Network Security
Session 4

Hakim Sabzevari university
Dr.Malekzadeh

Security Solutions

Authentication

Authentication

- Authentication is the process of determining whether someone or something is who or what it claims to be.
- This can include both User authentication and also Machine authentication.

Access Control = authentication + authorization + accounting

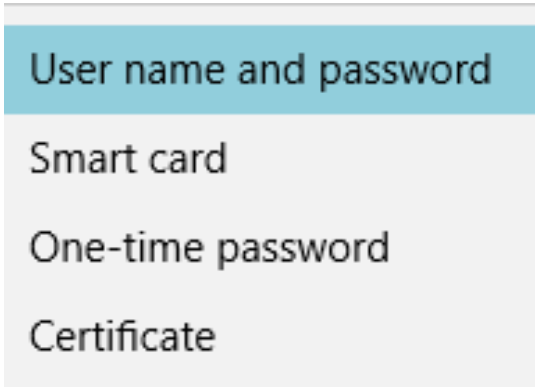
How authentication works

- During authentication, credentials provided by the user are compared to those on file in a database of authorized users' information either on the local operating system or through an authentication server.

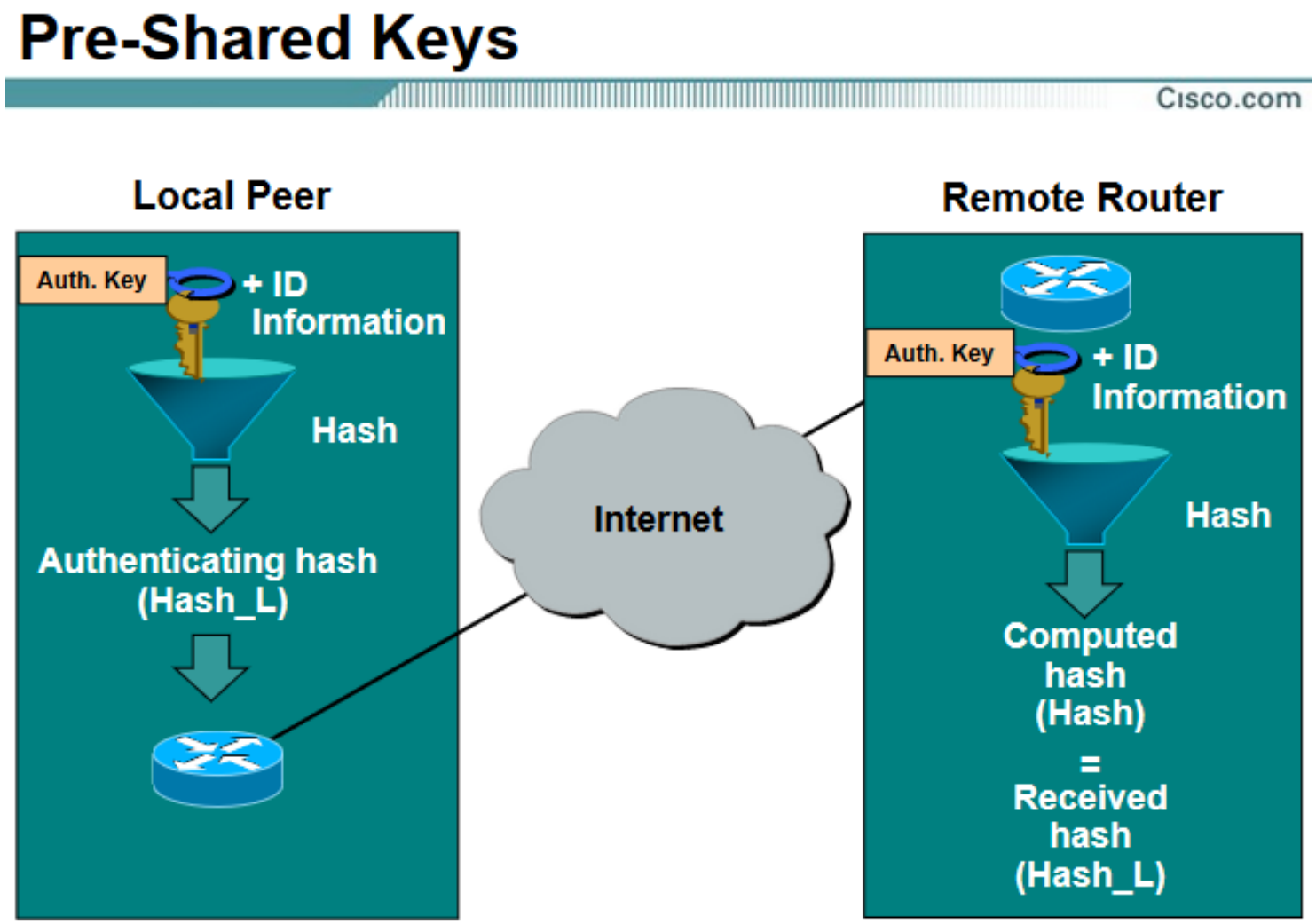
- If the credentials match, and the authenticated entity is authorized to use the resource, the process is completed and the user is granted access.

Authentication methods

- Common methods that can be used in an authentications system:
  - Pre-shared key authentication (username and password)
  - Factor-based Authentication
  - Public-Key Authentication



Pre-shared key authentication



Authentication factors

- Authentication can be done based on different parameters which are called authentication factors.
- An authentication factor represents some piece of data or attribute that can be used to authenticate a user requesting access to a system.
- Each authentication factor covers a range of elements used to authenticate or verify a person's identity prior to being granted access, approving a transaction request, signing a document or other work product, granting authority to others, and establishing a chain of authority.

