Bài 2. Xác thực và chữ ký điện tử

Nội dung

- 2.1. Vấn đề xác thực
- 2.2. Các phương pháp xác thực
- 2.3. Chữ ký điện tử
- 2.4. Chứng thực điện tử

2.1. Vấn đề xác thực

- Tại sao phải xác thực thông báo
  - Xác minh được nguồn gốc thông báo
  - Nội dung thông báo toàn vẹn không bị thay đổi
  - Thông báo được gửi đúng trình tự và thời điểm
- Mục đích để chống lại hình thức tấn công chủ động (xuyên tạc dữ liệu và giả mạo)
- Các phương pháp xác thực thông báo
  - Mã hóa thông báo
  - Sử dụng mã xác thực thông báo (MAC)
  - Sử dụng hàm băm

2.1. Vấn đề xác thực

- Trong thương mại điện tử, xác thực là một yêu cầu đặc biệt quan trọng:
  - Tránh việc giả mạo các bên giao dịch
  - Tránh bị thay đổi các thông tin giao dịch trong quá trình truyền dữ liệu

2.2. Các phương pháp xác thực

- Xác thực bằng mã hóa
  - Sử dụng mã hóa đối xứng
    - Đảm bảo thông báo được gửi đúng nguồn do chỉ bên gửi biết khóa bí mật
    - Không thể bị thay đổi bởi bên thứ ba do không biết khóa bí mật
  - Sử dụng mã hóa khóa công khai
    - Không những xác thực mà còn tạo ra được chữ ký số
    - Tuy nhiên, phức tạp và tốn thời gian hơn mã đối xứng

2.2. Các phương pháp xác thực

- Xác thực bằng mã hóa có nhược điểm:
  - Tốn thời gian để mã hóa cũng như giải mã toàn bộ thông báo
  - Nhiều khi chỉ cần xác thực mà không cần bảo mật thông báo (cho phép ai cũng có thể biết nội dung, chỉ cần không được sửa đổi)

2.2. Các phương pháp xác thực

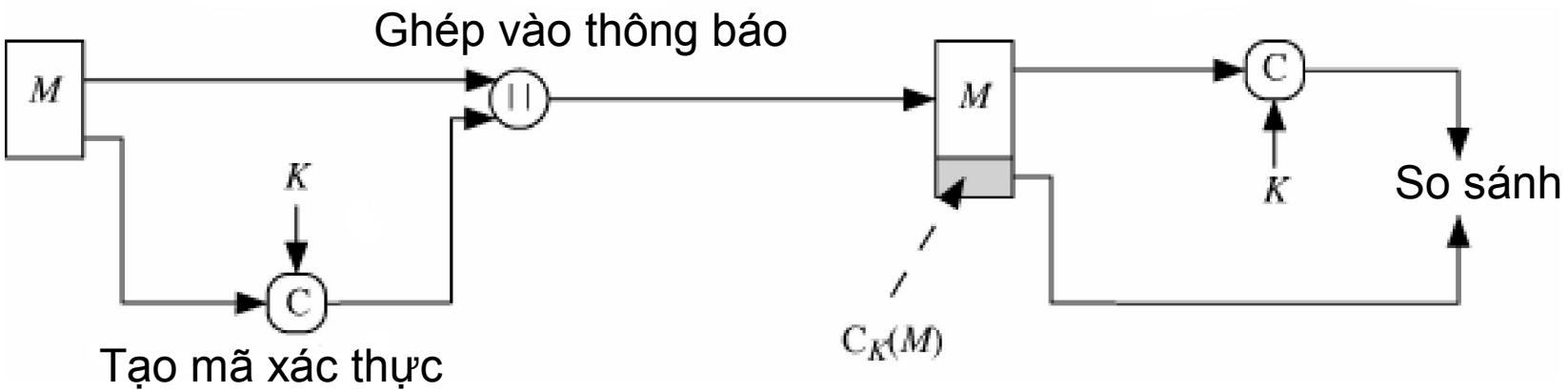
- Mã xác thực thông báo (MAC - Message Authentication Code)
  - Là một khối dữ liệu có kích thước nhỏ, cố định
    - Được tạo ra từ thông báo và khóa bí mật với một giải thuật cho trước: MAC = $C_K(M)$
    - Đính kèm vào thông báo
  - Lưu ý: Từ mã xác thực, không xác định ngược lại được thông báo (Tính một chiều)

