

BÀI 5. CHỮ KÝ SỐ

Bùi Trọng Tùng,
Viện Công nghệ thông tin và Truyền thông,
Đại học Bách khoa Hà Nội

1

1

Nội dung

- Khái niệm cơ bản về chữ ký số
- Một số phương pháp ký số
- Giao thức chữ ký số
- Hạ tầng khóa công khai PKI

2

2

KHÁI NIỆM CƠ BẢN

3

3

Khái niệm – Digital Signature

- Chữ kí số(Digital Signature) hay còn gọi là chữ ký điện tử là đoạn dữ liệu được bên gửi gắn vào văn bản gốc để chứng thực nguồn gốc và nội dung của văn bản
- Yêu cầu:
 - Tính xác thực: người nhận có thể chứng minh được văn bản được ký bởi người gửi
 - Chống từ chối: người gửi không thể phủ nhận được hành động ký vào văn bản
 - Tính toàn vẹn: người nhận có thể chứng minh được không có ai sửa đổi văn bản đã được ký
 - Không thể tái sử dụng: mỗi chữ ký chỉ có giá trị trên 1 văn bản
 - Không thể giả mạo
- Đề nghị của Diffie-Hellman: Sử dụng khóa cá nhân trong mật mã công khai để tạo chữ ký.

4

4

Chữ ký số

- Hàm sinh khóa: $\text{Gen}()$
- Hàm ký $S(\text{sk}, m)$
 - Đầu vào:
 - sk: Khóa ký
 - m: Văn bản cần ký
 - Đầu ra: chữ ký số sig
- Hàm kiểm tra: $V(\text{pk}, m, \text{sig})$
 - Đầu vào:
 - pk: Khóa thẩm tra
 - m, sig
 - Đầu ra: True/False
- Tính đúng đắn: $V(\text{pk}, m, S(\text{sk}, m)) = \text{True}$
- Hàm ký phải có tính ngẫu nhiên
- Bất kỳ ai có khóa sk đều có thể tạo chữ ký
- Bất kỳ ai có khóa pk đều có thể kiểm tra chữ ký

5

5

Tấn công vào chữ ký số

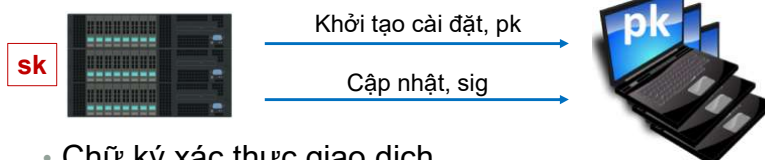
- Kẻ tấn công chọn trước một số bản tin m_1, m_2, \dots, m_q và có chữ ký của bản tin đó $\text{sig}_i \leftarrow S(\text{sk}, m_i)$
- Mục tiêu: Tạo ra chữ ký cho bản tin $m \notin \{m_1, m_2, \dots, m_q\}$
- Yêu cầu đối với chữ ký số: Xác suất tấn công thành công là không đáng kể
- Quiz: Nếu kẻ tấn công tìm được 2 bản tin m_1, m_2 sao cho $V(\text{pk}, m_1, \text{sig}) = V(\text{pk}, m_2, \text{sig}) \forall (\text{sk}, \text{pk})$ thì chữ ký số đó có an toàn không?

6

6

Một số ứng dụng của chữ ký số

- Chữ ký xác thực phần mềm



- Chữ ký xác thực giao dịch



- Chữ ký xác thực thư điện tử: DKIM

• ...

7

7

Khi nào cần sử dụng chữ ký số?

