



HUTECH

Đại học Công nghệ Tp.HCM

Bài 8: Bảo mật Web & Email

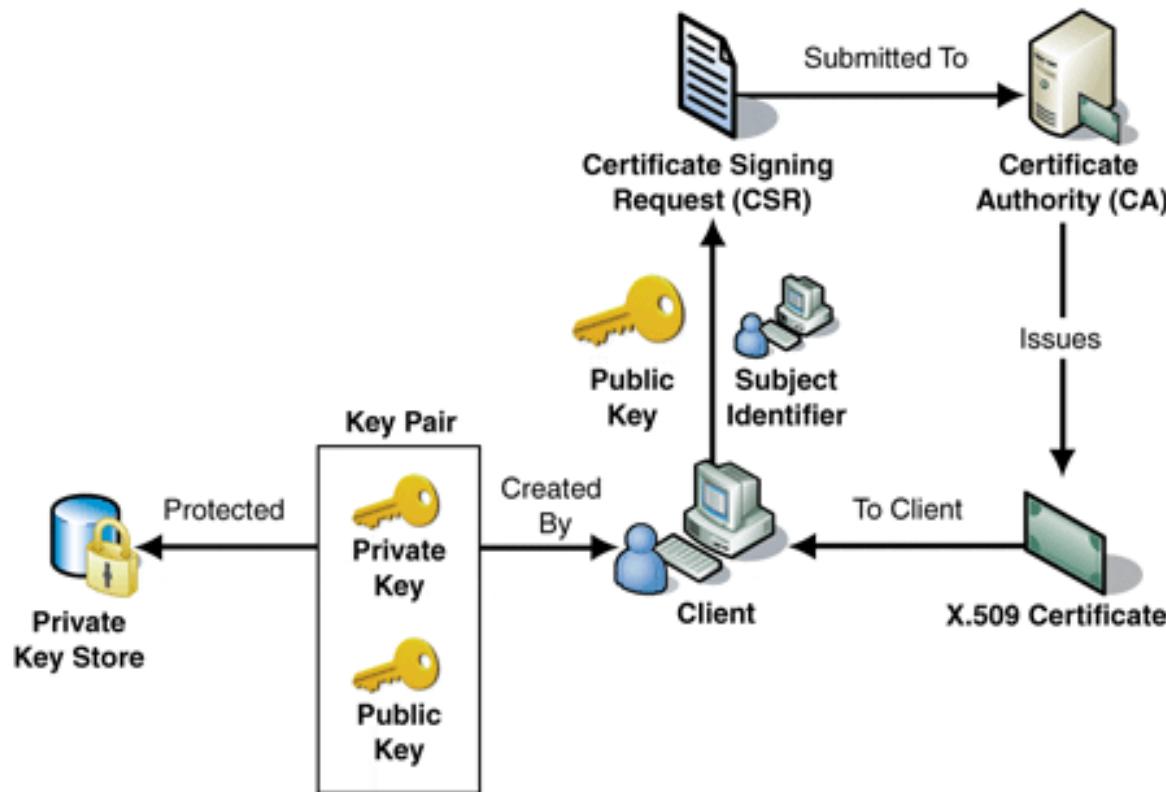
HIENTH

Trình bày:
Ths. Lương Trần Hy Hiển
<http://hienlth.info/hutech/baomatthongtin>

Nội dung

1. Dịch vụ xác thực X.509
2. Giao thức bảo mật Web SSL
3. Bảo mật email PGP

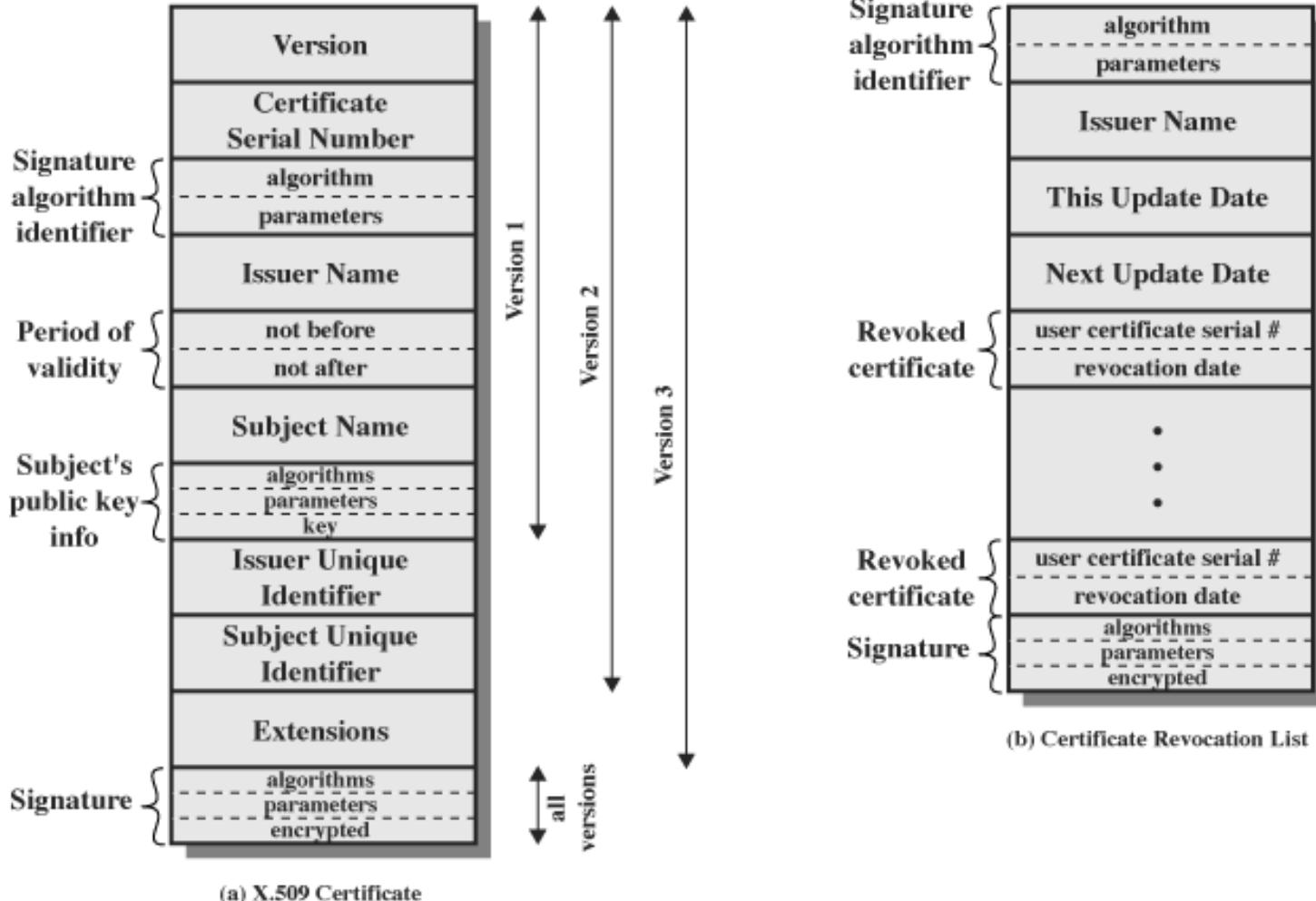
1. Dịch vụ xác thực X.509



Dịch vụ xác thực X.509

- Nằm trong loạt khuyến nghị X.500 của ITU-T nhằm chuẩn hóa dịch vụ thư mục
 - Servers phân tán lưu giữ CSDL thông tin người dùng
- Định ra một cơ cấu cho dịch vụ xác thực
 - Danh bạ chứa các chứng thực khóa công khai
 - Mỗi chứng thực bao gồm khóa công khai của người dùng ký bởi một bên chuyên trách chứng thực đáng tin
- Định ra các giao thức xác thực
- Sử dụng mật mã khóa công khai và chữ ký số
 - Không chuẩn hóa giải thuật nhưng RSA khuyến nghị

Khuôn dạng X.509



(a) X.509 Certificate

(b) Certificate Revocation List

Cấu trúc và ví dụ một chứng chỉ X.509

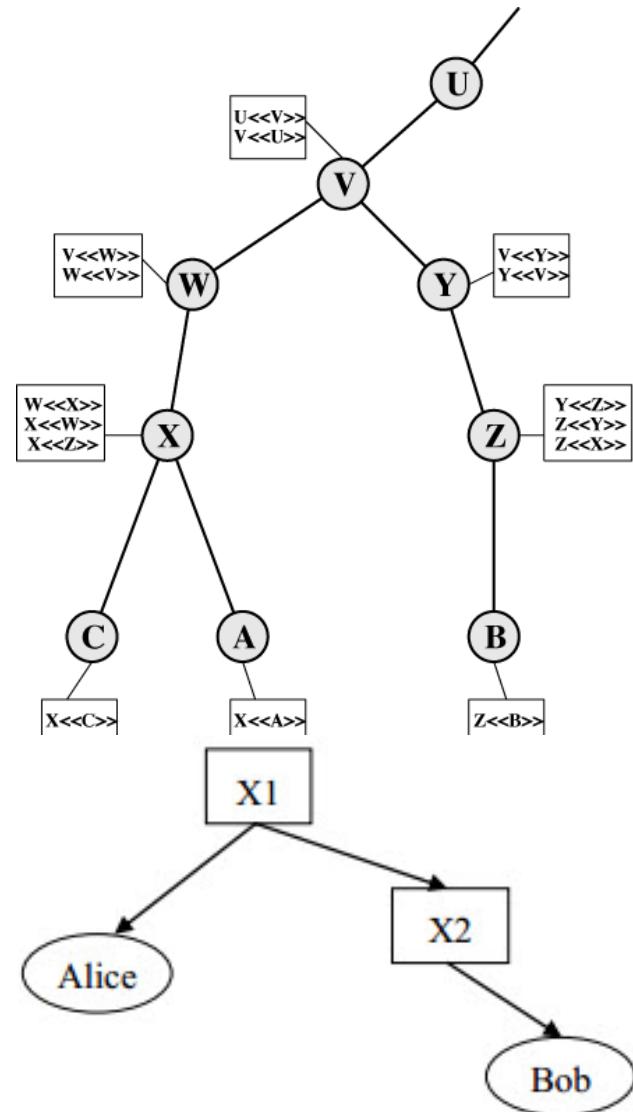
Version
Serial Number
Certificate Signature Algorithm
Issuer Name
Validity (Not Before, Not After)
Subject
Subject Public Key Algorithm
Subject Public Key
Issuer Unique Identifier
Subject Unique Identifier
Extension for version 3
Certificate Signature Algorithm
Certificate Signature Value

| Version 3 |
| 05:A0:4C |
| PKCS #1 SHA-1 With RSA Encryption |
| OU = Equifax Secure Certificate Authority; O = Equifax |
| 04/01/2006 17:09:06 PM GMT - 04/01/2011 17:09:06 PM GMT |
| CN= login.yahoo.com; OU= Yahoo; O= Yahoo! Inc. |
| PKCS #1 RSA Encryption |
| 30 81 89 02 81 81 00 b5 6c 4f ee ef 1b 04 5d be... |
| PKCS #1 SHA-1 With RSA Encryption |
| 50 25 65 10 43 e1 74 83 2f 8f 9c 9e dc 74 64 4e... |

Nhận chứng thực CA

- Cứ có khóa công khai của CA (cơ quan chứng thực) là có thể xác minh được chứng thực
- Chỉ CA mới có thể thay đổi chứng thực
 - Chứng thực có thể đặt trong một thư mục công khai
- Cấu trúc phân cấp CA
 - Người dùng được chứng thực bởi CA đã đăng ký
 - Mỗi CA có hai loại chứng thực
 - Chứng thực thuận: Chứng thực CA hiện tại bởi CA cấp trên
 - Chứng thực nghịch: Chứng thực CA cấp trên bởi CA hiện tại
- Cấu trúc phân cấp CA cho phép người dùng xác minh chứng thực bởi bất kỳ CA nào

Phân cấp X.509



Không thể chỉ có một trung tâm chứng thực CA duy nhất mà có thể có nhiều trung tâm chứng thực. Mỗi người sử dụng khác nhau có thể đăng ký chứng thực tại các CA khác nhau.

