



CHỨNG THỰC THỰC THẺ và ĐIỀU KHIỂN TRUY CẬP

(Entity Authentication and Access Control)

Nội dung chính

1. Khái niệm cơ bản
2. Các phương pháp chứng thực và điều khiển truy cập
 1. Chứng thực bằng Password
 2. Chứng thực bằng Challenge-Response
 3. Chứng thực bằng ZERO-KNOWLEDGE
 - Chứng thực bằng Biometrics

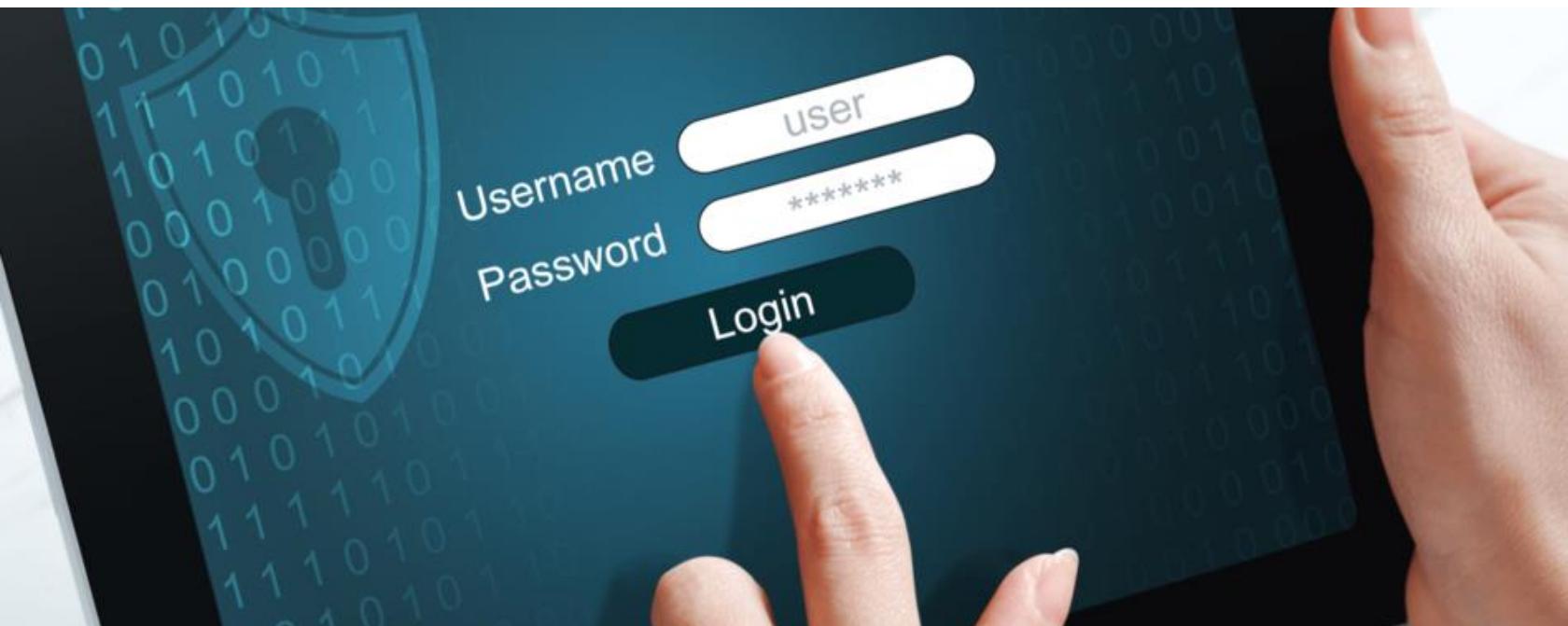
Chứng thực/xác thực

- Chứng thực (Authentication)

- là một hành động nhằm thiết lập hoặc chứng minh một cái gì đó (hoặc một người nào đó) đáng tin cậy, có nghĩa là, những lời khai báo do người đó đưa ra hoặc về vật đó là sự thật.
- một quy trình dùng để xác minh sự nhận dạng của một người dùng, hoặc thông điệp/dữ liệu
- Phải cung cấp một nhân tố nào đó để chứng thực

Chứng thực/xác thực

- **Ví dụ: Web Application Authentication**
 - Nhận dạng bạn là ai
 - Bạn được quyền sử dụng/ truy xuất thông tin dữ liệu nào



Chứng thực/xác thực

- Mobile Connect Authentication

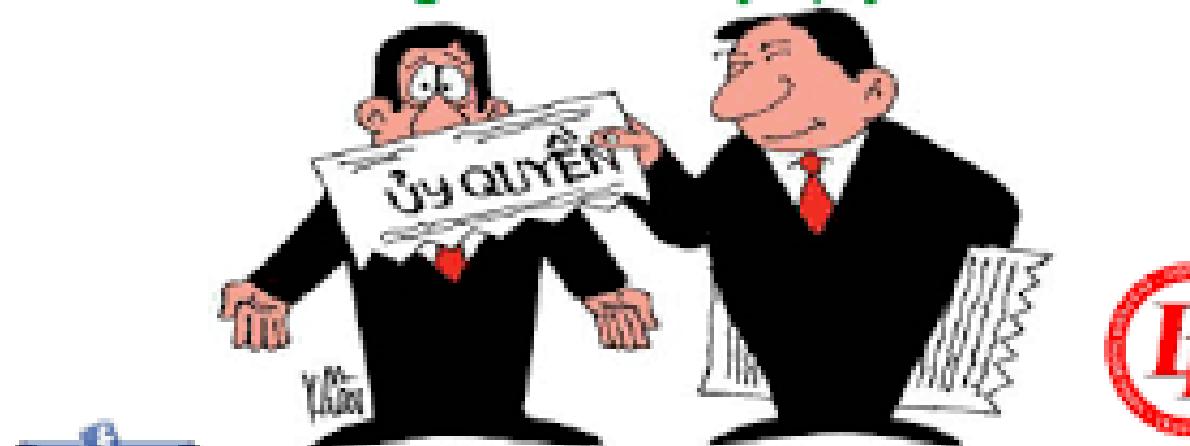


Sự ủy quyền

- **Sự ủy quyền hay sự cấp phép (Authorization)**

- một quy trình nhằm xác minh rằng một người dùng biết trước, có quyền lực để thao tác một quá trình hoạt động nào đó hay không.
- Sự chứng thực phải được tiến hành trước sự ủy quyền

Người ủy quyền có được thực hiện
công việc đã ủy quyền?

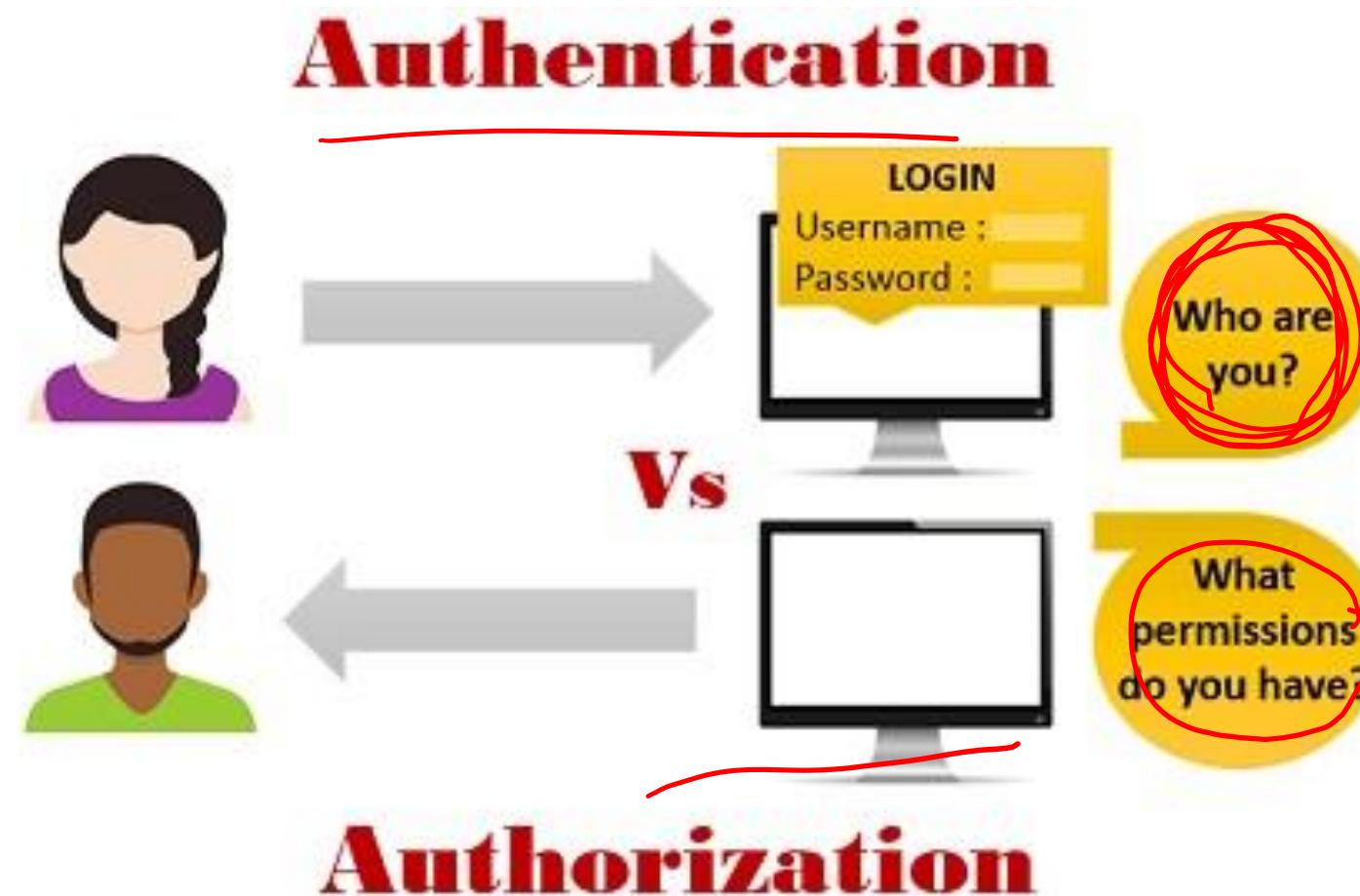


Sự ủy quyền

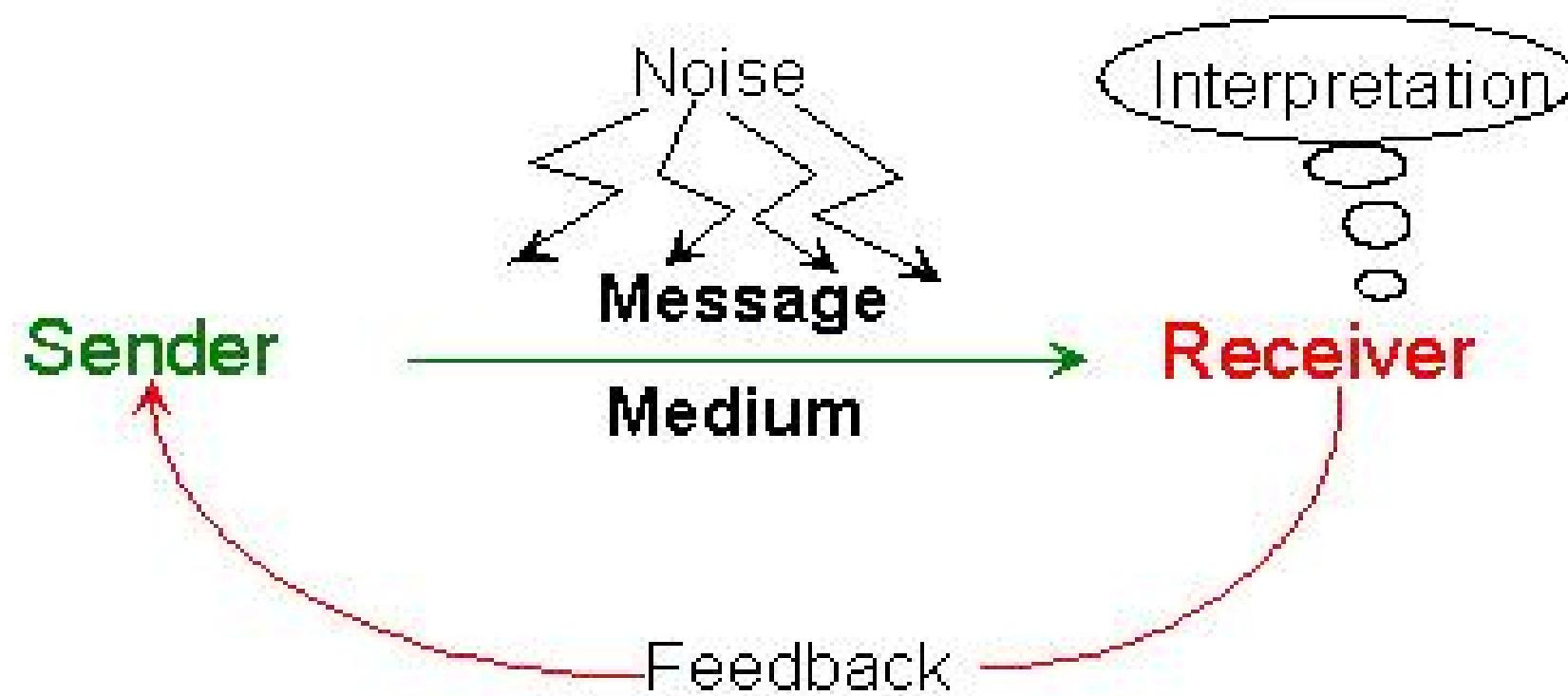
Các quyền:

- Quyền đọc (*Read (R)*)
 - Đọc nội dung của tập tin
 - Liệt kê danh sách thư mục
- Quyền viết (*Write (W)*)
 - Cộng thêm
 - Sinh tạo cái mới
 - Xóa bỏ
 - Đổi tên
- Quyền thi hành (*Execute (X)*): thi hành (chạy) chương trình ứng dụng.

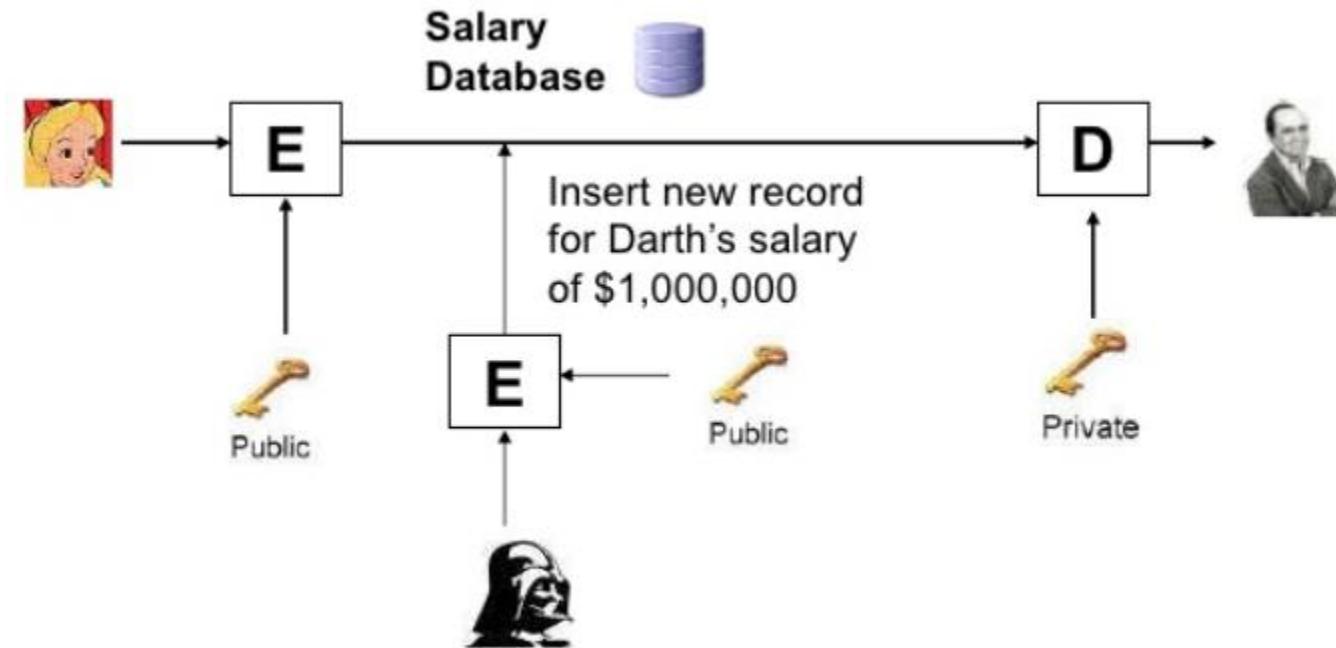
Authetication vs. Authorization



Trao đổi thông điệp

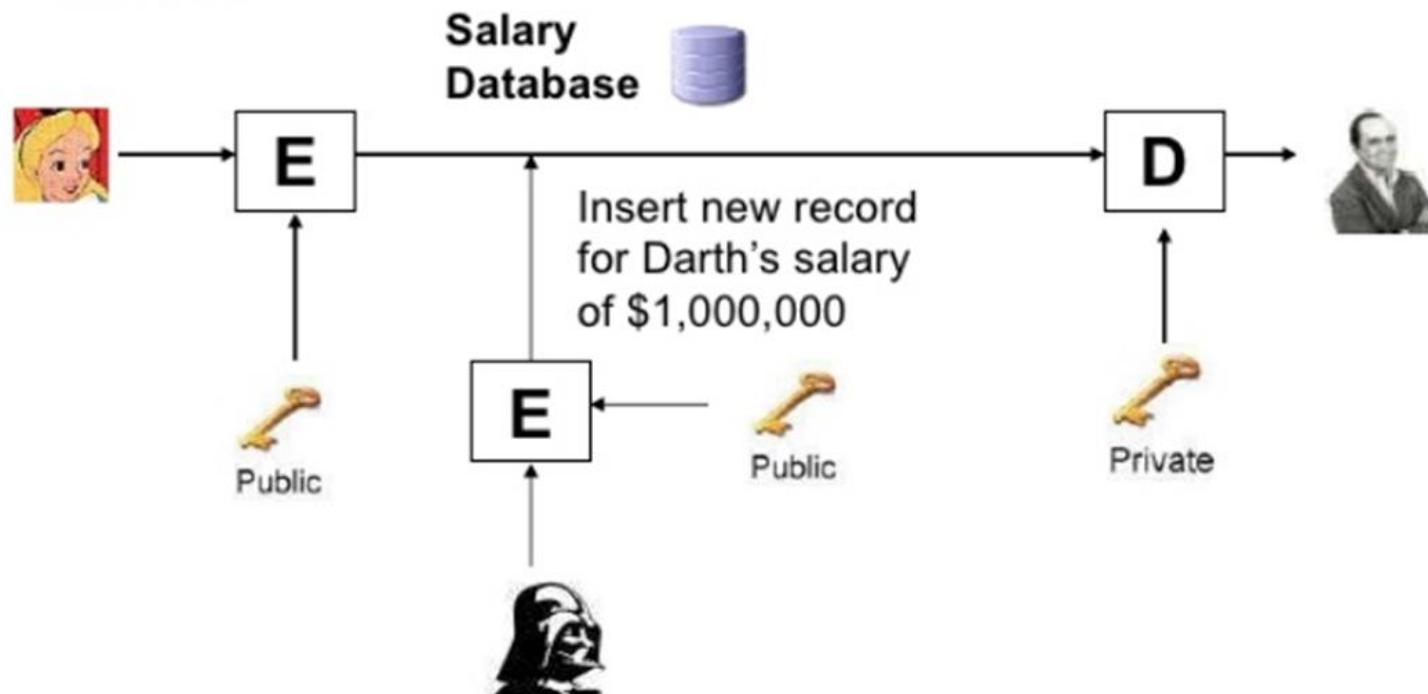


Trao đổi thông điệp



Trao đổi thông điệp

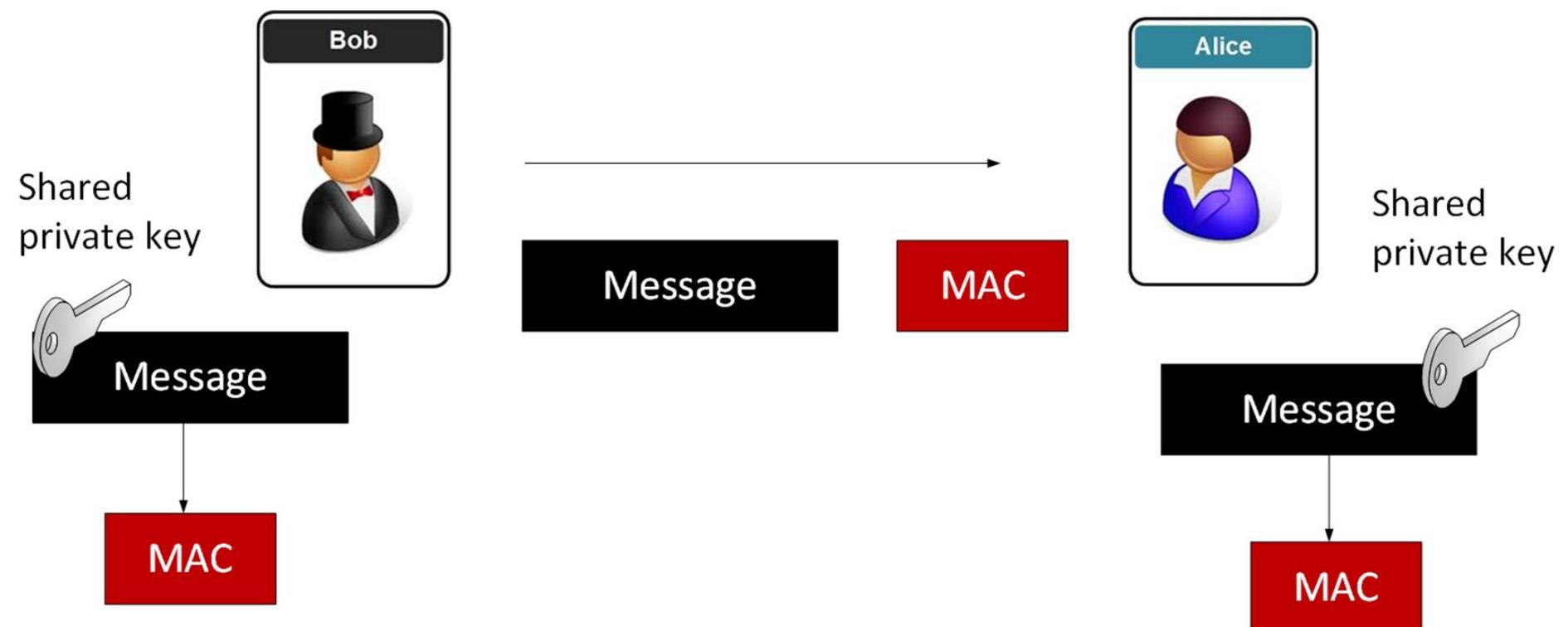
- Vấn đề?