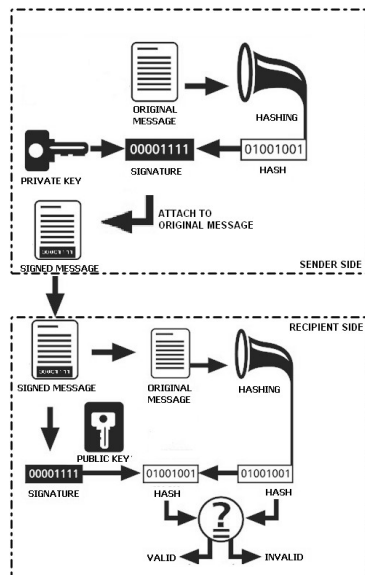
- Nếu 1 bên ký và 1 bên xác thực: sử dụng MAC/HMAC
 - 2 bên cần chia sẻ trước 1 khóa bí mật
 - Không có khả năng chống từ chối: bên nhận có thể thay đổi nội dung và ký lại
- Nếu 1 bên ký và nhiều bên xác thực: sử dụng chữ ký số
 - Bên ký cần công bố khóa công khai của mình
 - Có khả năng chống từ chối

8

8

Chữ ký số dựa trên hàm băm

- **Phía gửi** : hàm ký
 1. Băm bản tin gốc, thu được giá trị băm h
 2. Mã hóa giá trị băm bằng khóa riêng → chữ kí số sig
 3. Gắn chữ kí số lên bản tin gốc (m || sig)
- **Phía nhận** : hàm xác thực
 1. Tách chữ kí số sig khỏi bản tin.
 2. Băm bản tin m, thu được giá trị băm h
 3. Giải mã sig với khóa công khai của người gửi, thu được h'
 4. So sánh : h và h'. Kết luận.



9

Chữ ký số dựa trên hàm băm

- Hàm ký: $\text{sig} = S(\text{sk}, m) = E(\text{sk}, H(m))$
- Hàm xác thực: $V(\text{pk}, m, \text{sig}) = V(\text{pk}, m, E(\text{sk}, H(m)))$

10

10

Một số phương pháp tạo chữ ký số

- Chữ ký số 1 lần: mỗi khóa chỉ dùng để ký 1 bản tin
 - Thuật toán Lamport
- Chữ ký số nhiều lần:
 - Chữ ký số RSA
 - Chữ ký số ElGamal
 - Chuẩn chữ ký số DSS
- Chữ ký mù: người ký không biết nội dung bản tin

11

11

Chữ ký số RSA

- **Sinh** cặp khóa: $k_U = (n, e)$, $k_R = (n, d)$
- **Chữ ký**: $\text{sig} = E(k_R, H(m)) = H(m)^d \bmod n$
- **Thẩm tra**: nếu $H(m) = \underbrace{\text{sig}^e \bmod n}_{D(k_U, \text{sig})}$ thì chấp nhận

12

12

Chuẩn chữ ký số DSS (Đọc thêm)

- Digital Signature Standard
- Các tham số:
 - Hàm băm H
 - L: là bội số của 64, $N \leq$ Kích thước mã băm
- Tạo khóa nhóm $k_{UG} = (p, q, g)$:
 - Số nguyên tố q kích thước N bit
 - Số nguyên p kích thước L bit, sao cho p-1 là bội số của q
 - Chọn h là ngẫu nhiên $2 \leq h \leq p-2$
 - $g = h^{(p-1)/q} \bmod p$
- Khóa riêng: x ngẫu nhiên thỏa mãn $0 < x < q$
- Khóa công khai: $y = g^x \bmod p$

13

13

Chuẩn chữ ký số DSS

- Tạo chữ ký:
 - Chọn giá trị $0 < k < q$ ngẫu nhiên
 - Tính $r = (g^k \bmod p) \bmod q$; nếu $r = 0$ thì chọn lại k
 - Tính $s = [k^{-1} (H(m) + xr)] \bmod q$; nếu $s = 0$ thì chọn lại k
 - Chữ ký (r, s)
- Thẩm tra chữ ký:
 - $w = (s)^{-1} \bmod q$
 - $u1 = [H(m)w] \bmod q$
 - $u2 = rw \bmod q$
 - $v = [(g^{u1}y^{u2}) \bmod p] \bmod q$
 - Nếu $v = r$ thì chữ ký hợp lệ

