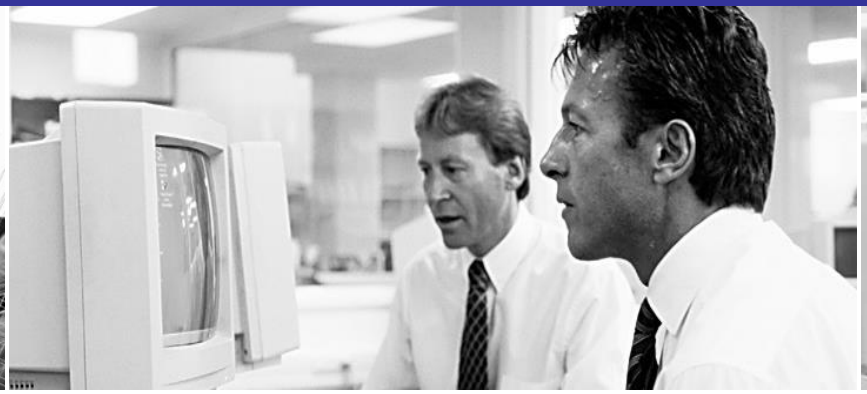
Chương 6
Hợp đồng trong TMĐT

Môn: THƯƠNG MẠI ĐIỆN TỬ



STU
Trần Quang
Khoa Công Nghệ Thông Tin

Hợp đồng là gì?

- Hợp đồng:

  Là sự thỏa thuận bằng văn bản, tài liệu giao dịch giữa các bên với sự quy định rõ ràng quyền và nghĩa vụ của mỗi bên để xây dựng và thực hiện nghĩa vụ của mình.

- Điều 388 của Bộ luật Dân sự Việt Nam 2005:

  Hợp đồng dân sự là sự thỏa thuận giữa các bên về việc xác lập, thay đổi hoặc chấm dứt quyền, nghĩa vụ dân sự

Hợp đồng điện tử

- Điều 11, mục 1, Luật mẫu về Thương mại điện tử UNCITRAL 1996: “Hợp đồng điện tử được hiểu là hợp đồng được hình thành thông qua việc sử dụng thông điệp dữ liệu”
- Đ33 Luật giao dịch điện tử của Việt Nam 2005: “Hợp đồng điện tử là hợp đồng được thiết lập dưới dạng thông điệp dữ liệu theo quy định của Luật này”

Thông điệp dữ liệu

- K12, điều 4: Thông điệp dữ liệu là “thông tin được tạo ra, được gửi đi, được nhận và (hoặc) lưu trữ bằng phương tiện điện tử”
- Điều 10. Hình thức thể hiện thông điệp dữ liệu: Thông điệp dữ liệu được thể hiện dưới dạng hình thức trao đổi dữ liệu điện tử, chứng từ điện tử, thư điện tử, điện tín, điện báo, fax và các hình thức tương tự khác (webpage, file âm thanh, file văn bản…)

Tính pháp lý của hợp đồng điện tử

- Luật mẫu về TMĐT do Ủy ban pháp luật thương mại quốc tế của Liên hợp quốc (UNCITRAL) ban hành năm 1996
- Luật mẫu về chữ ký điện tử được UNCITRAL ban hành năm 2001
- Công ước 2005 của Liên Hợp Quốc về hợp đồng điện tử quốc tế.
- Luật giao dịch điện tử Việt Nam

Tính pháp lý của hợp đồng điện tử

- Luật mẫu về TMĐT của UNCITRAL (1996)
  - Khi một thông điệp dữ liệu được sử dụng trong việc hình thành hợp đồng, giá trị pháp lý và hiệu lực thi hành của hợp đồng đó không thể bị phủ nhận chỉ với lý do duy nhất là một thông điệp dữ liệu đã được dùng vào mục đích đó
- Luật mẫu về chữ ký điện tử của UNCITRAL 2001
  - Chữ ký điện tử được tạo ra theo quy định của luật này có giá trị pháp lý như chữ ký trong văn bản giấy truyền thống