2.2. Các phương pháp xác thực

- Mã xác thực thông báo thực chất là kết hợp giữa các tính chất của mã hóa và hàm băm
  - Có kích thước nhỏ, đặc trưng cho thông báo (Tính chất của hàm băm)
  - Tạo ra bằng khóa bí mật (Tính chất của mã hóa)

2.2. Các phương pháp xác thực

- Phương pháp xác thực bằng MAC
  - Bên nhận thực hiện cùng giải thuật của bên gửi trên thông báo và khóa bí mật và so sánh giá trị thu được với MAC trong thông báo



2.2. Các phương pháp xác thực

- Ưu điểm của MAC
  - MAC chỉ hỗ trợ xác thực, không hỗ trợ bảo mật -> có lợi trong nhiều trường hợp (các thông báo công cộng, ...)
  - Có kích thước nhỏ, thời gian tạo ra nhanh hơn so với mã hóa toàn bộ thông báo
  - **Chú ý: MAC không phải là chữ ký điện tử**

2.3. Chữ ký điện tử

- Xác thực thông báo không có tác dụng khi bên gửi và bên nhận muốn gây hại cho nhau
  - Bên nhận giả mạo thông báo của bên gửi
  - Bên gửi từ chối thông báo đã gửi cho bên nhận
- -> cần chữ ký điện tử

2.3. Chữ ký điện tử

- Chữ ký điện tử không những giúp xác thực thông báo mà còn bảo vệ mỗi bên khỏi bên kia
- Chức năng chữ ký số
  - Xác minh tác giả và thời điểm ký thông báo
  - Xác thực nội dung thông báo
  - Là căn cứ để giải quyết tranh chấp

2.3. Chữ ký điện tử

- Yêu cầu của chữ ký điện tử:
  - Phụ thuộc vào thông báo được ký (đảm bảo kiểm tra tính xác thực của thông báo)
  - Sử dụng thông tin riêng của người gửi (tránh giả mạo và chối bỏ)
  - Tương đối dễ tạo và kiểm chứng
  - Rất khó giả mạo
  - Thuận tiện trong việc lưu trữ

2.3. Chữ ký điện tử

- Chữ ký điện tử có thể được phân làm 2 loại:
  - Chữ ký điện tử gián tiếp
  - Chữ ký điện tử trực tiếp

2.3. Chữ ký điện tử

- Chữ ký điện tử gián tiếp
  - Cần tham gia của bên trọng tài
    - Kiểm tra tính hợp lệ của chữ ký số
    - Giải quyết trong trường hợp có tranh chấp
  - An toàn phụ thuộc chủ yếu vào trọng tài
    - Cần được cả bên nhận và bên gửi tin tưởng
  - Có thể cài đặt với cả mã hóa đối xứng và mã hóa công khai

2.3. Chữ ký điện tử

- Kỹ thuật tạo chữ ký điện tử gián tiếp

(a) Mã hóa đối xứng, trọng tài thấy thông báo

(1) $X \rightarrow A : \; M \,\|\, E_{K_{XA}}[ID_X \,\|\, H(M)]$

(2) $A \rightarrow Y : \; E_{K_{AY}}[ID_X \,\|\, M \,\|\, E_{K_{XA}}[ID_X \,\|\, H(M)] \,\|\, T]$

(b) Mã hóa đối xứng, trọng tài không thấy thông báo

(1) $X \rightarrow A : \; ID_X \,\|\, E_{K_{XY}}[M] \,\|\, E_{K_{XA}}[ID_X \,\|\, H(E_{K_{XY}}[M])]$

(2) $A \rightarrow Y : E_{K_{AY}}[ID_X \,\|\, E_{K_{XY}}[M] \,\|\, E_{K_{XA}}[ID_X \,\|\, H(E_{K_{XY}}[M])] \,\|\, T]$