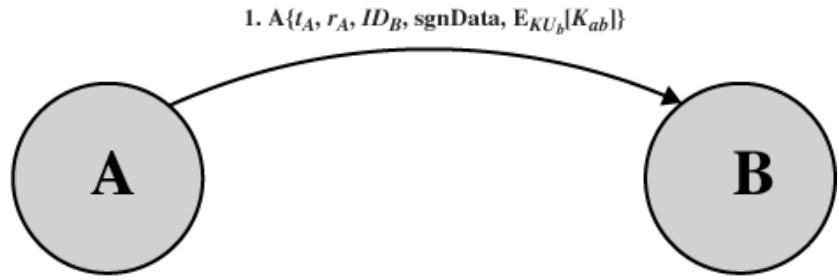
Để có thể trao đổi dữ liệu, một người cần phải tin tưởng vào khóa công khai của tất cả các trung tâm chứng thực.

Thu hồi chứng thực

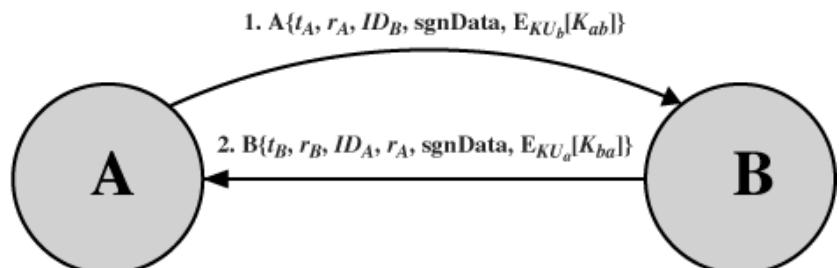
- Mỗi chứng thực có một thời hạn hợp lệ
- Có thể cần thu hồi chứng thực trước khi hết hạn
 - Khóa riêng của người dùng bị tiết lộ
 - Người dùng không còn được CA chứng thực
 - Chứng thực của CA bị xâm phạm
- Mỗi CA phải duy trì danh sách các chứng thực bị thu hồi (CRL)
- Khi nhận được chứng thực, người dùng phải kiểm tra xem nó có trong CRL không

Các thủ tục xác thực của X.509

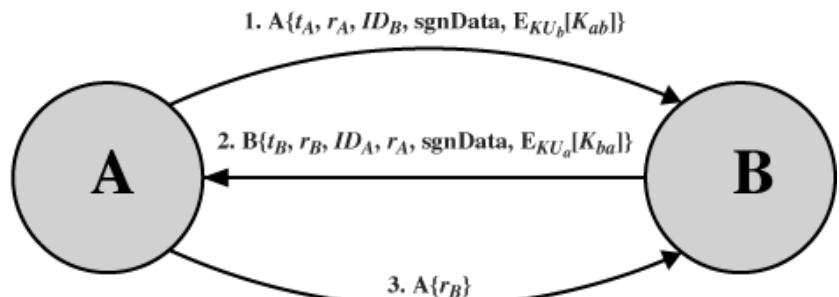
- Xác thực 1 chiều
- Xác thực 2 chiều
- Xác thực 3 chiều



(a) One-way authentication



(b) Two-way authentication



(c) Three-way authentication

Xác thực một chiều

- Một chiều A->B được sử dụng để thiết lập
 - Danh tính của A và rằng mẫu tin là từ A
 - Mẫu tin được gửi cho B
 - Tính toàn vẹn và gốc gác của mẫu tin
- Mẫu tin có thể bao gồm cả nhãn thời gian, ký hiệu đặc trưng của mẫu tin (nonce), danh tính của B và nó được ký bởi A. Có thể bao gồm một số thông tin bổ sung cho B như khoá phiên.

Xác thực hai chiều

- Hai mẫu tin $A \rightarrow B$ và $B \rightarrow A$ được thiết lập, ngoài mẫu tin từ A đến B như trên còn có:
 - Danh tính của B và trả lời từ B
 - Trả lời này dành cho A
 - Tính toàn vẹn và gốc gác của trả lời
- Trả lời bao gồm cả ký hiệu đặc trưng của mẫu tin (nonce) từ A, cả nhãn thời gian và ký hiệu đặc trưng trả lời từ B. Có thể bao gồm một số thông tin bổ sung cho A.

Xác thực ba chiều

- Ba mẫu tin $A \rightarrow B$, $B \rightarrow A$ và $A \rightarrow B$ được thiết lập như trên mà không có đồng hồ đồng bộ.
- Ngoài 2 chiều như trên còn có trả lời lại từ A đến B chứa bản sao nonce của trả lời từ B, nghĩa là các nhãn thời gian mà không cần kiểm tra.

X.509 phiên bản 3

Trong phiên bản 3 được bổ sung một số thông tin cần thiết trong giấy chứng nhận như: Email/URL, chi tiết về đợt phát hành, các ràng buộc sử dụng. Tốt hơn hết là đặt tên tương minh cho các cột mới xác định trong phương pháp mở rộng tổng quát. Các mở rộng bao gồm:

- Danh tính mở rộng
- Chỉ dẫn tính quan trọng
- Giá trị mở rộng

Các mở rộng xác thực

- Khoá và các thông tin đợt phát hành
- Bao trùm thông tin về đối tượng, khoá người phát hành, chỉ thị kiểu phát hành, chứng nhận
Đối tượng chứng nhận và các thuộc tính người phát hành
- Hỗ trợ có tên phụ, định dạng phụ cho các đối tượng và người phát hành
Chứng nhận các ràng buộc phát hành
- Cho phép sử dụng các ràng buộc trong chứng nhận bởi các CA khác

Cấp chứng chỉ

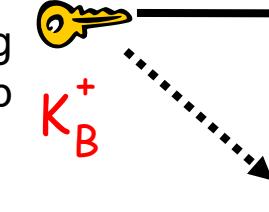
- Certification authority (CA): gắn kết khóa công cộng với thực thể E nào đó.
- E (người, router) đăng ký khóa công cộng của họ với CA.
 - E cung cấp “bằng chứng để nhận dạng” cho CA.
 - CA tạo ra chứng chỉ ràng buộc E với khóa công cộng của nó.
 - chứng chỉ chứa khóa công cộng của E được ký số bởi CA – CA nói “đây là khóa công cộng của E”



khóa công cộng
của Bob

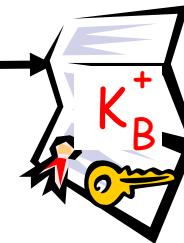
K_B^+

thông tin để
nhận dạng Bob



chữ ký số
(đã mã hóa)

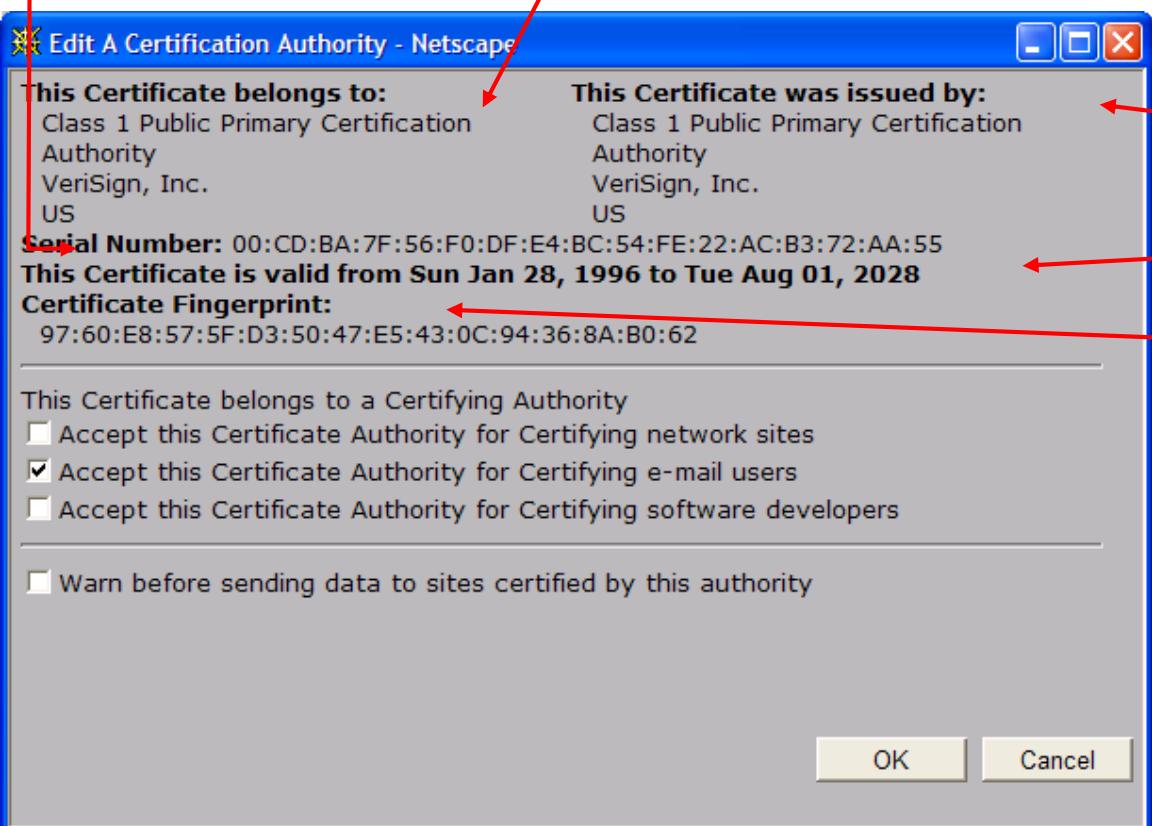
khóa
riêng
CA
 K_{CA}^-



chứng chỉ cho khóa
công cộng của Bob,
ký bởi CA

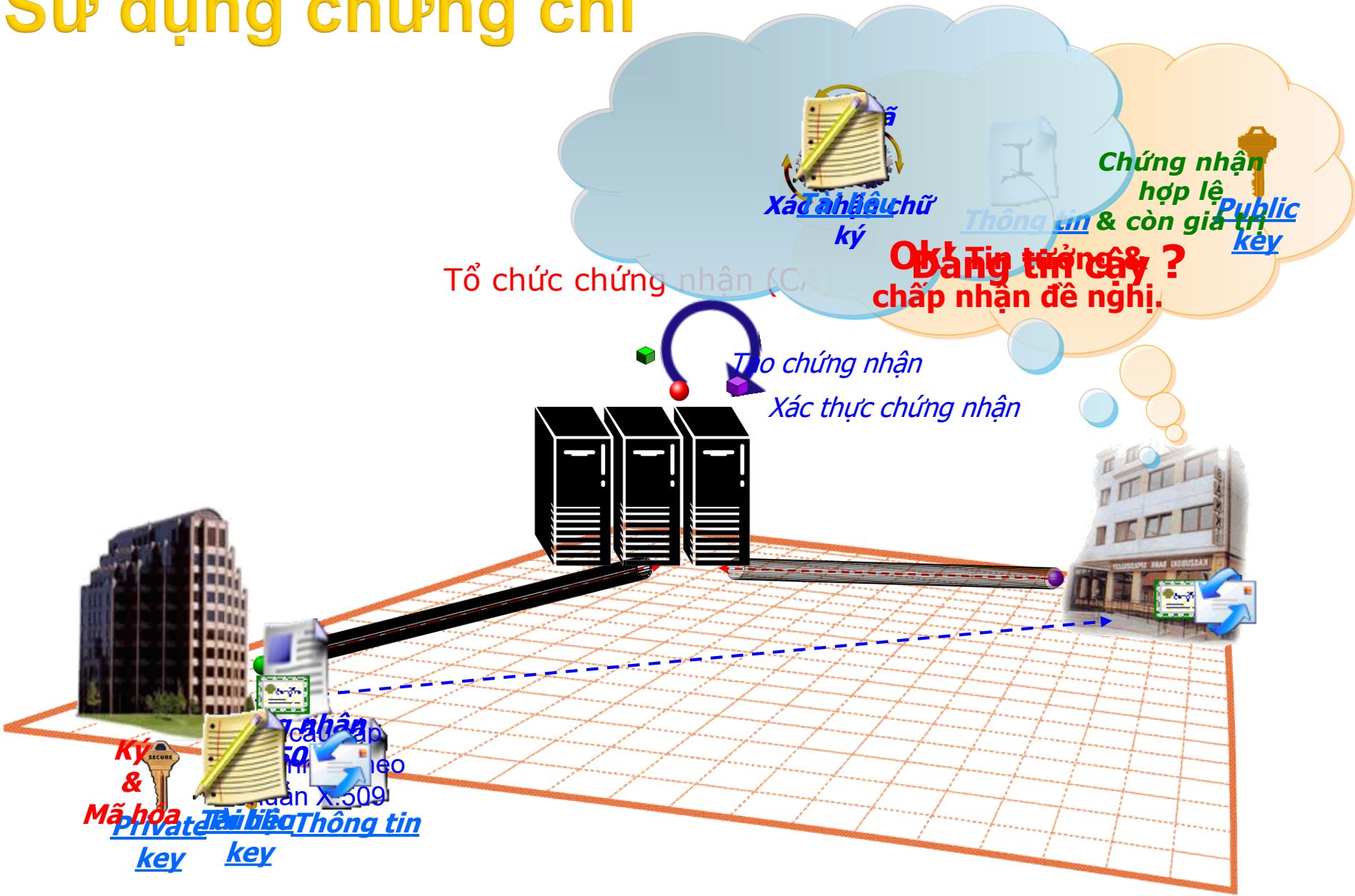
Mô tả chứng chỉ

- Số thứ tự (duy nhất)
- thông tin về người sở hữu chứng chỉ, bao gồm giải thuật và chính giá trị khóa (không hiển thị ra)