Tính pháp lý của hợp đồng điện tử

- Luật Giao dịch điện tử:
  - thừa nhận giá trị pháp lý của hợp đồng điện tử, quy định cụ thể các nguyên tắc giao kết và hình thức của hợp đồng điện tử.
  - chấp nhận giao kết hợp đồng có thể thực hiện thông qua thông điệp dữ liệu
- Luật Thương mại:
  - Trong hoạt động thương mại, các thông điệp dữ liệu đáp ứng các điều kiện, tiêu chuẩn kỹ thuật theo quy định của pháp luật được thừa nhận có giá trị pháp lý tương đương văn bản

Phân loại hợp đồng điện tử

- Hợp đồng truyền thống được đưa lên web
- Hợp đồng điện tử hình thành qua các giao dịch tự động trên Web
- Hợp đồng hình thành qua nhiều giao dịch bằng email
- Hợp đồng sử dụng chữ ký số

CHỮ KÝ SỐ

Mã hóa

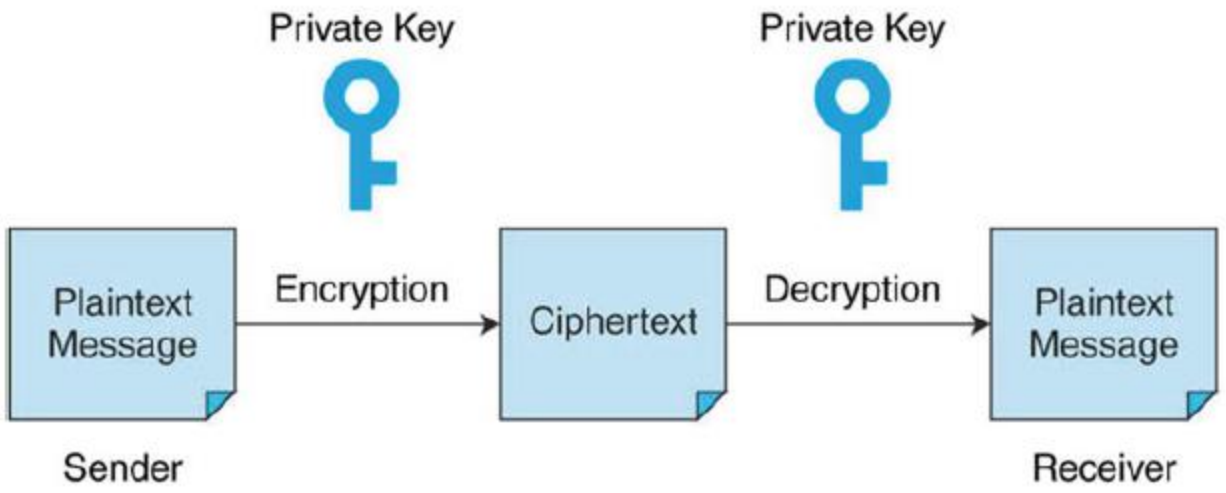
- Chuyển dữ liệu thành dạng mật mã làm cho người khác không thể đọc được, trừ người nhận và người gởi
- Bảo mật dữ liệu lưu trữ và dữ liệu trao đổi
- Đảm bảo
  - Sự toàn vẹn dữ liệu
  - Chống từ chối
  - Xác thực
  - Bảo mật

Symmetric Key Encryption

- Cần các khóa khác nhau cho mỗi giao dịch
- Advanced Encryption Standard (AES)
  - Sử dụng rộng rải khóa đối xứng
  - Dùng khóa 128-, 192-, 256-bits mã hóa
- Một số chuẩn khác dùng đến 2,048 bits