14

14

An toàn cho chữ ký số

- Tính an toàn của khóa cá nhân
 - Vấn đề: nếu khóa cá nhân bị kẻ tấn công đánh cắp, hắn có thể giả mạo chữ ký của người sở hữu khóa.
 - Giải pháp:
 - Bảo vệ bằng mật khẩu
 - Sử dụng thẻ thông minh(Smart Card)
 - Sử dụng thiết bị lưu trữ an toàn (USB Token)
- Tính tin cậy của khóa công khai.
 - Vấn đề: kẻ tấn công làm sử dụng khóa công khai giả mạo. Nếu người dùng bị đánh lừa, họ sẽ tin cậy vào chữ ký giả mạo
 - Giải pháp: sử dụng hệ thống PKI để phát hành khóa công khai dưới dạng chứng thư số

15

15

Bảo vệ khóa cá nhân(1)

- Khóa cá nhân được đóng gói vào file(ví dụ .pfx), lưu trên thiết bị nhớ thông thường (ổ cứng, USB...)
- File được bảo vệ bởi mật khẩu dạng mã PIN
- Mức an toàn thấp nhất:
 - Dễ dàng sao chép file chứa khóa
 - Mã PIN có thể bị đoán nhận

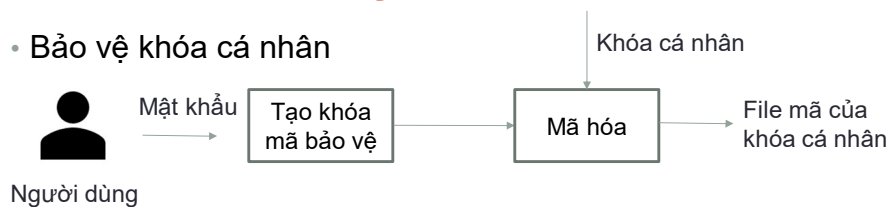


16

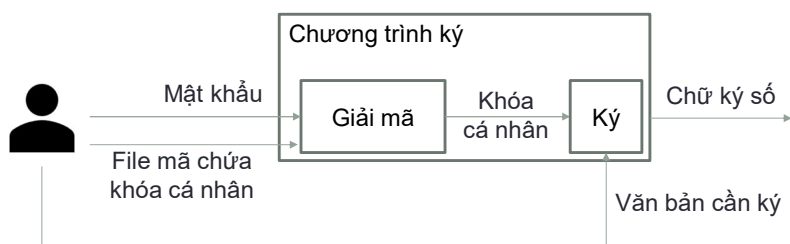
16

Mô hình sử dụng

- Bảo vệ khóa cá nhân



- Sử dụng khóa để tạo chữ ký

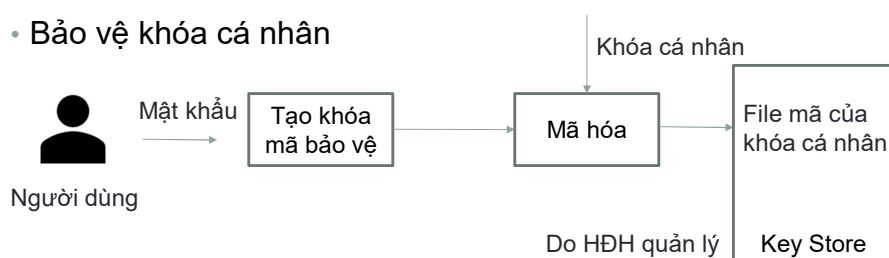


17

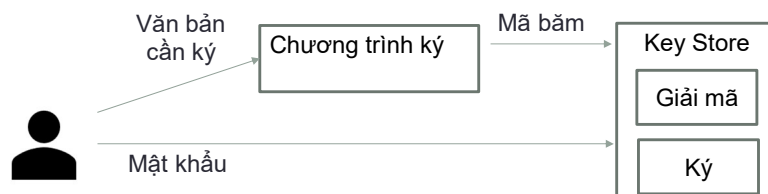
17

Cải tiến

- Bảo vệ khóa cá nhân



- Sử dụng khóa để tạo chữ ký

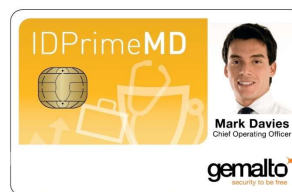


18

18

Bảo vệ khóa cá nhân(2)