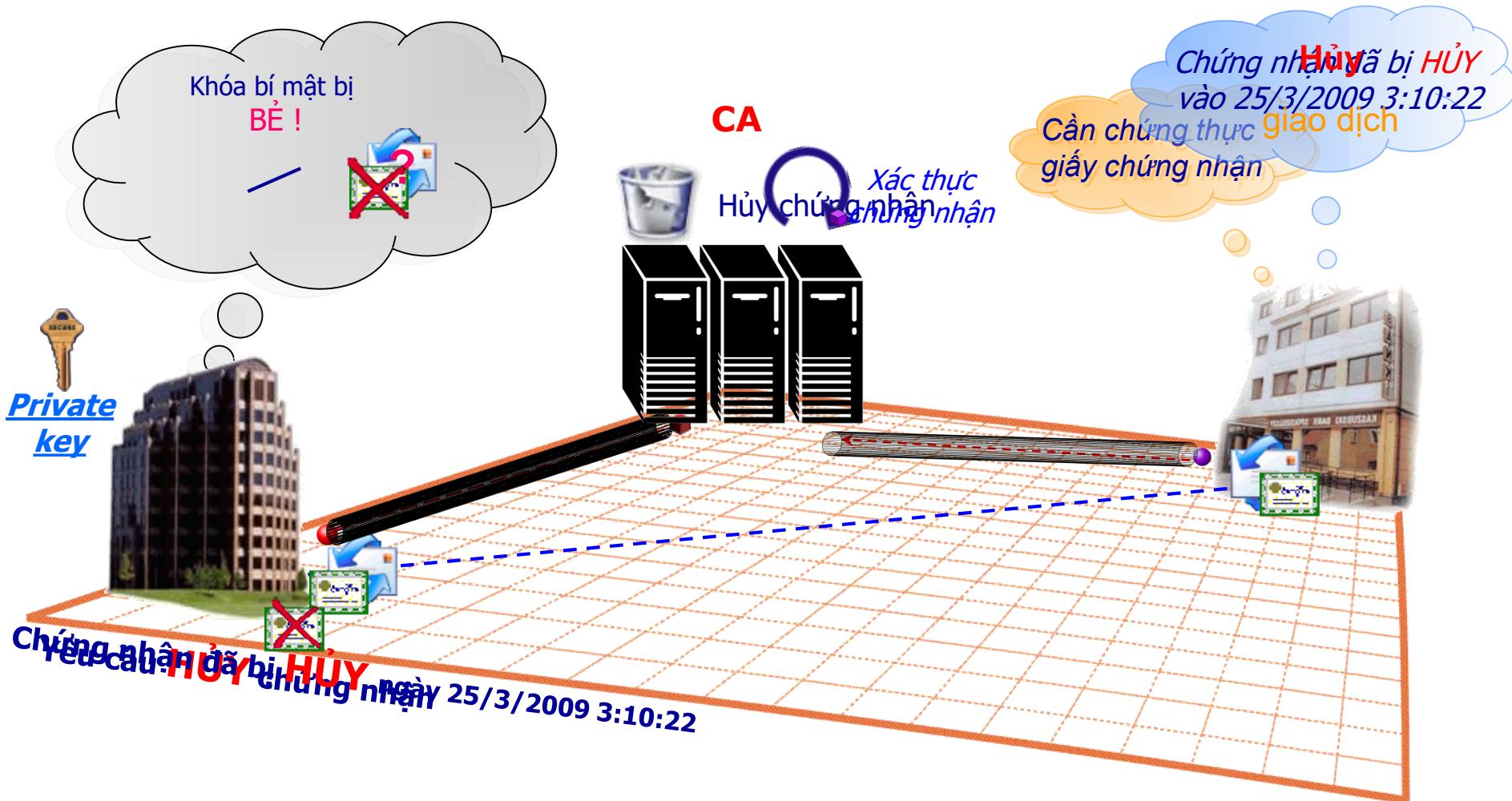


thông tin về người phát hành chứng chỉ
ngày kiểm tra tính hợp lệ
chữ ký số bởi người phát hành chứng chỉ

Sử dụng chứng chỉ



Sử dụng chứng chỉ



2. Giao thức bảo mật web SSL

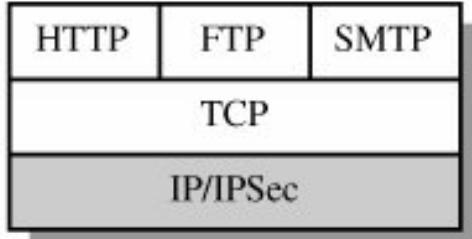
Tại sao cần bảo mật Web???

- Web được sử dụng rộng rãi bởi các công ty, tổ chức, và các cá nhân
- Các vấn đề đặc trưng đối với an ninh Web
 - Web dễ bị tấn công theo cả hai chiều
 - Tấn công Web server sẽ gây tổn hại đến danh tiếng và tiền bạc của công ty
 - Các phần mềm Web thường chứa nhiều lỗ an ninh
 - Web server có thể bị khai thác làm căn cứ để tấn công vào hệ thống máy tính của một tổ chức
 - Người dùng thiếu công cụ và kiến thức để đối phó với các hiểm họa an ninh

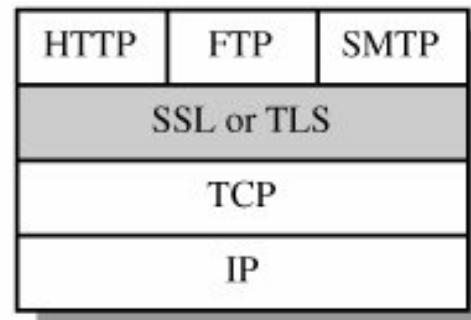
2. Giao thức bảo mật web SSL

Tại sao cần bảo mật Web???

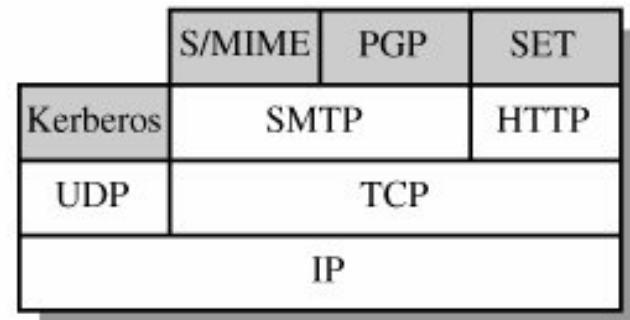
- Các hiểm họa đối với an ninh Web
 - Tính toàn vẹn
 - Tính bảo mật
 - Từ chối dịch vụ
 - Xác thực
- Các biện pháp an ninh Web



(a) Network level



(b) Transport level



(c) Application level

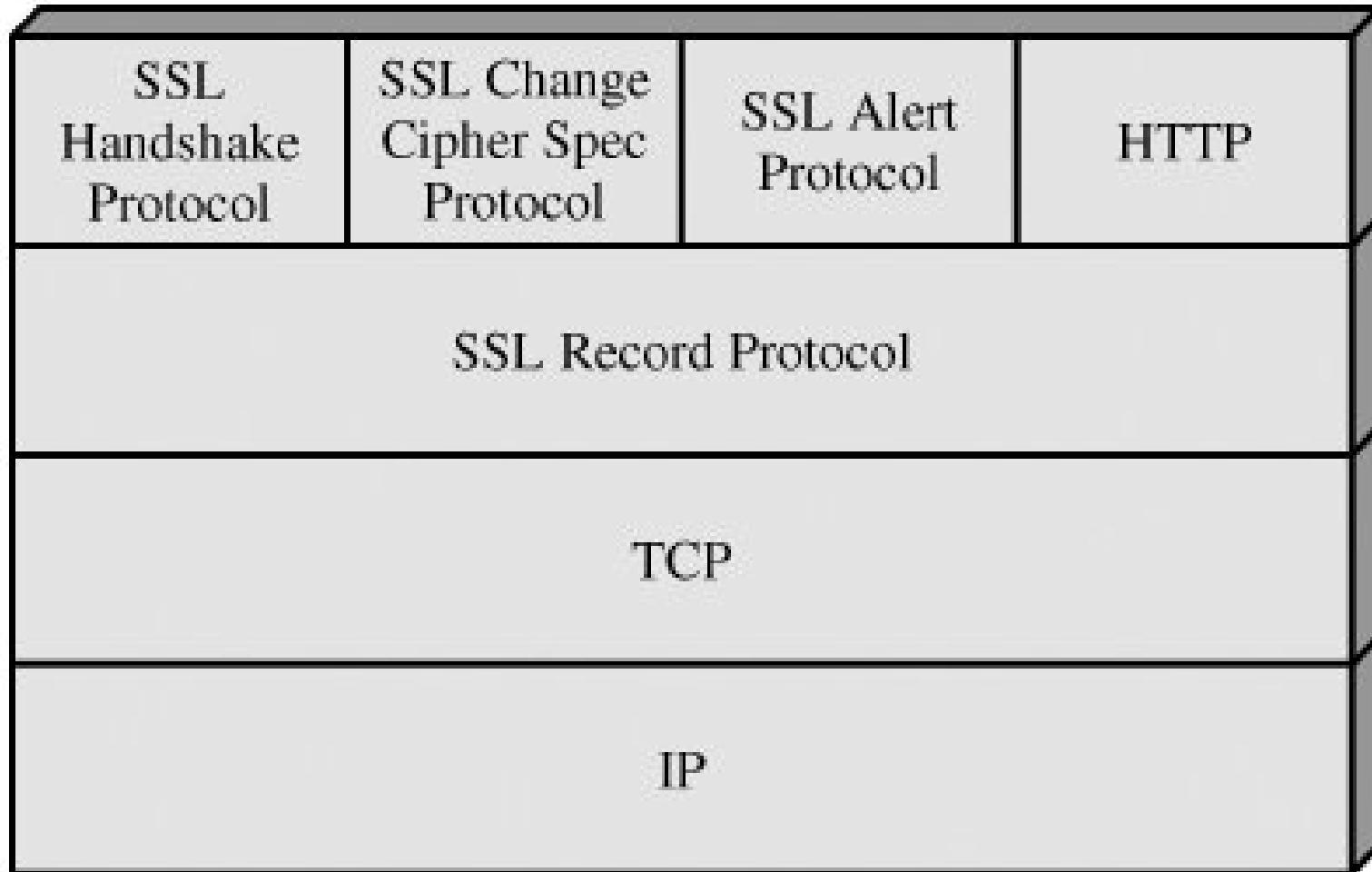
SSL



- Giao thức SSL (*Secure Socket Layer*) là một dịch vụ an ninh ở tầng giao vận, bảo mật dữ liệu trao đổi qua socket, do Netscape khởi xướng
- Phiên bản 3 được công bố dưới dạng bản thảo Internet
- Trở thành chuẩn TLS
 - Phiên bản đầu tiên của TLS ≈ SSLv3.1 tương thích ngược với SSLv3
 - Sử dụng TCP để cung cấp dịch vụ an ninh từ đầu cuối tới đầu cuối
 - Gồm 2 tầng giao thức



Kiến trúc tổng thể



Kiến trúc SSL

- **SSL Record Protocol:** Xử lý dữ liệu.
- **SSL Change Cipher Spec:** một message đơn 1 byte, cập nhật lại bộ mã hóa để sử dụng trên kết nối này.
- **SSL Alert:** được dùng để truyền cảnh báo liên kết SSL với đầu cuối bên kia.
- **SSL Handshake Protocol:** Giao thức này cho phép server và client chứng thực với nhau và thương lượng cơ chế mã hóa, thuật toán MAC và khóa mật mã được sử dụng để bảo vệ dữ liệu được gửi trong SSL record.