Ký hiệu :

X = Bên gửi

Y = Bên nhận

A = Trọng tài

M = Thông báo

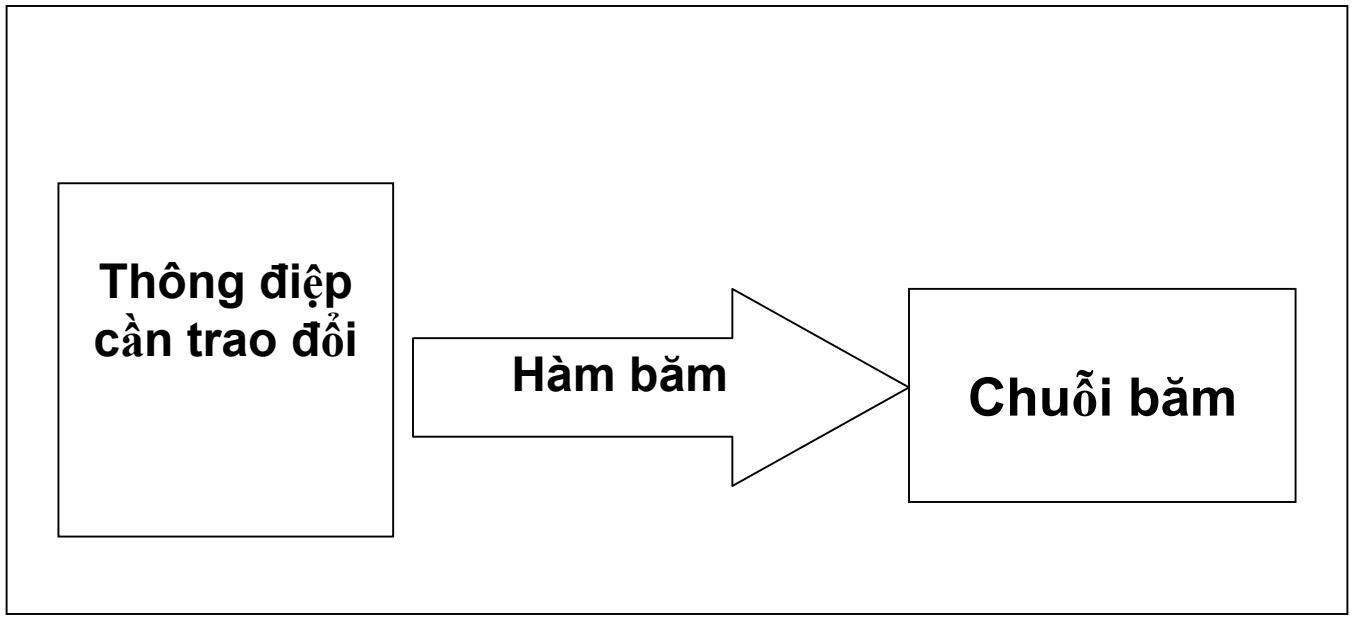
T = Nhãn thời gian

2.3. Chữ ký điện tử

- Chữ ký điện tử trực tiếp
  - Chỉ liên quan đến bên gửi và bên nhận (không cần sự tham gia của trọng tài)
  - Sử dụng mật mã khóa công khai để tạo chữ ký
  - Phải đảm bảo an toàn cho khóa bí mật của bên gửi