Symmetric Key Encryption

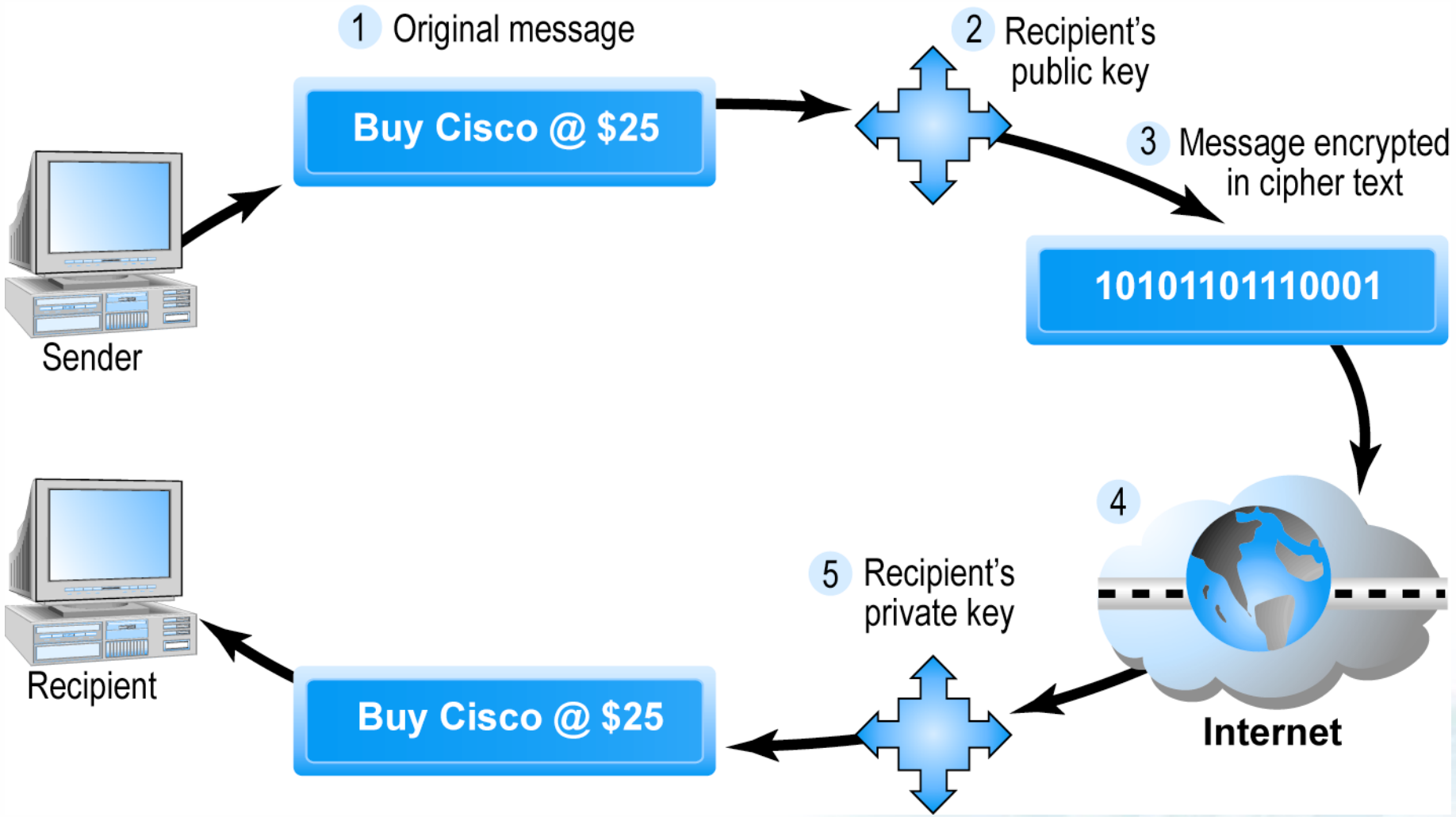
- Mã hóa khóa đối xứng, còn gọi là mã hóa khóa bí mật
- Cả người gởi và người nhận sử dụng cùng một khóa để mã hóa và giải mã



Hạ tầng khóa công khai

- Sử dụng cặp khóa
  - Public key (phổ biến rộng rải)
  - Private key (chủ sở hữu giữ bí mật)
- Cả 2 đều có thể dùng để mã hóa hoặc giải mã. Khi dùng khóa này để mã hóa, thì phải dùng khóa còn lại để giải mã
- Vi dụ: người gởi dùng public key để mã hóa, thì người nhận phải dùng private key để giải mã