Giao thức đổi đặc tả mã hóa SSL

SSL Change Cipher Spec Protocol

- Một trong ba giao thức chuyên dụng SSL sử dụng giao thức bản ghi SSL
- Chỉ gồm một thông báo chứa một byte dữ liệu có giá trị là 1
- Khiến cho trạng thái treo trở thành trạng thái hiện thời
 - Cập nhật đặc tả mã hóa cho kết nối

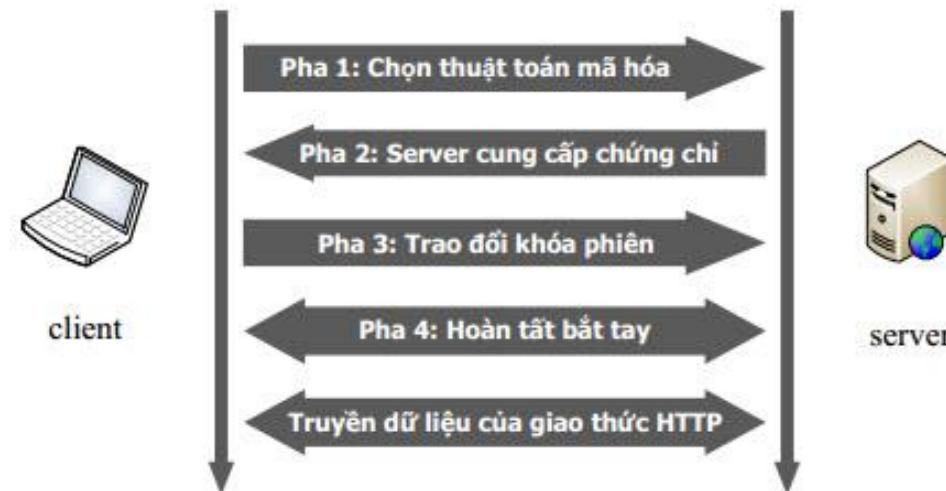
Giao thức báo động SSL

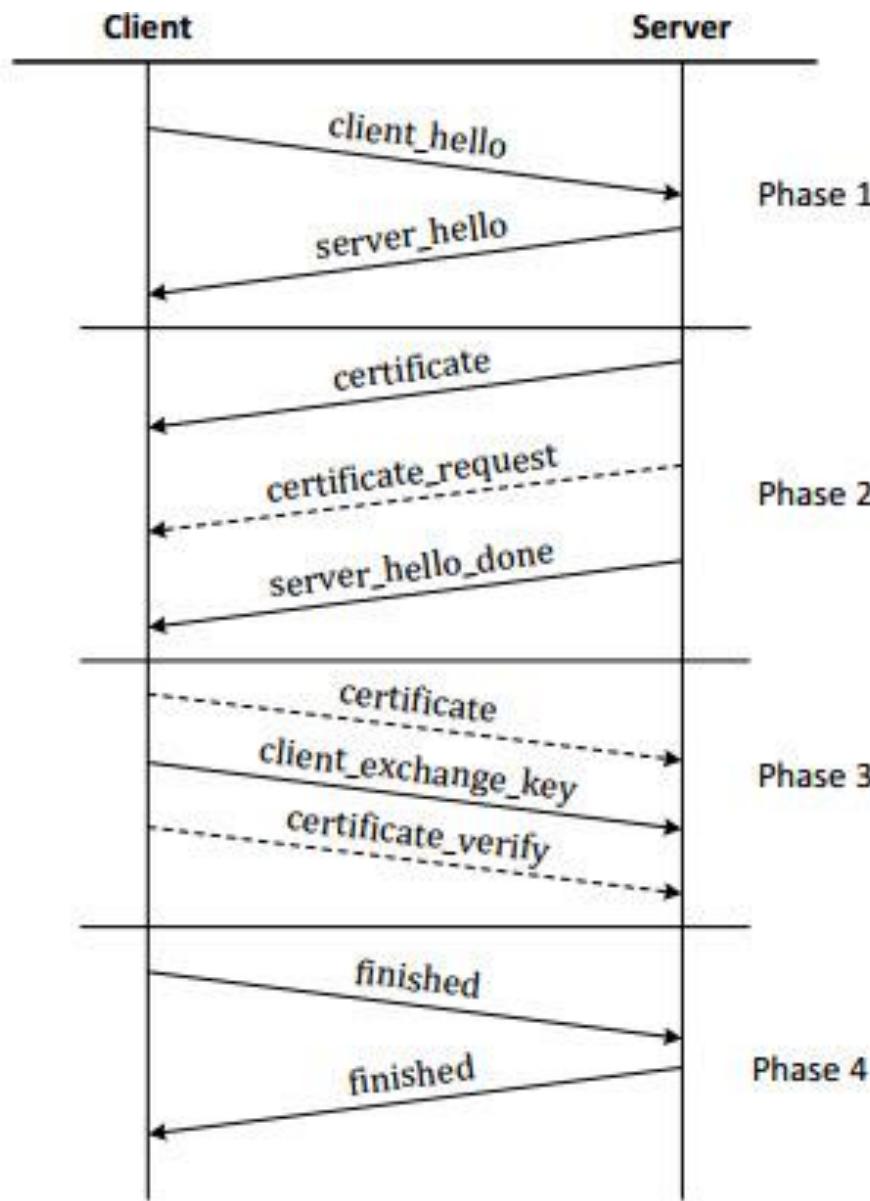
SSL Alert Protocol

- Dùng chuyển tải các nhắc nhở liên quan đến SSL tới các thực thể điểm nút
- Mỗi thông báo gồm 2 byte
 - Byte thứ nhất chỉ mức độ nghiêm trọng
 - Cảnh báo : có giá trị là 1
 - Tai họa : có giá trị là 2
 - Byte thứ hai chỉ nội dung nhắc nhở
 - Tai họa : unexpected_message, bad_record_mac, decompression_failure, handshake_failure, illegal_parameter
 - Cảnh báo : close_notify, no_certificate, bad_certificate, unsupported_certificate, certificate_revoked, certificate_expired, certificate_unknown

Giao thức bắt tay SSL

- Cho phép server và client
 - Xác thực lẫn nhau
 - Thỏa thuận các giải thuật mã hóa và MAC
 - Thỏa thuận các khóa mật mã sẽ được sử dụng
- Gồm một chuỗi các thông báo trao đổi giữa client và server
- Mỗi thông báo gồm 3 trường
 - Kiểu (1 byte)
 - Độ dài (3 byte)
 - Nội dung (≥ 0 byte)