- Khóa được lưu trữ trên chip điện tử (IC) của Smart Card
- Khi thực hiện ký số:
 - Giá trị băm được truyền vào chip IC
 - Chip IC mã hóa giá trị băm bằng khóa cá nhân (yêu cầu người dùng nhập mã PIN) → chữ ký số
 - Truyền chữ ký số từ Smart Card tới ứng dụng
- Yêu cầu:
 - Phải có đầu đọc chuyên dụng
 - Thư viện API để giao tiếp

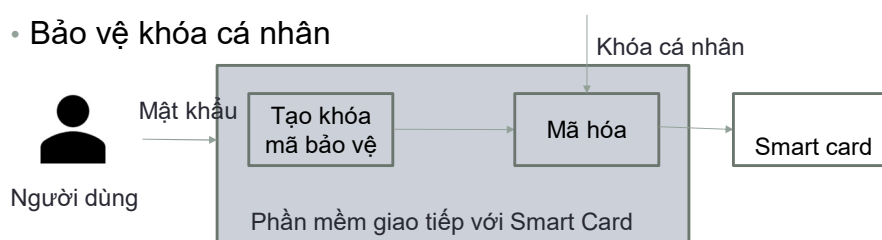


19

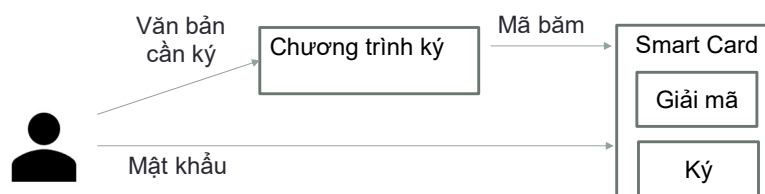
19

Smart card

- Bảo vệ khóa cá nhân



- Sử dụng khóa để tạo chữ ký



20

20

Bảo vệ khóa cá nhân (3)

- Khóa được lưu trữ trong thiết bị nhớ chuyên dụng, sử dụng giao tiếp USB
- Có nhiều mức độ giải pháp khác nhau:
 - Chỉ có chức năng lưu trữ khóa, cho phép ứng dụng truy xuất khóa cá nhân để sử dụng
 - Kịch bản sử dụng tương tự Smart Card
 - Khóa được sinh ngay trên thiết bị



21

21

2. GIAO THỨC CHỮ KÝ SỐ

22

22

Chữ ký điện tử có trọng tài

- Trọng tài (Trent – T) có nhiệm vụ:
 - Áp dụng một số lần kiểm tra lên bản tin, kiểm tra tính toàn vẹn của nội dung và nguồn gốc
 - Kiểm tra nhãn thời gian (timestamp) của bản tin
- (1) $A \rightarrow T: ID_A \parallel E(k_{UB}, m) \parallel S_A(E(k_{UB}, m)) \parallel T_A \parallel S_A(m_{AB})$
 $m_{AB} = ID_A \parallel E(k_{UB}, m) \parallel S_A(E(k_{UB}, m)) \parallel T_A$
 $S_A(E(k_{UB}, m)) = E(k_{RA}, H(\underbrace{E(k_{UB}, m)}_C))$
 $S_A(c) = E(k_{RA}, H(c))$
- (2) $T \rightarrow A: ID_A \parallel E(k_{UB}, m) \parallel S_A(E(k_{UB}, m)) \parallel T_A \parallel S_T(m_{AB})$
 $S_T(m_{AB}) = E(k_{RT}, H(m_{AB}))$
- (3) A gửi cho B bản tin 2

23

23

Chữ ký mù (Blind Signature)

- Một số giao dịch điện tử yêu cầu cần che giấu thông tin cá nhân của các bên tham gia:
 - Thương mại điện tử
 - Bầu cử điện tử
- Chữ ký mù: người ký không biết nội dung của văn bản
 - Người kiểm tra tính hợp lệ của phiếu bầu không được phép biết nội dung của phiếu (tên cử tri, người được cử tri bầu...)
 - Sau khi xác minh và chấp nhận cho khách hàng rút tiền, ngân hàng không thể kiểm tra lại trên tờ tiền điện tử lưu thông có tên người rút là gì.

