Bài 5. An toàn thanh toán điện tử

Nội dung

- 5.1. Đặc trưng của thanh toán điện tử
- 5.2. Giao thức SET

5.1. Đặc trưng của thanh toán điện tử

- Thương mại truyền thống: Tham gia bởi hai bên mua và bán
- Thương mại điện tử: Có sự tham gia của bên thứ 3 (Ngân hàng)

5.1. Đặc trưng của thanh toán điện tử

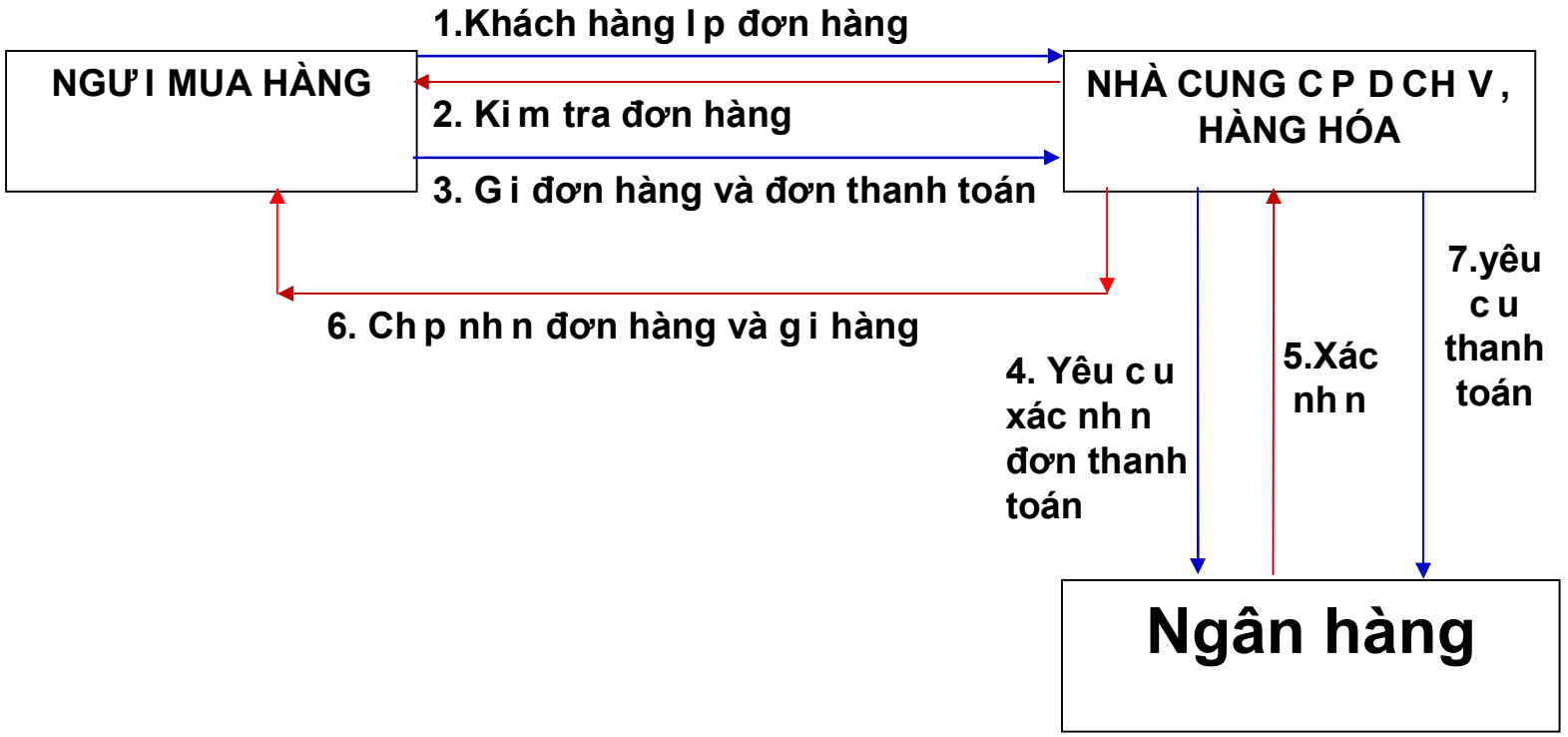
- Các giao dịch sử dụng tiền ảo, thông qua hệ thống ngân hàng
- Cần đảm bảo sự bảo mật và xác thực của các bên tham gia