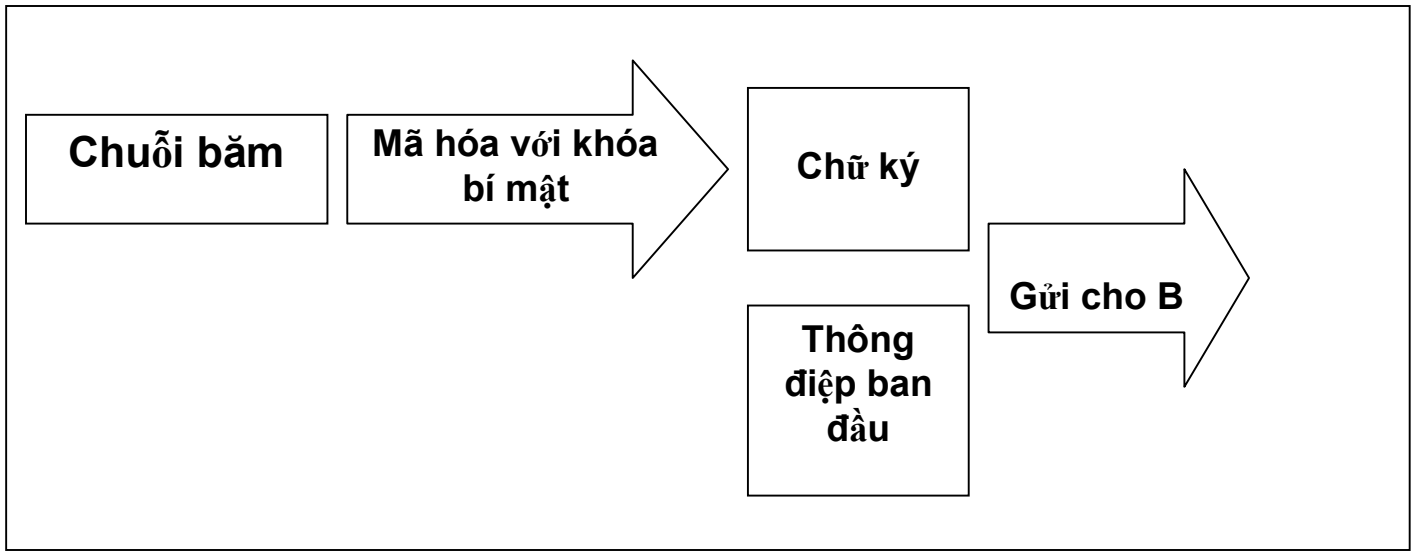
2.3. Chữ ký điện tử

- Tạo chữ ký điện tử trực tiếp:
  - Sử dụng hàm băm để tạo ra một chuỗi băm từ thông điệp ban đầu



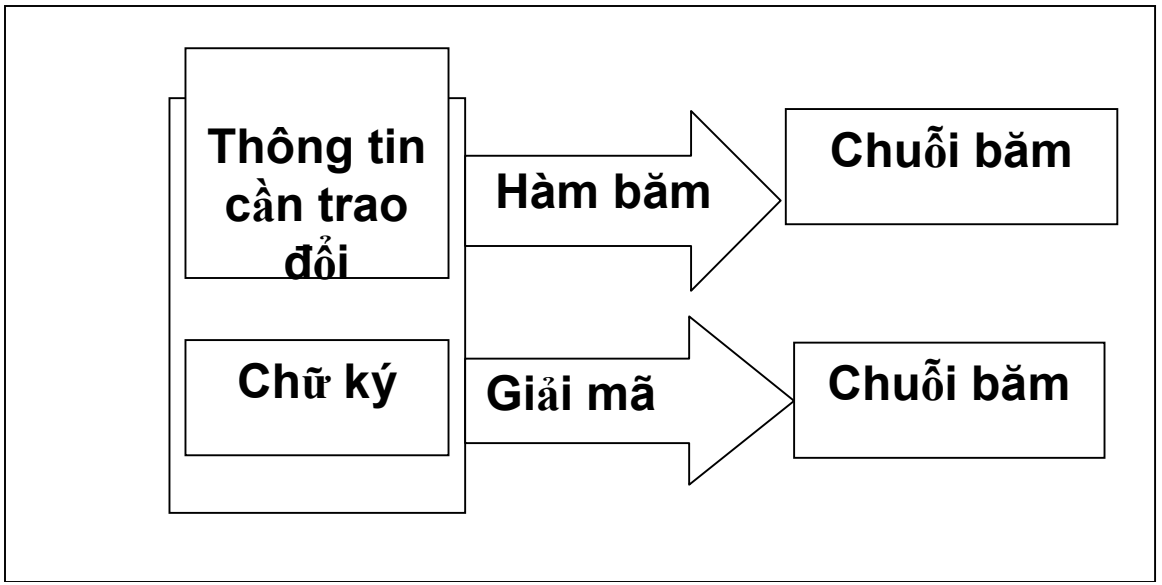
2.3. Chữ ký điện tử

- Dùng khóa bí mật của mình để mã hóa chuỗi băm này, kết quả đạt được chính là chữ ký điện tử của đoạn thông báo