Authentication factors cont…

- Currently used authentication factors include:
  - Knowledge factor: something you know such as password, PIN, or an answer to a question
  - Inherence factor: something you are like biometric data, such as fingerprints
  - Location factor: where you are
  - Time factor: when you are authenticating
  - Possession factor: something you have such as token, credit card, or mobile device

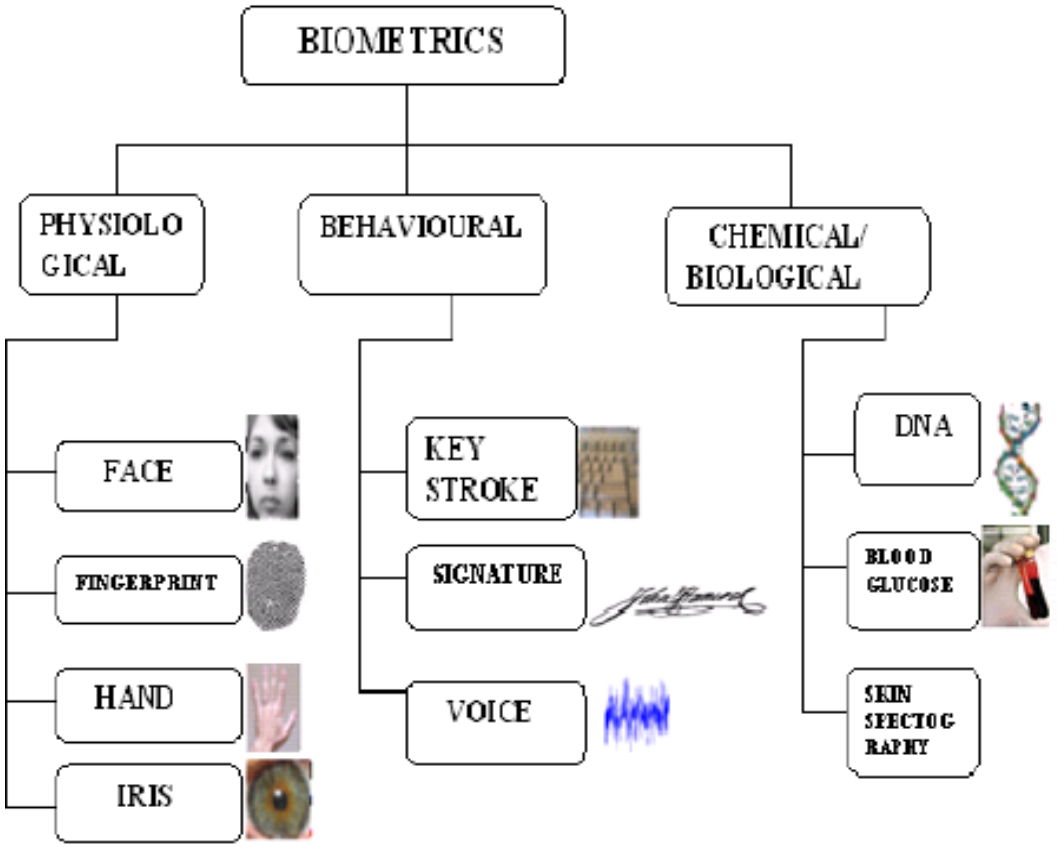
Knowledge factor

- Knowledge factor: "Something you know."

- The knowledge factor may be any authentication credentials that consist of information that the user knows, including a personal identification number (PIN), a user name, a password, or the answer to a secret question.

Inherence factor

- Inherence factor: "Something you are."
- The inherence factor is typically based on some form of biometric identification, including finger or thumb prints, facial recognition, retina scan or any other form of biometric data.



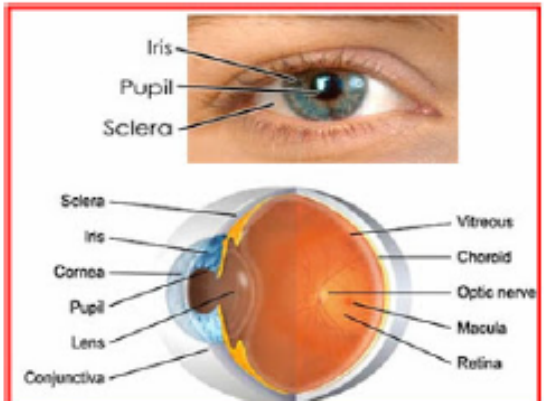
Inherence factor cont…

Iris scanner

IRIS - colored section of an eye
scan = 2 seconds of near IR imaging ☺
subject can be at some distance ☺
alcohol consumption changes iris ☹

Retina scanner

RETINA - cannot be seen by naked eye - the network of blood vessels
most reliable biometrics, aside from DNA ☺
scan = 20 seconds of low-energy IR scanning ☹
subject has to be close to scanner ☹



Possession factor

- Possession factor: "Something you have."