24

24

Chữ ký mù RSA cho Phiếu bầu điện tử

- Cơ quan bầu cử sử dụng cặp khóa $k_U = (e, n)$, $k_R = (d, n)$
 - Sau khi đã thực hiện xác thực với cơ quan bầu cử, Alice điền thông tin trên phiếu bầu. Thông tin này được ghi lên bản tin x :
 - Chọn 1 giá trị ngẫu nhiên r
 - Làm mù nội dung lá phiếu: $m' = (H(x) \cdot r^e) \bmod n$
 - Đưa cho cơ quan bầu cử ký
 - Cơ quan BC thực hiện ký mù

$$s' = (m')^d \bmod n = ((H(x))^d \cdot r) \bmod n$$
 - Alice xóa mù chữ ký: $s = s' \cdot r^{-1} \bmod n = (H(x))^d \bmod n$
- Lưu ý $1 < r^{-1} < n$ là giá trị sao cho $r \cdot r^{-1} \bmod n = 1$
- Phiếu điện tử của Alice (x, s)
 - Làm thế nào để cơ quan kiểm phiếu tin tưởng đây là phiếu bầu do cơ quan bầu cử phát hành?

Chữ ký
điện tử
của cơ
quan BC
lên X

25

25

Chữ ký mù một phần

- Ngăn chặn người gửi gian lận nội dung
- Giao thức:
 - (1) Alice gửi cho trọng tài n bản tin (đã được làm mù bởi n giá trị ngẫu nhiên khác nhau), trong đó có chứa 1 bản tin cần trọng tài ký
 - (2) Trọng tài yêu cầu Alice gửi k giá trị làm mù bất kỳ
 - (3) Trọng tài kiểm tra tính hợp lệ trong nội dung của k bản tin
 - (4) Nếu k bản tin trên là hợp lệ, trọng tài ký vào "siêu bản tin" được ghép từ $(n-k)$ bản tin còn lại

26

26

Chữ ký nhóm

- Yêu cầu: Chỉ xác thực được chữ ký và nhóm nào ký, không xác định được chính xác người ký
- Giao thức:
 - (1) Người quản trị tạo ra $n \times m$ cặp khóa
 - (2) Người quản trị phân phối cho mỗi thành viên của nhóm m cặp khóa
 - (3) Người quản trị công bố danh sách khóa công khai (thứ tự đã xáo trộn)
 - (4) Khi cần ký, mỗi người lựa chọn 1 khóa cá nhân ngẫu nhiên để ký
 - (5) Người xác thực tìm khóa công khai trong danh sách (3) để xác thực chữ ký

27

27

3. HẠ TẦNG KHÓA CÔNG KHAI

28

28

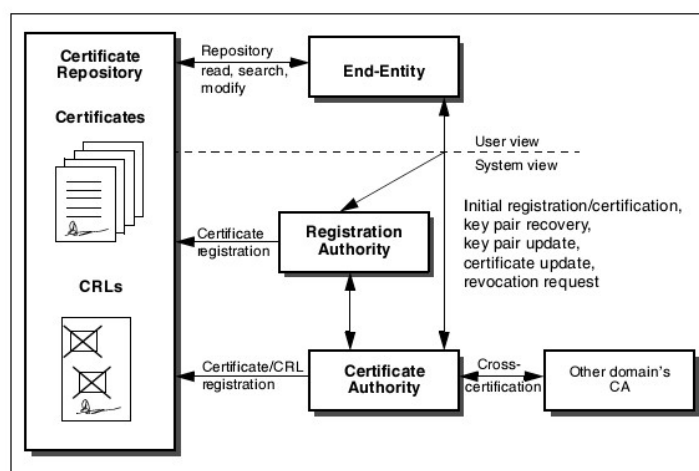
Hạ tầng khóa công khai PKI

- Public Key Infrastructure
- Hệ thống bao gồm phần cứng, phần mềm, chính sách, thủ tục cần thiết để tạo, quản lý và lưu trữ, phân phối và thu hồi các chứng thư số
- Chứng thư số: văn bản điện tử chứng thực khóa công khai
- Các thành phần:
 - RA(Registration Authority): Chứng thực thông tin đăng ký
 - CA(Certification Authority): Phát hành và quản lý chứng thư số
 - CR(Certificate Repository): Lưu trữ, chứng thực chứng thư số
 - EE(End-Entity): đối tượng sử dụng chứng thư số