Mã hóa bằng Public Key đơn giản



Chữ ký điện tử

- Chữ ký điện tử được gắn liền với một thông điệp dữ liệu nhằm giúp ta:
  - Xác định được tác giả của thông điệp dữ liệu đó
  - Khẳng định sự chấp thuận của người ký đối với nội dung của thông điệp dữ liệu → chống từ chối sau này

Điều kiện của một chữ ký điện tử

- Dữ liệu tạo chữ ký điện tử chỉ gắn duy nhất với người ký khi dữ liệu đó được sử dụng
- Dữ liệu tạo chữ ký điện tử chỉ thuộc sự kiểm soát của người ký tại thời điểm ký.
- Mọi thay đổi đối với chữ ký điện tử sau thời điểm ký đều có thể bị phát hiện.
- Mọi thay đổi đối với nội dung của dữ liệu sau thời điểm ký đều có thể bị phát hiện.

Chữ ký số (Digital Signature)

- Có thể được giám định, xác nhận nhanh với các công cụ điện tử.
- Chữ ký số giúp doanh nghiệp, người dân có thể kê khai nộp thuế, chuyển tiền trực tiếp qua mạng Internet.
- Doanh nghiệp có thể xây dựng hệ thống mua bán trực tuyến, đảm bảo thanh toán trực tuyến với chứng thư đã được xác nhận; có thể ký kết hợp đồng qua mạng.

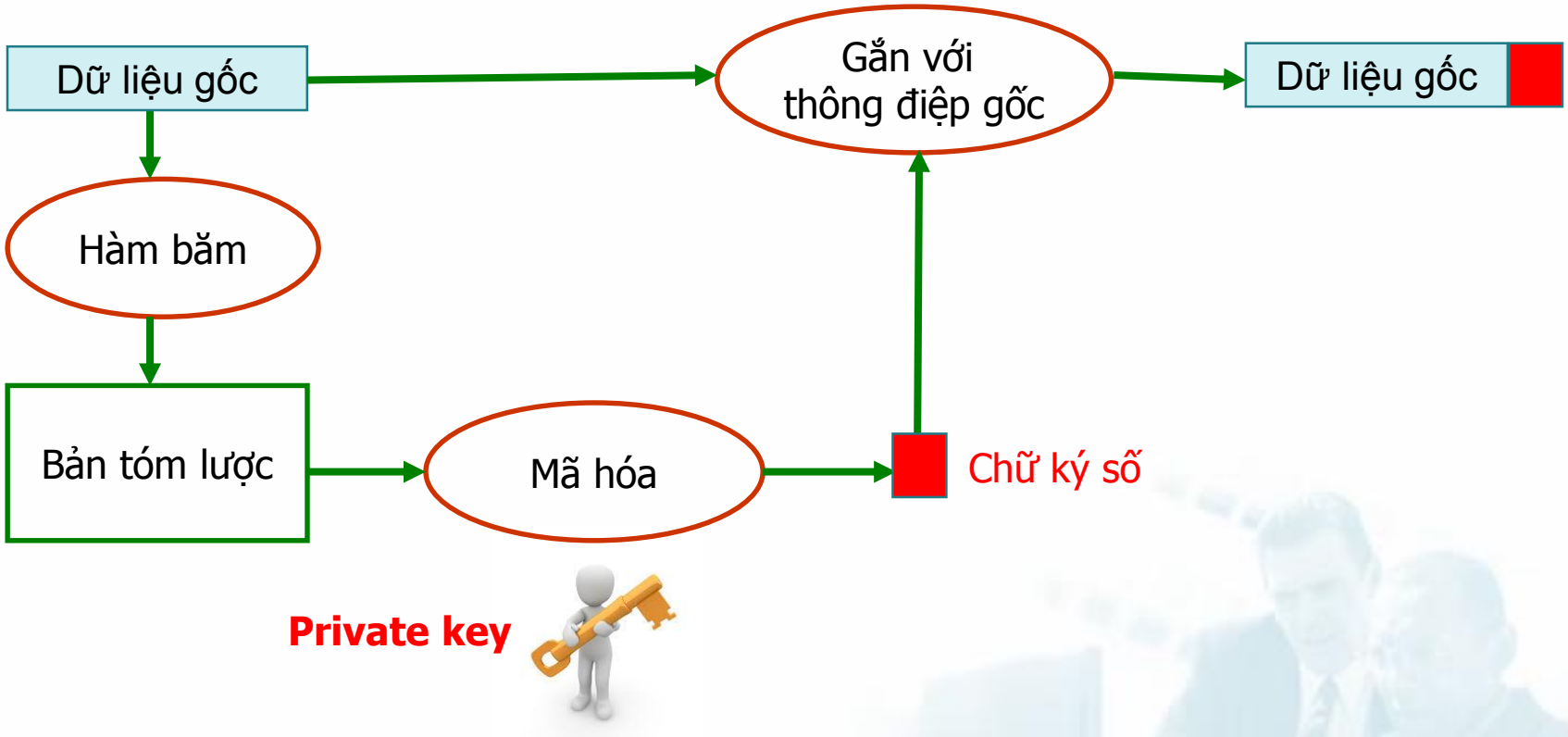
Chữ ký số (Digital Signature)