- Cân cát áp

Chứng thực thông điệp

- Chứng thực thông điệp (Message Authentication)
 - Xác thực nguồn gốc thông điệp
 - Xác thực tính toàn vẹn của thông điệp
 - Chống từ chối thông điệp



1. Chứng thực thực thể

- Entity là gì:

Có thể là một con người, tiến trình, client, hoặc một server. Thực thể mà identity cần được chứng minh được gọi là **người yêu cầu (Claimant)**; bên mà cố gắng chứng minh identity của claimant được gọi là **người thẩm định (Verifier)**

1. Chứng thực thực thể

- **Chứng thực thực thể (Entity Authentication):**
 - Là một kỹ thuật được thiết kế cho phép một bên (party) chứng minh sự nhận dạng (identity) của một bên khác.
 - Xác thực thực thể là tạo ra liên kết giữa định danh và đối tượng, thực thể gồm 2 bước
 - Chủ thẻ cung cấp một định danh trong hệ thống
 - Chủ thẻ cung cấp thông tin xác thực có thể chứng minh sự liên kết giữa định danh và chủ thẻ

1. Chứng thực thực thể

Cách Chứng thực thực thể (Entity Authentication):

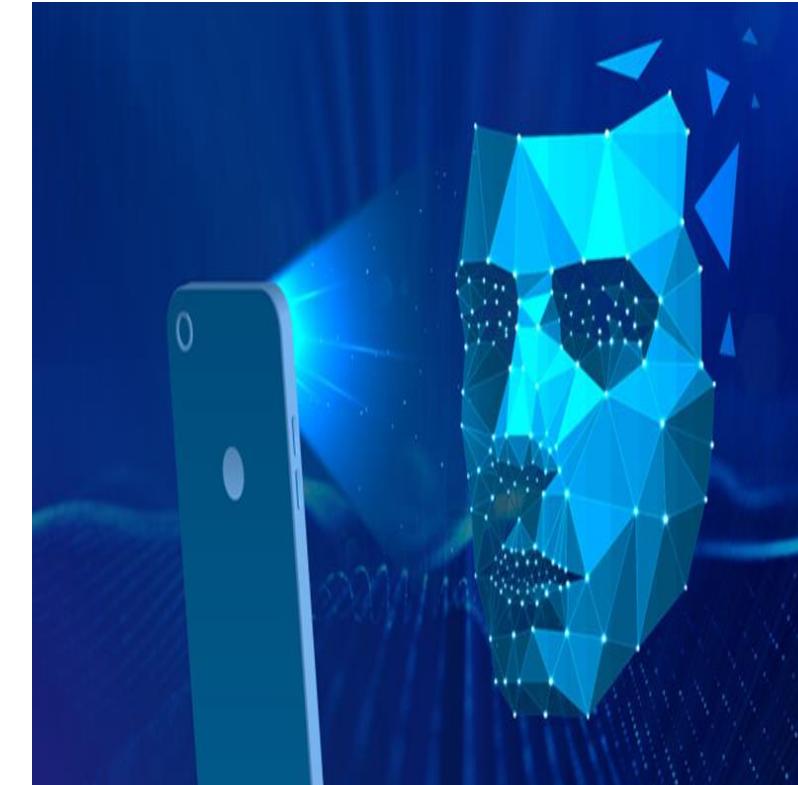
- Chủ thẻ là gì (What the entity is)
- Cái chủ thẻ biết (What the entity knows)
- Cái chủ thẻ có (What the entity has)
- Vị trí của chủ thẻ (Where the entity is)

Các loại vật chứng (Verification Categories)

Claimant có thể trình ra identify của cô ta cho Verifier. Có ba loại vật chứng:

- **Something known**: Là một bí mật chỉ được biết bởi claimant mà có thể được kiểm tra bởi verifier. Ví dụ: Password, Pin, secret key, private key.
- **Something possessed**: là một thứ mà có thể chứng minh nhận dạng của claimant. Ví dụ: passport, bằng lái xe, chứng minh nhân dân, credit card, smart card
- **Something inherent**: là một đặc tính vốn sẵn có của Claimant. Ví dụ: Chữ ký thông thường, vân tay, giọng nói, đặc tính khuôn mặt, võng mạc, và chữ viết tay.

Các loại vật chứng (Verification Categories)



Sự khác biệt

- Chứng thực thông điệp (Message authentication or data-origin authentication):
 - Không cần xảy ra theo thời gian thực; Ví dụ: Alice gửi thông điệp cho Bob, khi Bob chứng thực thông điệp thì Alice có thể không cần phải có mặt ngay trong tiến trình giao tiếp
 - Chứng thực cho từng thông điệp
- Chức thực thực thể (Entity Authentication)
 - Theo thời gian thực. Ví dụ: Alice cần online và tham gia tiến trình giao tiếp, thông điệp chỉ được trao đổi khi được chứng thực
 - Chứng thực trong suốt section

Điều khiển truy cập

- Cấp phép hoặc từ chối phê duyệt sử dụng các tài nguyên xác định.
- Là cơ chế của hệ thống thông tin cho phép hoặc hạn chế truy cập đến dữ liệu hoặc các thiết bị.
- Nhiệm vụ điều khiển truy cập trong an ninh máy tính bao gồm:
 - Nhận diện: Người dùng trình ra các vật chứng để chứng minh sự nhận diện
 - Chứng thực: Kiểm tra, xác minh các ủy quyền
 - Ủy quyền: Cấp các quyền để thực hiện hành động truy cập
 - Truy cập: thực hiện truy xuất các tài nguyên xác định



2. Phương pháp chứng thực và điều khiển truy cập

Mật khẩu (Password)

Sinh trắc học (Biometrics)

2. Dùng mật khẩu (Passwords)

- **Mật khẩu:** một chuỗi ký tự hoặc một nhóm từ được sử dụng để xác thực thực thể
- **Thực thể(entity):** cần xác thực (người dùng, thiết bị, ứng dụng,...)
- **Người thẩm định(Verifier):** kiểm tra tính hợp lệ của mật khẩu

2. Passwords

Một số điểm yếu trên hệ thống xác thực bằng mật khẩu:

- Lưu trữ mật khẩu trong CSDL không an toàn
- Truyền mật khẩu trên kênh không an toàn
 - Người dùng không cẩn trọng
 - Sử dụng mật khẩu yếu
 - Ghi chép mật khẩu vào văn bản
 - Chia sẻ mật khẩu cho người khác (vô tình hay cố ý)

2. Passwords

- **Lưu trữ mật khẩu dưới dạng rõ**
 - Nguy cơ mất an toàn cao nhất
- **Lưu mật khẩu dưới dạng bản mã:**
 - An toàn khi sử dụng hệ mật mã tốt, bảo vệ khóa giải mã an toàn
 - Hạn chế: cần thao tác giải mã bất cứ khi nào cần xác thực
- **Lưu mật khẩu dưới dạng mã băm:**
 - Chi phí thấp hơn
 - Hạn chế: nguy cơ bị tấn công dò đoán dựa trên từ điển. Có thể hạn chế bằng cách đưa thêm “salt” vào mật khẩu trước khi băm
- **Sử dụng máy chủ lưu trữ:**
 - Người thẩm tra yêu cầu máy chủ chuyển mật khẩu để xác thực
 - Người thẩm tra đưa cho máy chủ thông tin người dùng. Máy chủ xác thực và thông báo lại kết quả

2. Passwords

Tấn công vào hệ xác thực bằng mật khẩu

- **Tấn công thụ động:** nghe lén, quan sát quá trình nhập mật khẩu
 - Nhìn trộm
 - Sử dụng chương trình key logging
 - Tấn công kênh bên
 - Chặn bắt gói tin
- **Tấn công chủ động**
 - Giả mạo chương trình cung cấp dịch vụ
 - Giả mạo chương trình khách
 - Tấn công man-in- the – middle
 - Tấn công vào máy chủ vật lý cung cấp dịch vụ

2. Passwords

- Chứng thực mật khẩu là phương pháp đơn giản và lâu đời nhất, được gọi là Password-based Authentication, password là một thứ mà claimant biết.
- Một Password được dùng khi một người dùng cần truy xuất một hệ thống để sử dụng nguồn tài nguyên của hệ thống.
- Mỗi người dùng có một **định danh người dùng (user identification) công khai** và một **password bí mật**.
- Có 2 cơ chế password:
 - **Fixed password**
 - và **one-time password**

2.1 Fixed Password

- Là một password được dùng lặp đi lặp lại mỗi lần truy xuất
- Có 3 cơ chế được xây dựng theo hướng này
 - **User ID và Password File**
 - **Hashing the password**
 - **Salting the password**
 - **Two identification techniques are combined**

2.1 Fixed Password

- User ID và Password File

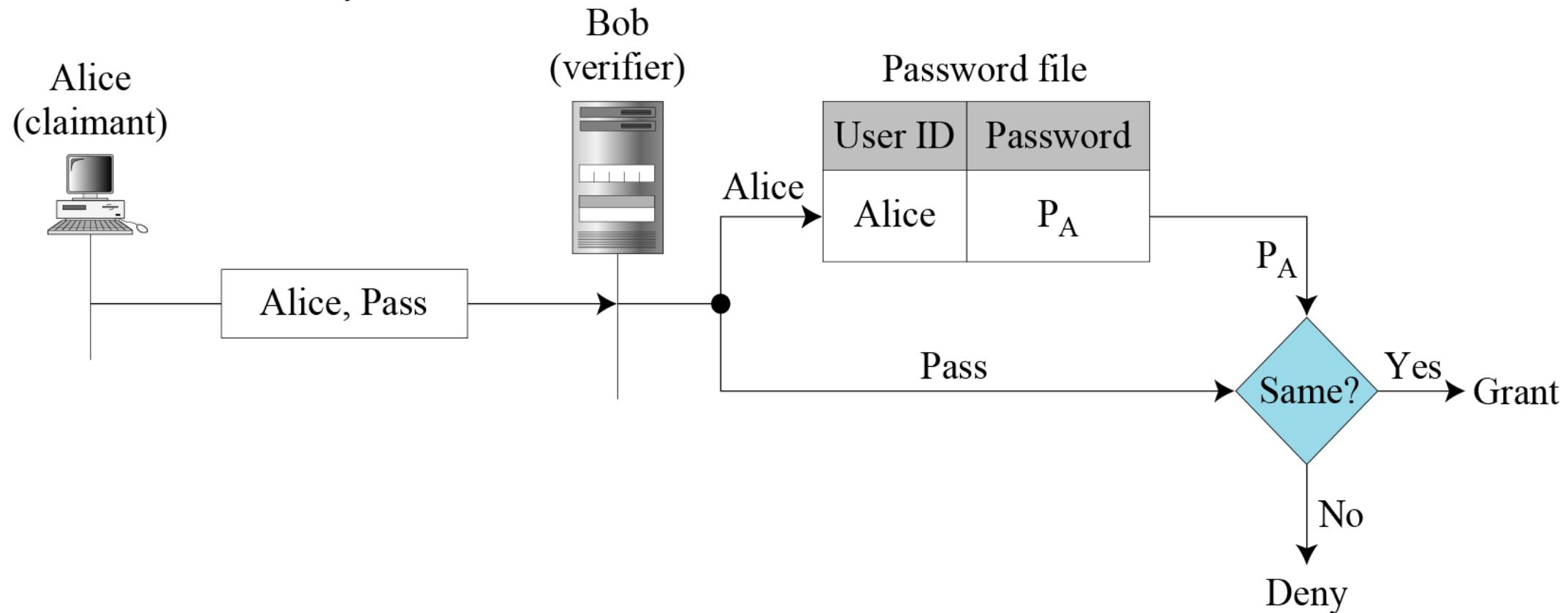
- Rất thô sơ, User ID và Password được lưu trong một tập tin.
- Để truy xuất tài nguyên, người dùng gửi bản rõ của User ID và Password đến hệ thống. Nếu Password trùng khớp với Password trong hệ thống, thì quyền truy xuất được gán ngược lại từ chối.

2.1 Fixed Password

- User ID và Password File

P_A : Alice's stored password

Pass: Password sent by claimant

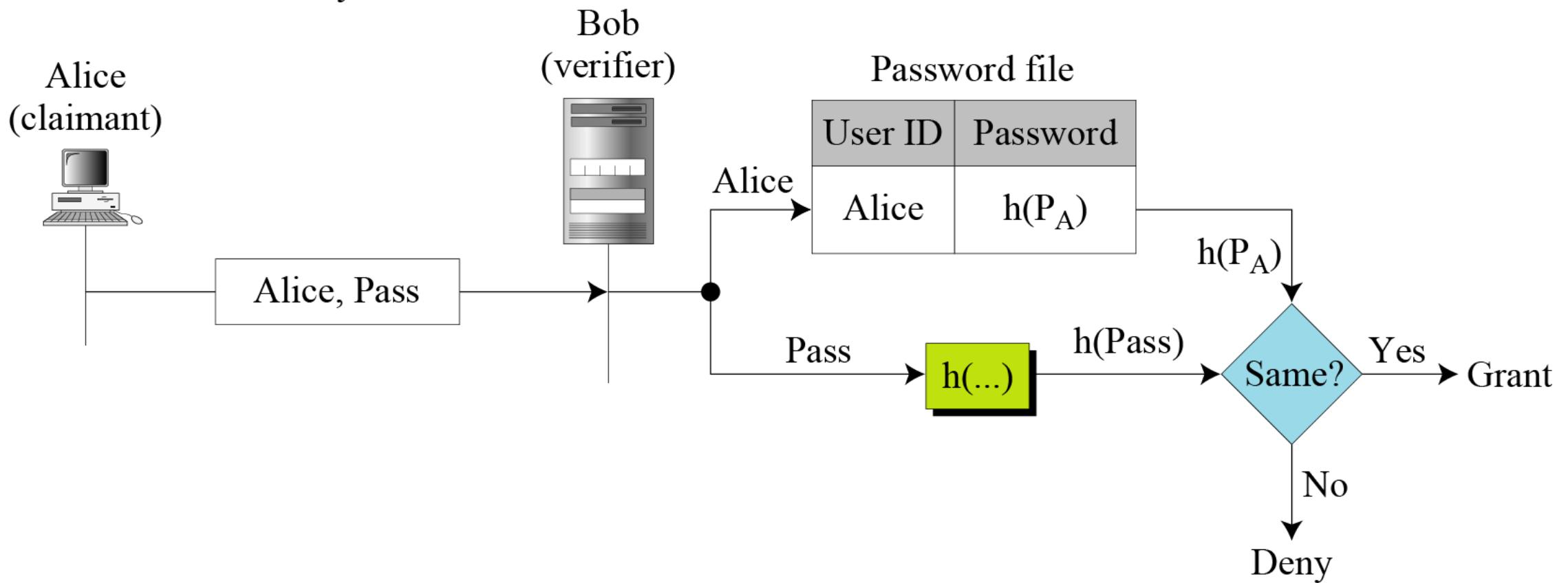


2.1 Fixed Password

- Hashing the password

P_A : Alice's stored password

Pass: Password sent by claimant



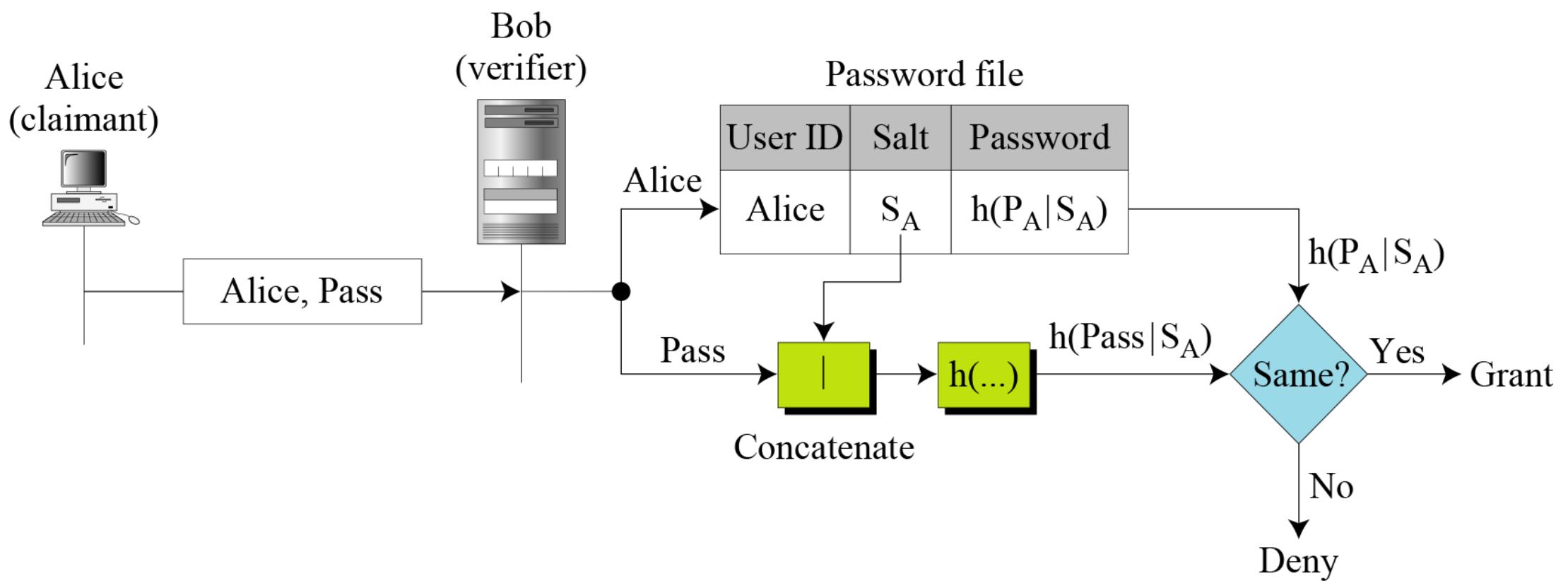
2.1 Fixed Password

- Salting the password

P_A : Alice's password

S_A : Alice's salt

Pass: Password sent by claimant



2.1 Fixed Password

- **Two identification techniques are combined**

A good example of this type of authentication is the use of an ATM card with a PIN (personal identification number).