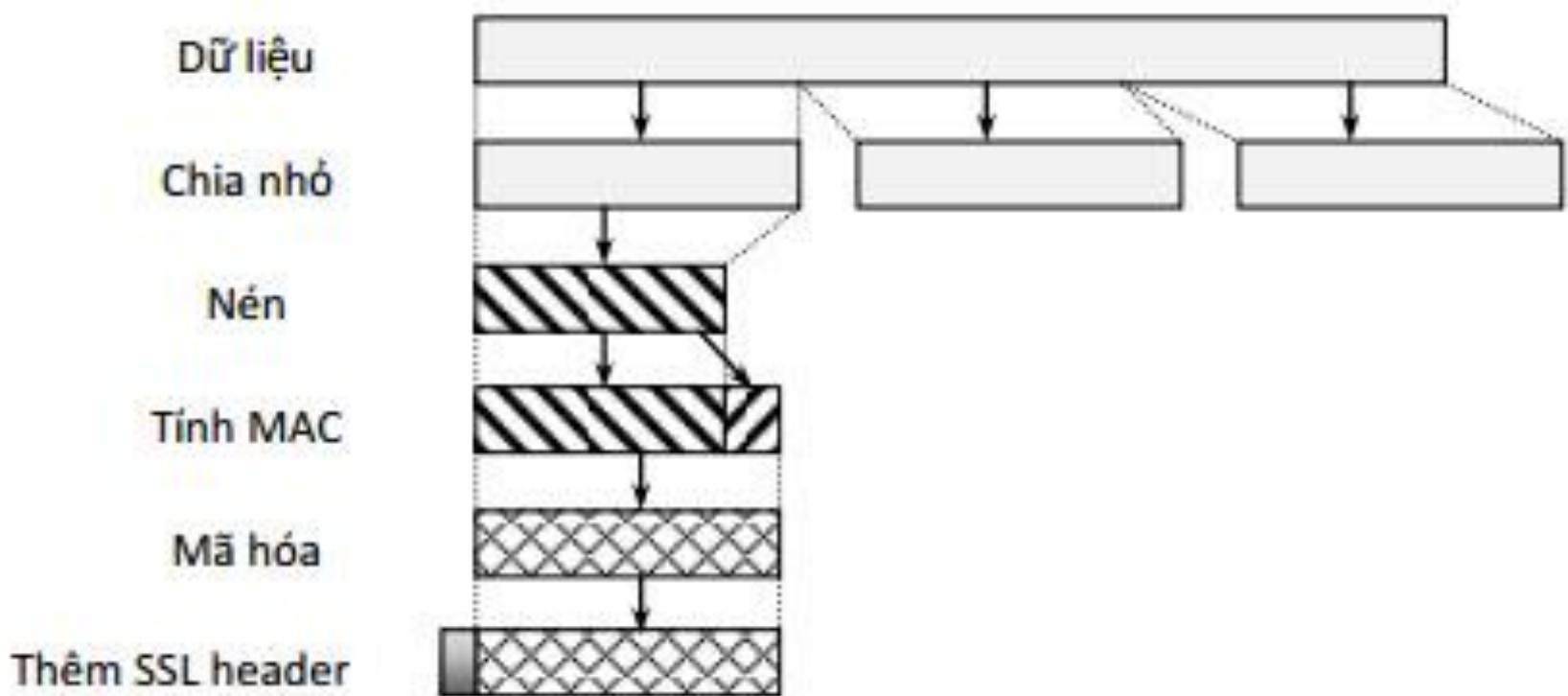




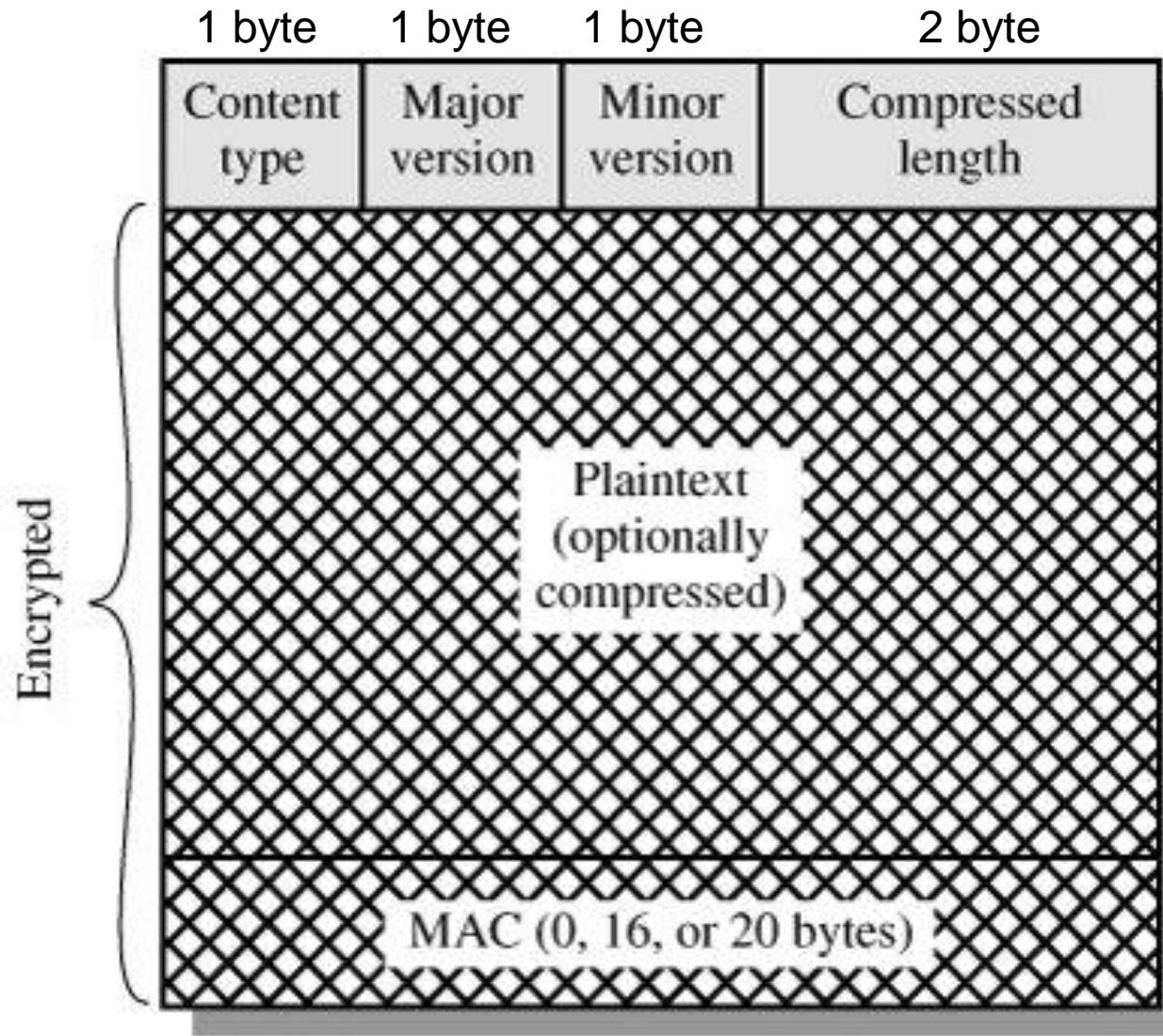
Giao thức bắt tay SSL

Giao thức bản ghi SSL

- Cung cấp các dịch vụ bảo mật và xác thực
 - Khóa bí mật chung do giao thức bắt tay xác lập



Khuôn dạng bản ghi SSL



3. Bảo mật mail PGP

HIENTH

Giới thiệu

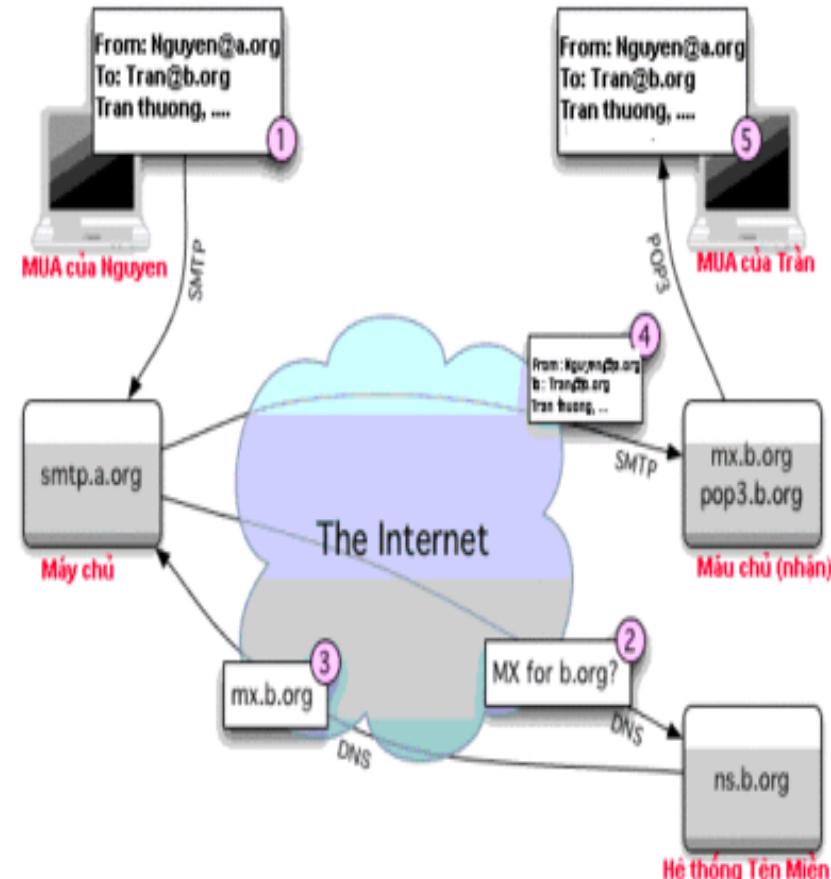
- E-mail là hình thức liên lạc phổ biến, dễ bị tấn công
- Các hình thức quấy nhiễu e-mail:
 - Chặn nhận, đọc, gửi thư
 - Thay đổi, giả mạo nội dung thư
 - Thay đổi, giả mạo địa chỉ gửi thư
 - Thay đổi, giả mạo nội dung thư (lừa đảo)
 - Thay đổi, giả mạo địa chỉ nhận thư
 - Nội dung email chứa virus, worm, trojan
 - Gửi thư rác, quảng cáo, tuyên truyền
 - Tấn công phân phối thư...

Giới thiệu (tt)

- Hiện nay các thông báo không được bảo mật
 - Có thể đọc được nội dung trong quá trình thông báo di chuyển trên mạng
 - Những người dùng có đủ quyền có thể đọc được nội dung thông báo trên máy đích
 - Thông báo dễ dàng bị giả mạo bởi một người khác
 - Tính toàn vẹn của thông báo không được đảm bảo
- Chính sách an ninh e-mail có thể thay đổi, bổ sung hoặc giản lược tùy hệ thống

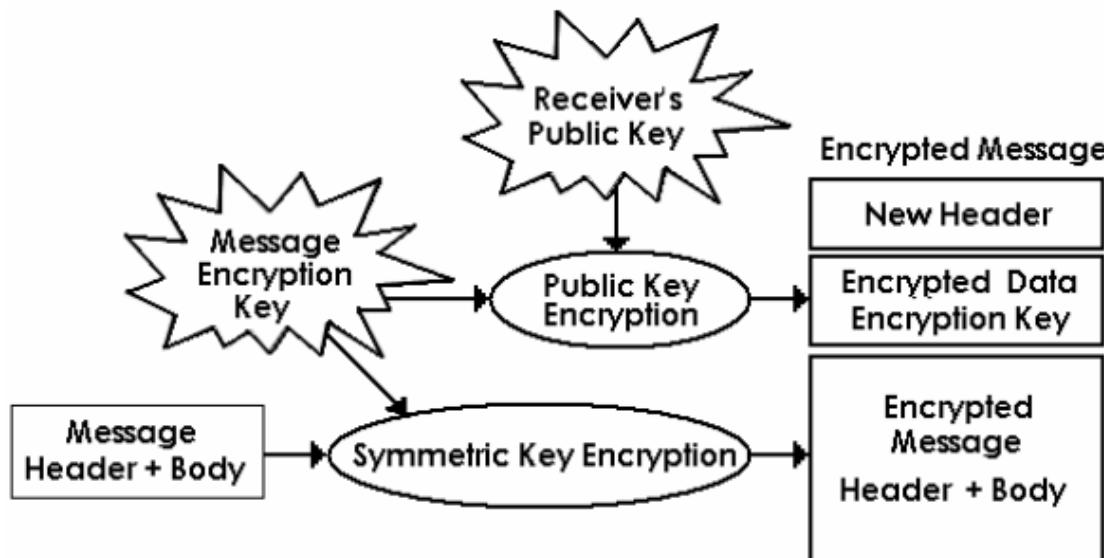
E-Mail

- Kỹ thuật gửi thư điện tử đến SMTP Server
- Có rất nhiều lỗi bảo mật
- Sử dụng giao thức SMTP (TCP 25) để gửi mail
- Sử dụng giao thức POP3/IMAP (TCP 110/143) để nhận mail



An ninh e-mail

- Công tác an ninh e-mail được thực hiện đồng thời và trong suốt đối với user:
 - Khởi tạo: from, to, subject, body...
 - Cấu trúc: header, body, attachment
 - Mật hóa: sử dụng các pp mã (ngẫu nhiên, công khai...)



Đóng gói e-mail

- Mỗi thành phần email được mã hóa theo nhiều thuật toán khác nhau (DES, 3-DES, RSA, AES...)

From noname@net.net
Received: from post.isp.net by mail.pfleeger.com
with SMTP id AA9439; Tue, 22 June 15:14:06 GMT
Date: Tue, 22 Jun 04:12:25 EDT
From: Anonymous <noname@net.net>
To: pfleeger@tisuk.co.uk
Subject: Book example

Proc-Type: 4,ENCRYPTED
DEK-Info: DES-CBC,EE2516152EF97DA2...
Key-Info: RSA,1Bk9ac...

From president@whitehouse.gov
Received: from post.isp.net by mail.pfleeger.com
with SMTP id AA9439; Tue, 22 June 15:14:06 GMT
Date: Tue, 22 Jun 04:12:25 EDT
From: The President <president@whitehouse.gov>
To: pfleeger@pfleeger.com
Subject: Book example

Hope this works as a convincing example of
encrypted e-mail for your book.
We all need security.

Cheers!