2.3. Chữ ký điện tử

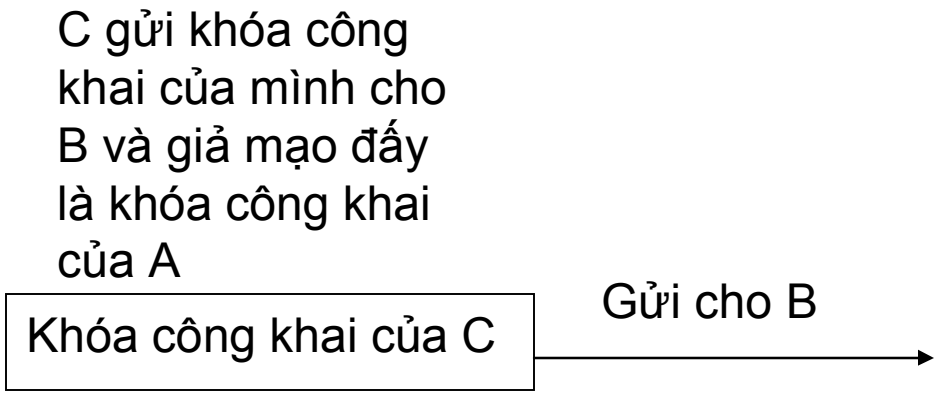
- Xác thực thông báo:
  - Giải mã chữ ký bằng khóa công khai
  - Tạo ra chuỗi băm từ thông tin nhận được
  - So sánh hai kết quả



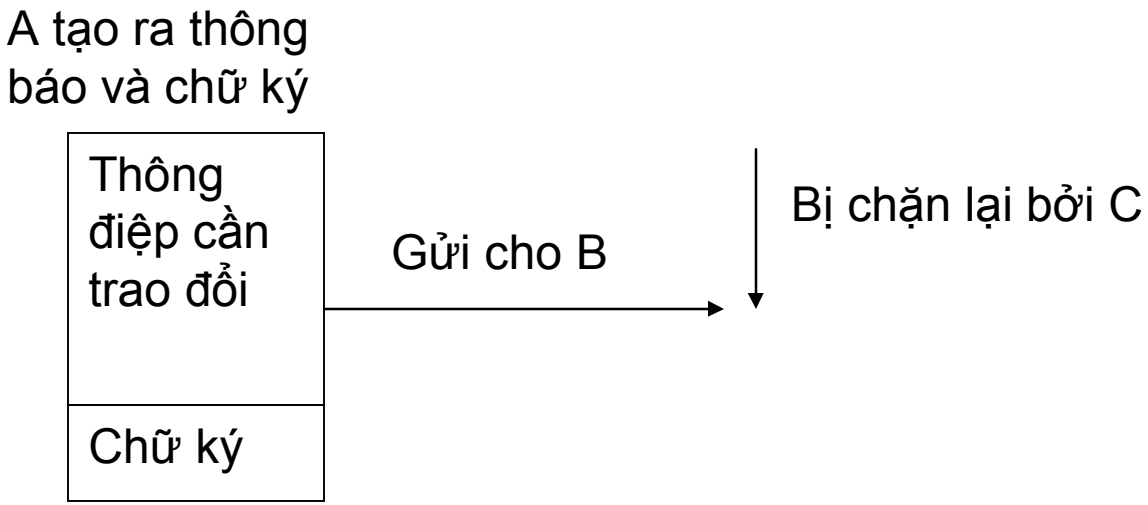
2.3. Chữ ký điện tử

- Giả mạo chữ ký điện tử
  - Trong nhiều trường hợp, người nhận không biết khóa công khai của người gửi
  - Kẻ tấn công có thể lợi dụng để giả mạo khóa công khai của người gửi, từ đó tạo ra chữ ký giả mạo