5.1. Đặc trưng của thanh toán điện tử

- Các thông tin trao đổi trong quá trình giao dịch điện tử
  - Đơn hàng (Order Information)
  - Đơn thanh toán (Payment Information)

5.1. Đặc trưng của thanh toán điện tử

Mô hình giao dịch điện tử đơn giản



5.1. Đặc trưng của thanh toán điện tử

- Các thông tin cần xác thực:
  - Đơn hàng
  - Đơn thanh toán
  - Sự liên quan giữa hai thông tin trên

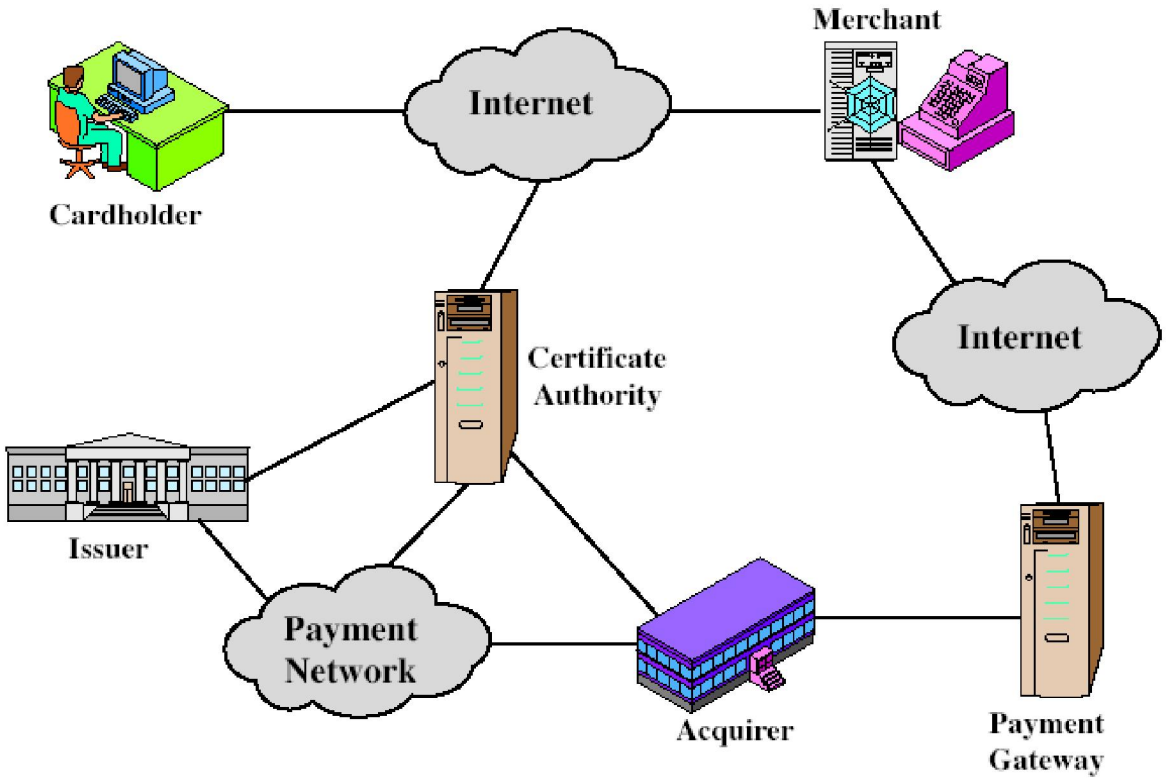
5.1. Đặc trưng của thanh toán điện tử

- Có những thông tin bí mật đối với các bên tham gia:
  - Thông tin cá nhân của người mua cần được giữ bí mật đối với người bán
  - Thông tin mua bán cần được giữ bí mật đối với ngân hàng