--The Prez

Header

Encrypted Message Key

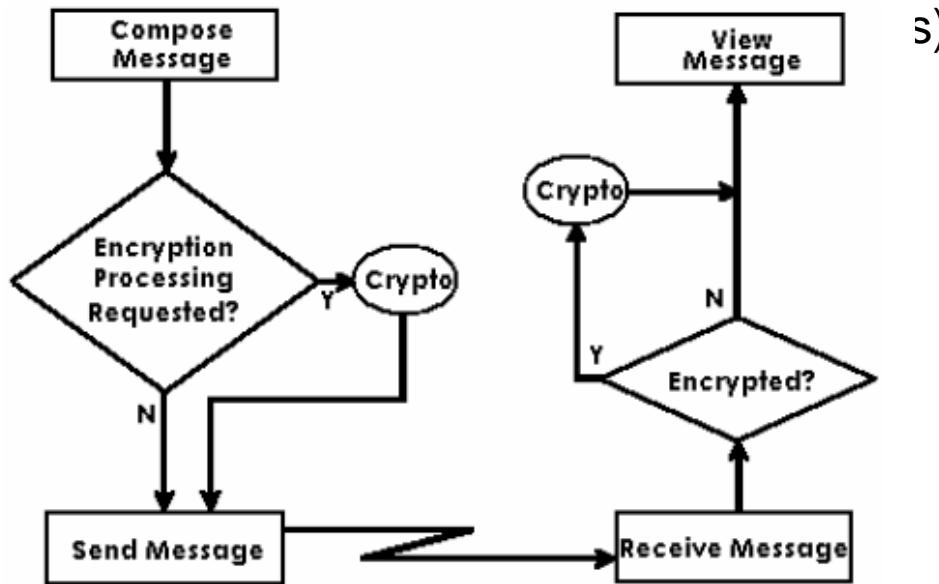
Encrypted Body

Encrypted with Recipient's Public Key

Encrypted with (Random) Message Key

Gửi, nhận e-mail

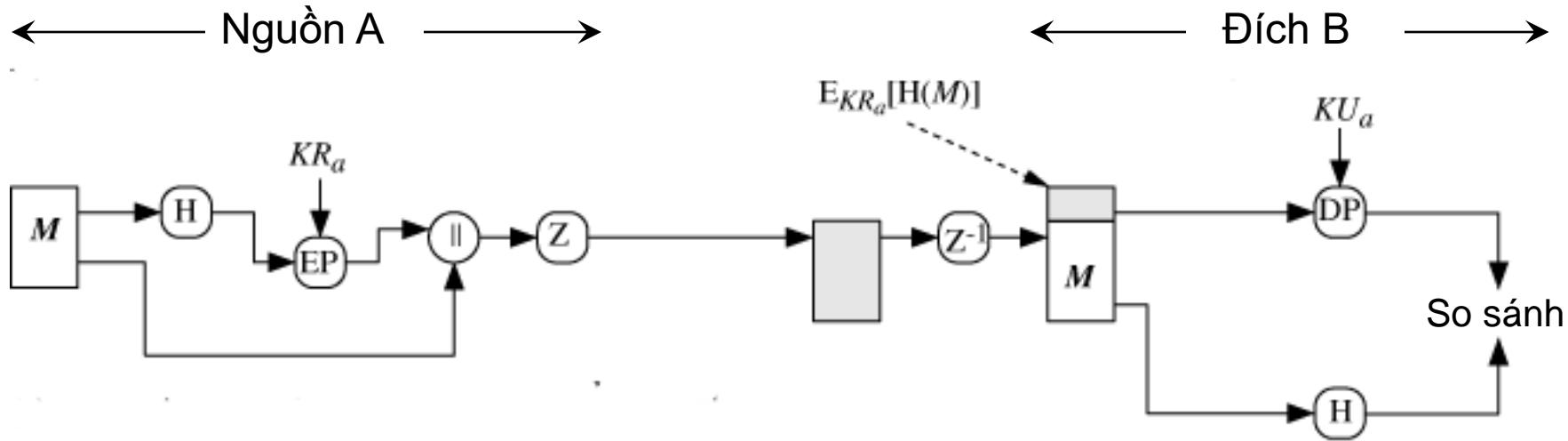
- Trong mô hình OSI, e-mail được chuyển qua mạng dưới dạng các gói tin
- Đến nơi nhận, các gói tin được tích hợp, bóc tách gói, giải mã và tái hiện nội dung email ban đầu
- Các giải pháp xác thực và bảo mật thường dùng
 - PGP (Pretty Good Privacy)
 - S/MIME



PGP (*Pretty Good Privacy*)

- Do Phil Zimmermann phát triển vào năm 1991
- Chương trình miễn phí, chạy trên nhiều môi trường khác nhau (phần cứng, hệ điều hành)
 - Có phiên bản thương mại nếu cần hỗ trợ kỹ thuật
- Dựa trên các giải thuật mật mã an ninh nhất
- Chủ yếu ứng dụng cho thư điện tử và file
- Độc lập với các tổ chức chính phủ
- Bao gồm 5 dịch vụ: **xác thực, bảo mật, nén, tương thích thư điện tử, phân và ghép**
 - Ba dịch vụ sau trong suốt đối với người dùng

Xác thực trong PGP



M = Thông báo gốc

H = Hàm băm

\parallel = Ghép

Z = Nén

Z^{-1} = Giải nén

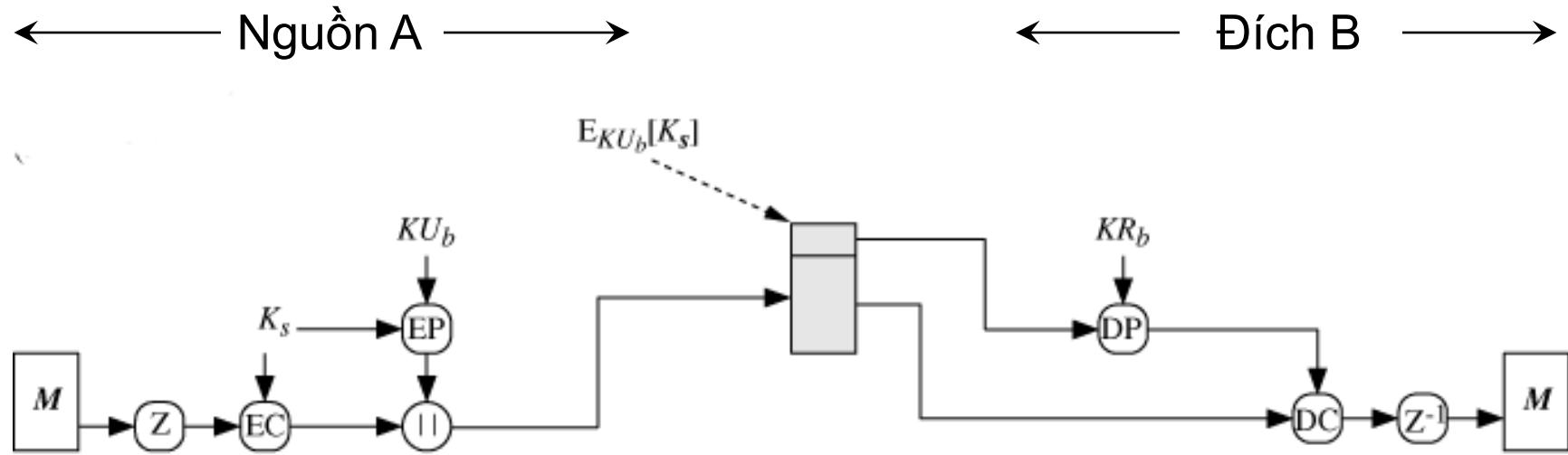
EP = Mã hóa khóa công khai

DP = Giải mã khóa công khai

KR_a = Khóa riêng của A

KU_a = Khóa công khai của A

Bảo mật trong PGP



EC = Mã hóa đối xứng

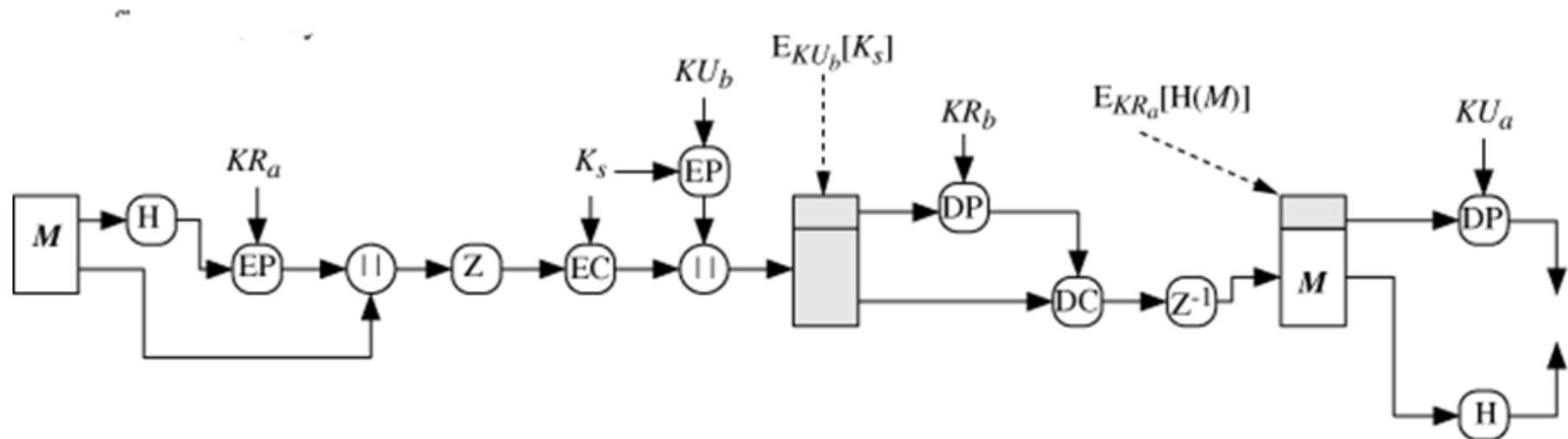
DC = Giải mã đối xứng

K_s = Khóa phiên

Bảo mật và Xác thực trong PGP

Nguồn A

Đích B



Nén của PGP

- PGP nén thông báo sau khi ký nhưng trước khi mã hóa, sử dụng giải thuật ZIP
- Ký trước khi nén
 - Thuận tiện lưu trữ và kiểm tra, nếu ký sau khi nén thì
 - Cần lưu phiên bản nén với chữ ký, hoặc
 - Cần nén lại thông báo mỗi lần muốn kiểm tra
 - Giải thuật nén không cho kết quả duy nhất
 - Mỗi phiên bản cài đặt có tốc độ và tỷ lệ nén khác nhau
 - Nếu ký sau khi nén thì các chương trình PGP cần sử dụng cùng một phiên bản của giải thuật nén
- Mã hóa sau khi nén
 - Ít dữ liệu sẽ khiến việc mã hóa nhanh hơn
 - Thông báo nén khó phá mã hơn thông báo thô

Tương thích thư điện tử của PGP

- PGP bao giờ cũng phải gửi dữ liệu nhị phân
- Nhiều hệ thống thư điện tử chỉ chấp nhận văn bản ASCII (các ký tự đọc được)
 - Thư điện tử vốn chỉ chứa văn bản đọc được
- PGP dùng giải thuật cơ số 64 chuyển đổi dữ liệu nhị phân sang các ký tự ASCII đọc được
 - Mỗi 3 byte nhị phân chuyển thành 4 ký tự đọc được
- Hiệu ứng phụ của việc chuyển đổi là kích thước thông báo tăng lên 33%
 - Nhưng có thao tác nén bù lại

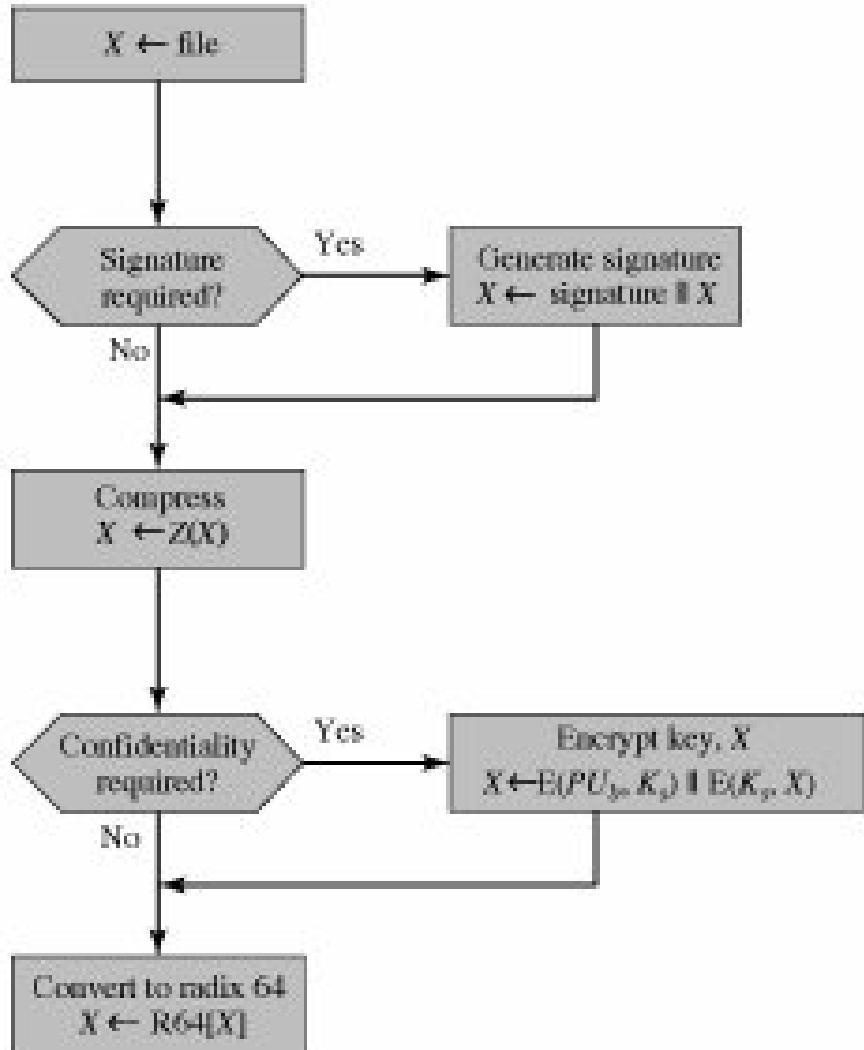
Bảng chuyển đổi cơ số 64

6-bit value	character encoding						
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/
						(pad)	=