29

29

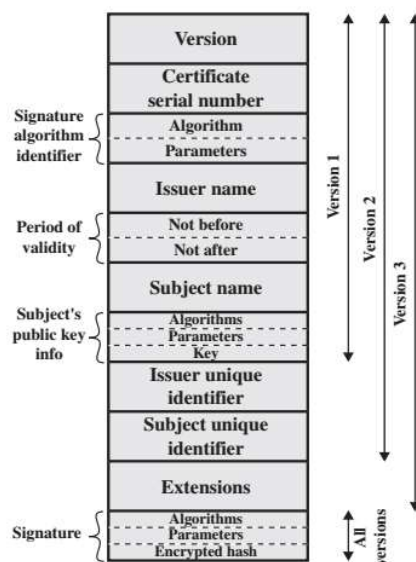
Các thành phần của PKI



30

30

Chứng thư số X.509



31

31

Chứng thư số X.509

- Version: phiên bản của chứng thư số
- Số serial của chứng thư số (tối đa 20 byte)
- Algorithm: Thuật toán chữ ký số được CA sử dụng để ký
- Issuer: Thông tin cơ quan cấp chứng thư số
 - C: Quốc gia
 - CN: Tên giao dịch của CA
 - DN: Tên định danh
 - O: Tên tổ chức phát hành
 - ST: Tên đơn vị hành chính trực thuộc trung ương
- Validity: Thời gian hiệu lực của chứng thư số
 - Not Before: Ngày bắt đầu có hiệu lực
 - Not after: Ngày hết hiệu lực

32

32

Chứng thư số X.509(tiếp)

- Subject: Thông tin người được cấp chứng thư
 - Các trường con tương tự thông tin tổ chức phát hành
- Subject's Public Key Information: Thông tin khóa công khai
 - Algorithm: Thuật toán tạo khóa
 - Public Key: Giá trị khóa
- Signature: chữ ký số của cơ quan cấp chứng thư số
- Issuer UID: định danh của cơ quan cấp chứng thư số
- Subject UID: định danh của người được cấp chứng thư
- Extensions: Các trường mở rộng khác

33

33

Xác thực chứng thư số

Chứng thư số cần được kiểm tra tính tin cậy:

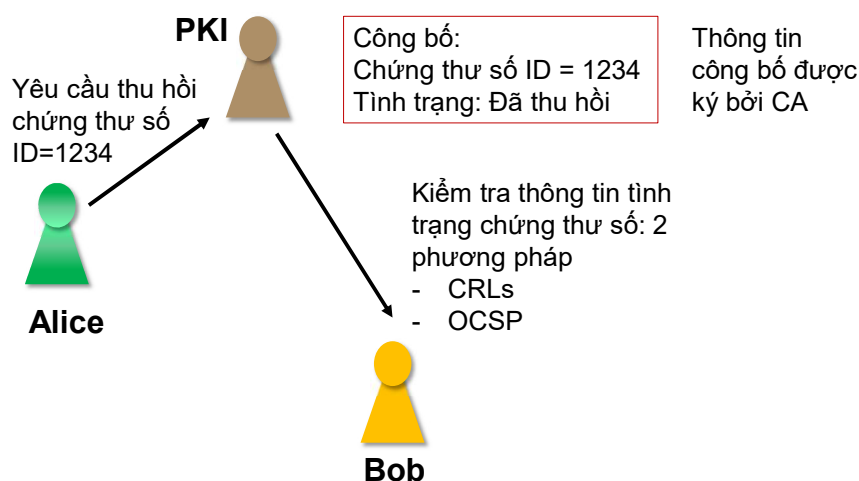
- Kiểm tra tên thực thể sử dụng có khớp với tên đăng ký trong chứng thư số
- Kiểm tra hạn sử dụng của chứng thư số
- Kiểm tra tính tin cậy của CA phát hành chứng thư số
- Kiểm tra trạng thái thu hồi chứng thư số
- Kiểm tra chữ ký trên chứng thư số để đảm bảo chứng thư không bị sửa đổi, làm giả