2.2 One-Time Password

- **One-time Password:**
- Là mật khẩu **sử dụng một lần duy nhất** gồm một dãy các ký tự hoặc chữ số ngẫu nhiên được gửi đến số điện thoại nhằm xác nhận giao dịch.
- Mã OTP được tạo ra dựa trên bộ vi xử lý hoặc thẻ khóa kích thước bờ túi tạo mã số và chữ số để xác thực quyền truy cập vào hệ thống hoặc giao dịch. Sau 30s đến 2 phút, mã này sẽ thay đổi một lần.



2.2 One-Time Password

- Mã OTP có thể được triển khai bằng phần cứng, phần mềm hoặc theo yêu cầu.
- Mã OTP được dùng làm **bảo mật 2 lớp** trong các giao dịch xác minh đăng nhập và đặc biệt là giao dịch với tài khoản ngân hàng, nhờ đó, giảm thiểu tối đa rủi ro bị tấn công khi lộ mật khẩu hay tin tặc tấn công.



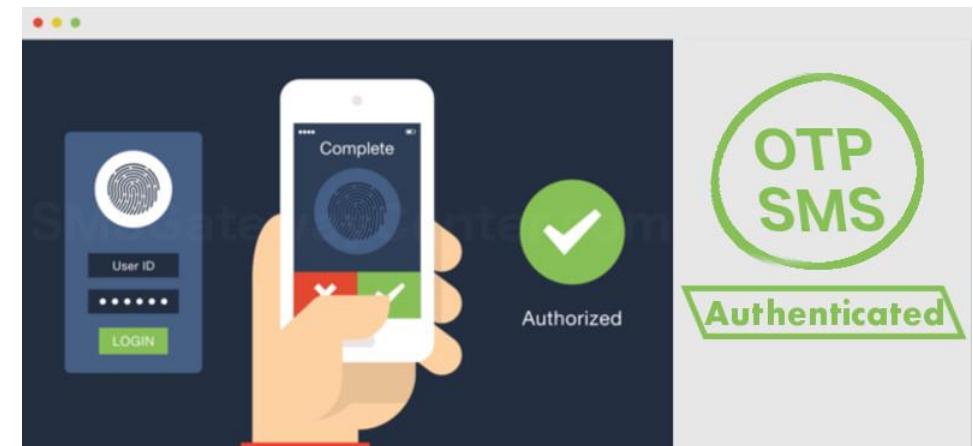
2.2 One-Time Password

Những loại mã OTP phổ biến hiện nay

- SMS OTP
- TOKEN KEY (TOKEN CARD)
- SMART OTP – SMART TOKEN

SMS OTP

- Mã OTP được gửi qua SMS đến số điện thoại của khách hàng khi cần xác thực giao dịch
- Đa số ngân hàng tại Việt Nam: OTP vietcombank, otp techcombank, otp sacombank, otp bidv
- Bạn đang ở trong khu vực sóng kém hoặc ngoài vòng phủ sóng thì bạn không thể nhận được mã SMS OTP → SMS OTP sẽ không sử dụng được.



TOKEN KEY (TOKEN CARD)

- Là thiết bị bảo mật mà doanh nghiệp cung cấp dịch vụ cung cấp cho khách hàng
- Token Key có thể tạo ra **mã OTP gồm 6 ký tự**, cứ sau mỗi phút nó sẽ tự động được tạo ra mà không cần thông qua Internet.
- Mỗi tài khoản phải đăng ký riêng một Tokey key, và thông tin về Token key được thay đổi sau một khoảng thời gian quy định.
- Loại thiết bị này cực kỳ tiện lợi khi luôn mang theo bên người. Tuy nhiên, bạn cần phải bảo quản thật cẩn thận.



SMART OTP

- Smart OTP là dạng OTP tốt nhất hiện nay
- Smart OTP là sự kết hợp hài hòa giữa Token Key và SMS OTP.
- Smart OTP có thể được sử dụng mọi lúc mọi nơi vì nó được tích hợp sẵn trên ứng dụng của điện thoại. Khi có phiên giao dịch trực tuyến thì Smart OTP sẽ được gửi về ứng dụng trên smartphone.
- Hai ngân hàng đã sử dụng cách thanh toán tiền Online bằng phương thức Smart OTP và SMS OTP là Vietcombank và TPBank. Người dùng phải kê khai thông tin và đăng ký trực tiếp với ngân hàng họ muốn. Lưu ý, mỗi thiết bị chỉ nên dùng 1 mã OTP riêng biệt.

Mã OTP có thực sự an toàn?

- Mã OTP là lớp bảo mật cuối cùng trước khi hoàn tất giao dịch. Do đó, phải cẩn thận kiểm tra lý do và số tiền (nếu có trong tin nhắn xác thực giao dịch) trước khi nhập mã OTP.
- Với SMS OTP, khi mất điện thoại, bạn cần phải báo ngay cho ngân hàng để khóa tạm thời tính năng này. Với Token, bạn phải luôn mang theo nó bên mình và đặt mật khẩu có tính phức tạp và lưu giữ để phòng khi quên.
- Mã OTP sẽ an toàn tuyệt đối nếu như bạn tuân thủ đúng các nguyên tắc cũng như quy trình sử dụng dịch vụ Internet Banking mà ngân hàng đưa ra.

2.2 One-Time Password

Có 3 hướng triển khai mã OTP

Hướng 1: User và System **thỏa thuận một danh sách các Password**

- Mỗi Password trong danh sách được dùng một lần
- System và User phải giữ gìn danh sách Password
- Nếu User không dùng các password một cách tuần tự thì System phải thực hiện tìm kiếm và so khớp
- Password chỉ hợp lệ một lần và không sử dụng lại

2.2 One-Time Password

Hướng 2: User và System thỏa thuận cập nhật một cách tuần tự Password

- User và System thỏa thuận một Password gốc, P_1 mà Password này chỉ hợp lệ cho lần đầu tiên truy suất.
- Trong quá trình truy xuất lần đầu tiên này, user phát sinh một password mới P_2 , và mã hóa password này với khóa là P_1 , P_2 là password cho lần truy xuất kế tiếp và cứ thế tiếp tục phát sinh P_{i+1} từ P_i cho lần truy xuất thứ P_{i+1}
- Nếu đối phương đoán ra được P_1 thì có thể tìm được tất cả các Password khác

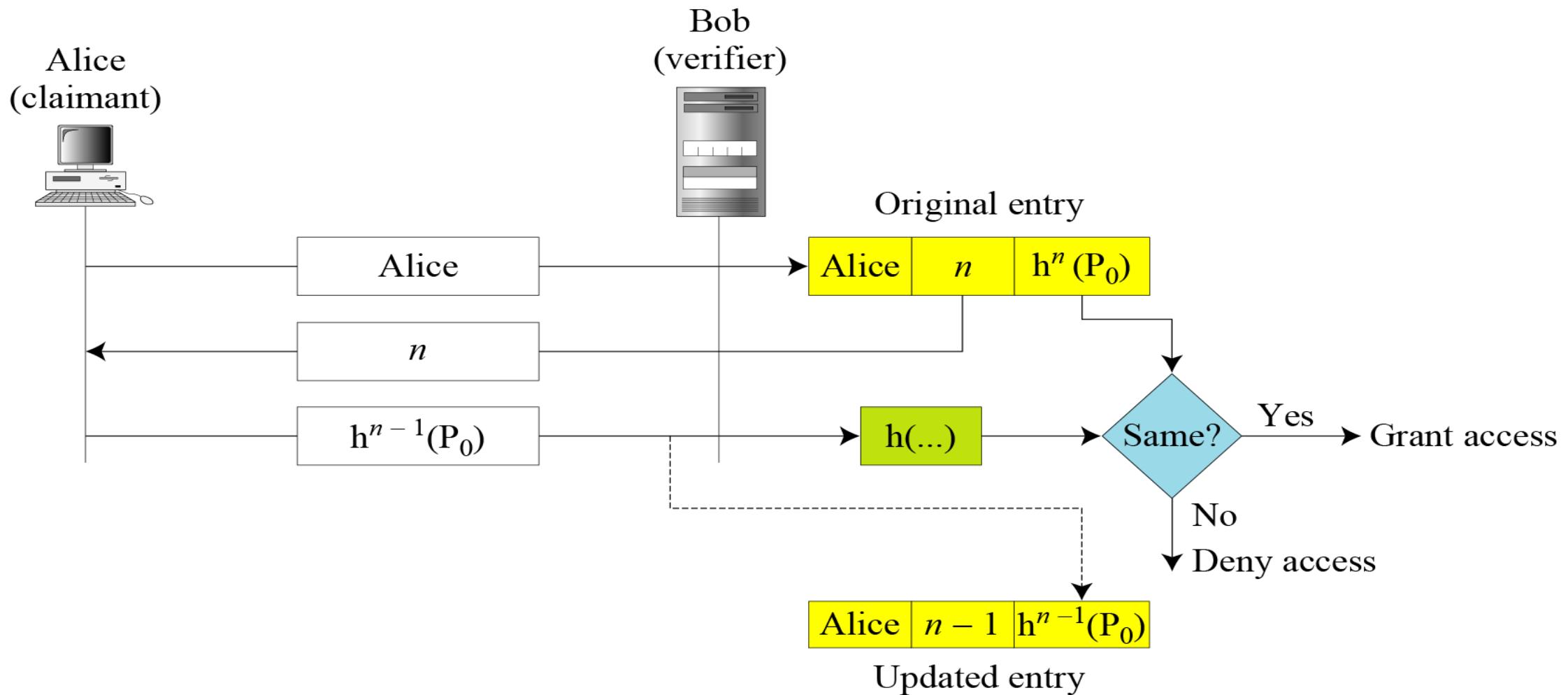
2.2 One-Time Password

Hướng 3: User và System tạo ra **một Password được cập nhật một cách tuần tự sử dụng hàm băm.**

- Hướng này được đề xuất bởi Leslie Lamport
- User và System đồng thuận một Password gốc, P_0 và số đếm n. System tính $h^n(P_0)$ với h^n được áp dụng hàm băm lần thứ n
 - $h^n(x)=h(h^{n-1}(x)), h^{n-1}(x)=h(h^{n-2}(x)), \dots, h^2(x)=h(h(x)), h^1(x)=h(x)$
- System lưu nhận dạng của user thông qua giá trị n và giá trị $h^n(P_0)$

2.2 One-Time Password

- Lamport one-time password



3. Challenge-Response

- Dùng chứng thực bằng Password, để chứng minh nhận dạng Claimant cần trình ra password bí mật, tuy nhiên password này có bị tiết lộ
- Với chứng thực bằng Challenge-response, **claimant chứng minh rằng cô ta biết một bí mật (secret) mà không cần gửi chúng đi.** Nói cách khác, claimant không cần gửi bí mật cho verifier, verifier hoặc có hoặc tự tìm ra chúng
- **Challenge là một giá trị biến đổi theo thời gian được gửi bởi Verifier, Response là kết quả của một hàm được áp dụng trên challenge**

3. Challenge-Response

Có 3 hướng chính để tạo nên Challenge-response

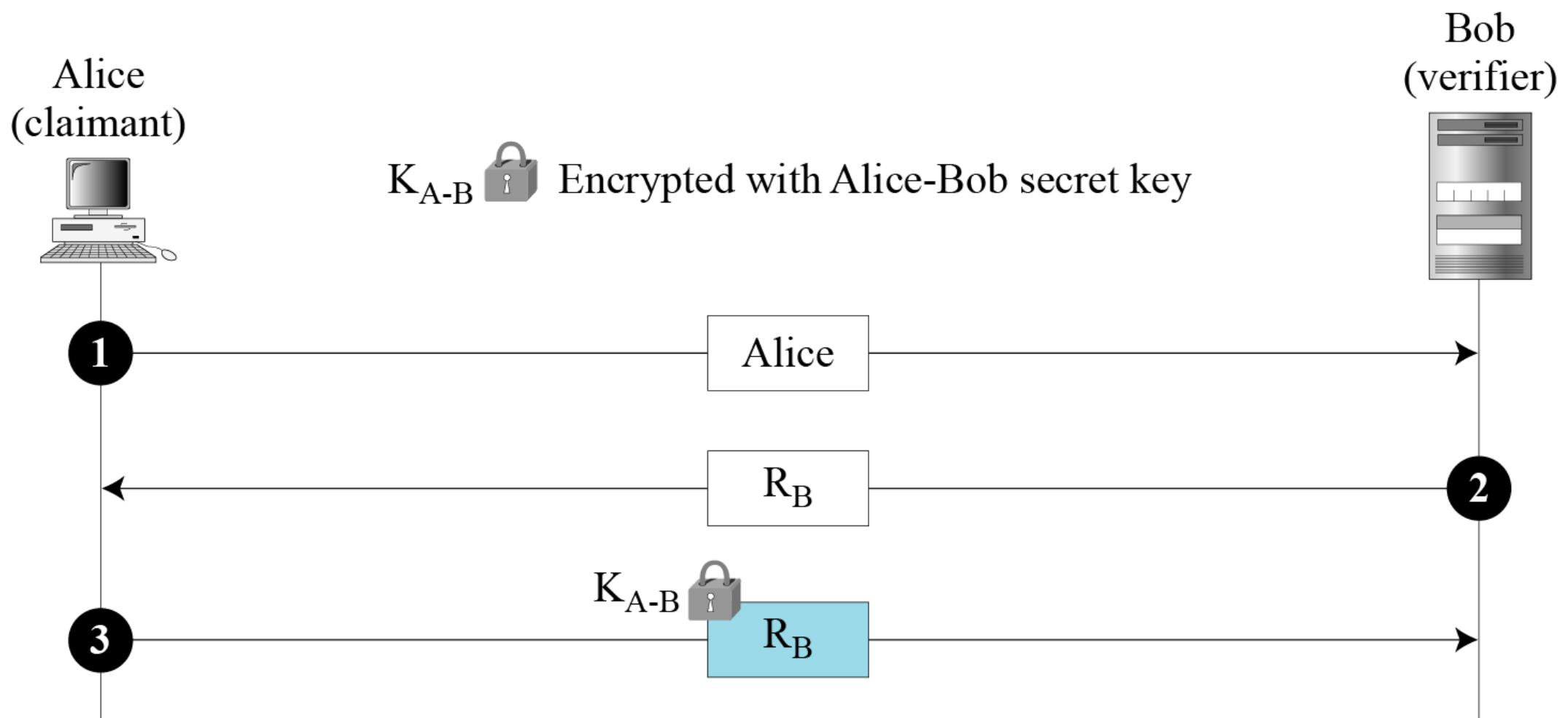
- **Using A Symmetric-Key Cipher**
- **Using Keyed-Hash Functions**
- **Using An Asymmetric-Key Cipher**
- **Using Digital Signature**

3.1 Using A Symmetric-Key Cipher

- Bí mật (secret) ở đây là **khóa bí mật được chia sẻ** giữa Claimant và Verifier. Sử dụng **hàm mã hóa** áp dụng cho challenge này. Có vài hướng theo cơ chế này
- Hướng 1: Nonce challenge