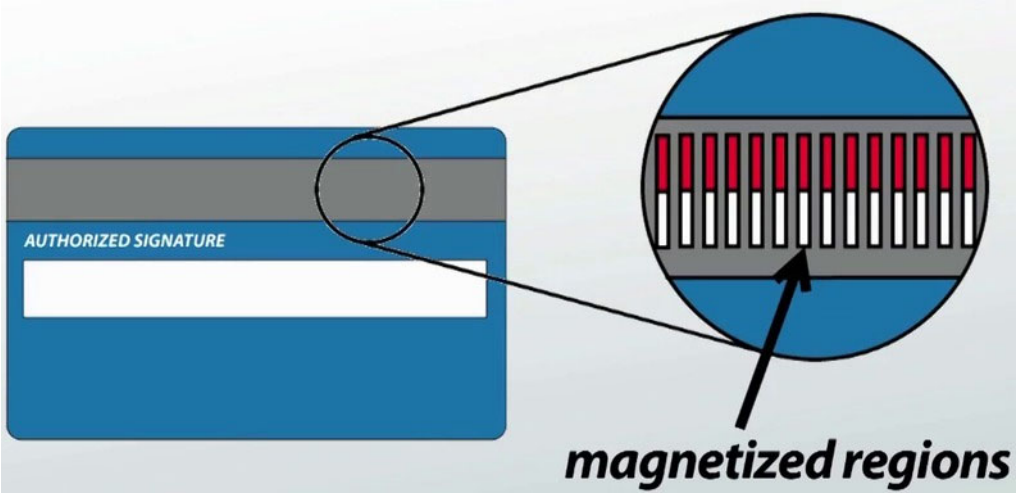
- The possession factor may be any credential based on items that the user can own and carry with them, including hardware devices like:
  - a security token
  - or a mobile phone used to accept a text message or to run an authentication app that can generate a one-time password or PIN.

Security Token

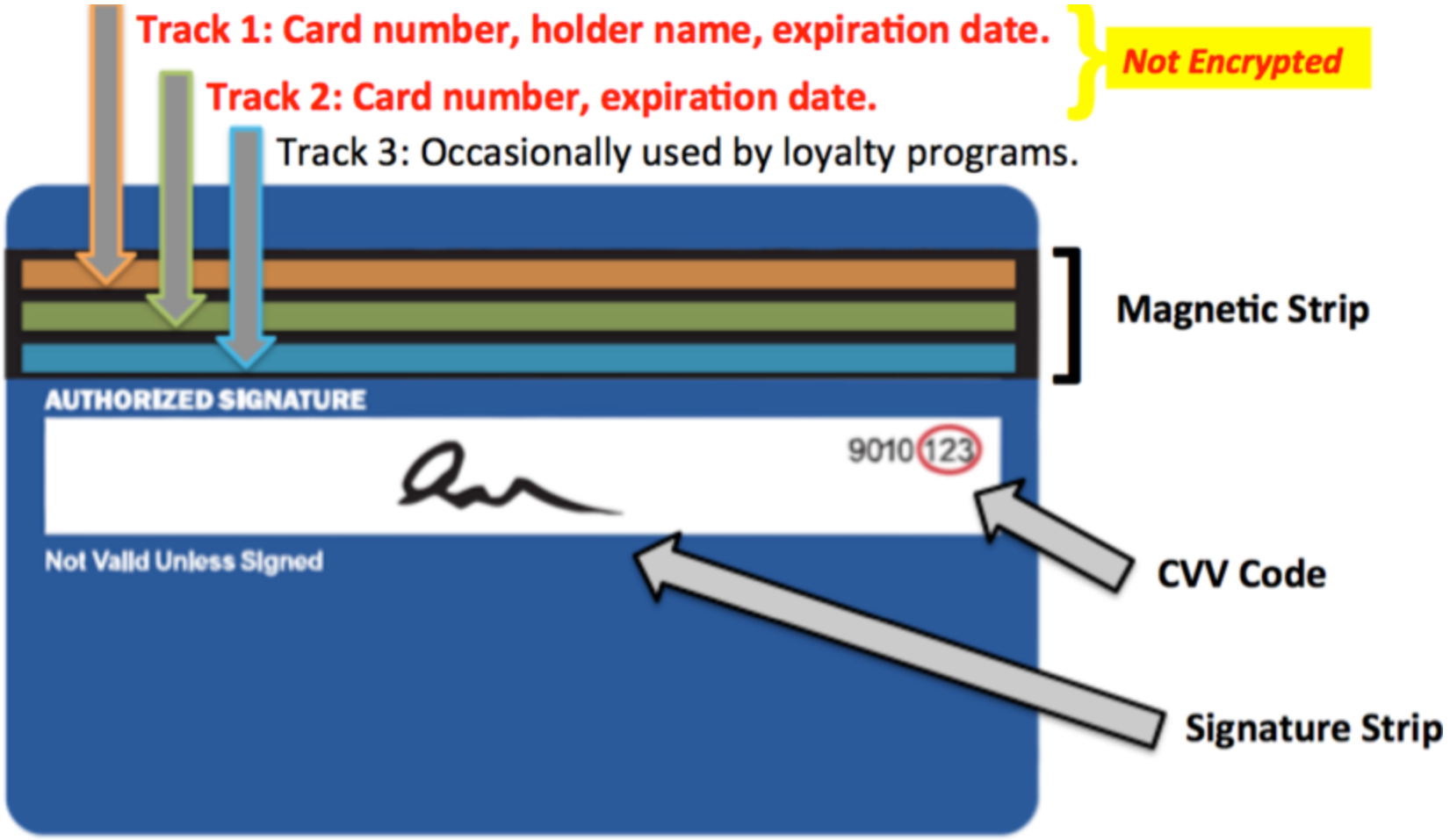
- The security tokens are generally divided into 2 groups:
  - Hardware token: are physical devices
    - swipe cards
    - smart card
      - RFID
      - NFC
    - synchronous tokens: one-time password (OTP) keyfobs
    - asynchronous tokens: challenge-response
  - Soft token: incorporated into smartphones

Swipe cards

- A magnetic stripe card/Magstripe card/Swipe card is a card with a stripe that contains information identifying you and the card. Information stored in the stripe includes your name, account number, and the card's expiration date.
- The Personal Identification Number (PIN) is not on the card -- it is encrypted in a database. For example, before you get cash from an ATM, the ATM encrypts the PIN and sends it to the database to see if there is a match.
- Magnetic Stripe cards can be read "by contact" by a magnetic card reader normally found on POS, ATMs, Hotel doors and other readers integrated on specific devices.