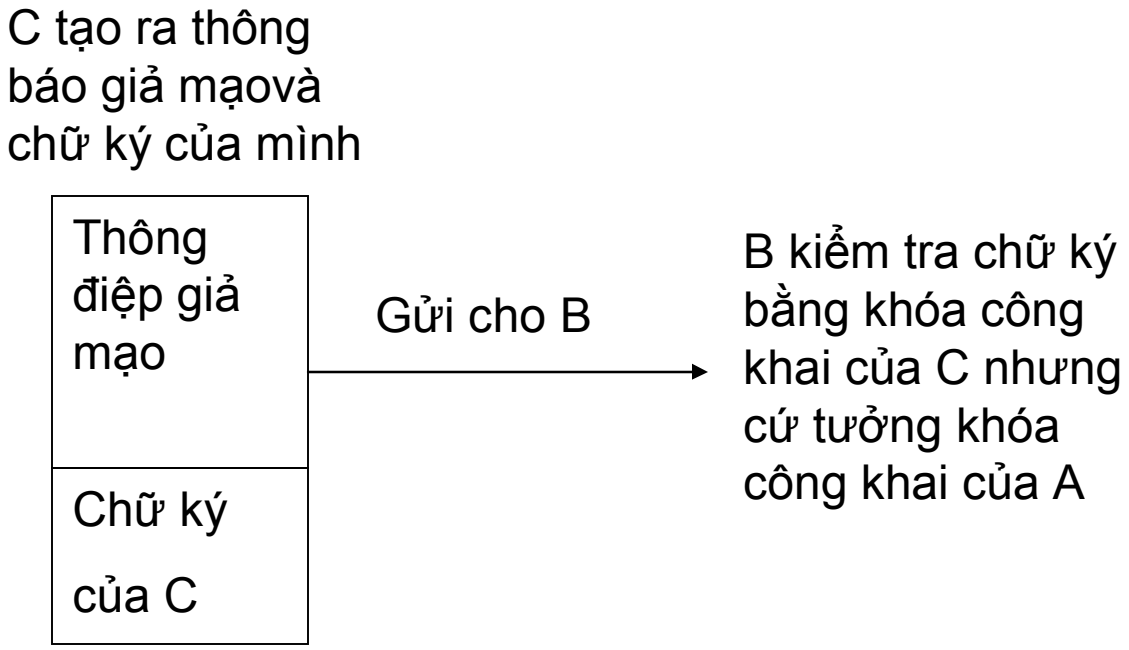
2.3. Chữ ký điện tử



2.3. Chữ ký điện tử



2.3. Chữ ký điện tử



2.3. Chữ ký điện tử

- Cần các phương pháp phân phối an toàn để chống giả mạo khóa công khai
- Phân phối khóa công khai bằng một trong các phương pháp sau
  - Thông báo công khai
  - Thư mục công khai
  - Cơ quan chứng thực khóa công khai
  - Giấy chứng nhận khóa công khai (Chứng thực điện tử)

2.3. Chữ ký điện tử

- Thông báo công khai
  - Thông báo rộng rãi cho mọi người thông qua email hoặc các news groups.
  - Dễ bị giả mạo