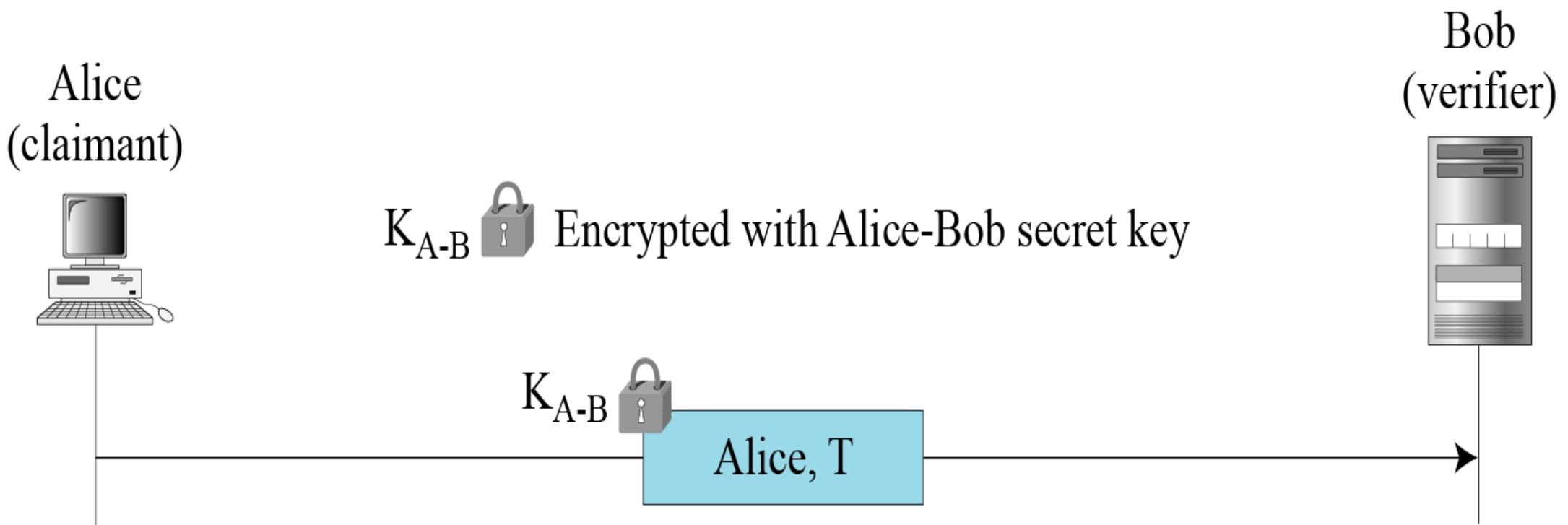
3.1 Using A Symmetric-Key Cipher

- Hướng 1: Nonce challenge



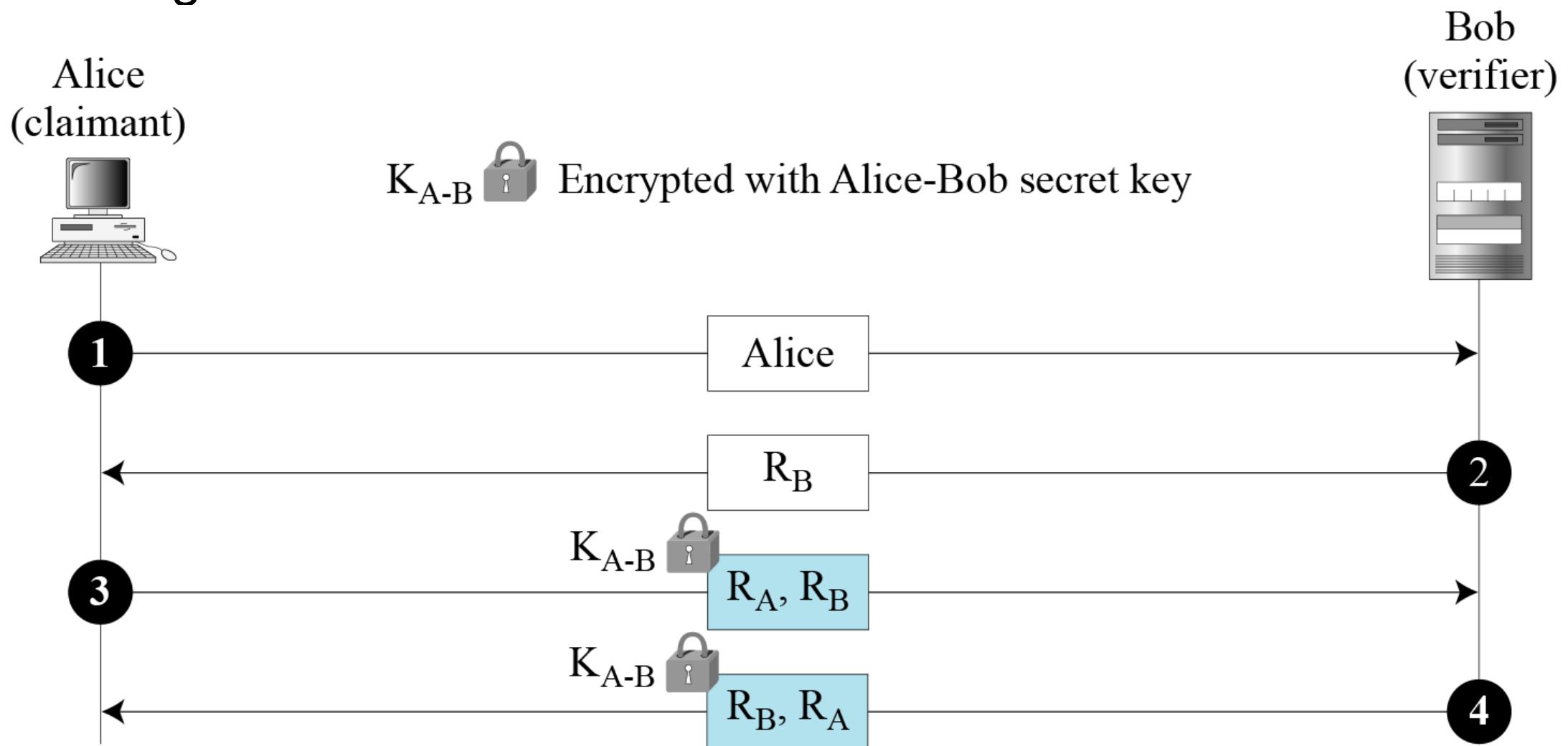
3.1 Using A Symmetric-Key Cipher

- Hướng 2: **Timestamp challenge**



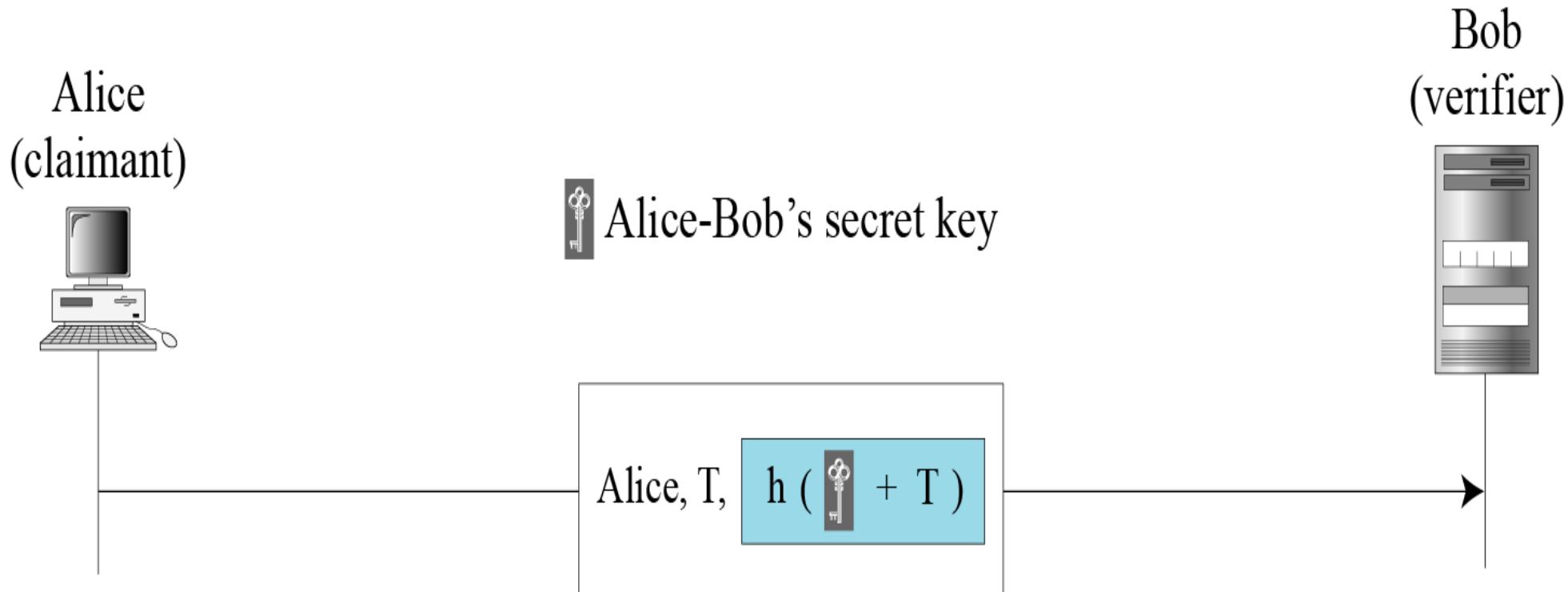
3.1 Using A Symmetric-Key Cipher

- Hướng 3: Bidirectional authentication



3.2 Using Keyed-Hash Functions

- Thay vì dùng mã hóa/giải mã cho chứng thực thực thể, chúng ta cũng có thể dùng một Keyed-has function (MAC)
- Keyed-hash function

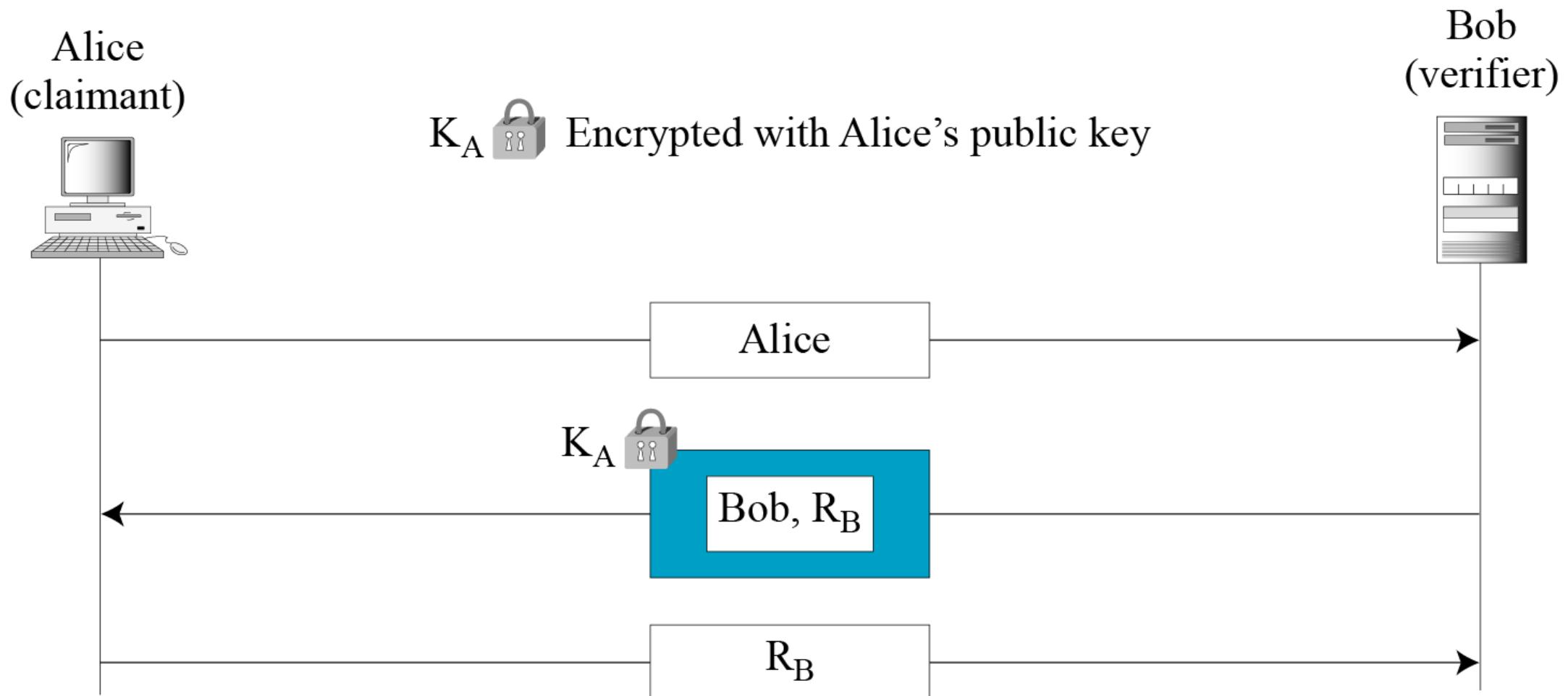


3.3 Using an Asymmetric-Key Cipher

- Sử dụng mã hóa khóa bất đối xứng, Secret là private key của Claimant. Claimant phải chỉ ra rằng private của cô ta có liên quan đến Public key bằng cách Verifier mã hóa challenge bằng cách dùng Public key của claimant, sau đó claimant giải mã bằng private key
- Có hai hướng theo cơ chế này.

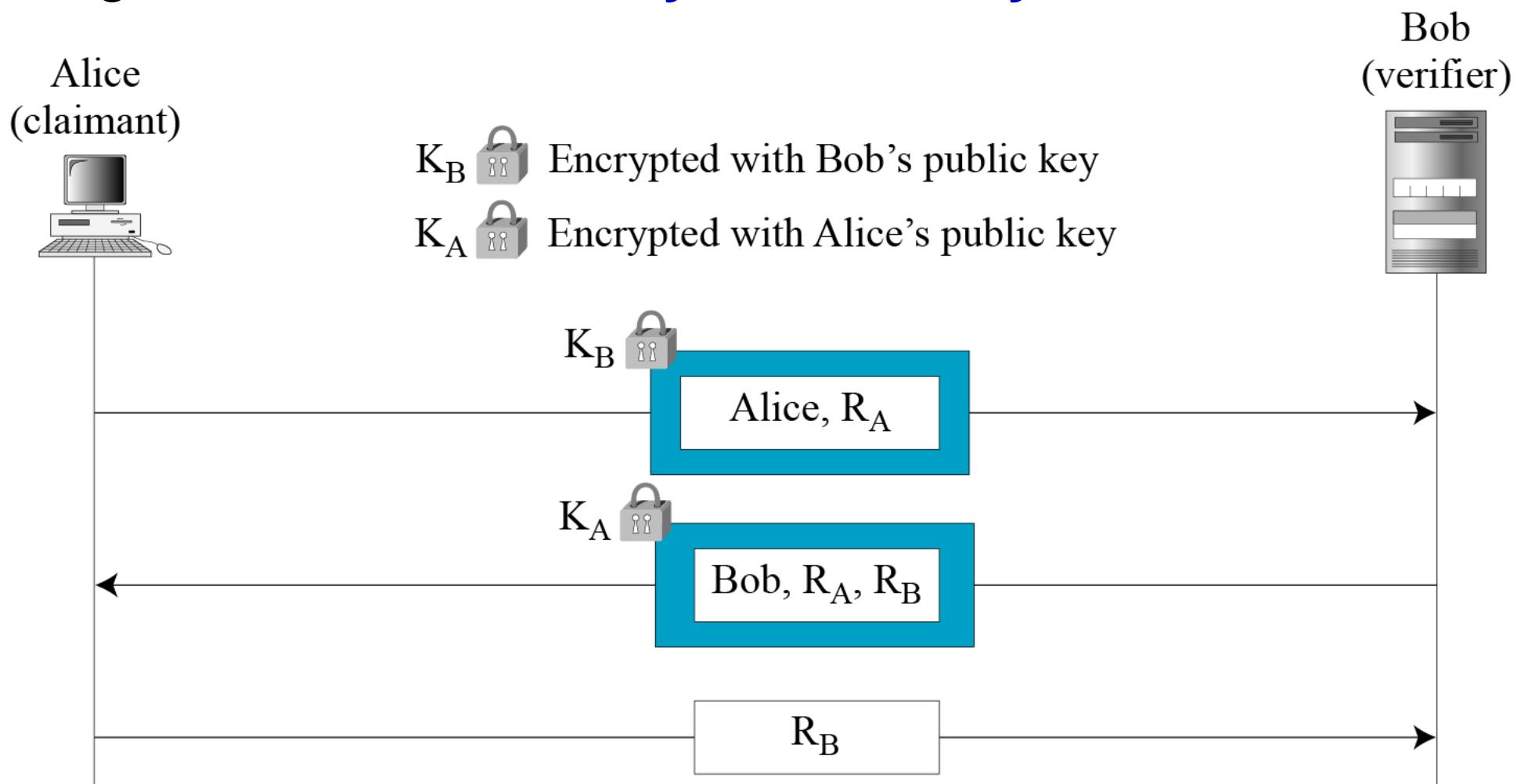
3.3 Using an Asymmetric-Key Cipher

- Hướng 1: Unidirectional, asymmetric-key authentication



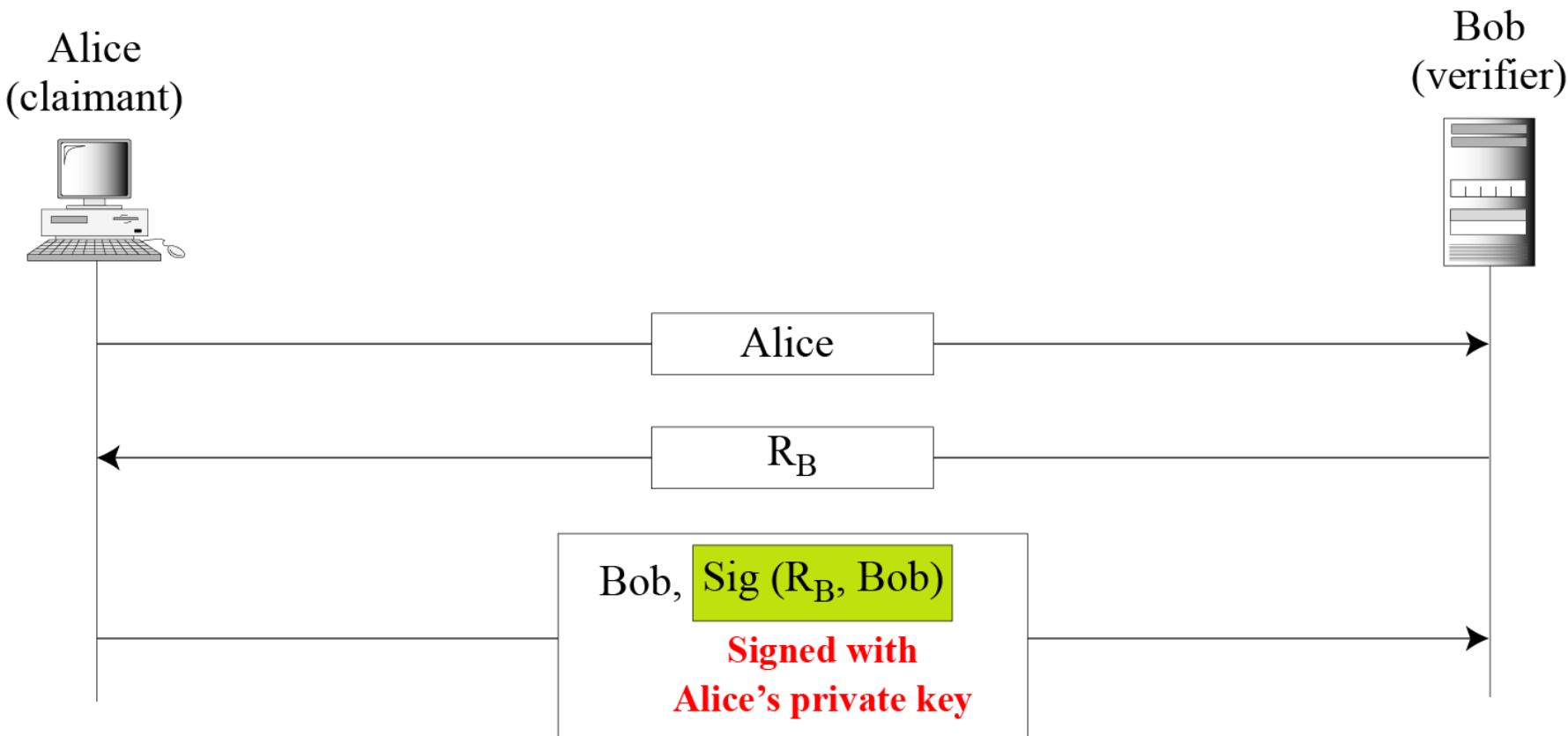
3.3 Using an Asymmetric-Key Cipher

- Hướng 2: **Bidirectional, asymmetric-key**



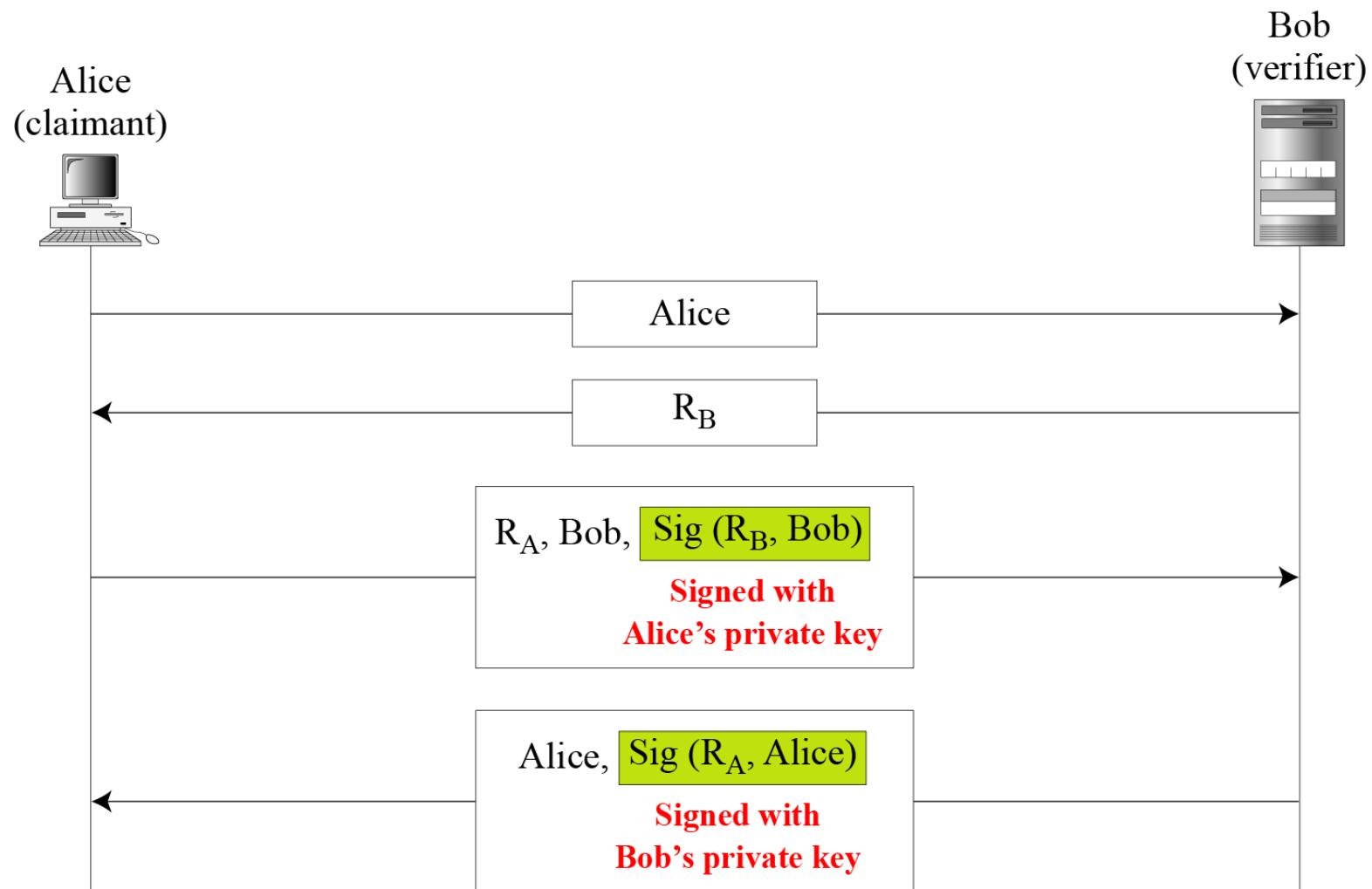
3.4 Using Digital Signature

- Digital Signature được dùng để chứng thực thực thể. Claimant dùng Private để tạo chữ ký
- Hướng 1: **Digital signature, unidirectional**



