các giao dịch

Cổng thanh toán (Payment gateway)

- Đây là chức năng được điều hành bởi cơ quan tài chính hoặc một bên thứ ba tin cậy nào đó để xử lý các thông điệp thanh toán của nhà bán hàng.
- Nhà bán hàng trao đổi các thông điệp SET với cổng thanh toán qua Internet, trong khi cổng thanh toán có các kết nối trực tiếp tới hệ thống xử lý tài chính của các cơ quan tài chính

Bên cấp chứng chỉ (CA)

- Đây là thực thể tin cậy để phát hành các chứng chỉ khoá công khai X.509v3 cho các chủ thẻ, nhà bán hàng và các cổng thanh toán
- Người ta thường sử dụng một hệ thống CA đa cấp, sao cho tất cả các bên tham gia không cần phải được xác thực trực tiếp bởi bên gốc thẩm quyền.

Các bước thực hiện giao dịch

1. **Khách hàng mở tài khoản**. Khách hàng mở một tài khoản thẻ tín dụng, tại một ngân hàng có hỗ trợ thanh toán điện tử và SET.
2. **Khách hàng nhận được một chứng chỉ**. Sau khi xác minh nhận dạng thích hợp, khách hàng nhận được một chứng chỉ số X.509v3, được ngân hàng ký. Chứng chỉ này thiết lập một mối quan hệ giữa cặp khóa của khách hàng với thẻ tín dụng được cấp phát.

3. **Nhà bán hàng có các chứng chỉ của mình**. Một người bán hàng phải sở hữu hai chứng chỉ cho hai cặp khoá-công-khai của mình: một để ký các thông điệp và một để trao đổi khóa.

4. **Khách hàng đặt đơn hàng**. Khách hàng chọn các món hàng cần mua rồi gửi danh sách hàng hoá cho người bán. Người bán gửi lại khách một đơn hàng có chứa danh mục hàng hoá đã chọn, số lượng, đơn giá và tổng số tiền.

5. **Người bán được xác minh**. Cùng với đơn hàng, người bán hàng gửi một bản sao chứng chỉ, nhờ vậy khách hàng có thể xác minh được rằng mình đang giao dịch với một cửa hàng có thực và hợp lệ.
6. **Gửi đơn hàng và thông tin thanh toán**. Khách hàng gửi cả đơn hàng và các thông tin thanh toán cho người bán, cùng với chứng chỉ khách hàng của mình. Thông tin thanh toán (bao gồm chi tiết về thẻ tín dụng) được mã hóa sao cho người bán hàng không thể đọc được. Chứng chỉ khách hàng cho phép người bán xác minh khách hàng.

7. **Người bán yêu cầu cấp phép thanh toán**. Người bán gửi thông tin thanh toán cho cổng an ninh thanh toán, yêu cầu xác nhận chủ thẻ có khả năng thanh toán đơn hàng.