34

34

Thu hồi chứng thư số

- Thực hiện khi khóa của người dùng mất an toàn

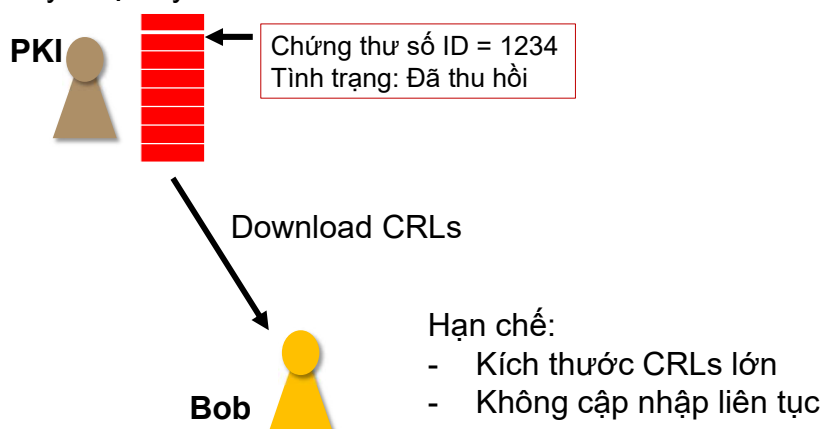


35

35

CRLs

- PKI công bố danh sách chứng thư số bị thu hồi. Danh sách này được ký bởi CA

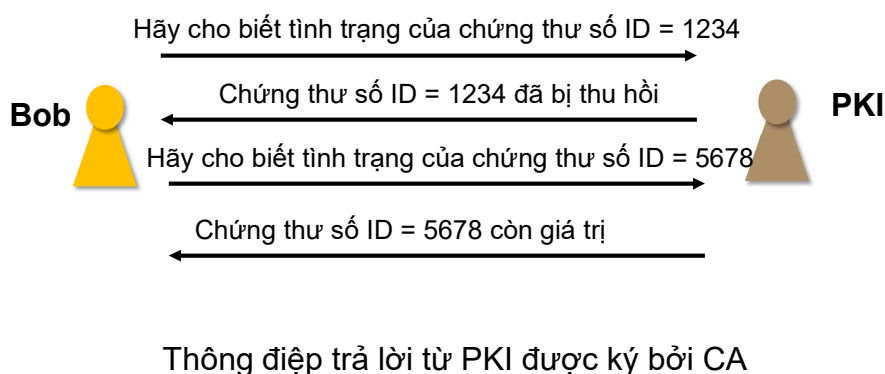


36

36

OCSP

- Dịch vụ kiểm tra trạng thái chứng thư số trực tuyến(Online Certificate Status Protocol)



37

37

Kiến trúc PKI

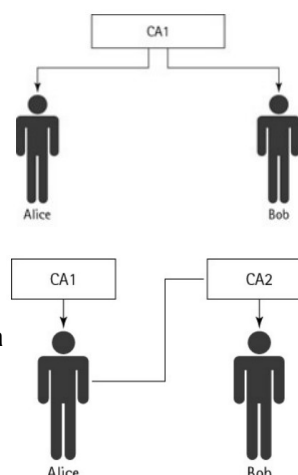
- Kiến trúc PKI rất đa dạng, tương ứng theo mô hình hoạt động của mỗi tổ chức
- Các kiến trúc PKI sau được phân loại dựa trên số lượng CA, tổ chức và mối quan hệ giữa chúng:
 - Kiến trúc đơn CA (Single CA)
 - Kiến trúc PKI xí nghiệp (Enterprise PKI)
 - Kiến trúc PKI lai (Hybrid PKI)