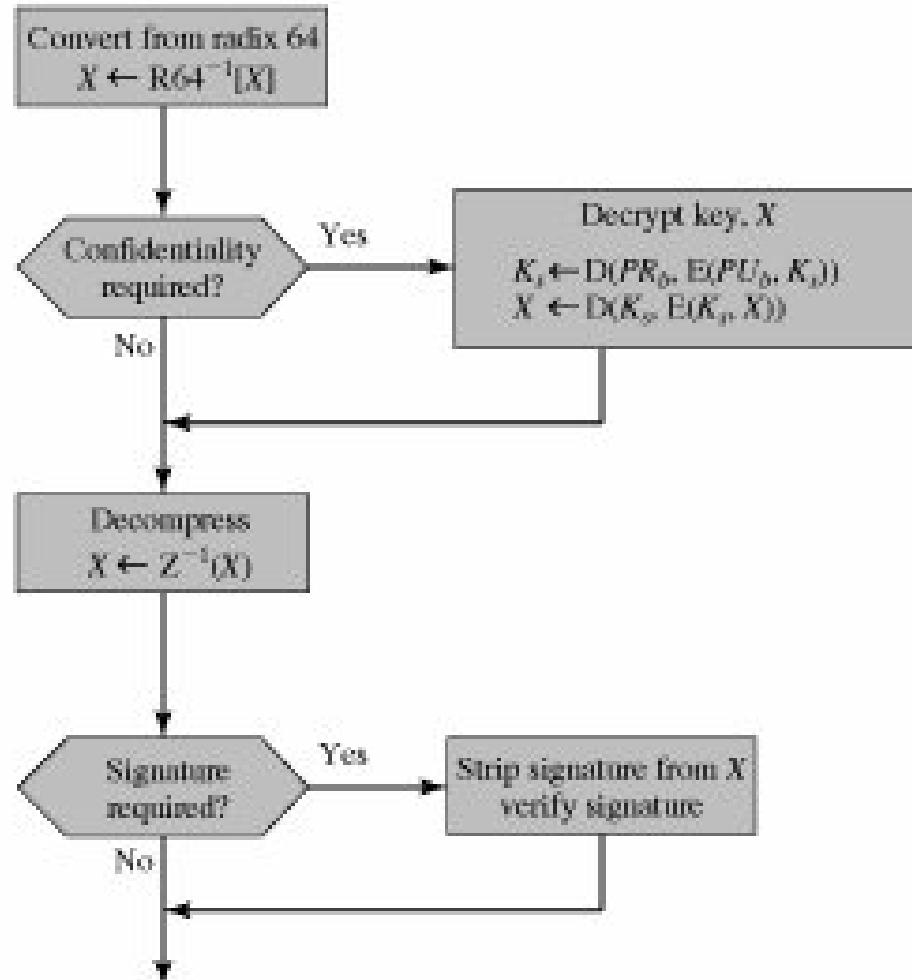
Phân và ghép của PGP

- Các giao thức thư điện tử thường hạn chế độ dài tối đa của thông báo
 - Ví dụ thường là 50 KB
- PGP phân thông báo quá lớn thành nhiều thông báo đủ nhỏ
- Việc phân đoạn thông báo thực hiện sau tất cả các công đoạn khác
- Bên nhận sẽ ghép các thông báo nhỏ trước khi thực hiện các công đoạn khác

Sơ đồ xử lý PGP



(a) Generic transmission diagram (from A)



(b) Generic reception diagram (to B)

Khóa phiên PGP

- Cần sử dụng một khóa phiên cho mỗi thông báo
 - Độ dài 56 bit với DES, 128 bit với CAST-128 và IDEA, 168 bit với 3DES
- Cách thức sinh khóa phiên cho CAST-128
 - Sử dụng chính CAST-128 theo phương thức CBC
 - Từ một khóa 128 bit và 2 khối nguyên bản 64 bit sinh ra 2 khối bản mã 64 bit tạo thành khóa phiên 128 bit
 - Hai khối nguyên bản đầu vào được sinh ngẫu nhiên dựa vào chuỗi các phím gõ từ người dùng
 - Khóa đầu vào được sinh từ các khối nguyên bản đầu vào và khóa phiên đầu ra trước đó

Khóa công khai/khóa riêng PGP

- Người dùng có thể có nhiều cặp khóa công khai/khóa riêng
 - Nhu cầu thay đổi cặp khóa hiện thời
 - Giao tiếp với nhiều nhóm đối tác khác nhau
 - Hạn chế lượng thông tin mã hóa với mỗi khóa để nâng cao độ an toàn
- Cần chỉ ra khóa công khai nào được sử dụng để mã hóa khóa phiên
- Cần chỉ ra chữ ký của bên gửi tương ứng với khóa công khai nào

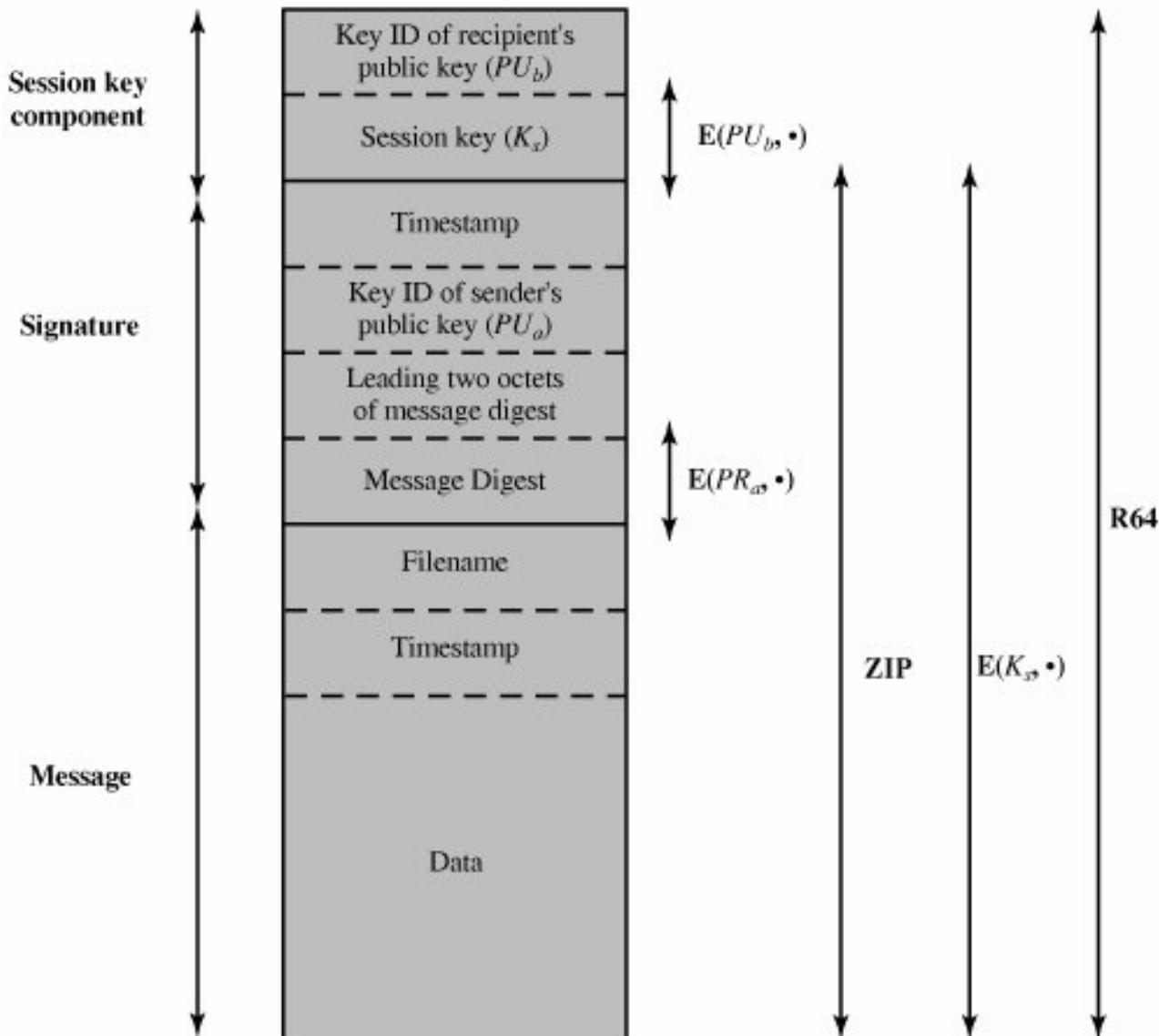
Định danh khóa công khai PGP

- Để chỉ ra mã công khai nào được sử dụng có thể truyền khóa công khai cùng với thông báo
 - Không hiệu quả
 - Khóa công khai RSA có thể dài hàng trăm chữ số thập phân
- Định danh gắn với mỗi khóa công khai là 64 bit trọng số nhỏ nhất của nó
 - ID của $KU_a = KU_a \text{ mod } 2^{64}$
 - Xác suất cao là mỗi khóa công khai có một định danh duy nhất

Khuôn dạng thông báo PGP

Content

Operation



Vòng khóa PGP

- Mỗi người dùng PGP có hai vòng khóa
 - Vòng khóa riêng chứa các cặp khóa công khai/khóa riêng của người dùng hiện thời
 - Có thể được chỉ mục bởi định danh khóa công khai (**Key ID**) hoặc định danh người dùng (**User ID**)
 - Khóa riêng được mã hóa sử dụng khóa là giá trị băm của mật khẩu nhập trực tiếp từ người dùng
 - Vòng khóa công khai chứa các khóa công khai của những người dùng quen biết với người dùng hiện thời
 - Có thể được chỉ mục bởi định danh khóa công khai hoặc định danh người dùng

Cấu trúc các vòng khóa PGP

Private-Key Ring

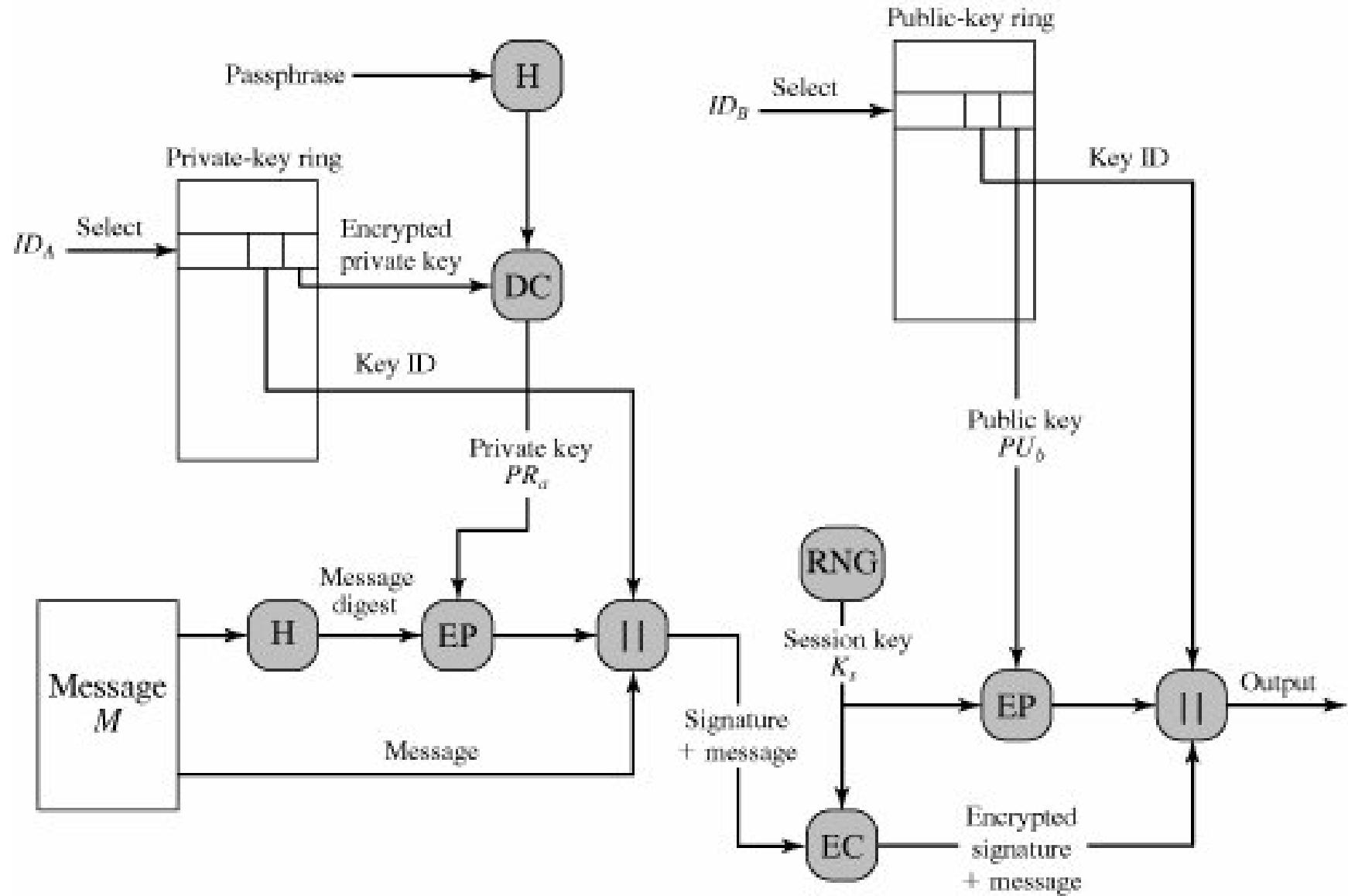
Timestamp	Key ID*	Public Key	Encrypted Private Key	User ID*
•	•	•	•	•
•	•	•	•	•
•	•	•	•	•
T_i	$PU_i \text{ mod } 2^{64}$	PU_i	$E(H(P_i), PR_i)$	User i
•	•	•	•	•
•	•	•	•	•
•	•	•	•	•