3.4 Using Digital Signature

- Hướng 2: **Digital signature, bidirectional authentication**



4. ZERO-KNOWLEDGE ZKP

- Trong chứng thực Challenge-response, bí mật của claimant không được gửi đến verifier, mà Claimant áp dụng một hàm trên challenge gửi bởi Verifier mà bao gồm cả bí mật của cô ta. Trong vài phương pháp Challenge-response, verifier biết bí mật của claimant, mà có thể bị lạm dụng bởi những verifier không trung thực. Nói một cách khác, Verifier có thể trích lọc ra được những thông tin về bí mật từ claimant bằng cách chọn trước một tập các challenge.
- Trong chứng thực Zero-knowledge, Claimant không tiết lộ bất kỳ cái gì mà có thể gây nguy hại đến bảo mật của bí mật. **Claimant chứng minh với verifier rằng cô ta biết một bí mật mà không hề tiết lộ nó.**

s : Alice's private key
 v : Alice's public key
 r : Random number

Alice
(claimant)



Bob
(verifier)



n is public

1 $x = r^2 \bmod n$

2

Witness

x

4 $y = rs^c \bmod n$

5

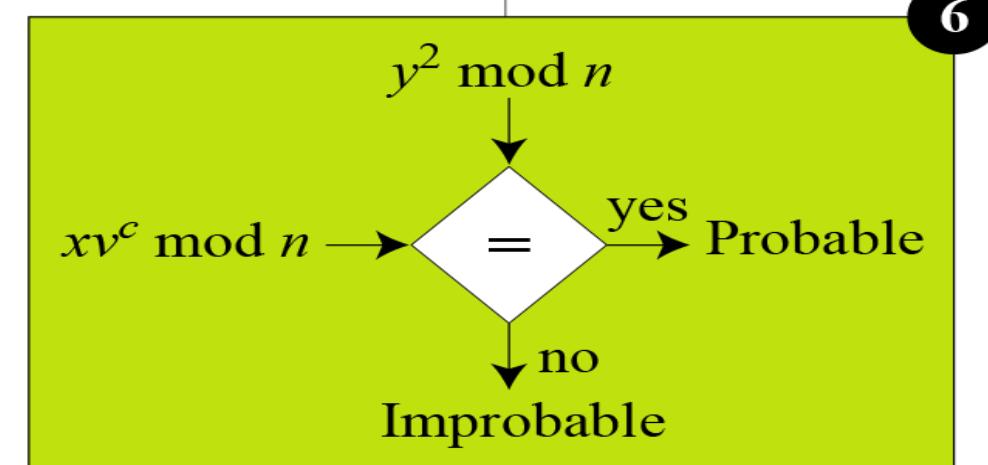
Challenge

c

3

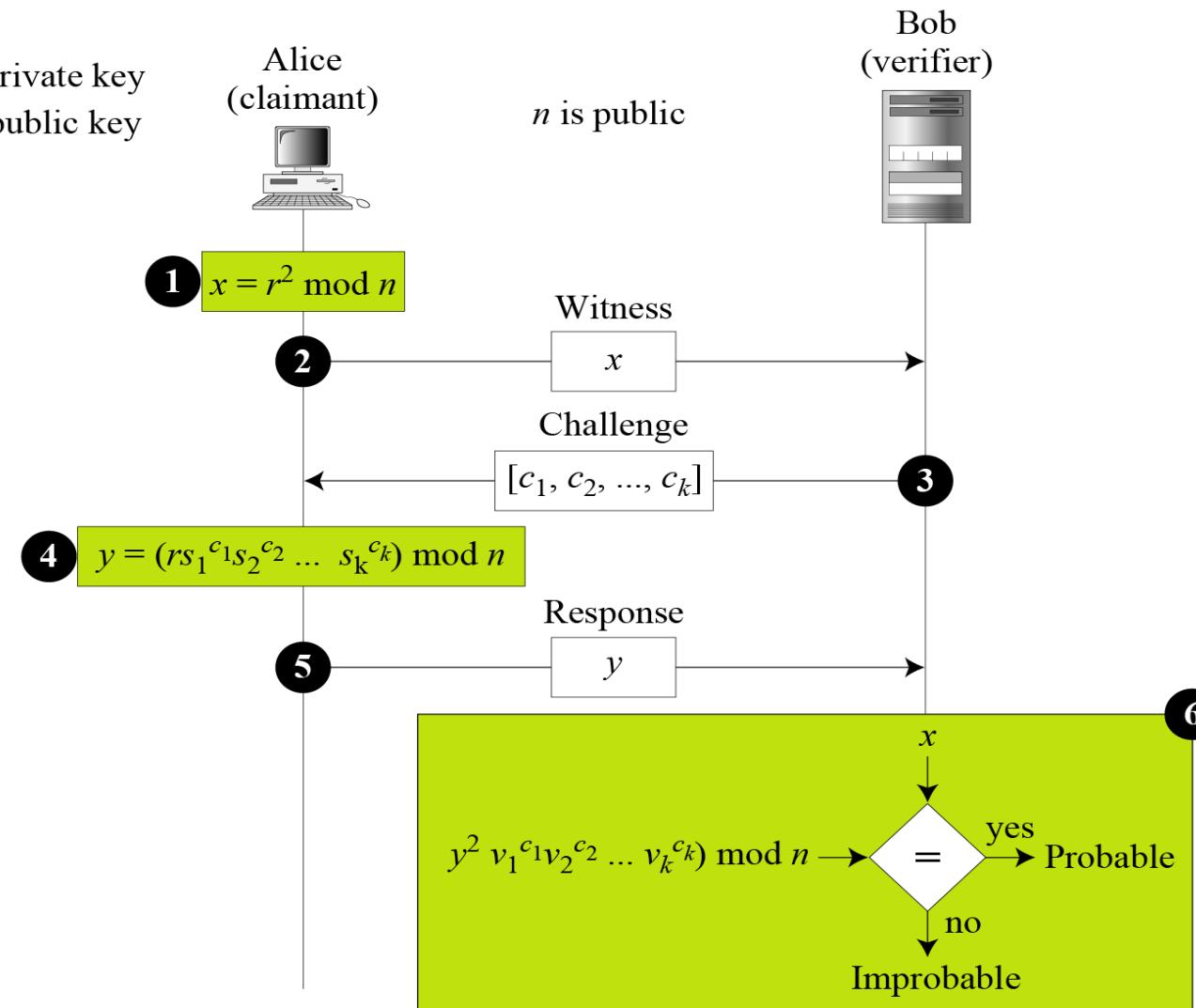
Response

y



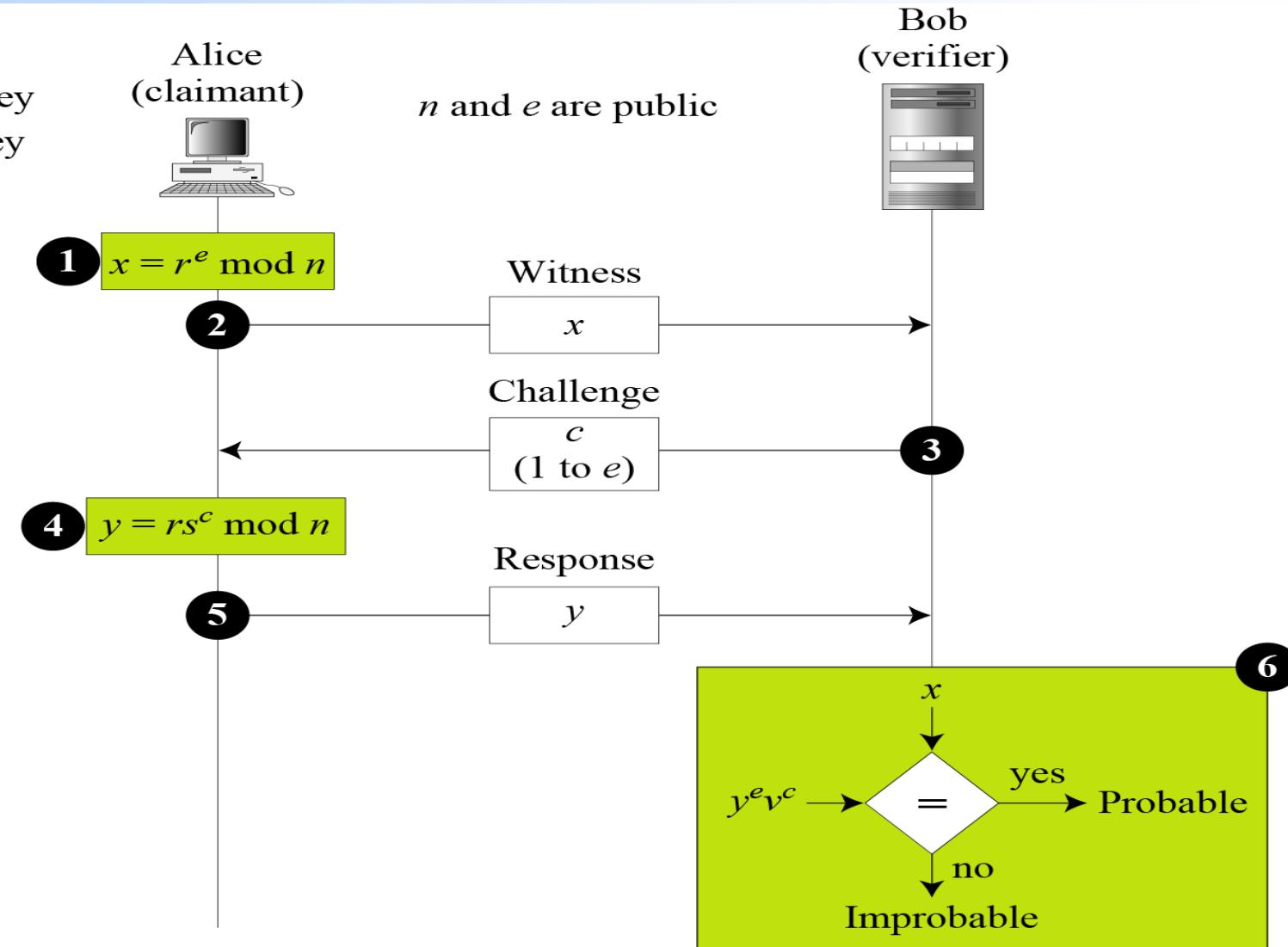
4.2 Giao thức Feige-Fiat-Shamir

$[s_1, s_2, \dots, s_k]$: Alice's private key
 $[v_1, v_2, \dots, v_k]$: Alice's public key
 r : Random number



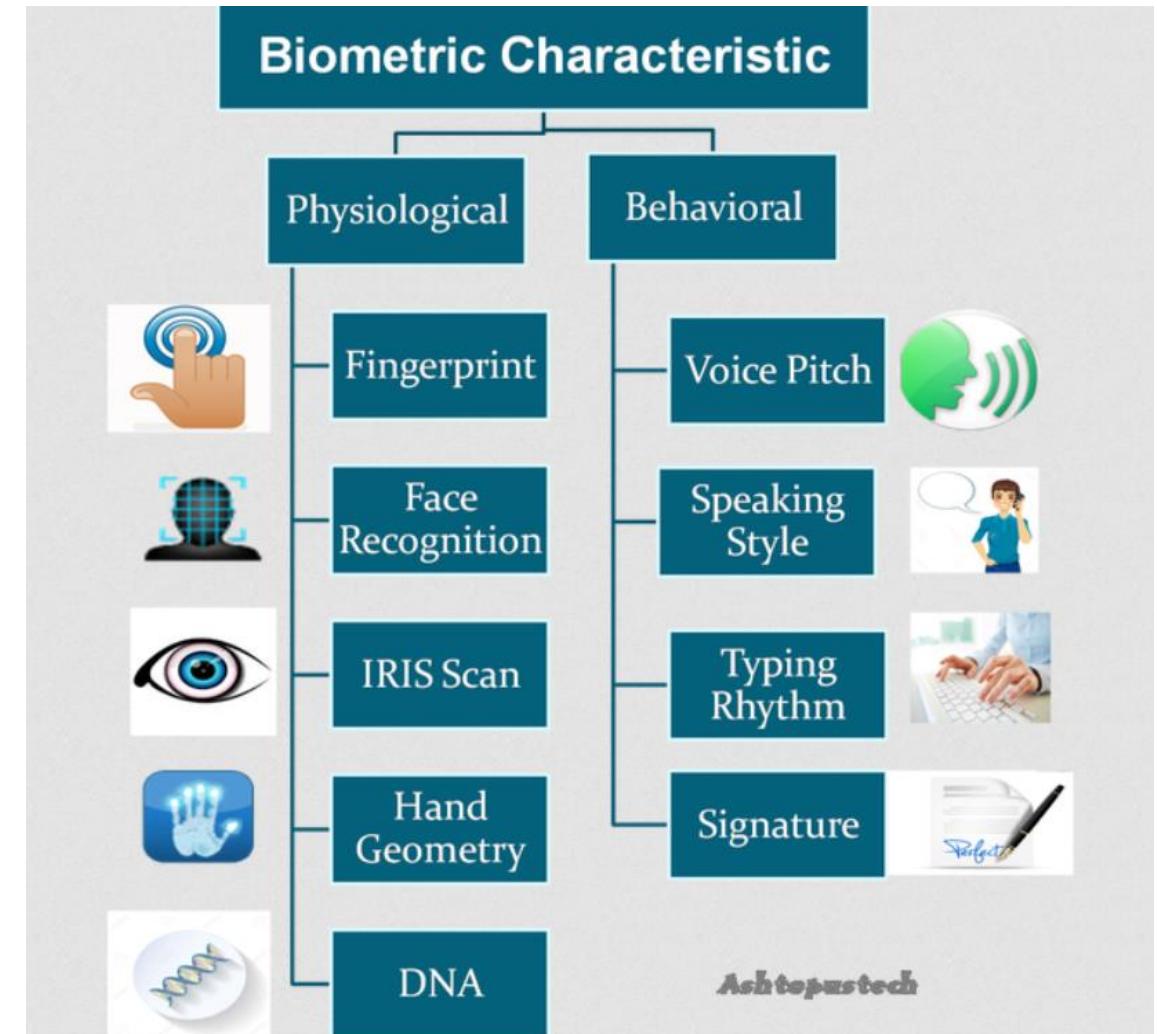
4.3 Giao thức Guillou-Quisquater

s : Alice's private key
 v : Alice's public key
 r : Random number

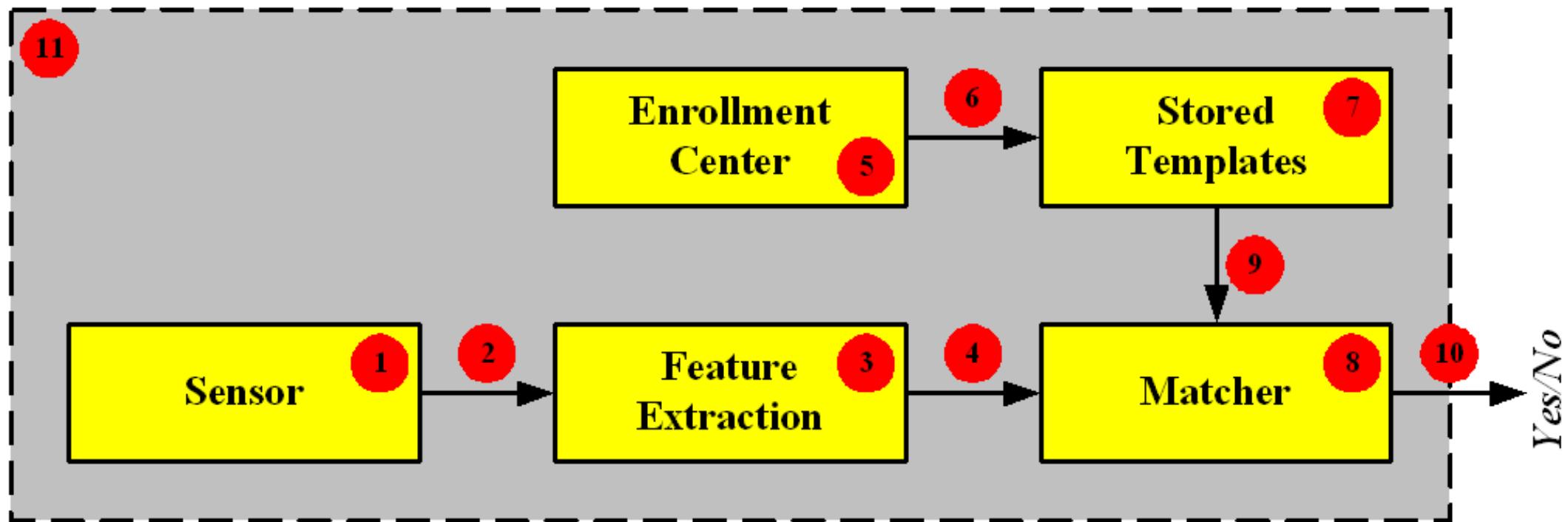


5. Biometrics

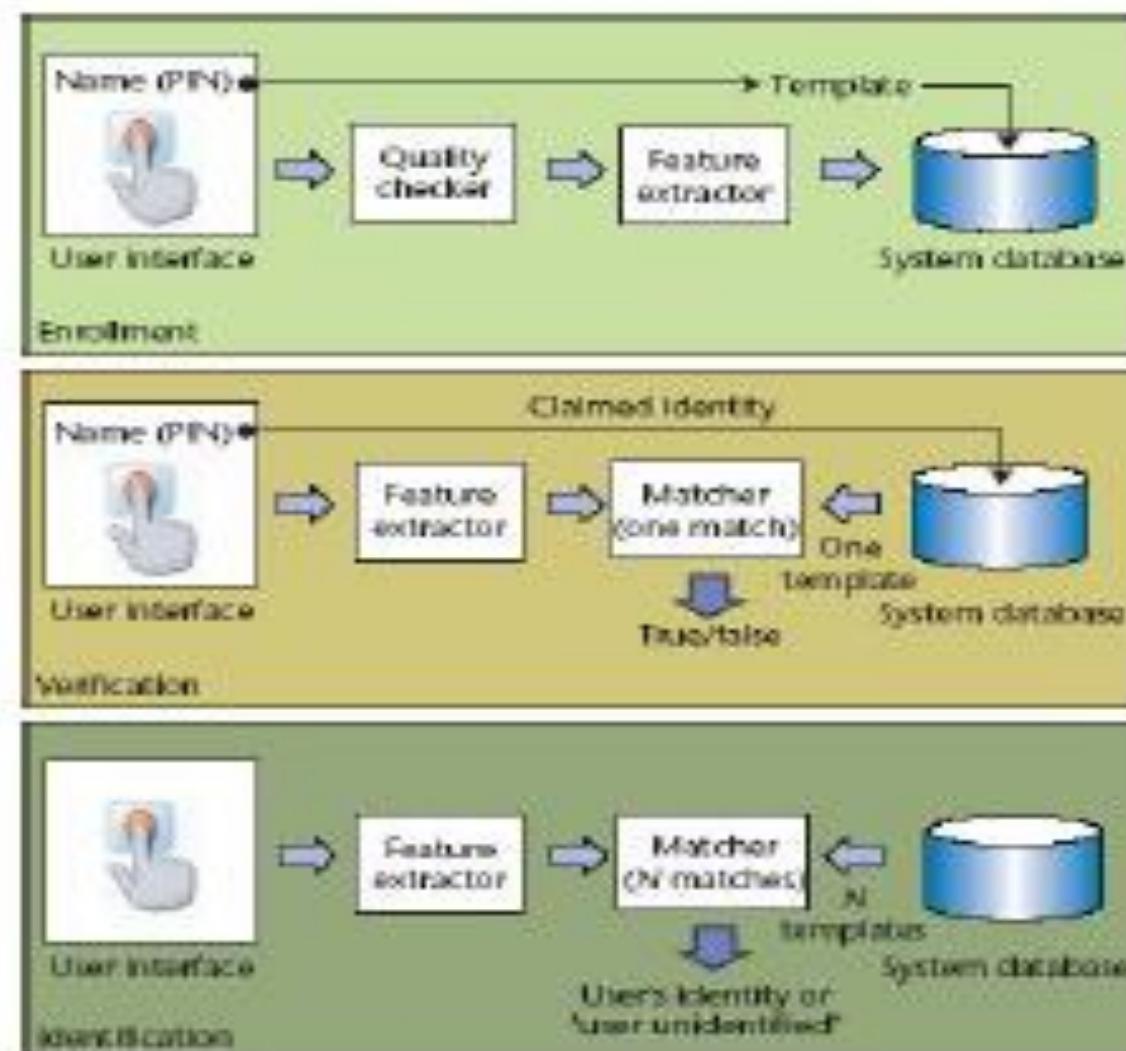
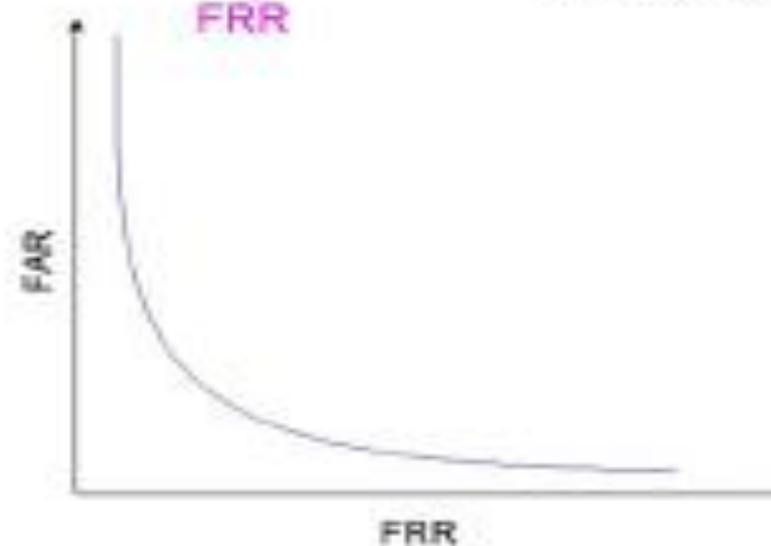
- Sinh trắc học (Biometric) là phép đo lường về các đặc tính sinh lý học hoặc hành vi học mà nhận dạng một con người.
- Sinh trắc học đo lường các đặc tính mà không thể đoán, ăn cắp hoặc chia sẻ.