38

38

Kiến trúc đơn CA

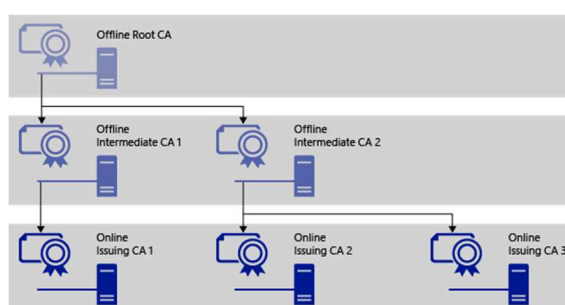
- Chỉ sử dụng 1 CA trong hệ thống PKI
- Đơn giản, phù hợp với hệ thống nhỏ
- Không có khả năng mở rộng
- Mô hình danh sách tin cậy: 2 thực thể sử dụng chứng thư số được phát hành bởi 2 CA khác nhau
 - Mỗi CA có danh sách các CA mà nó tin cậy
 - Mỗi CA phải nằm trong danh sách tin cậy của CA còn lại
 - Hạn chế: Luôn đòi hỏi phải đồng bộ. Ví dụ: 1 CA ngừng hoạt động



39

39

Kiến trúc PKI phân cấp

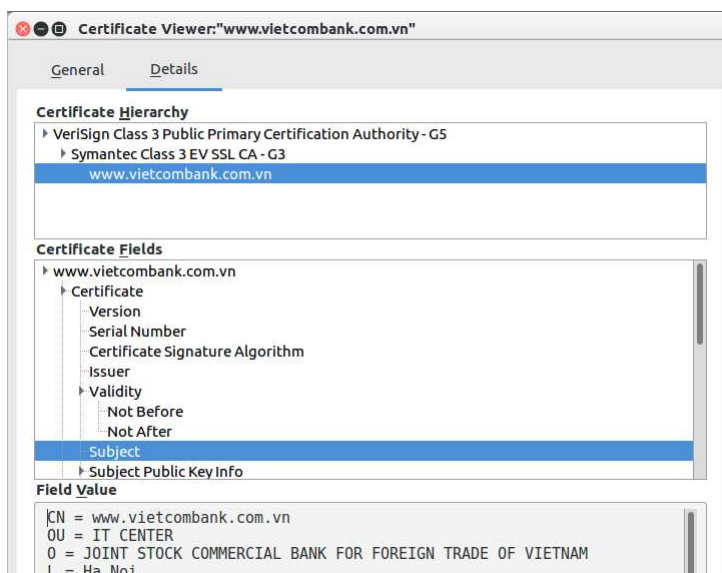


- Mỗi CA chứng thực cho tất cả các CA cấp dưới của nó
- Dễ dàng mở rộng
- Yêu cầu: Root CA cần được giữ an toàn tuyệt đối (thông thường Root CA luôn nằm ở phân vùng mạng offline)

40

40

Chứng thư số trong kiến trúc PKI phân cấp



41

41

Chuỗi xác thực

- Một chứng thư được phát hành bởi hệ thống PKI phân cấp cần được chứng thực theo một chuỗi hướng từ nút gốc tới nút lá trong cây phân cấp
- Ví dụ: Một chứng thư trong kiến trúc phân cấp



"I'm  because I say so!"



"I'm  because  says so"











"I'm  because  says so"

42

42

Chuỗi chứng thực

- ✓  “I’m  because I say so!”
- ✓  “I’m  because  says so”
- ✓  “I’m  because  says so”

Chuỗi xác thực từ chối chứng thư số nếu có bất kỳ bước nào cho kết quả xác thực thất bại

43

43

Tổng kết

- Chữ ký số:
 - Sử dụng hệ mật mã khóa công khai
 - Tạo chữ ký: người gửi dùng khóa cá nhân của mình để mã hóa mã băm của bản tin
 - Xác thực chữ ký: người nhận sử dụng khóa công khai của người gửi để xác thực
 - Cần đảm bảo an toàn cho khóa cá nhân và xác thực khóa công khai
- PKI
 - Phát hành chứng thư số để xác thực khóa công khai của người dùng
 - Chứng thư số X.509: chứa khóa thông tin công khai của người dùng, được xác thực bởi chữ ký số của CA

44

44