Swipe cards cont…



Smart cards

- A smart card/Europay MasterCard Visa (EMV) card, which is similar in size to a credit card or ATM card, stores data on a thin microchip embedded in the card.
- Smart cards contain a processor and have input, process, output, and storage capabilities.
- When you insert the smart card in a specialized card reader, the information on the smart card is read and, if necessary, updated.
- Uses of smart cards include SIM cards; ID cards, storing medical records such as vaccination data and other health care or identification information; tracking information such as customer purchases or employee attendance; storing a prepaid amount of money such as for student purchases on campus; authenticating users such as for Internet purchases or building access.

Smart cards cont…

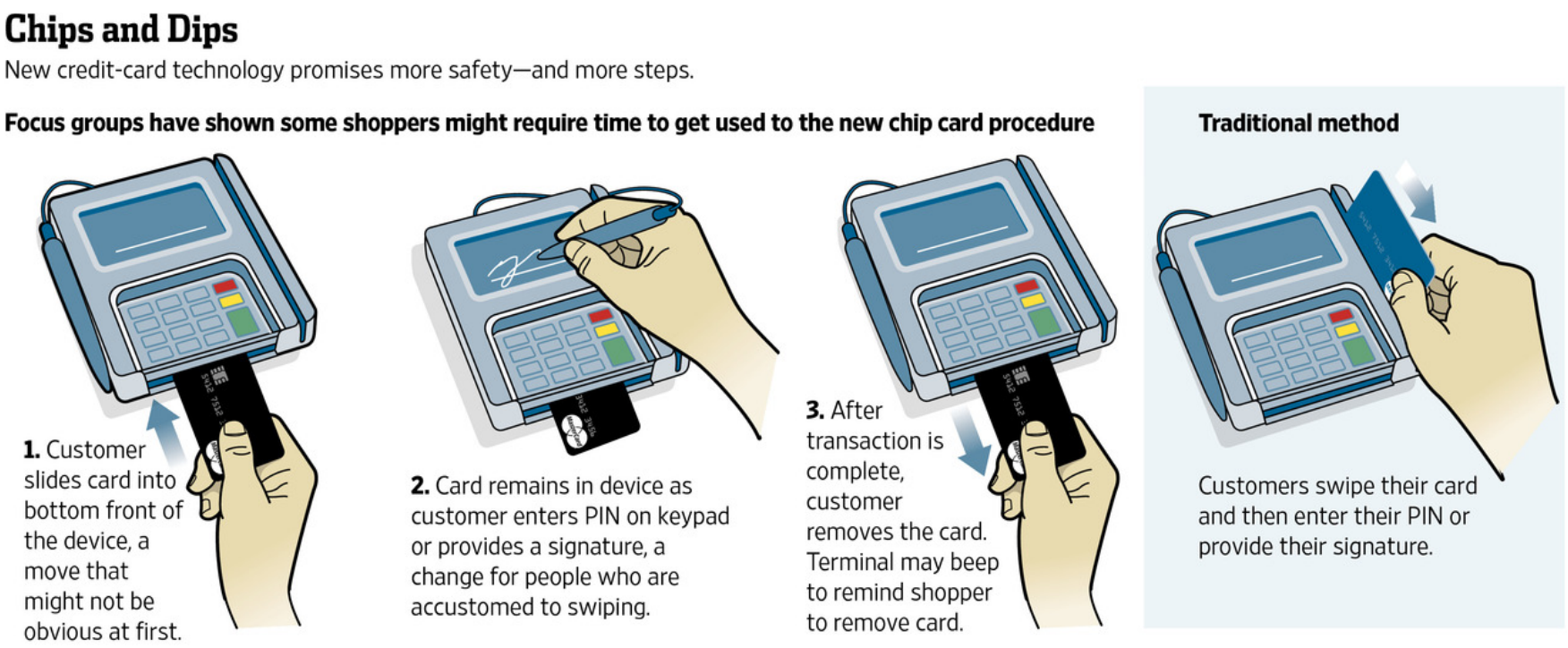
- There are two types of smart cards:
  - Contact cards: the card connects to a reader with direct physical contact
  - Contactless cards: the card connects to a reader with a remote contactless (chip+antenna) interface.

Contact smart cards

- There are two types of chip contact cards:
  - chip and PIN cards: A consumer will enter their PIN to authorize a purchase like magnetic strip cards.
  - chip and signature cards: A consumer using a chip and sign card will sign to authorize a purchase

	How it works	How to use	How to verify	Can be used abroad
Swipe & Sign	Magnetic Stripe	Swipe	Signature	Sometimes
Chip & Sign	Microchip	Insert	Signature (PIN upon request)	Mostly
Chip & PIN	Microchip	Insert	PIN	Yes

Contact smart cards cont…



Card dipping is the insertion of a card into a reader

Contactless smart cards

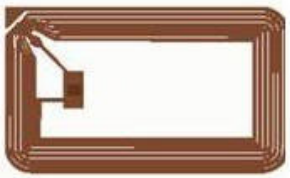
- The Contactless card connects to a reader with a remote contactless (chip+antenna) interface.