Qui trình xác thực bằng Biometrics



Xác thực bằng sinh trắc (biometric)



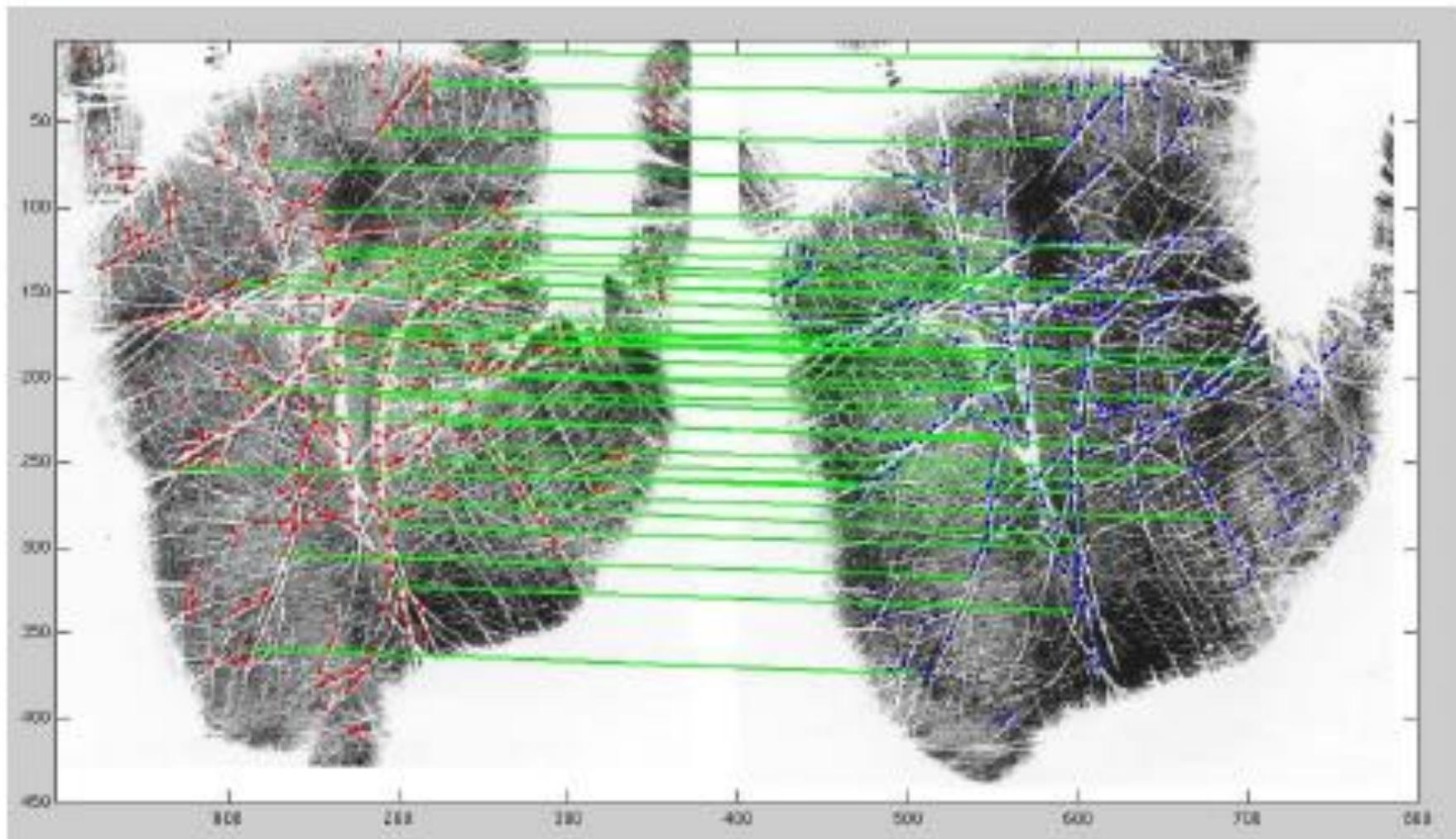
5. Biometrics

Dấu vân tay



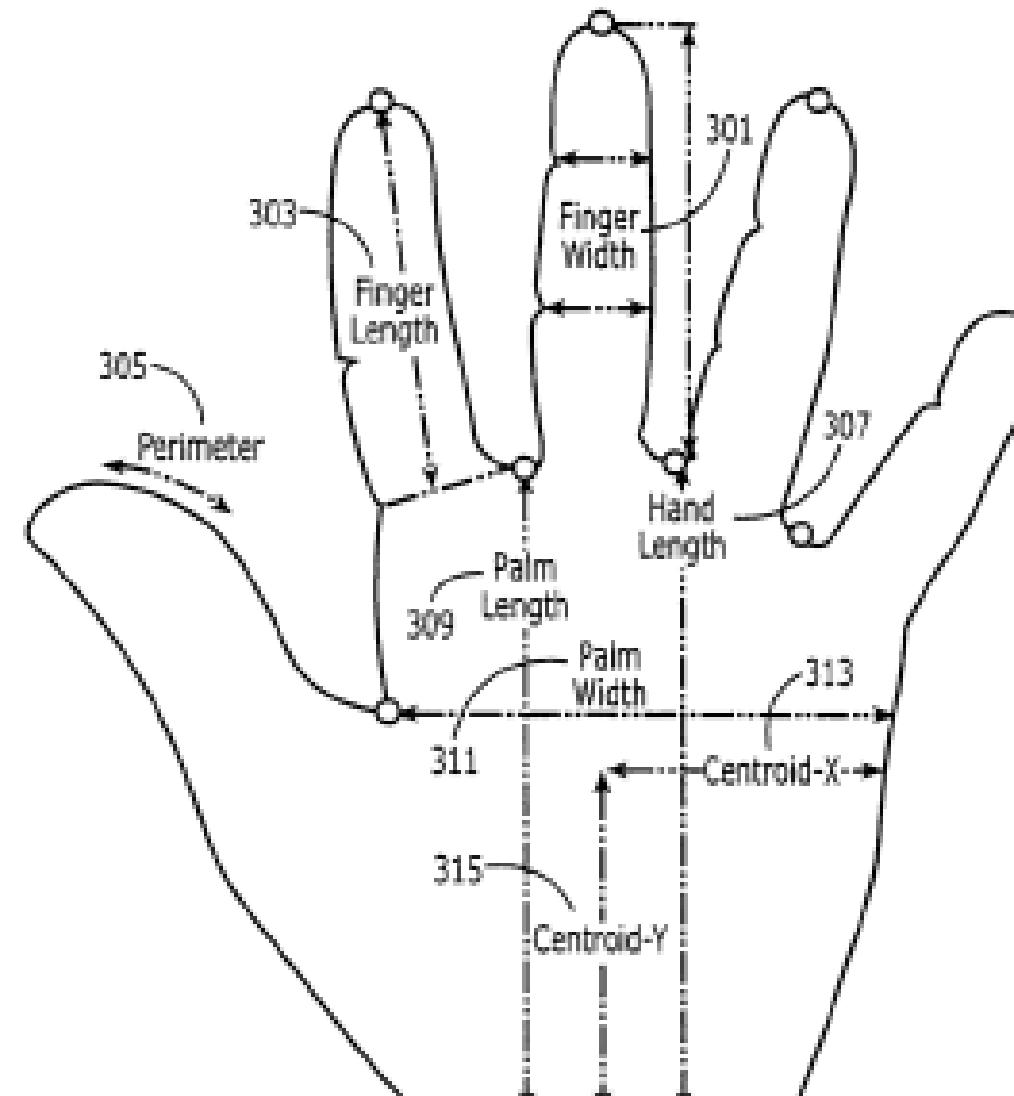
5. Biometrics

Vân lòng bàn tay

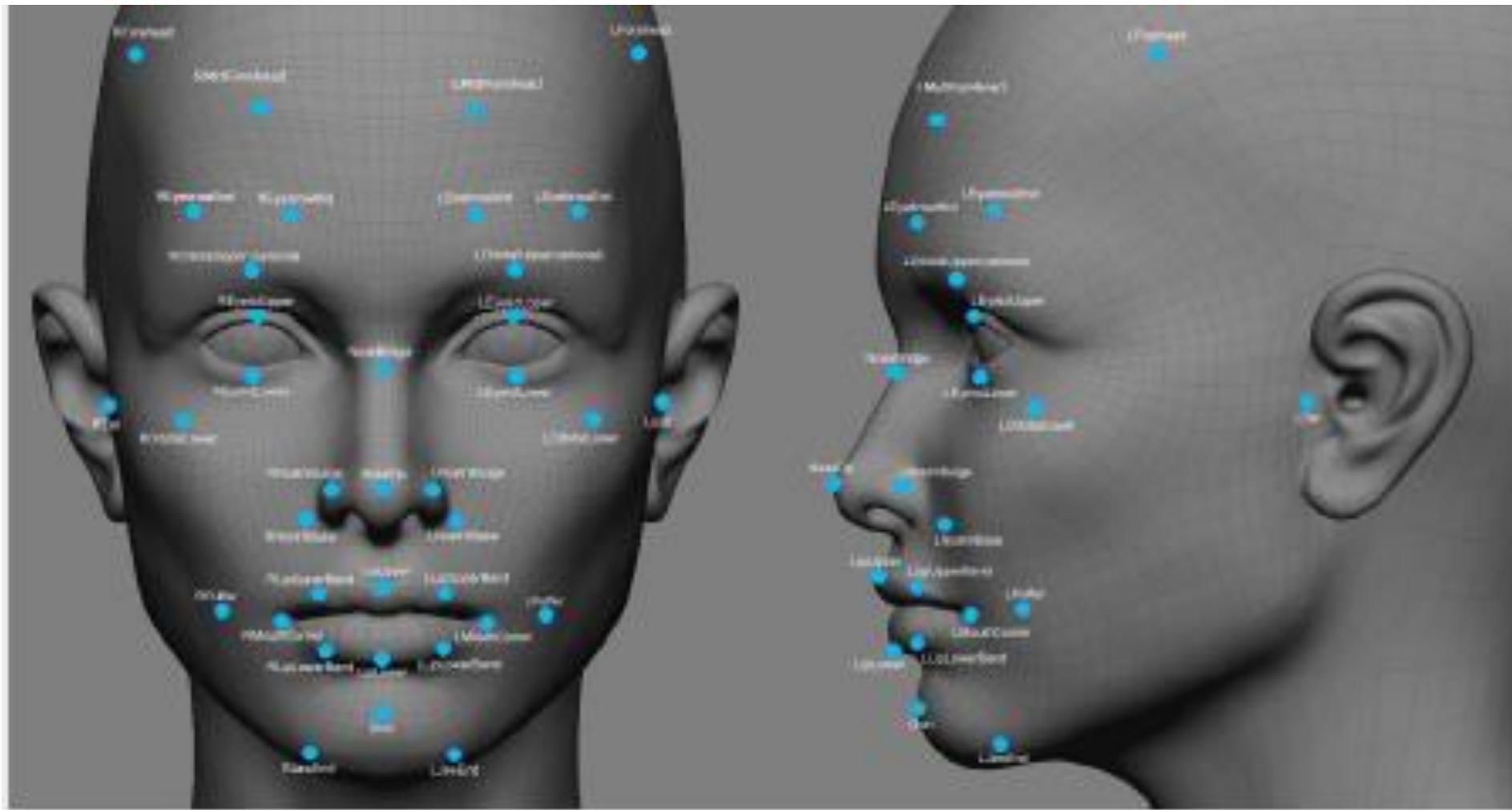


5. Biometrics

Cấu trúc bàn tay



5. Biometrics



5. Biometrics

Xác thực bằng sinh trắc



5. Biometrics

Những khuyết điểm khi sử dụng hệ xác thực bằng sinh trắc

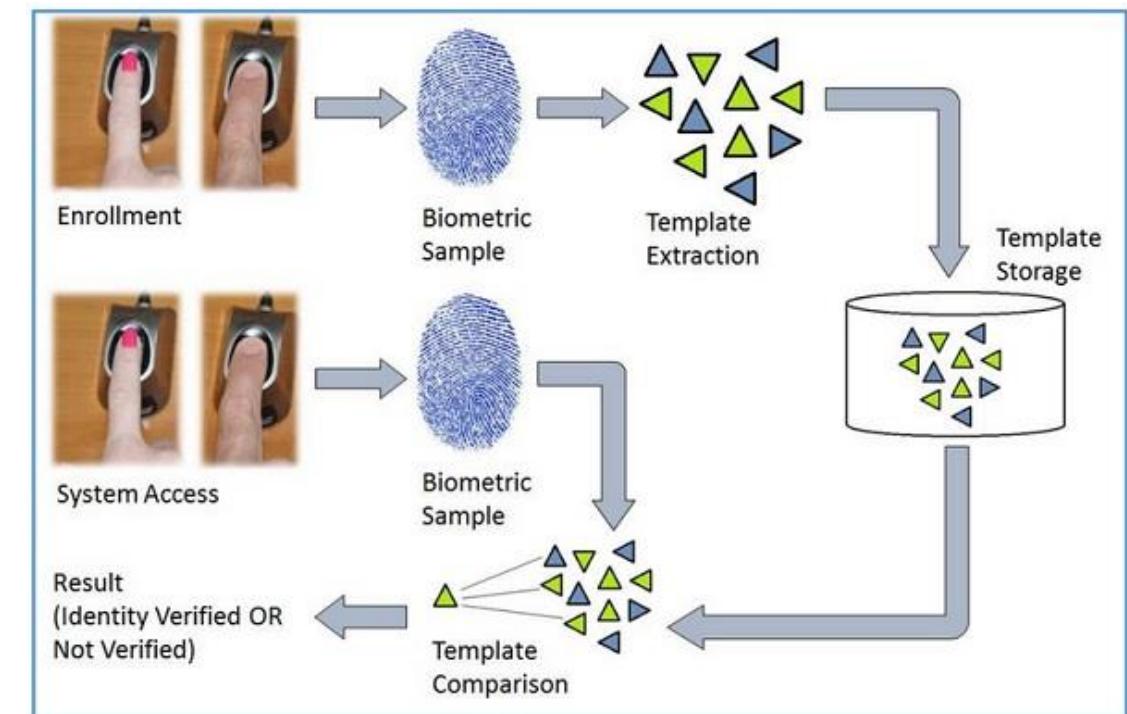
- Chi phí tính toán
- Giá thành cao
- Tính không ổn định
- Không bền vững
- Lo ngại của người dùng liên quan đến sức khỏe

Qui trình xác thực bằng Biometrics

- Chúng ta sẽ thảo luận các vấn đề sau
 - Components (thành phần)
 - Enrollment (ghi nhận vào)
 - Authentication (chứng thực)
 - Techniques (Kỹ thuật)
 - Accuracy (độ chính xác)
 - Applications (các ứng dụng)

Components

- Vài Component cần cho sinh trắc học, bao gồm:
 - các thiết bị thu nhận đặc tính của sinh trắc học
 - Chương trình xử lý các đặc tính sinh trắc học
 - Các thiết bị lưu trữ.



Enrollment

- Trước khi dùng bất cứ kỹ thuật sinh trắc học để chứng thực, đặc tính tương ứng của mỗi người trong cộng đồng cần phải có sẵn trong CSDL, quá trình này được gọi là enrollment

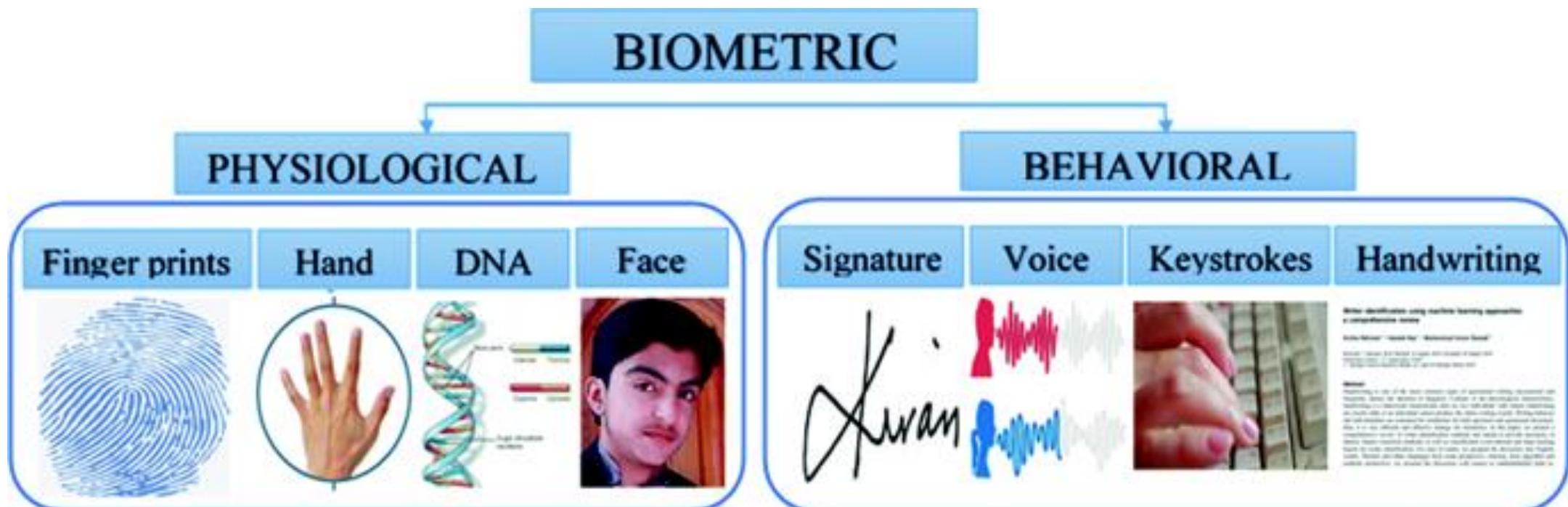


Authentication

- Chứng thực (Authentcation) được thực hiện bởi sự thẩm tra (Verification) hoặc nhận dạng (identication)
 - **Verification:** Đặc tính của một người được so khớp với một mẫu tin đơn trong CSDL để xác định cô ta có phải là người mà cô ta đang tự khai không
 - **Identication:** Đặc tính của một người được so khớp với tất cả các mẫu tin có trong CSDL để xác định cô ta có một mẫu tn trong CSDL.