5.2. Giao thức SET

- Phát triển năm 1996 bởi MasterCard, Visa, …
- Đặc tả mở về mã hóa và bảo mật nhằm bảo vệ các giao dịch thẻ tín dụng trên Internet
  - Không phải hệ thống trả tiền điện tử
- Là một tập hợp các định dạng và giao thức
  - Đảm bảo truyền tin an toàn giữa các bên tham gia
  - Đảm bảo tính tin cậy (Sử dụng chứng thực X.509v3)
  - Đảm bảo tính riêng tư (Bí mật giữa các bên tham gia)

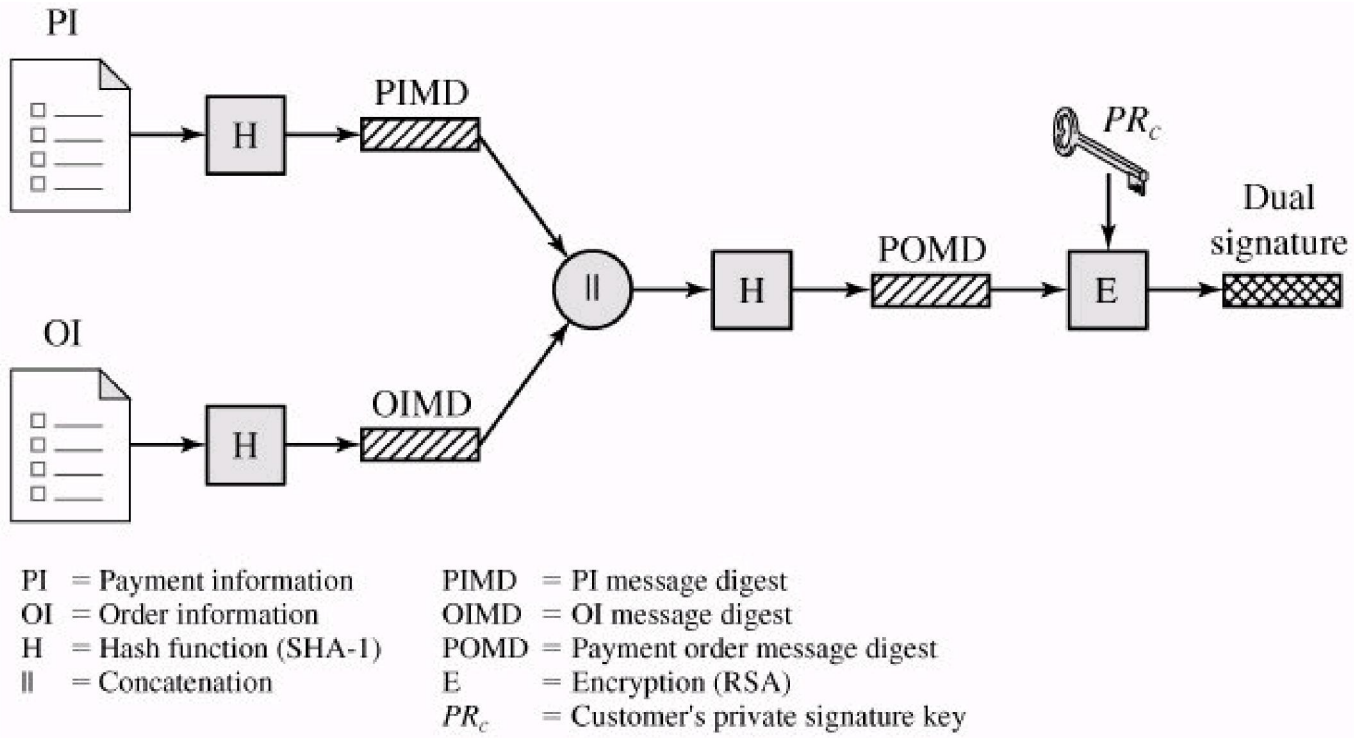
5.2. Giao thức SET



5.2.1. Chữ ký kép

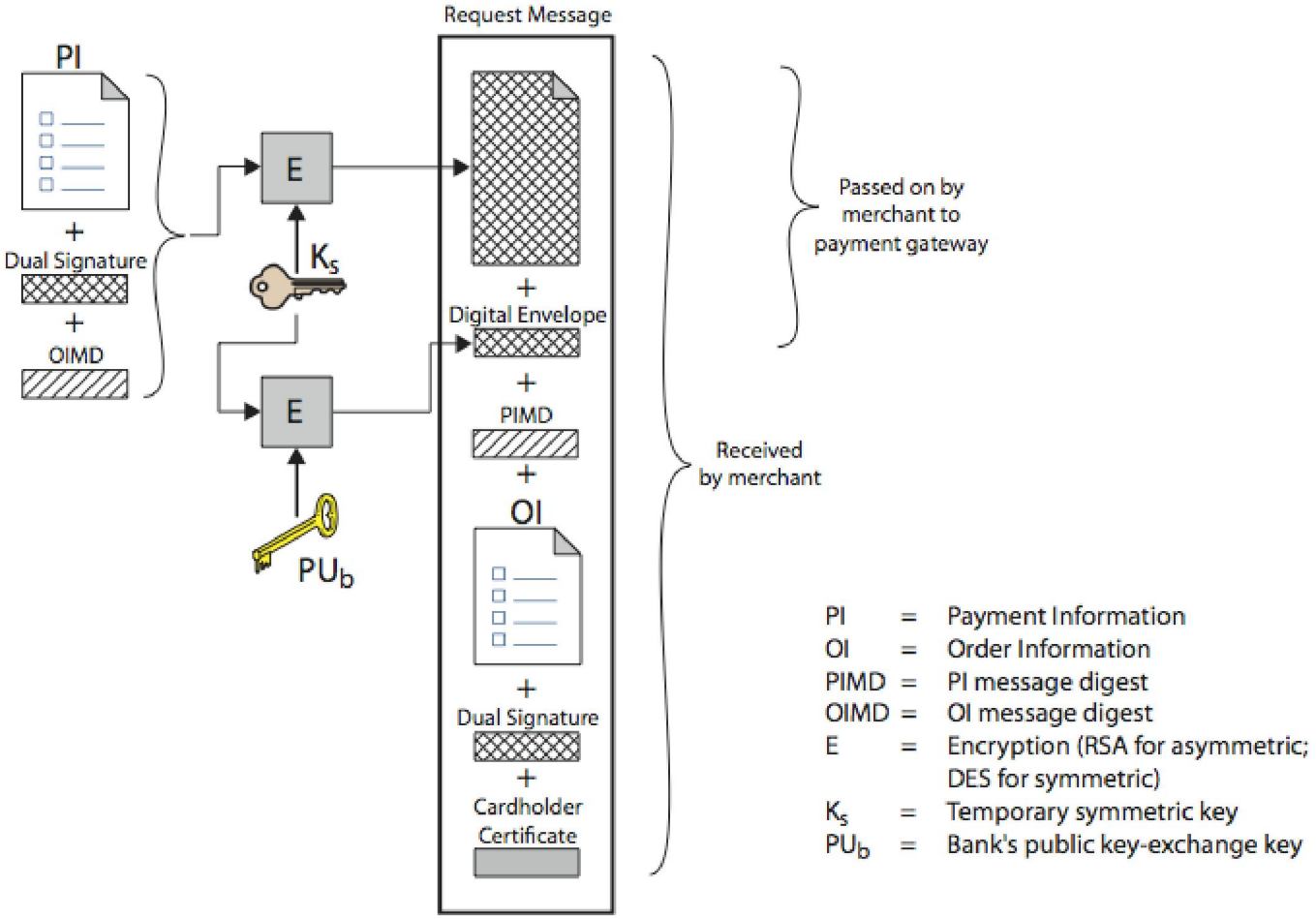
- Người mua tạo ra hai thông báo
  - Đơn hàng (OI) cho người bán
  - Đơn thanh toán (PI) cho ngân hàng
- Người bán không được biết thông tin về PI
- Ngân hàng không được biết thông tin về OI
- Nhưng phải xác định được OI và PI có liên hệ với nhau