- They use radio frequency identification (RFID) or near field communication (NFC).

RFID

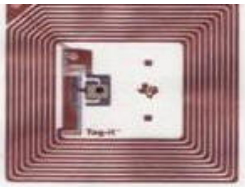
- A form of Smart Card is RFID tag with the following applications:
  - Access Control System
  - Identification
  - Object Tracking
  - …

RFID Tags Types



Paper Tag

EPC Tag



Inlay Tag

Button Tag

Metal Tag

Glue Tag

Key Tag

Glass Tube Tag

Ear Tag

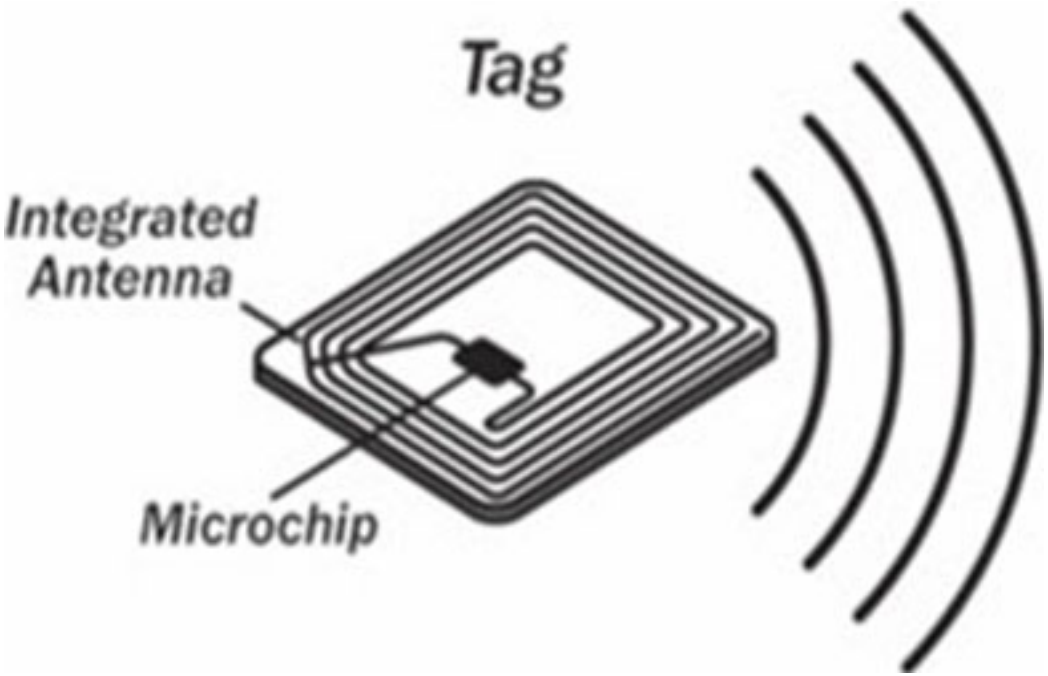
Ceramic Tag

Disc Tag

Pocket Tag

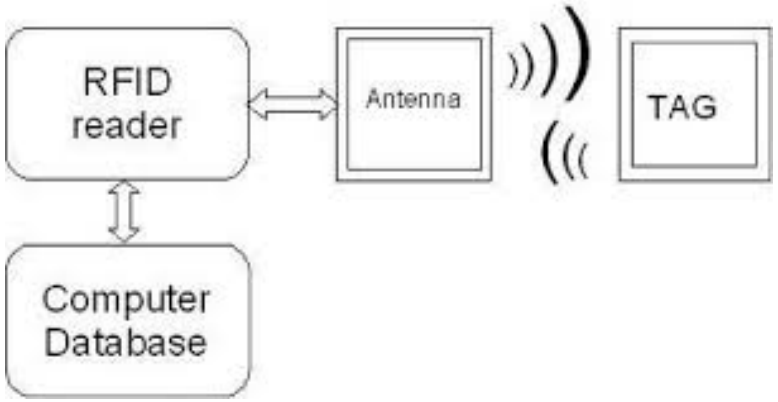
RFID cont…

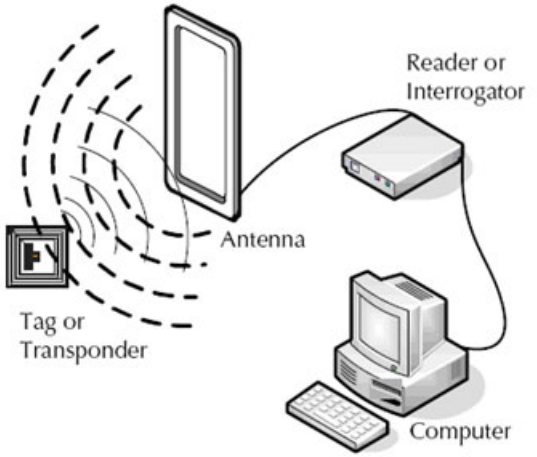
- Tags, which includes all of the information about a product, will typically contain an antenna and microchip