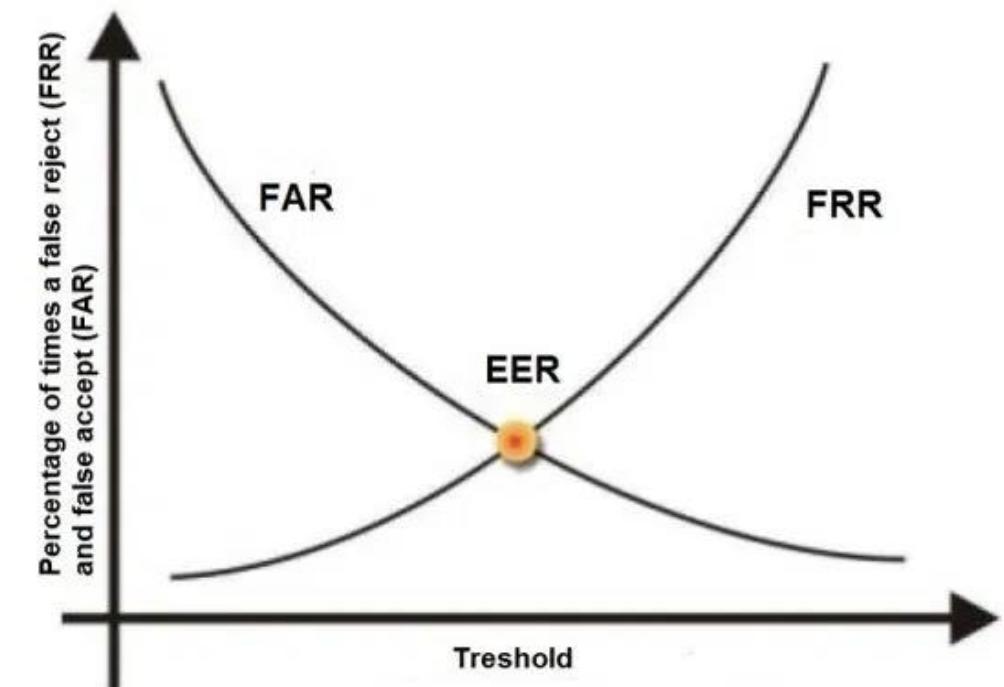
Techiques

- Các kỹ thuật sinh trắc học có thể được chia thành hai hướng chính: sinh lý học và dáng điệu học



Accuracy

- Độ chính xác (Accuracy) của các kỹ thuật sinh trắc học được đo lường bằng cách dùng hai tham số:
 - **False Rejection Rate (FRR)**
 - **False Acceptance Rate (FAR)**



Applications

- Rất nhiều ứng dụng của sinh trắc học đã được áp dụng trong nhiều lĩnh vực khác nhau.
 - Kiểm soát truy cập nơi làm việc
 - Điều khiển truy xuất hệ thống và thông tin nhạy cảm
 - Thực thi các giao dịch thương mại điện tử trực tuyến
 - Nhận dạng tội phạm bằng cách phân tích DNA
 - Kiểm soát nhập cư
- Ví dụ: truy xuất các thiết bị, các hệ thống thông tin, giao dịch ở các điểm bán (trả tiền) điều tra bằng cách phân tích AND hoặc vân tay

Sinh trắc học-2

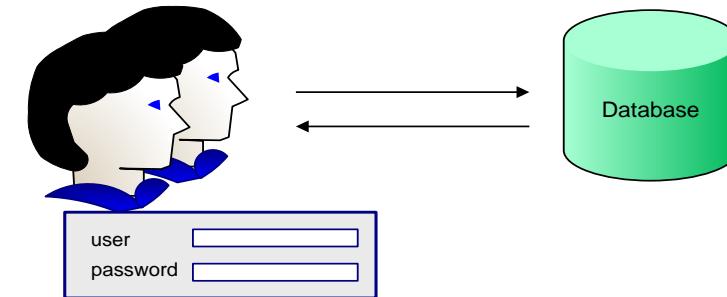
- **Ưu điểm**
 - Có thể rất chính xác
 - Nhanh: thời gian chứng thực nhỏ hơn 1s
 - Sự tác động của người dùng thấp
 - Kết hợp nhiều yếu tố: vân tay, võng mạc, giọng nói,...
 - Biometrics không thể bị mất, đánh cắp, bỏ quên. Nó nhất quán và vĩnh cửu
 - Nó không thể được chia sẻ hoặc dùng bởi người khác
 - Không đòi hỏi phải ghi nhớ như mật khẩu, mã Pin
 - Biometric luôn luôn sẵn dùng cho cá nhân và duy nhất
-

Sinh trắc học-2

- Nhược điểm

- Giá thành: triển khai hệ thống sinh trắc học đòi hỏi chi phí cho phần cứng và phần mềm.
- Có thể nhận diện sai: mặc dù đúng người nhưng hệ thống không chấp nhận
- Các bộ đọc luôn đặc tính của sinh trắc học có những lỗi nhất định
 - Từ chối người dùng hợp lệ
 - Chấp nhận người dùng không hợp lệ

Các ứng dụng: Chứng thực người dùng



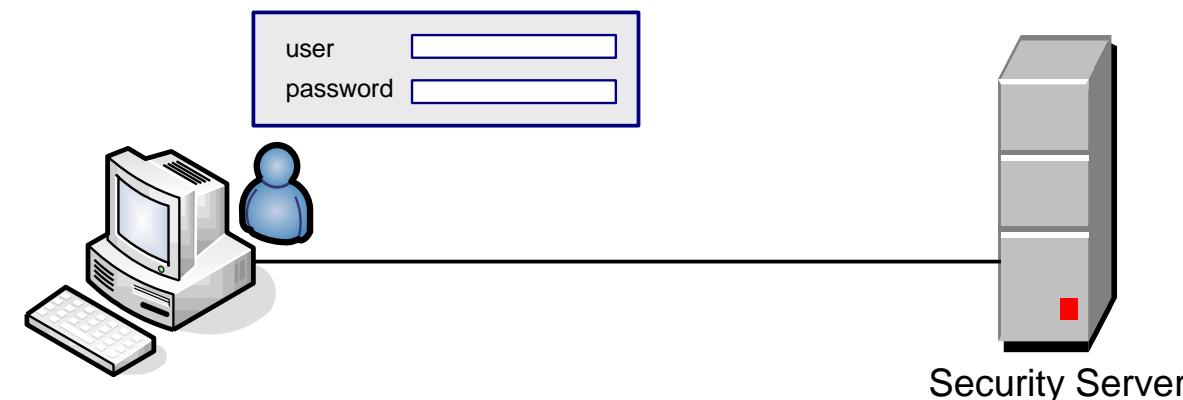
- Chứng thực người dùng:
 - Là quá trình thiết lập tính hợp lệ của người dùng trước khi truy cập thông tin trong hệ thống.
 - Thường sử dụng phương pháp chung là username/password

Các ứng dụng: Chứng thực người dùng

- username/password
- CHAP
- Kerberos
- Password dùng 1 lần
- Thẻ password (Token password)
- Chứng chỉ (Certificates)
- Sinh trắc học
- Kết hợp nhiều phương pháp

Các ứng dụng: Username/Password

- Là loại chứng thực phổ biến nhất
- Truyền username/password đến Server
- Ví dụ
 - Dial-up



Các ứng dụng: Username/Password

- Các vấn đề
 - Thời gian duy trì
 - Thay đổi mật khẩu thường xuyên hay không?
 - Có nguy cơ bị lấy mất
 - Keyloggers
 - Phần mềm: theo dõi phím bấm
 - Phần cứng: thiết bị gắn giữa bàn phím và CPU để theo dõi phím bấm

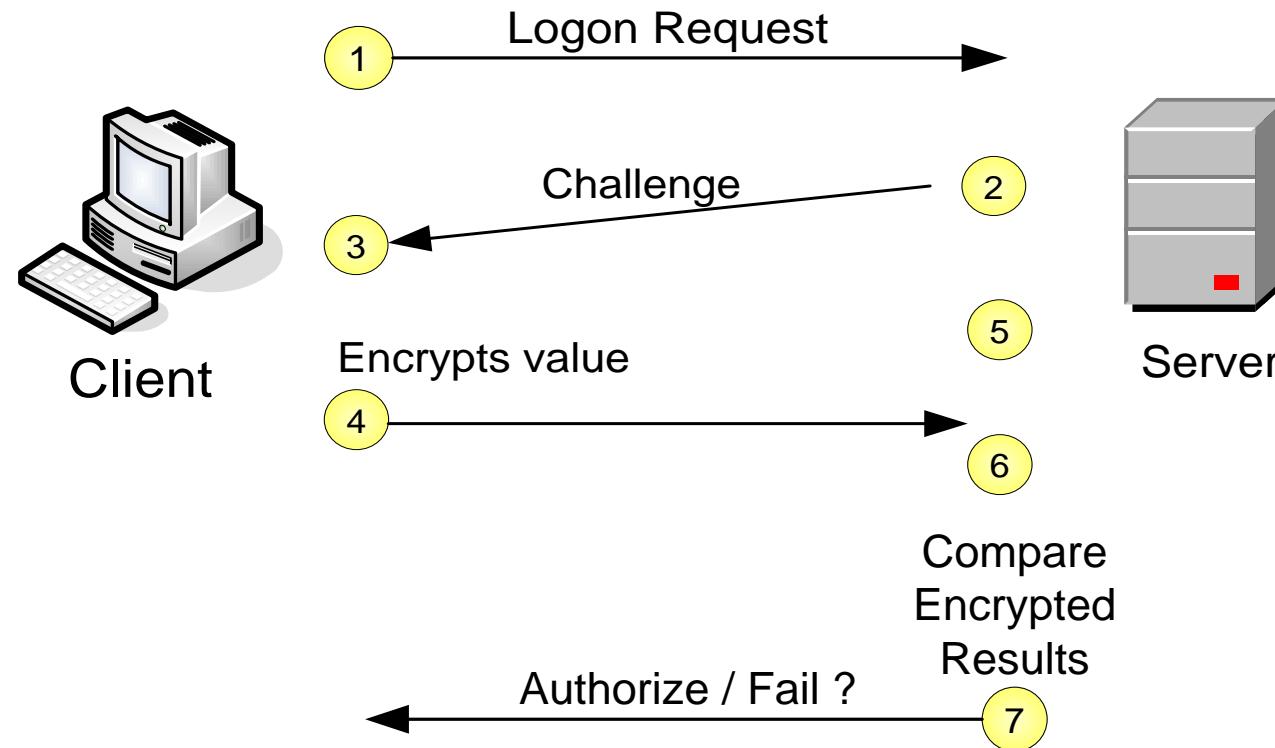
Các ứng dụng: Username/Password

- Giải pháp
 - Đặt mật khẩu dài
 - Bao gồm chữ cái, số, biểu tượng
 - Thay đổi password: 01 tháng/lần
 - Không nên đặt cùng password ở nhiều nơi
 - Xem xét việc cung cấp password cho ai
 - Ví dụ: *Tomatotree650*

Các ứng dụng: CHAP

- CHAP (Challenge Hanshake Authentication Protocol)
 - Mật khẩu người dùng: bảo mật
 - Số ngẫu nhiên: dùng để mã hóa
 - Sử dụng trong remote login, PPP, PRAS, xác thực dịch vụ web
 - Triển khai: [MS CHAP version 2](#)

Các ứng dụng: CHAP



Các ứng dụng: CHAP

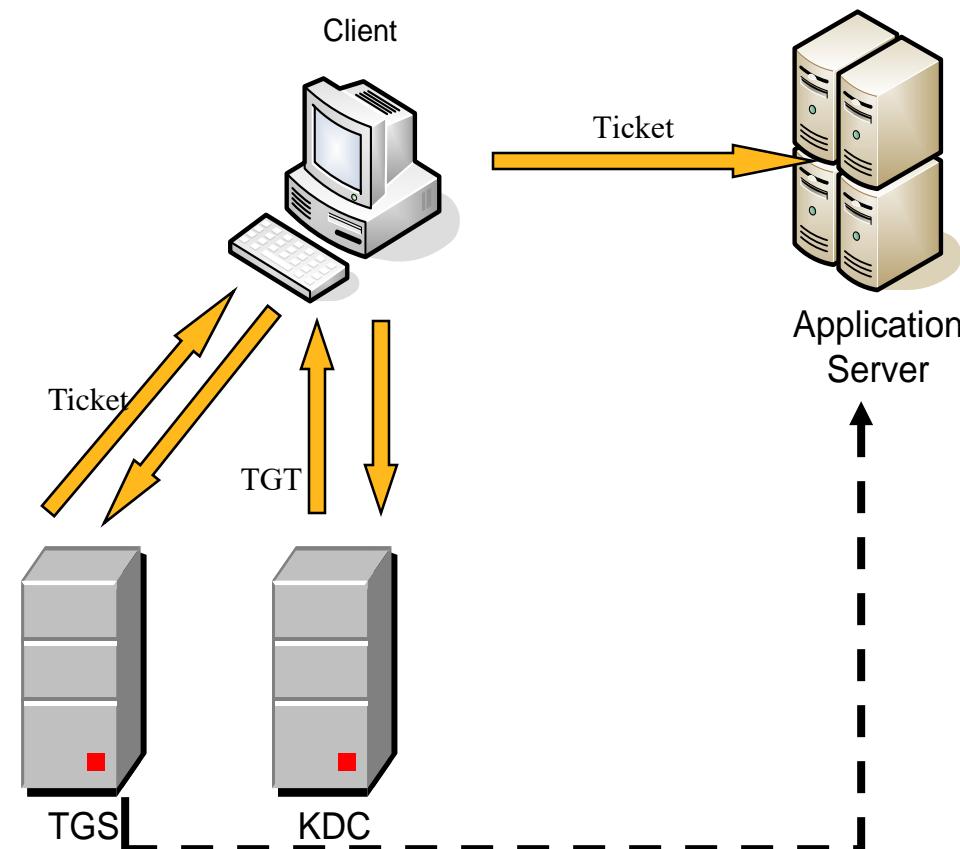
- Hoạt động của CHAP
 - Client gửi yêu cầu
 - Server đưa ra challenge
 - Client mã hóa (băm) challenge với secret và gửi cho Server
 - Client được xác thực khi kết quả giống nhau.

Các ứng dụng: Kerberos

- Bắt đầu phát triển tại MIT năm 1980
- Microsoft đưa Kerberos vào Windows 2000 và .NET
 - Ticket: sự cấp phép cụ thể
 - Ticket Grant Ticket (TGT): được đưa ra bởi Central Authority cho phép người dùng yêu cầu một dịch vụ nào đó.
 - Key Distribution Center (KDC): máy chủ cung cấp cho Client TGT, chứng thực và cho phép user yêu cầu một dịch vụ nào đó.
 - Ticket Granting Server (TGS): máy chủ kiểm tra Client có được phép nhận một ticket hay không.

Các ứng dụng: Kerberos -2

- Quá trình hoạt động

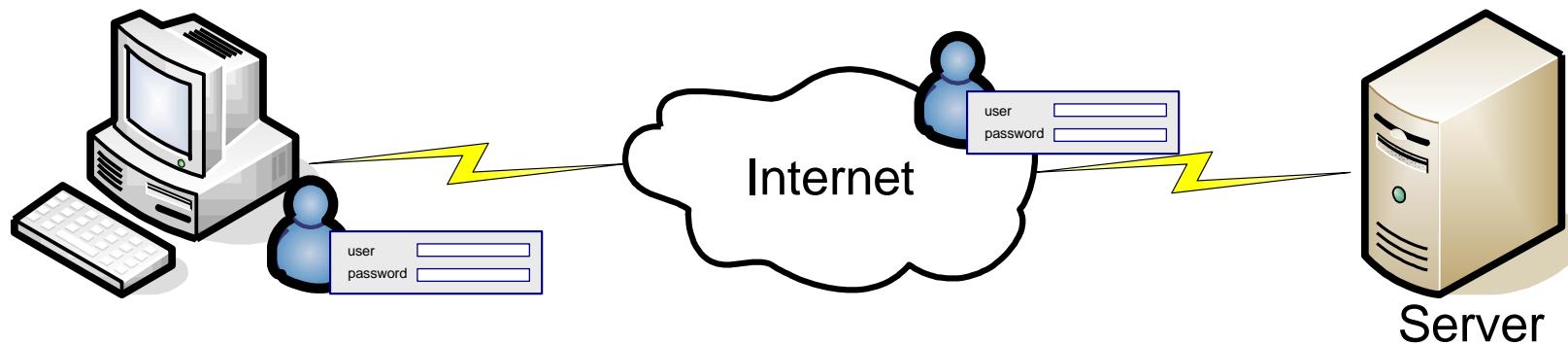


Các ứng dụng: Kerberos -3

- Kerberos Process
 - Chứng thực người dùng
 - Client liên lạc với KDC yêu cầu chứng thực
 - TGT nhận được từ KDC
 - Cho phép client yêu cầu một dịch vụ cụ thể nào đó
 - Ticket cho dịch vụ được nhận từ TGS
 - Client đưa ticket cho máy chủ ứng dụng
 - Khi đã được chứng thực, quyền truy nhập được cấp cho người dùng

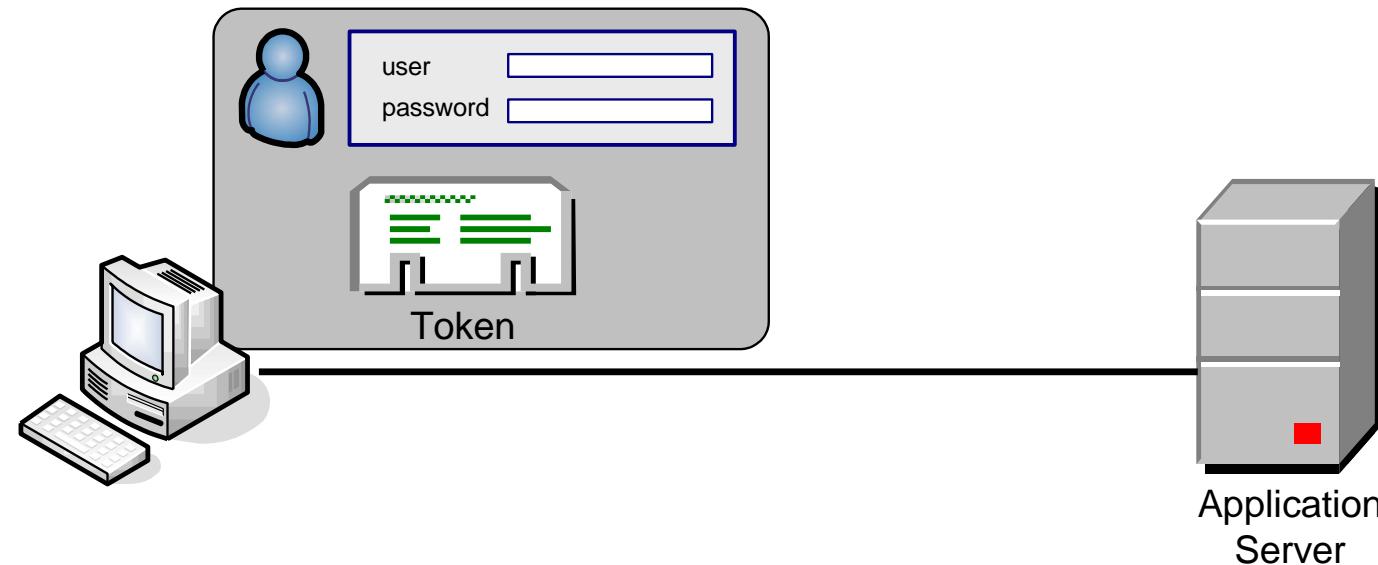
Các ứng dụng: Password sử dụng một lần

- Người dùng có chương trình sinh password
- Có thể gửi dạng “clear” qua môi trường không an toàn