5.2.1. Chữ ký kép



- Tạo ra chữ ký kép bằng cách mã hóa kết hợp cả đơn hàng và đơn thanh toán

5.2.2. Mô hình giao dịch an toàn

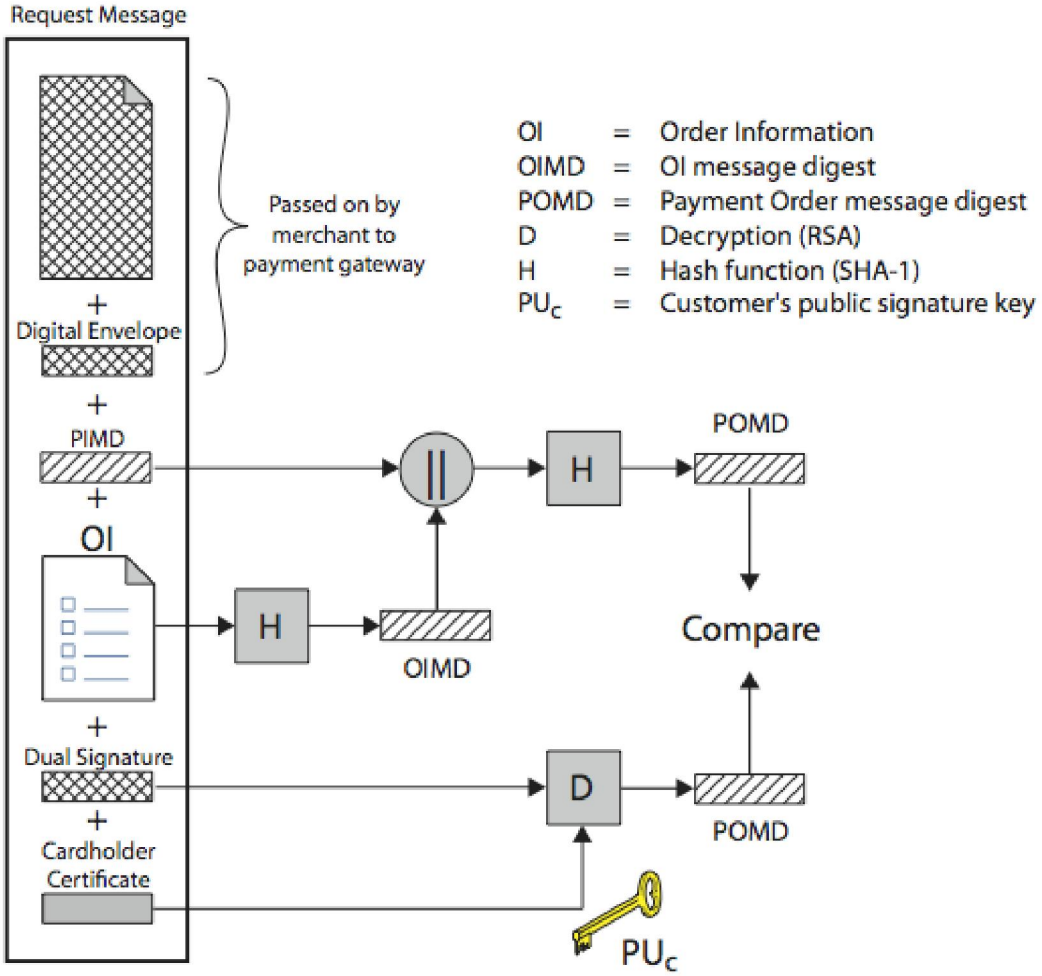


Yêu cầu mua

5.2.2. Mô hình giao dịch an toàn

- Yêu cầu mua (Purchase Request)
  - Đơn thanh toán, mã băm của đơn hàng, chữ ký kép được mã hóa bởi khóa công khai của ngân hàng (giữ bí mật với người bán)
  - Đơn hàng, mã băm của đơn thanh toán, chữ ký kép được gửi trực tiếp cho người bán

5.2.2. Mô hình giao dịch an toàn



Kiểm tra yêu cầu

5.2.2. Mô hình giao dịch an toàn

- Kiểm tra yêu cầu
  - Lấy khoa công khai của người mua qua Certificate
  - Giải mã chữ ký kép bằng khóa công khai (1)
  - Băm đơn hàng và kết hợp với mã băm của đơn thanh toán (2)
  - So sánh (1) và (2) để kiểm tra

5.2.2. Mô hình giao dịch an toàn

- Kiểm tra tại ngân hàng
  - Giải mã thông tin nhận được để lấy đơn thanh toán, mã băm của đơn hàng và chữ ký kép
  - Xác thực chữ ký kép qua các thông tin nhận được