Public-Key Ring

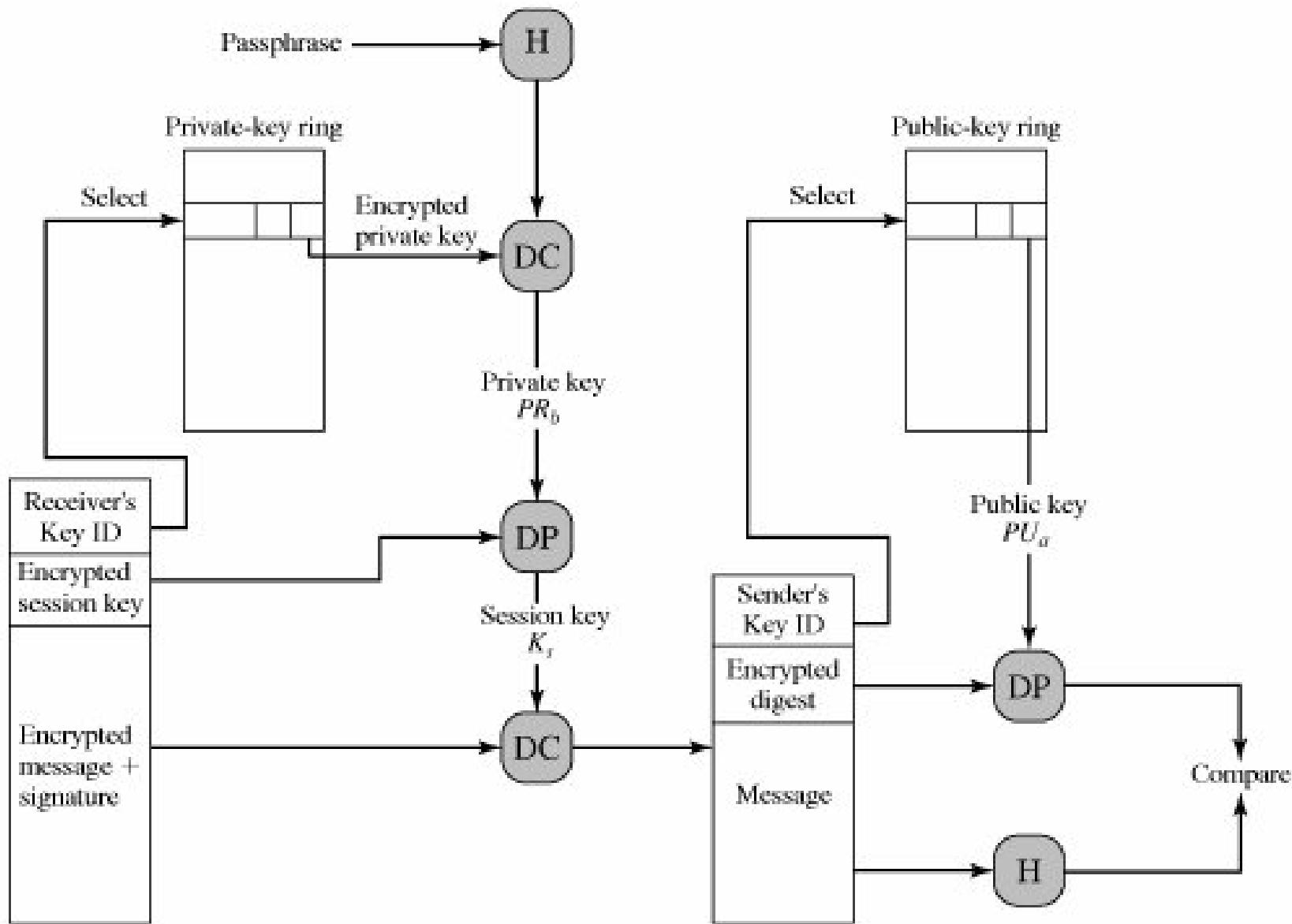
Timestamp	Key ID*	Public Key	Owner Trust	User ID*	Key Legitimacy	Signature(s)	Signature Trust(s)
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•
T_i	$PU_i \text{ mod } 2^{64}$	PU_i	trust_flag_i	User i	trust_flag_i		
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•

* = field used to index table

Sơ đồ tạo thông báo PGP



Sơ đồ nhận thông báo PGP



Quản lý khóa PGP

- Thay vì dựa trên các CA (cơ quan chứng thực), đối với PGP mỗi người dùng là một CA
 - Có thể ký cho những người dùng quen biết trực tiếp
- Tạo nên một mạng lưới tin cậy
 - Tin các khóa đã được chính bản thân ký
 - Có thể tin các khóa những người dùng khác ký nếu có một chuỗi các chữ ký tới chúng
- Mỗi khóa có một chỉ số tin cậy
- Các người dùng có thể thu hồi khóa của họ

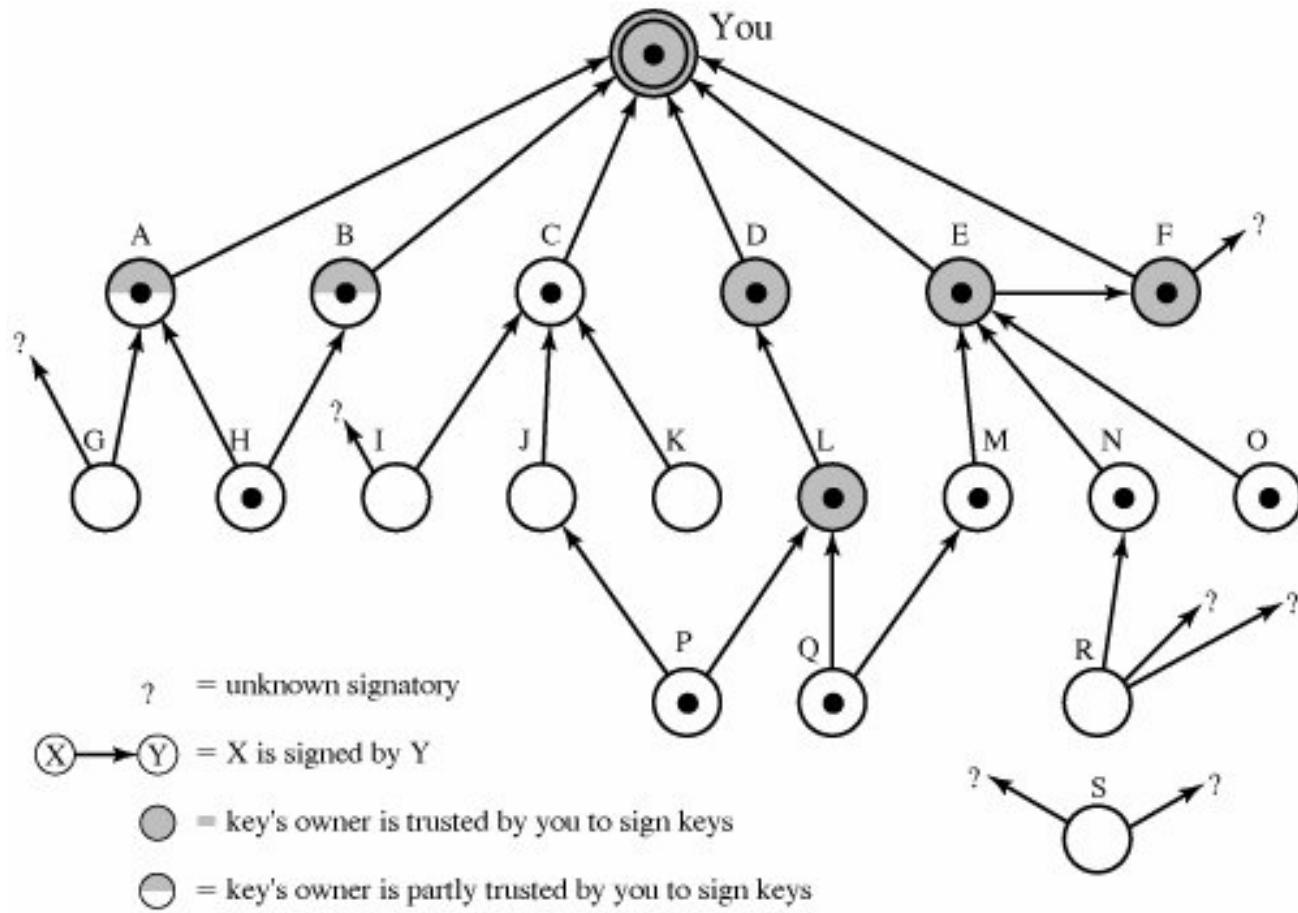
Mô hình tin cậy PGP (1)

- Với mỗi khóa công khai người dùng ấn định độ tin cậy vào chủ nhân của nó trong trường **Owner trust**
 - Giá trị *ultimate trust* được tự động gán nếu khóa công khai có trong vòng khóa riêng
 - Giá trị người dùng có thể gán là *unknown*, *untrusted*, *marginally trusted*, hay *completely trusted*
- Giá trị các trường **Signature trust** được sao chép từ các trường **Owner trust** tương ứng
 - Nếu không có thì được gán giá trị *unknown user*

Mô hình tin cậy PGP (2)

- Xác định giá trị của trường **Key legitimacy**
 - Nếu khóa công khai có ít nhất một chữ ký với giá trị **Signature trust** là *ultimate* thì **Key legitimacy** là *ultimate*
 - Nếu không, **Key legitimacy** được tính bằng tổng có trọng số các giá trị **Signature trust**
 - Các chữ ký *completely trusted* có trọng số là $1/X$
 - Các chữ ký *marginally trusted* có trọng số là $1/Y$
 - X và Y là các tham số do người dùng xác định
 - Nếu tổng số đạt hoặc vượt ngưỡng 1 thì **Key legitimacy** được gán giá trị *complete*

Ví dụ mô hình tin cậy PGP



Thu hồi khóa công khai

- Lý do thu hồi khóa công khai
 - Địch thủ biết nguyên bản khóa riêng
 - Địch thủ biết bản mã khóa riêng và mật khẩu
 - Tránh sử dụng cùng một khóa trong một thời gian dài
- Quy trình thu hồi khóa công khai
 - Chủ sở hữu phát hành chứng thực thu hồi khóa
 - Cùng khuôn dạng như chứng thực bình thường nhưng bao gồm chỉ dấu thu hồi khóa công khai
 - Chứng thực được ký với khóa riêng tương ứng khóa công khai cần thu hồi
 - Mau chóng phát tán chứng thực một cách rộng rãi để các đối tác kịp thời cập nhật vòng khóa công khai

Q & A