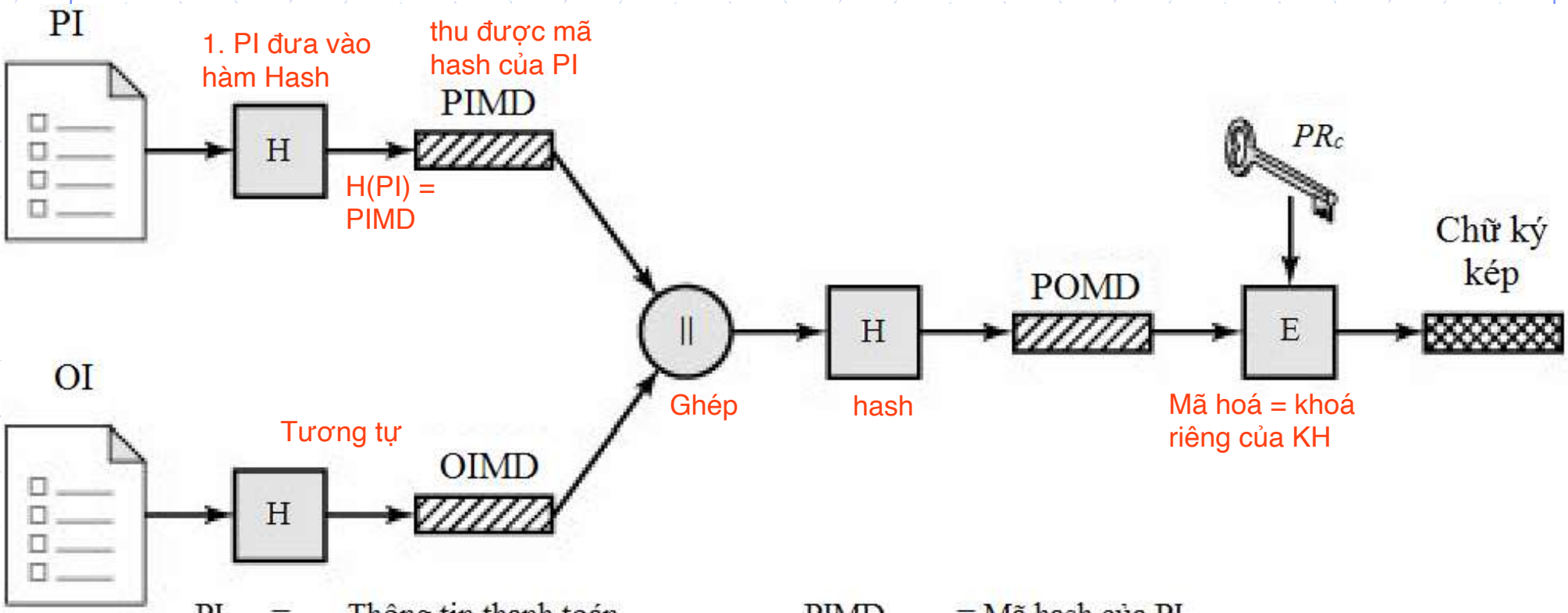
8. **Người bán xác nhận đơn hàng**. Người bán gửi xác nhận đơn hàng cho khách hàng.

9. **Người bán cung cấp hàng hóa hoặc dịch vụ**. Người bán chuyên chở hàng hóa hoặc áp dụng dịch vụ cho khách hàng.
10. **Người bán yêu cầu thanh toán**. Yêu cầu này được gửi tới cổng an ninh thanh toán là nơi giải quyết tất cả các thủ tục thanh toán

Chữ ký kép

- Khách hàng muốn gửi thông tin đơn hàng (Order Information - OI) cho người bán và thông tin thanh toán (Payment Information - PI) cho ngân hàng.
- Người bán không cần phải biết mã thẻ thanh toán của khách hàng, và ngân hàng không cần phải biết chi tiết đơn hàng của khách hàng.
- Chữ ký kép nhằm liên kết OI và PI của một giao dịch, tránh ghép nhầm OI của giao dịch này với PI của giao dịch khác, làm cơ sở để giải quyết tranh chấp sau này.

Xây dựng chữ ký kép



PI	=	Thông tin thanh toán
OI	=	Thông tin đơn hàng
H	=	Hàm hash (SHA-1)
‖	=	Phép nối

PIMD	= Mã hash của PI
OIMD	= Mã hash của OI
POMD	= Mã hash của đề nghị thanh toán
E	= Hàm mã hóa (RSA)
PR_c	= Khóa riêng cho chữ ký của khách hàng

- Như vậy chữ ký kép sẽ có dạng:

$$\mathbf{DS = E(}\boldsymbol{PR}_{\mathbf{c}}\mathbf{, [H(H(PI)||H(OI)])}$$

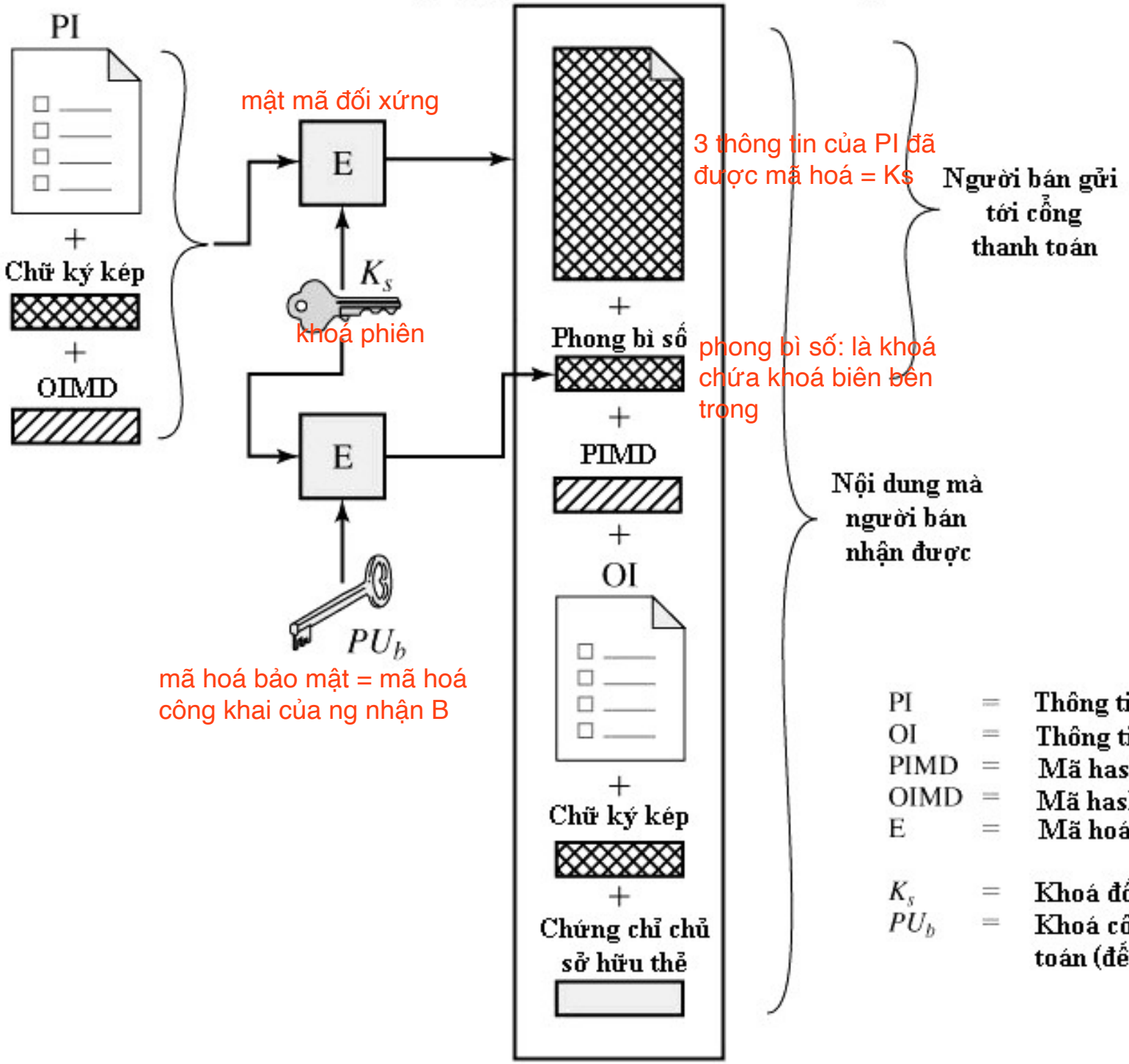
với: + H(PI) = PIMD

+ H(OI) = OIMD

+ PR_c = khoá riêng của khách hàng

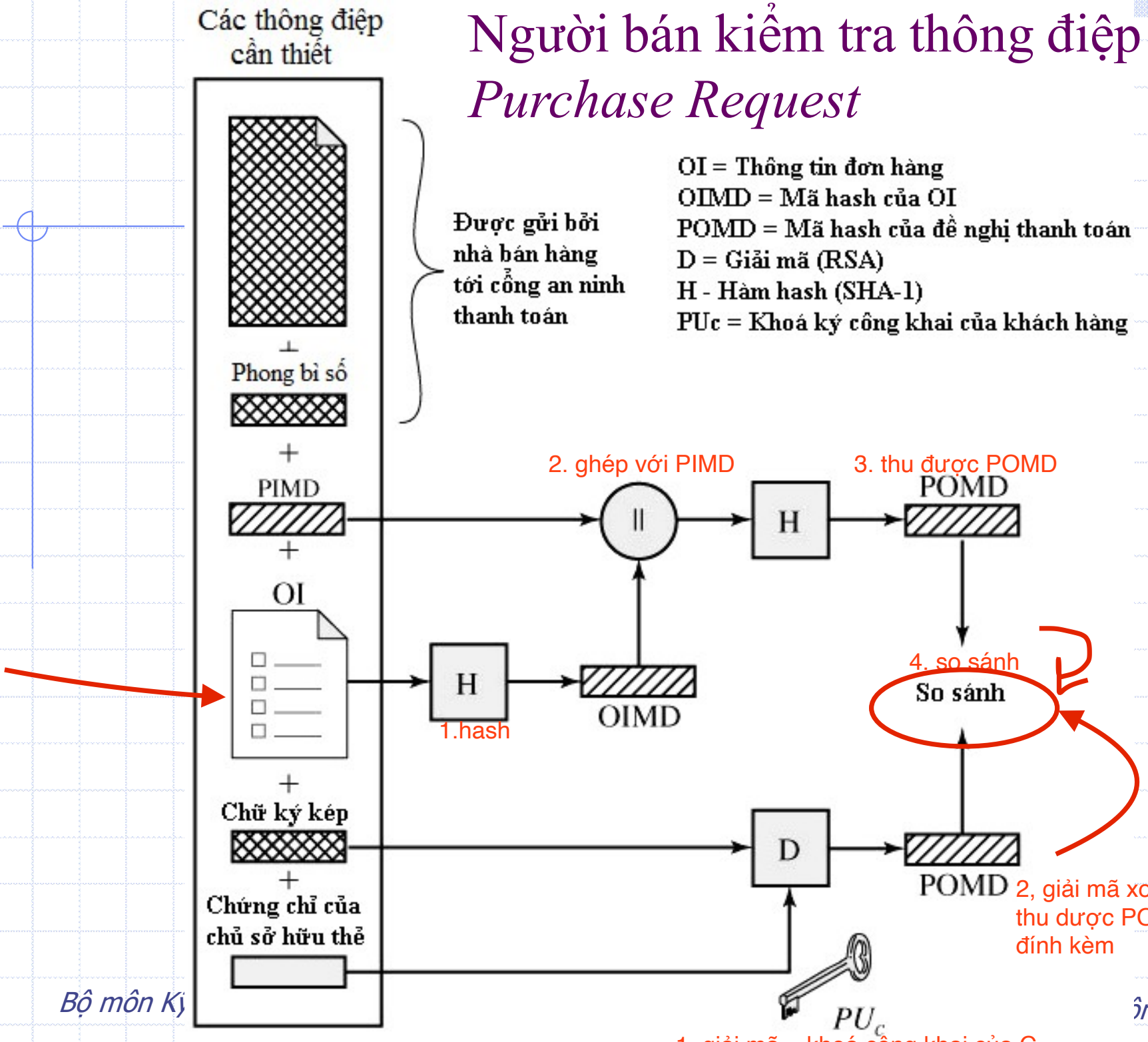
- Chữ kí kép được gắn với OI để gửi cho người bán, và gắn với PI để gửi cho cổng thanh toán.
- Cả hai thông tin nói trên được đặt trong một thông điệp *Purchase Request* – *"Yêu cầu mua sắm"* do khách hàng tạo ra và gửi cho người bán. (xem hình trang sau)
- Người bán tách các thông tin liên quan tới PI từ thông điệp *Purchase Request* rồi gửi cho cổng thanh toán

Thông điệp yêu cầu mua sắm *Purchase Request*



PI	=	Thông tin thanh toán
OI	=	Thông tin đặt hàng
PIMD	=	Mã hash của PI
OIMD	=	Mã hash của OI
E	=	Mã hoá (RSA cho bất đối xứng DES cho đối xứng)
K_s	=	Khoá đối xứng tạm thời
PU_b	=	Khoá công khai của cổng thanh toán (để trao đổi khoá K_s)

Người bán kiểm tra thông điệp *Purchase Request*



- Để kiểm tra chữ kí kép
  DS= E(PR_c, [H(H(PI)||H(OI)]) của khách hàng, người bán cần nhận được OI và mã hash của PI (PIMD).
- Người bán sẽ tính toán 2 giá trị sau:
  + H(PIMD||H(OI))
  + D(PU_c, DS)
- Nếu hai giá trị bằng nhau thì chữ ký của khách hàng là hợp lệ

- Tương tự, để kiểm tra chữ kí kép DS= E(PR_c, [H(H(PI)||H(OI)]) của khách hàng, cổng thanh toán cần nhận được PI và mã hash của OI (OIMD).
- Cổng thanh toán sẽ tính 2 giá trị sau:
  + H(H(PI)||OIMD)
  + D(PU_c, DS)
- Nếu hai giá trị bằng nhau thì chữ ký của khách hàng là hợp lệ

BTVN: vẽ sơ đồ kiểm tra chữ ký kép tại cổng thanh toán

Hết Phần 4_3