- Dựa trên hạ tầng khóa công khai (PKI)
- Mỗi người có 1 cặp khóa gồm:
  - Khóa bí mật dùng để tạo chữ ký số
  - khóa công khai dùng để thẩm định chữ ký số → xác thực

Mã hóa Public Key và chữ ký số

- Hàm băm (Hash function)
  - Sử dụng thuật toán để tạo ra dãy số có chiều dài cố định từ message gọi là hash digest
- Hash digest sẽ được gởi cùng với message đến người nhận để kiểm tra sự toàn vẹn
- Kỹ thuật này cho phép xác thực, kiểm tra sự toàn vẹn, chống từ chối

Tạo chữ ký số (Digital signature)



Thẩm định chữ ký số

Public key

Giải mã

Giải mã được ?

No

Không đúng người gửi

Yes

Bản tóm lược

Dữ liệu đã bị thay đổi

No

Dữ liệu

Tách

So sánh

Giống nhau ?

Yes

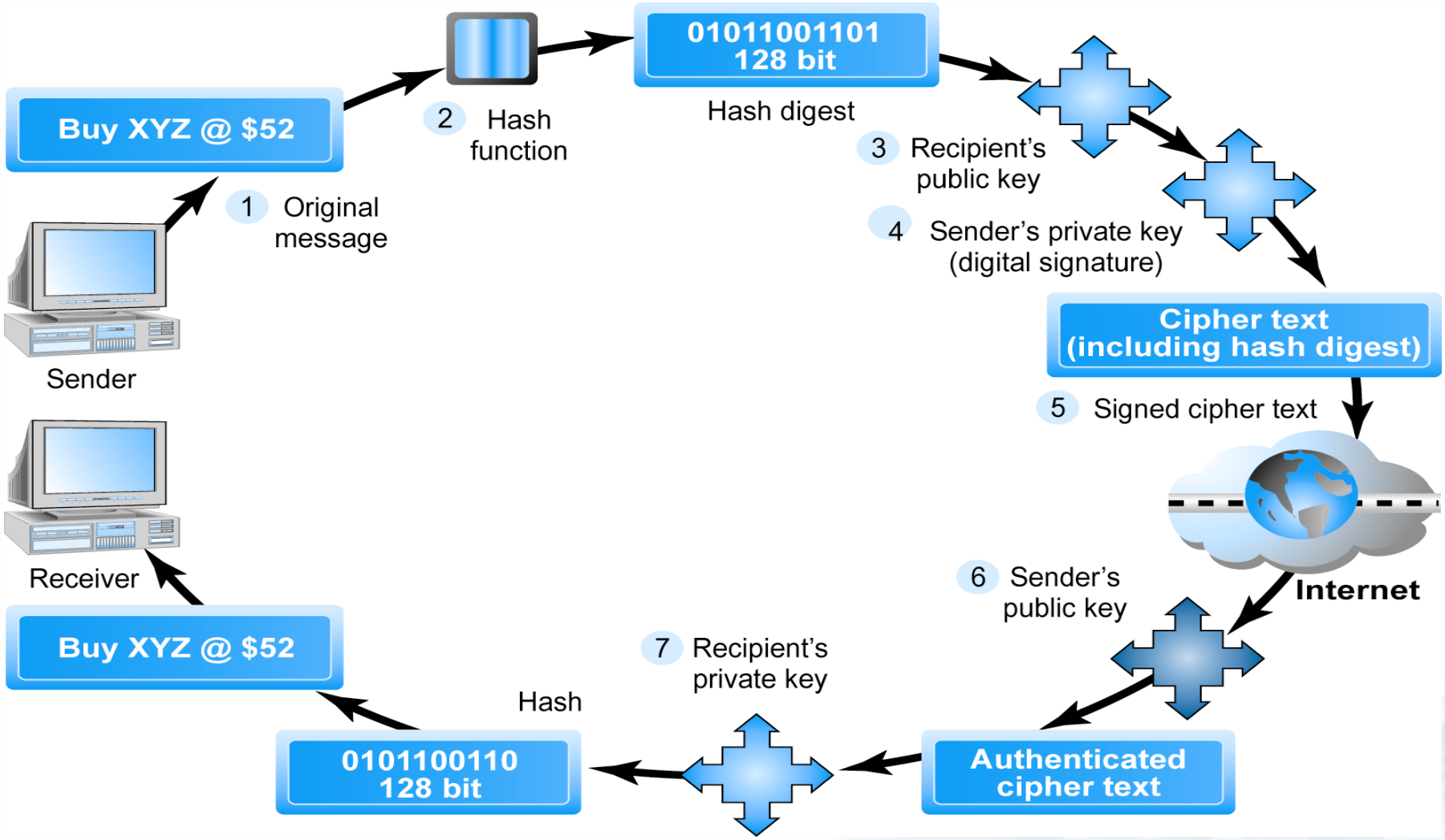
Dữ liệu

Hàm băm

Bản tóm lượcc

Dữ liệu nhận toàn vẹn

Mã hóa Public Key dùng chữ ký số



Hợp đồng điện tử, con dấu điện tử

- Hợp đồng điện tử không bắt buộc phải có chữ ký điện tử. Việc sử dụng chữ ký điện tử hay sử dụng chữ ký điện tử được chứng thực phụ thuộc vào thỏa thuận giữa các bên tham gia hợp đồng.
- Tuy nhiên, nhằm đảm bảo an toàn và tạo cơ sở pháp lý đầy đủ trong giải quyết tranh chấp, việc sử dụng chữ ký điện tử trong giao kết hợp đồng luôn được khuyến khích.