How RFID Works

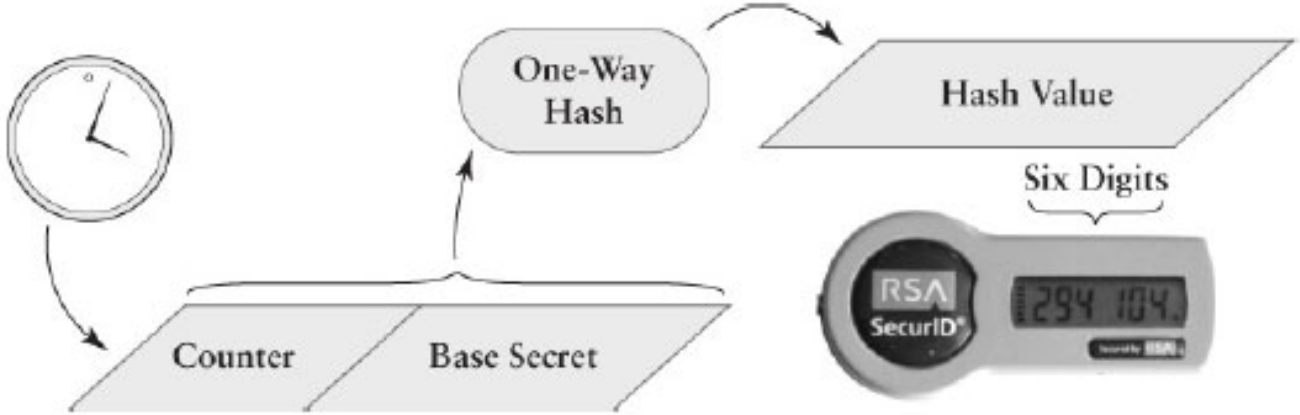
- An RFID system consists of an RFID tag and a reader to decode and interprets data on a tag. These three pieces fit into a process where:
  - Data is first stored in an RFID tag in either a read-only or read-write format. The tag is either battery powered or passive.
  - When the tag comes within range of a scanning antenna, electromagnetic (EM) energy triggers the tag to start sending data in the form of radio waves.
  - These radio waves are picked up by the antenna and send to the reader which decodes the waves as digital information.





Synchronous tokens: one-time password (OTP) keyfobs

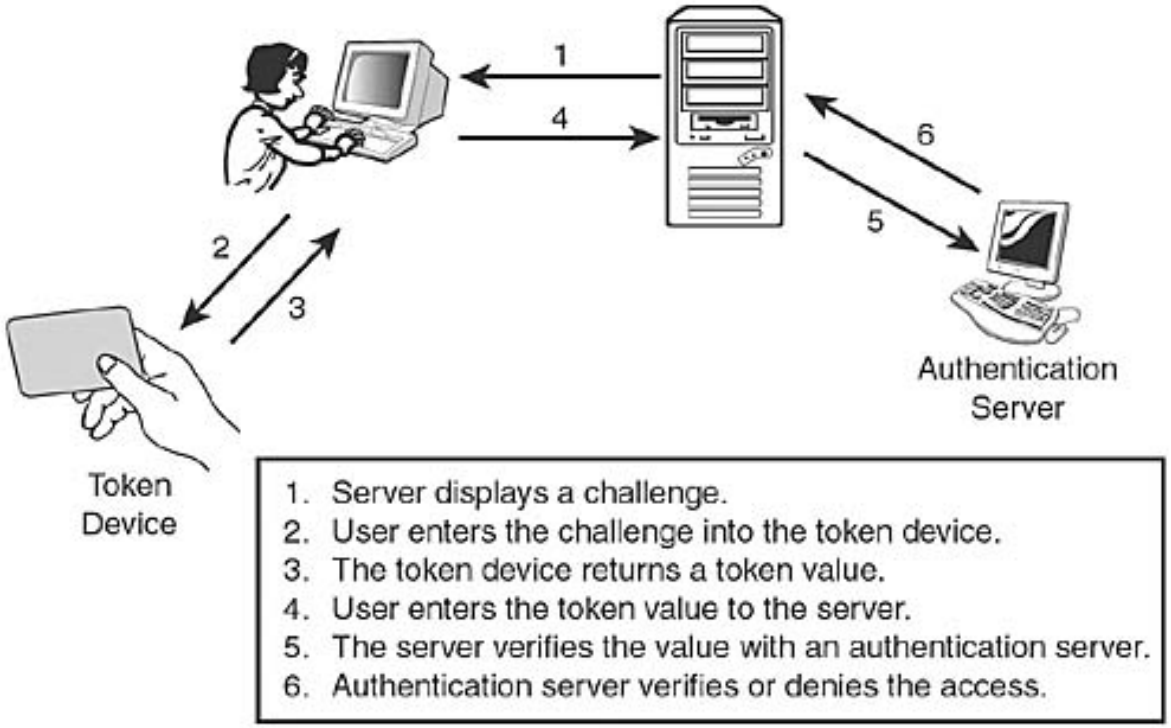
- Small LCD device that generates a unique new password periodically on demand (e.g., every 60 seconds).
- The Keyfob/token combines 'base secret' with clock to generate new password
- token and authentication server must have their clocks synchronized – which is often a challenge!