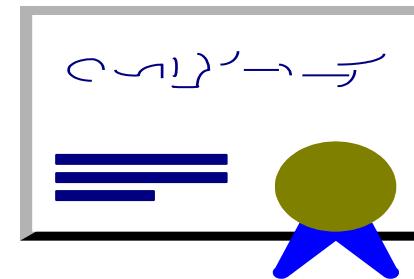


Các ứng dụng: Token password

- Được coi là một trong những phương pháp an toàn nhất
- Thẻ bài mang một số thông tin cá nhân
- Người dùng ngoài mật khẩu còn phải có thẻ bài

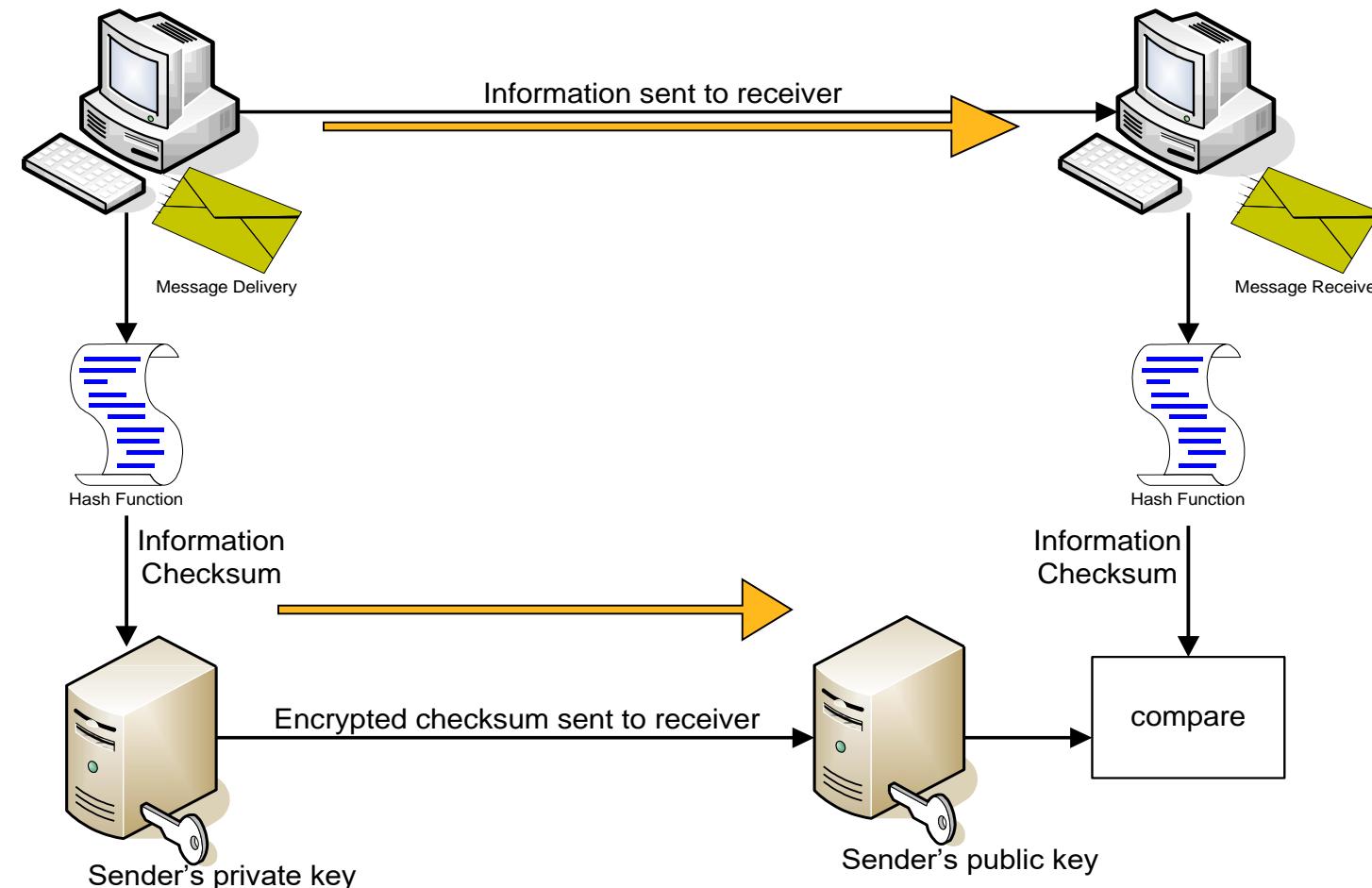


Các ứng dụng: Certificates

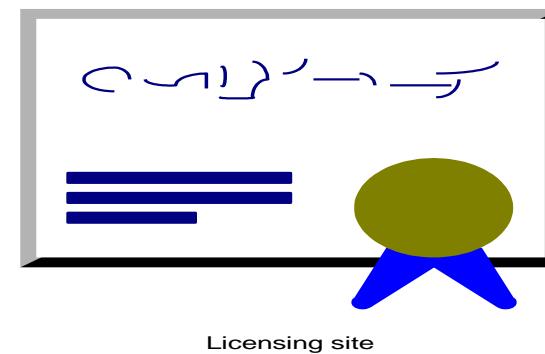


- Một Server (Certificates Authority - CA) tạo ra các certificates
 - Có thể là vật lý: smartcard
 - Có thể là logic: chữ ký điện tử
- Sử dụng public/private key (bất cứ dữ liệu nào được mã hóa bằng public key chỉ có thể giải mã bằng private key)
- Sử dụng “công ty thứ 3” để chứng thực

Các ứng dụng: Certificates - 2



Các ứng dụng: Certificates - 3



Được sử dụng phổ biến trong chứng thực web, smart cards, chữ ký điện tử cho email và mã hóa email

- Nhược điểm

- ✓ Triển khai PKI (Public Key Infrastructure) kéo dài và tốn kém
- ✓ Smart cards làm tăng giá triển khai và bảo trì
- ✓ Dịch vụ CA tốn kém

Các ứng dụng: Sinh trắc học

- Mống mắt/võng mạc
- Vân tay
- Giọng nói

Các ứng dụng: Kết hợp nhiều phương pháp (Multi-factor)

- Sử dụng nhiều hơn một phương pháp chứng thực
 - Mật khẩu/ PIN
 - Smart card
 - Sinh trắc học
- Kết hợp nhiều phương pháp chứng thực tạo sự bảo vệ theo chiều sâu với nhiều tầng bảo vệ khác nhau

Kết hợp nhiều phương pháp (Multi-factor)

- Ưu điểm
 - Giảm sự phụ thuộc vào password
 - Hệ thống chứng thực mạnh hơn
 - Cung cấp khả năng cho Provides Public Key Infrastructure (PKI)
- Nhược điểm
 - Tăng chi phí triển khai: đầu tư thiết bị, đào tạo người dùng và quản trị
 - Tăng chi phí duy trì: do tính không tương thích giữa các nhà SX
 - Chi phí nâng cấp: sự không ổn định của nhà SX

Điều khiển truy cập/Phân quyền SD

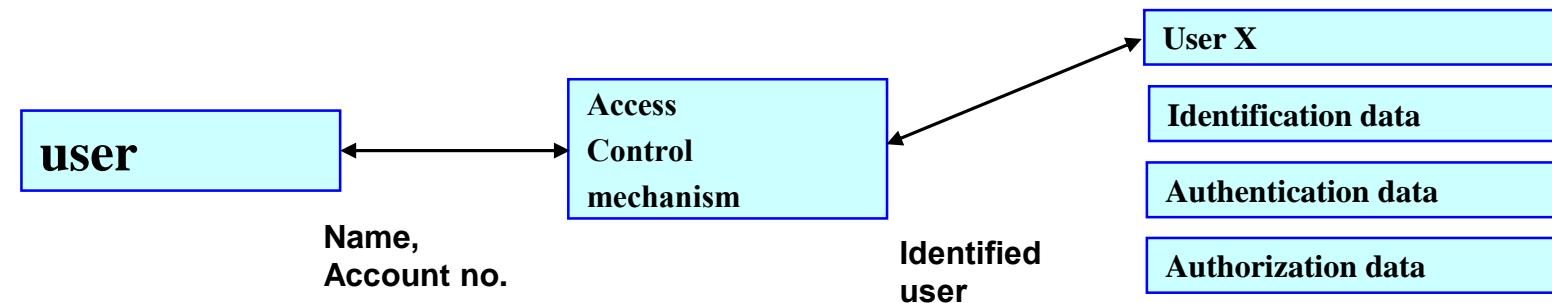
- Mô hình điều khiển truy cập
- Quá trình điều khiển truy cập
- Các loại điều khiển truy cập

Điều khiển truy cập

- Điều khiển truy cập là quá trình giới hạn *quyền sử dụng* của người dùng đã được chứng thực đối với *tài nguyên hệ thống*, cũng như hạn chế các tác động của người dùng đối với tài nguyên hệ thống và đảm bảo người dùng chỉ tác động được các tài nguyên trong phạm vi được cấp quyền đó.

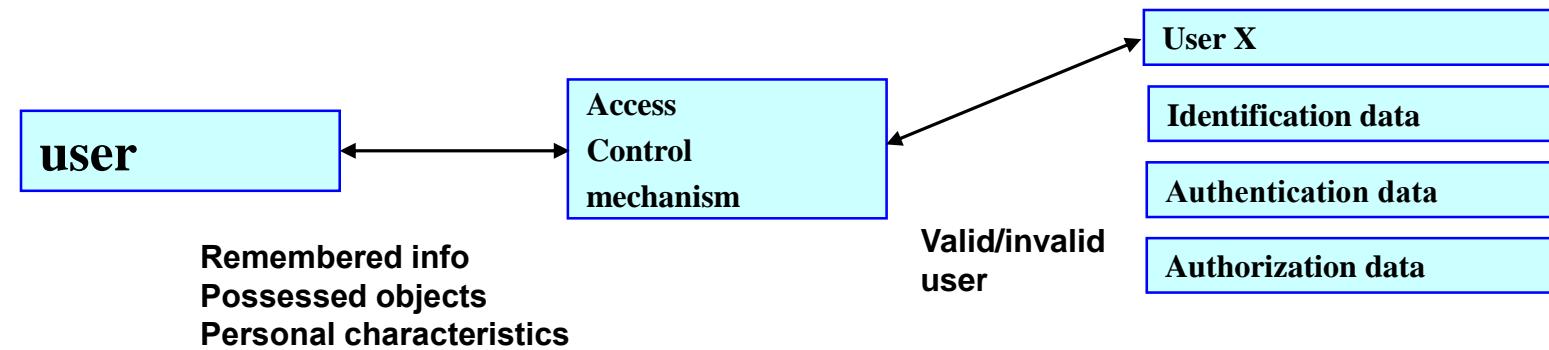
Điều khiển truy cập

- Quá trình điều khiển truy cập
 - Xác định người dùng (Identification)



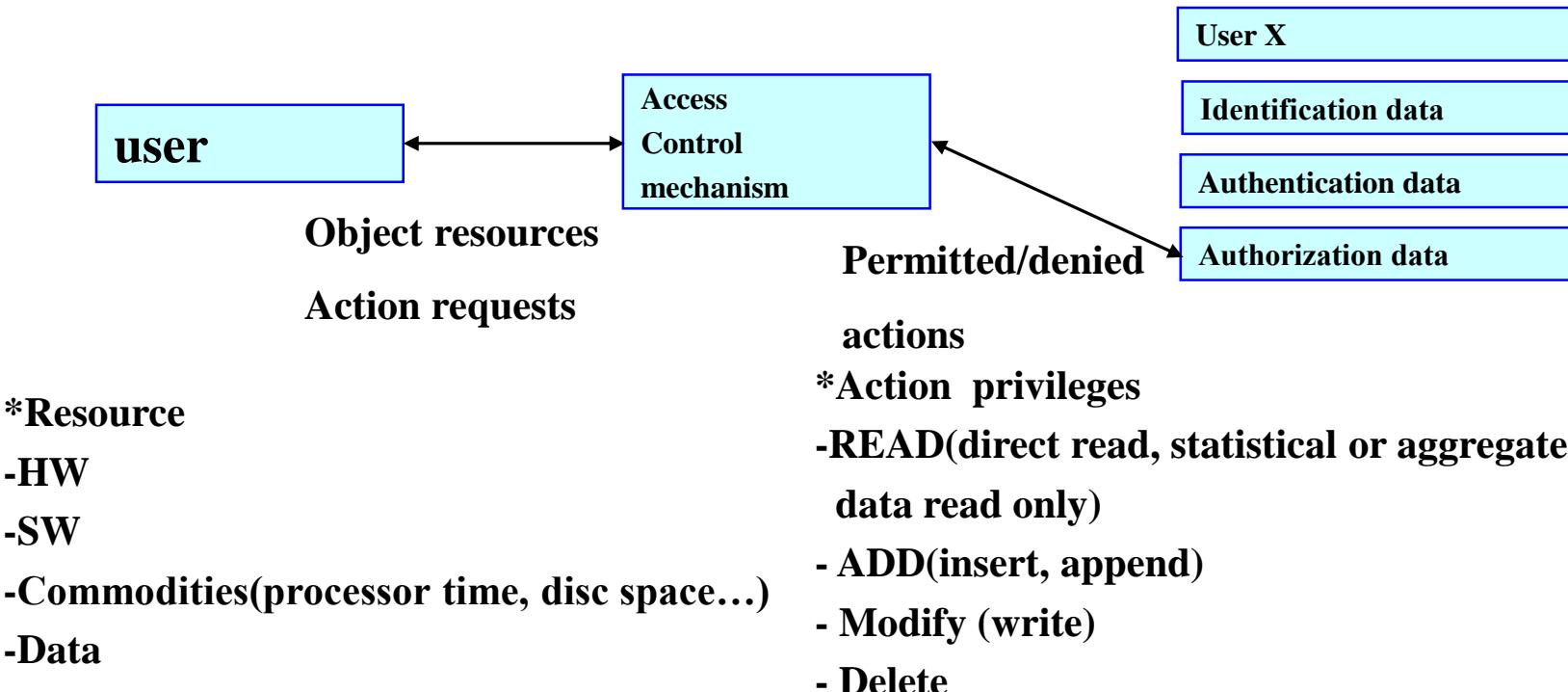
Điều khiển truy cập

- Chứng thực người dùng



Điều khiển truy cập

- Phân quyền sử dụng

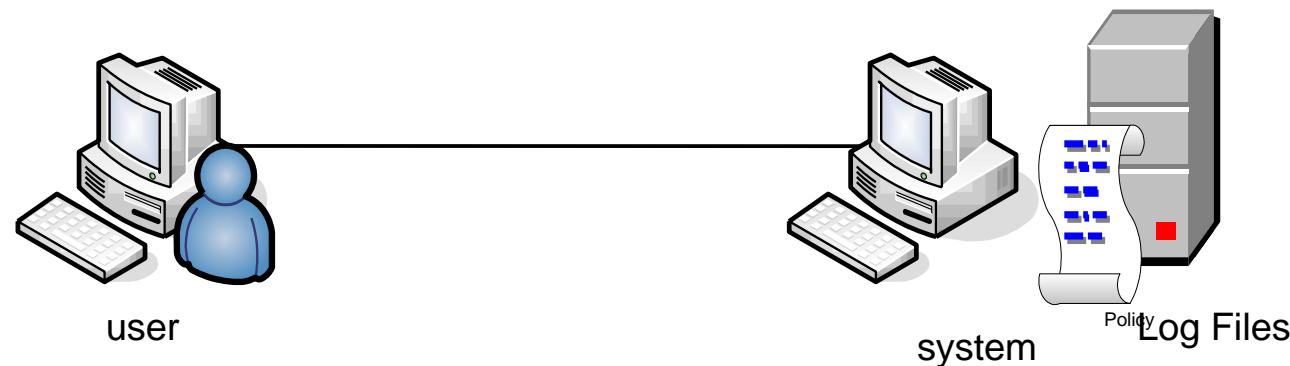


Điều khiển truy cập

- Các loại điều khiển truy cập
 - Truy cập bắt buộc
 - Truy cập tùy ý
 - Truy cập theo người dùng

Điều khiển truy cập

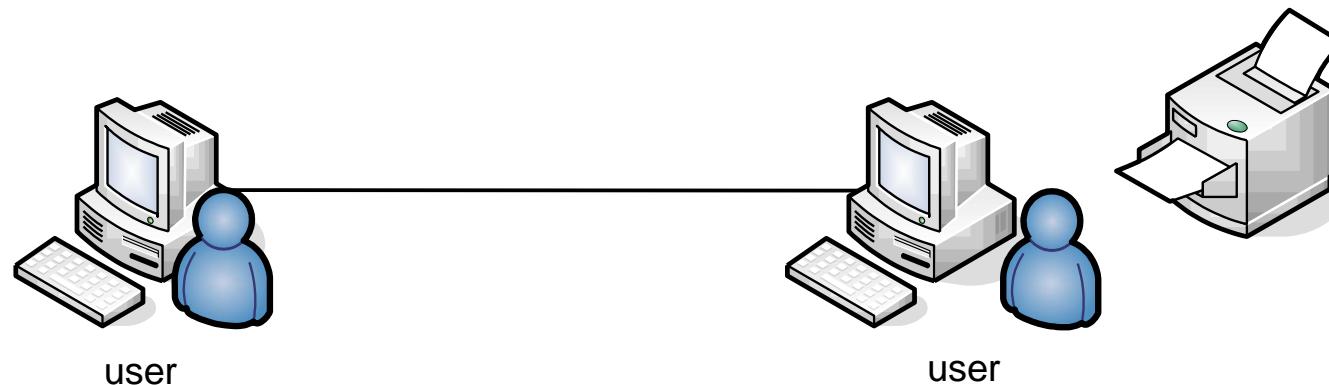
- Điều khiển truy cập bắt buộc (Mandatory Access Control)



- Việc bảo vệ dữ liệu không được quyết định bởi người dùng thông thường
- Hệ thống yêu cầu phải bảo vệ dữ liệu
- Ví dụ: Thư mục dùng chung trên máy chủ, người dùng không thể thay đổi được

Điều khiển truy cập

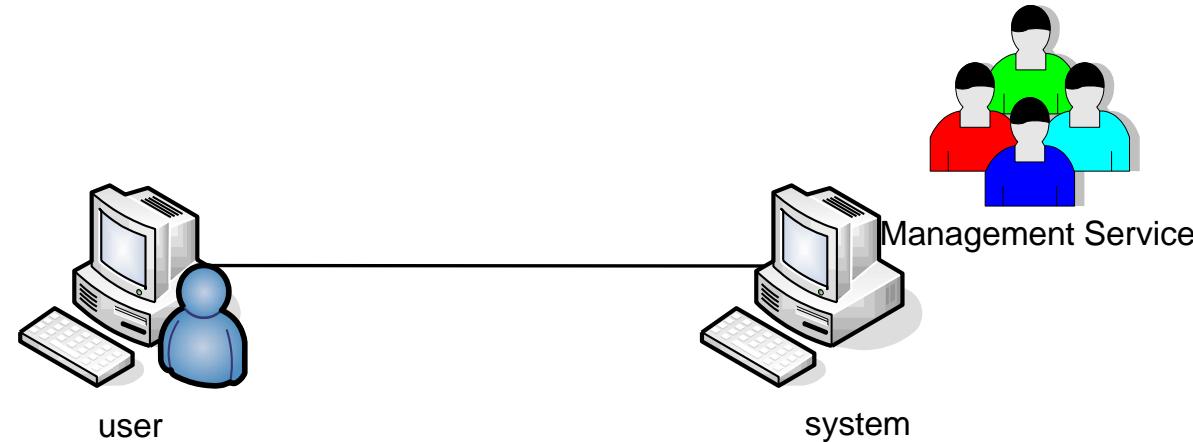
- Điều khiển truy cập tùy ý (Discretionary Access Control)



- Người dùng tự mình tạo quyền truy nhập
- Ví dụ: Chia sẻ máy in cho người khác sử dụng

Điều khiển truy cập

- Điều khiển truy cập theo người dùng (Role-based Access Control)



- Quyền truy cập được định nghĩa theo vai trò của người dùng:

- * Administrator
- * Power User
- * Dial-up User
- *

Tổng kết

- Chứng thực người dùng – phân quyền sử dụng
 - Khái niệm
 - Các phương pháp chứng thực người dùng

Thảo luận

- Nhóm 1: RADIUS
- Nhóm 2: Kerberos
- Nhóm 3: CHAP
- Nhóm 4: Certificate
- Yêu cầu: mô tả hệ thống/ triển khai thực nghiệm trên môi trường giả lập