Hợp đồng điện tử, con dấu điện tử

- Luật Giao dịch điện tử nêu rõ đối với các văn bản pháp luật quy định cần đóng dấu như hợp đồng gọi là hợp đồng điện tử.
- Con dấu không chỉ mang ý nghĩa xác thực tính pháp lý của chữ ký mà nó còn thể hiện được xuất xứ của chữ ký đó
- Vấn đề đặt ra là nên ký chữ ký điện tử một lần hay hai lần (1 chữ ký điện tử xác nhận người ký và chữ ký còn lại đảm nhiệm chức năng của con dấu).

Cơ quan chứng thực (CA)

- Giả sử A muốn gửi thông điệp cho B và mã hóa theo phương pháp khóa công khai, thì A cần public key của B
- Hacker có thể tự sinh ra một cặp khóa public key/private key, sau đó gởi cho A và nói đây là khóa public key của B
- A dùng public key giả này mà tưởng là của B thì dẫn đến hệ quả mọi thông tin A truyền đi đều bị hacker đọc được.

Cơ quan chứng thực (CA)

- Vì vậy cần có một bên thứ ba được tin cậy đứng ra chứng nhận public key.
- Public key certificate được xem như là một hộ chiếu hay chứng minh thư.
- Các tổ chức này gọi là Certificate Authority (CA) - tổ chức chứng nhận khóa công khai như: VeriSign, Entrust, CyberTrust, v.v...