- Hardware token:
  - swipe cards
  - smart card
    - RFID
    - NFC
  - synchronous tokens:
  - asynchronous tokens:
- Soft token:

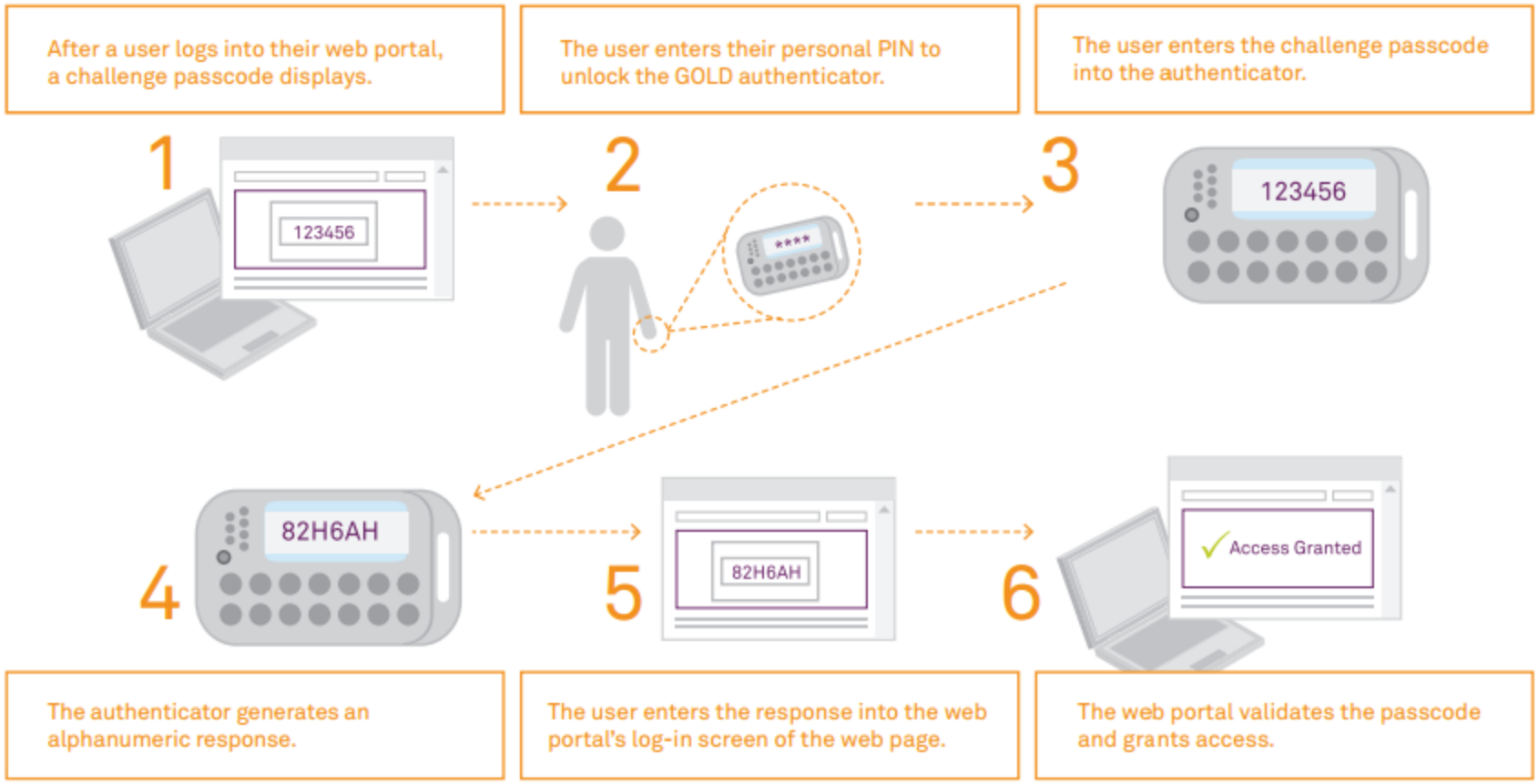
Asynchronous tokens: challenge-response

- An asynchronous token also generates an OTP, but do not use time synchronization between token and authentication server. Instead, a random challenge/nonce is generated and sent to the user who enters the challenge into the token device. The token generates a response that the user sends back to the authenticator.



Asynchronous tokens cont…

- The challenge response mechanism requires users to validate a numeric challenge on their authenticator device. Only after validation, the device generates an OTP passcode which is used to complete the authentication procedure.



Soft token

- A soft token is a software-based security token that generates a single-use login PIN which is an automatically generated numeric or alphanumeric string of characters that authenticates a user. This password is only valid for one login session or transaction for a fixed period of time (e.g. 90 seconds).
  - It can be used, as a second step, to confirm a transaction (رمز تایید).
  - It can be used for new users, or for users who lost their passwords and are given a one-time password to log in and change to a new password.

- SMS is used as a delivery channel for a one-time password generated by information system.

  - Hardware token:
    - swipe cards
    - smart card
      - RFID
      - NFC
    - synchronous tokens:
    - asynchronous tokens:
  - Soft token:

Authentication factors cont…

- Adding authentication factors to the authentication process typically improves security.

- Based on the number of factor used for authentication we have:
  - single-factor authentication
  - multi-factor authentication

single-factor authentication

- Traditional authentication depends on the use of a password file, in which user IDs are stored together with hashes of the passwords associated with each user.
- Authenticating a user with a user ID and a password is usually considered the most basic type of authentication, and it depends on the user knowing two pieces of information: the user ID or username, and the password.
- Since this type of authentication relies on just one authentication factor, it is a type of single-factor authentication.

multi-factor authentication (2FA)

- Two-factor authentication adds an additional layer of security to the authentication process by making it harder for attackers to gain access to a person's devices or online accounts, because knowing the victim's password alone is not enough to pass the authentication check.