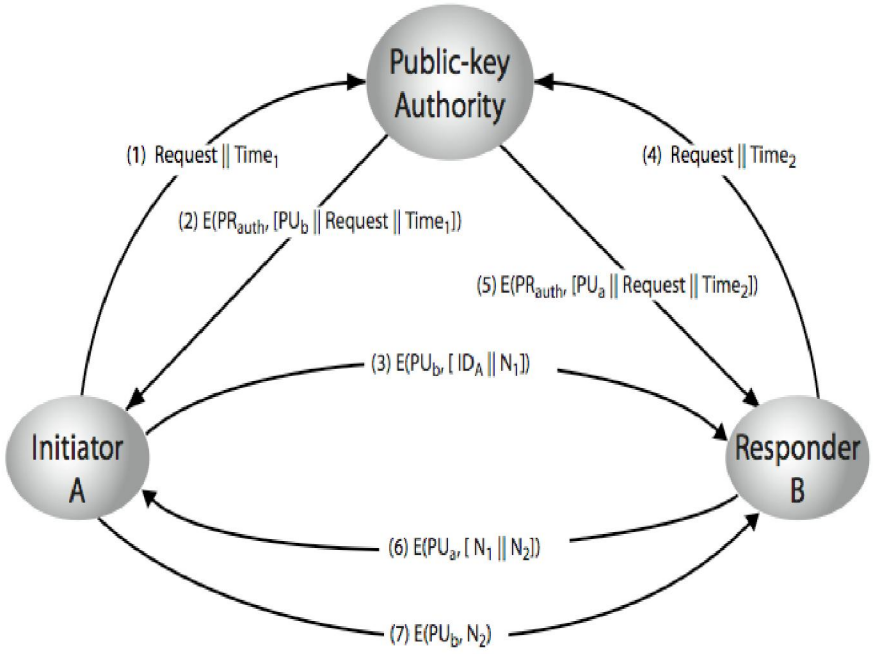
2.3. Chữ ký điện tử

- Thư mục khóa công khai
  - Người dùng đăng ký khóa trên một thư mục công khai
  - Thư mục phải được quản lý bởi một tổ chức đáng tin cậy
  - An toàn hơn nhưng vẫn có thể bị giả mạo

2.3. Chữ ký điện tử

- Cơ quan chứng thực khóa công khai
  - Sử dụng một cơ quan chứng thực để quản lý các khóa công khai
  - Người dùng phải lấy trực tiếp khóa công khai từ cơ quan chứng thực
  - Người dùng phải biết khóa công khai của cơ quan chứng thực

2.3. Chữ ký điện tử



Lấy khóa công khai từ cơ quan chứng thực

2.3. Chữ ký điện tử

- Không thể truy nhập vào cơ quan chứng thực -> không thể lấy được khóa công khai
- -> Cần sử dụng giấy chứng nhận khóa công khai (Chứng thực điện tử)