Cơ quan chứng thực (CA)

- Cơ quan chứng thực: cơ quan cung cấp dịch vụ chữ ký số cho các bên tham gia ký kết.
- Nhiệm vụ: tạo ra cặp khóa công khai và bí mật và cấp chứng thư số cho các thuê bao (doanh nghiệp, tổ chức và cá nhân đăng ký sử dụng dịch vụ).
- Chứng thư số: thông điệp dữ liệu trong đó có các nội dung cơ bản như: thông tin về cá nhân, tổ chức được cấp chứng thư số, khóa công khai, thời hạn sử dụng, số chứng chỉ, chữ ký số và thông tin của tổ chức cấp chứng chỉ số

Nội dung của chứng thư số

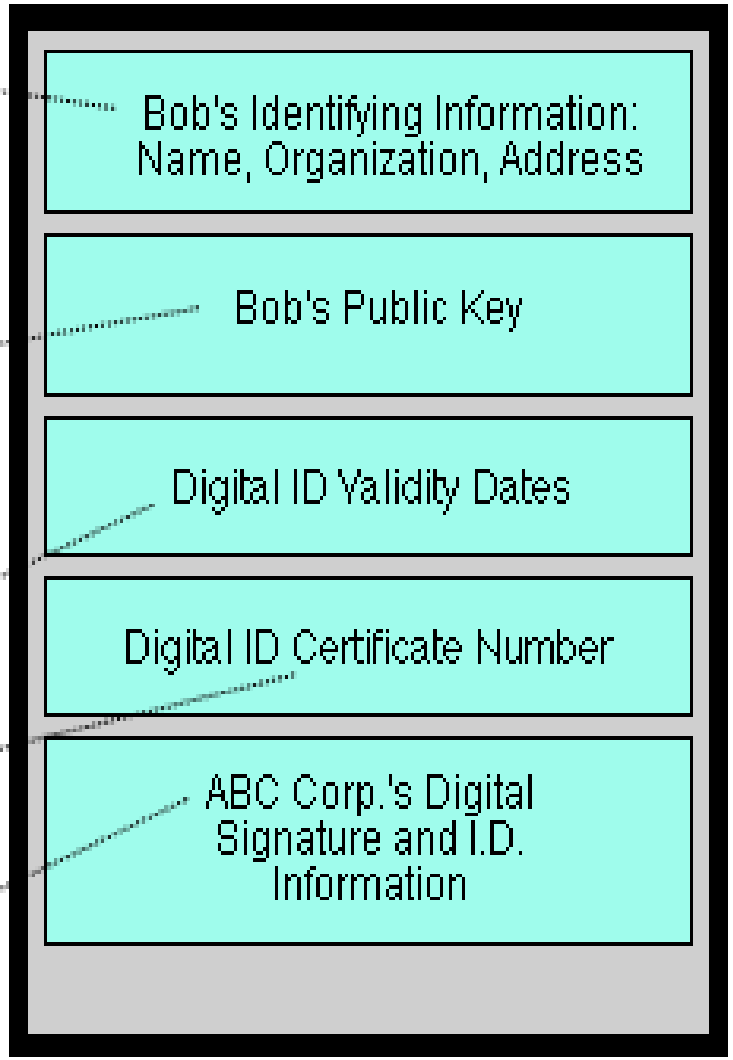
1. *Thông tin của tổ chức, cá nhân được cấp chứng chỉ số*