- Strong authentication usually refers to authentication that uses at least two factors, where those factors are of different types.

- The distinction is important; since both username and password can be considered types of knowledge factor, basic username and password authentication could be said to use two knowledge factors to authenticate -- however, that would not be considered a form of two-factor authentication (2FA). Likewise for authentication systems that rely on "security questions," which are also "something you know," to supplement user ID and passwords.

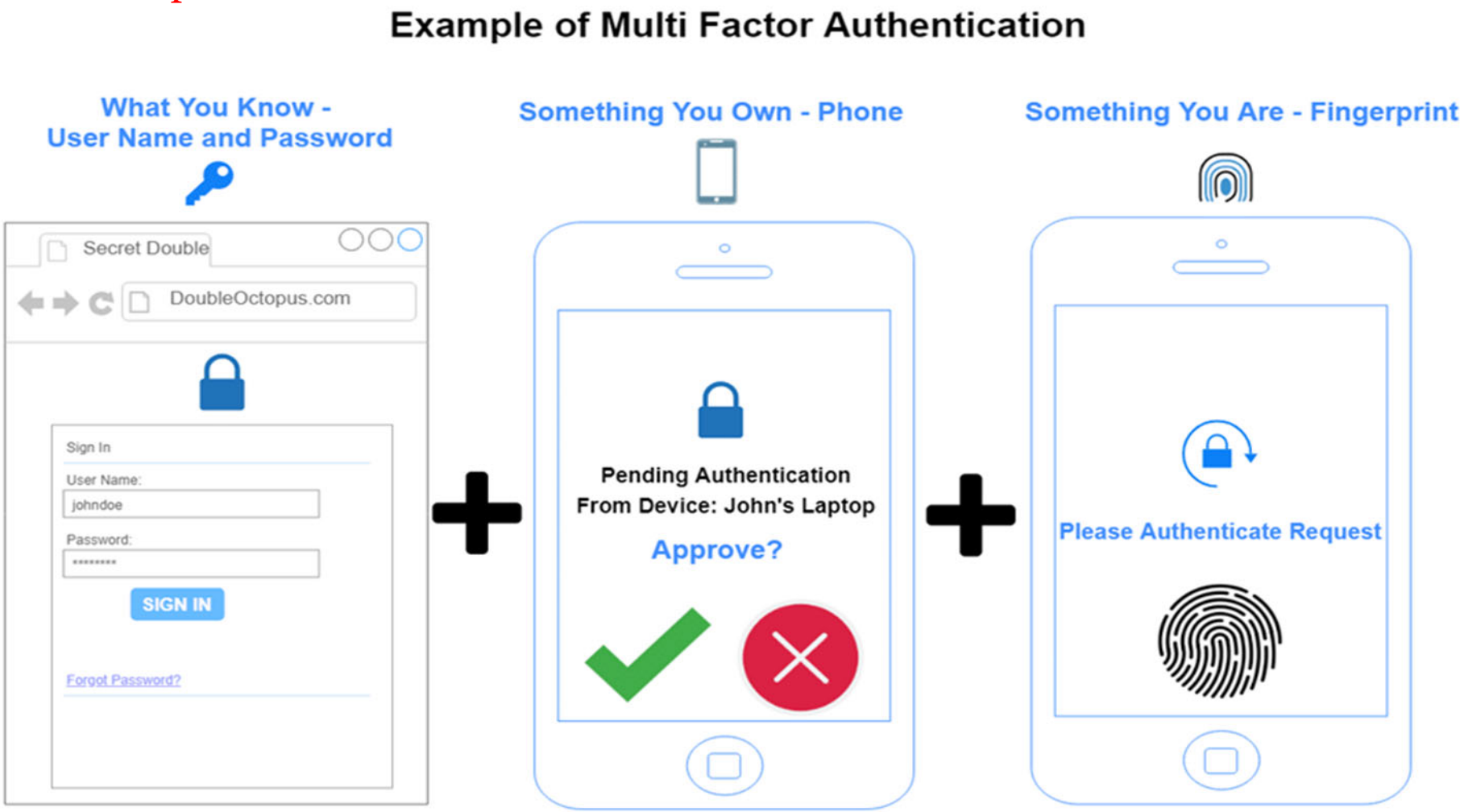
multi-factor authentication cont…

- Multi-factor authentication (MFA) is a method of confirming a user's claimed identity in which a user is granted access only after successfully presenting 2 or more pieces of evidence (or factors) to an authentication mechanism: knowledge (something they and only they know), possession (something they and only they have), and inherence (something they and only they are).

- Two-factor authentication (2FA) is a type (subset) of multi-factor authentication. It is a method of confirming a user's claimed identity by utilizing a combination of *two* different factors: 1) something they know, 2) something they have, or 3) something they are.

multi-factor authentication cont…

- With multi-factor authentication, a user must prove at least 2 of these independent factors.



Public-key authentication

- In conventional password authentication, you prove you are who you claim to be by proving that you know the correct password. This means that if the server has been hacked, or spoofed, an attacker can learn your password.

- Public key authentication solves this problem. Public key authentication is an alternative means of identifying yourself to a login server, instead of typing a password. It is more secure and more flexible, but more difficult to set up.

- The motivation for using public key authentication over simple passwords is security.

  - Pre-shared key authentication (username and password)
  - Factor-based Authentication
  - Public-Key Authentication