2.4. Chứng thực điện tử

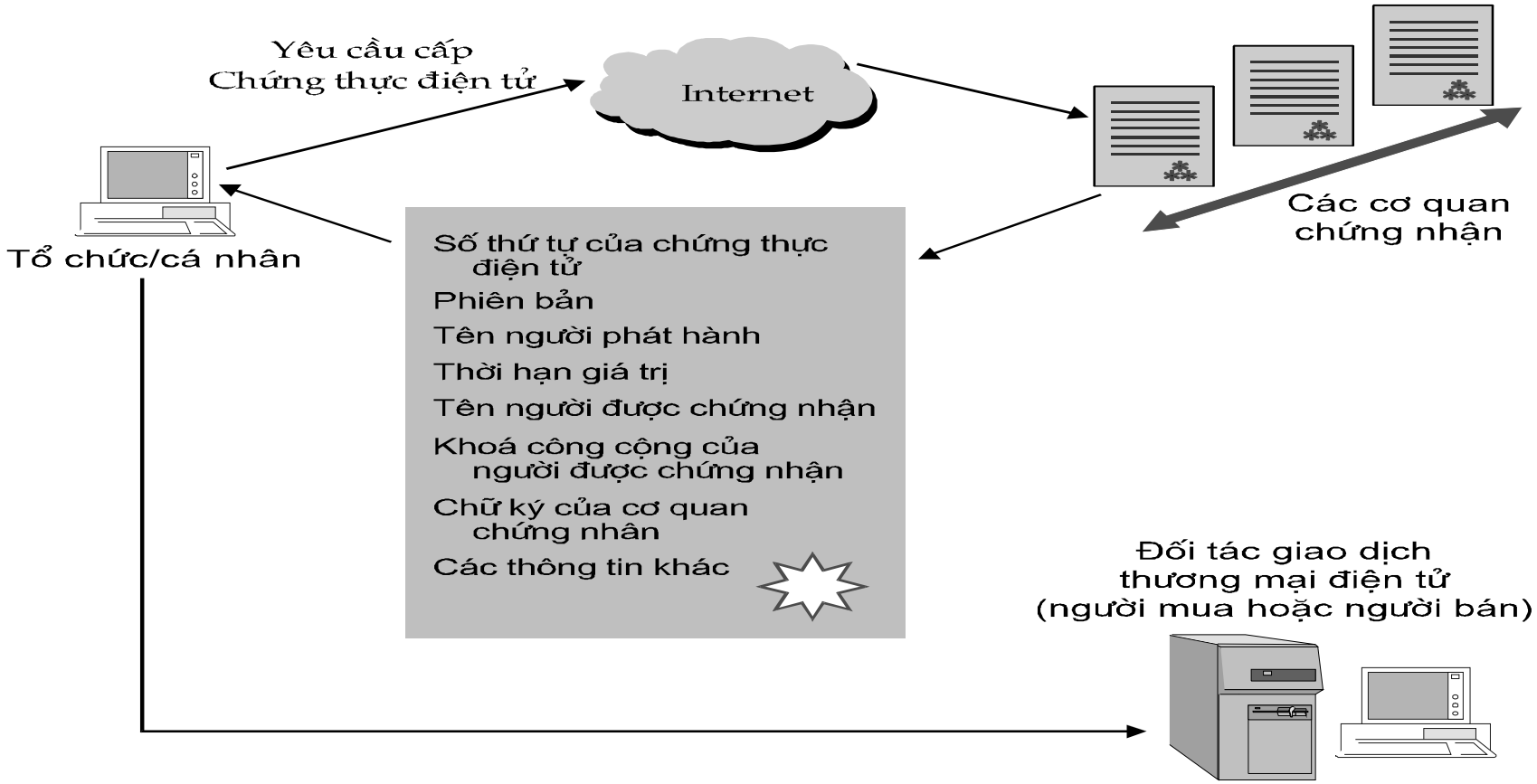
- Chứng thực điện tử giúp chứng thực danh tính và các thông tin của những người tham gia vào việc truyền tin
- Chứng thực điện tử được cấp bởi một cơ quan chứng thực có uy tín trên thế giới

2.4. Chứng thực điện tử

- Một chứng thực điện tử bao gồm:
  - Khóa công khai của người sở hữu chứng thực điện tử.
  - Các thông tin riêng của người sở hữu chứng thực.
  - Hạn sử dụng.
  - Tên cơ quan cấp chứng thực điện tử.
  - Số hiệu của chứng thực.
  - Chữ ký của nhà cung cấp.

2.4. Chứng thực điện tử

Sơ đồ cấp chứng thực điện tử:



2.4. Chứng thực điện tử

- Quy trình cấp chứng thực điện tử
  - (1) Tạo ra một cặp khóa công khai và khóa bí mật của riêng mình
  - (2) Gửi yêu cầu xin cấp chứng thực điện tử
  - (3) CA nhận và kiểm tra sự chính xác của thông tin nhận được
  - (4) CA sẽ tạo ra một chứng thực điện tử

2.4. Chứng thực điện tử

- Quy trình cấp chứng thực điện tử (tiếp)
  - (5) CA chia thành các đoạn băm => tiến hành mã hóa bằng khóa bí mật của mình => gửi trở lại cho đơn vị đăng ký chứng thực điện tử
  - (6) Chứng thực được sao một bản và chuyển tới thuê bao, có thể thông báo lại tới CA là đã nhận được
  - (7) CA có thể lưu giữ bản sao của chứng thực điện tử
  - (8) CA ghi lại các chi tiết của quá trình tạo chứng chỉ vào nhật ký kiểm toán.

2.4. Chứng thực điện tử

- Trước khi trao đổi thông tin, bên gửi phải cho bên nhận chứng thực điện tử của mình
- Bên nhận sẽ kiểm tra chứng thực, lấy ra khóa công khai của bên gửi
- Nhờ đó, khóa công khai mới không bị giả mạo