2. *Khóa công khai của tổ chức, cá nhân được cấp chứng chỉ số*

3. *Hạn sử dụng*

4. *Số chứng chỉ*

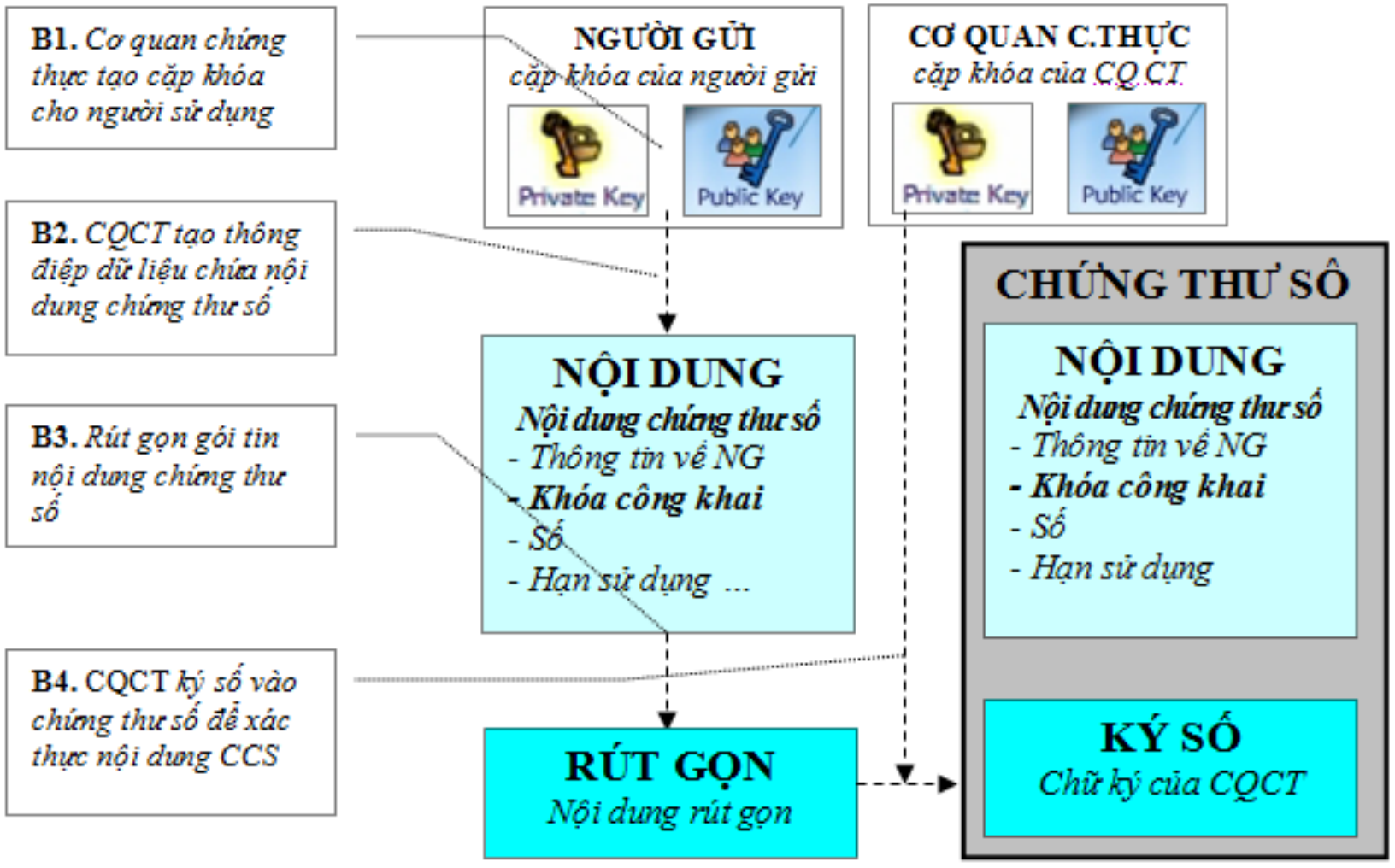
5. *Chữ ký số của tổ chức cấp chứng chỉ số (CA)*



Quy trình tạo chứng thư điện tử

- Bước 1: Cơ quan chứng thực tạo ra cặp khóa công khai và bí mật cho người sử dụng
- Bước 2: Cơ quan chứng thực tạo thông điệp nội dung chứng thư số với đầy đủ các thông tin cần thiết
- Bước 3: Rút gọn chứng thư số và ký xác nhận bằng khóa bí mật của mình
- Bước 4: Gắn chữ ký số vào thông điệp chứa nội dung chứng thư số để tạo thành chứng thư số

Quy trình tạo chứng thư điện tử



Phong bì số (Digital Envelope)

- Phong bì số là quá trình mã hoá sử dụng public key được người nhận thông báo cho các đối tác biết để sử dụng khi họ muốn gửi thông điệp cho mình
- Khóa này được dùng để mã hoá thông tin mà người gửi muốn gửi cho người nhận
- Chỉ duy nhất người nhận là mở được thông điệp để đọc (do giữ private key)