Authentication

What is Authentication ?

Authentication is the act of confirming the truth of an attribute of a datum or entity.

This might involve confirming the identity of a person or software program, tracing the origins of an artifact, or ensuring that a product is what its packaging and labeling claims to be.

Authentication often involves verifying the validity of at least one form of identification.

Authentication in simple term

- Positive verification of identity (man or machine)
- Verification of a person's claimed identity
- 3 Categories:
  - What you know
  - What you have
  - Who you are

Review: 3 Categories

- What you know
  - Password
  - PIN
- What you have
  - e-Token
  - RFID
  - Certificate
- Who you are
  - Biometrics

Four main types of authentication available are:

- Password based authentication
- Certificate based authentication
- E-Token based authentication
- Biometric based authentication

Password based authentication :

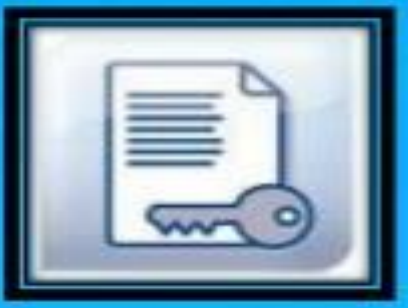
- Password are the most common form of authentication.
- Password may be a string of alphabets ,numbers and special characters
- This password is compulsorily to be known by the ENTITY or the THING or a PERSON that is being Authenticated

How does the Authentication Process takes places(password)..

Steps :

1. Prompts for user id and password.
2. User enters user id and password.
3. User id and password validation.
4. Authentication result back to the server.
5. Inform user accordingly.

Certificate based authentication :



- A certificate is a digital document that at a minimum includes a Distinguished Name (DN) and an associated public key.

- The certificate is digitally signed by a trusted third party known as the Certificate Authority (CA).Digital Certificates can then be reused for user authentication.

- Certificate based authentication is stronger as compared to password based authentication.

- Because here the user is expected to HAVE something(CERTIFICATE) rather than to KNOW something(PASSWORD).

Certificate based authentication is an electronic document that contains information on:

(1) The Entity it belongs to…

(2) The Entity it was issued by…

(3) Unique serial number or some other unique identification…

(4) Valid dates …

(5) A Digital fingerprint…

How does the Authentication Process takes places(certificate)..

Steps :

1. Creation, storage and distribution of DC(Digital Certificate).
2. Login request (user to server).
3. Server creates a random challenge.
4. User signs the random challenge.
5. Server returns an appropriate message back to the user.

E-Token based authentication :

- An authentication token is a small device that generates a new random value every time it is used.
- This random value becomes the basis for authentication{an alternative to a password}
- Can be implemented on a USB key fob or a smart card.
- Data physically protected on the device itself
- May store credentials such as passwords, digital signatures and certificates, and private keys.

Usually an Authentication Token has the foll components or features:

1. Processor.
2. LCD for displaying outputs or random values.
3. Battery.
4. Small keypad for entering information.
5. Real-time clock.

optional

How does the Authentication Process takes places(e-token)..

Steps :

1. Creation of a token.
2. Use of token.
3. Token validation.
4. Server returns an appropriate message back to the user.

Biometric based authentication :

- **Biometrics** (or **biometric authentication**) refers to the identification of humans by their characteristics such as fingerprint, voice, Iris pattern of the eye, vein pattern, etc.

- Biometrics is used in computer science as a form of identification and access control.

- It is also used to identify individuals in groups that are under observation.

How does the Authentication Process takes places(Biometric)..

- The user database contains a sample of user's biometric characteristics

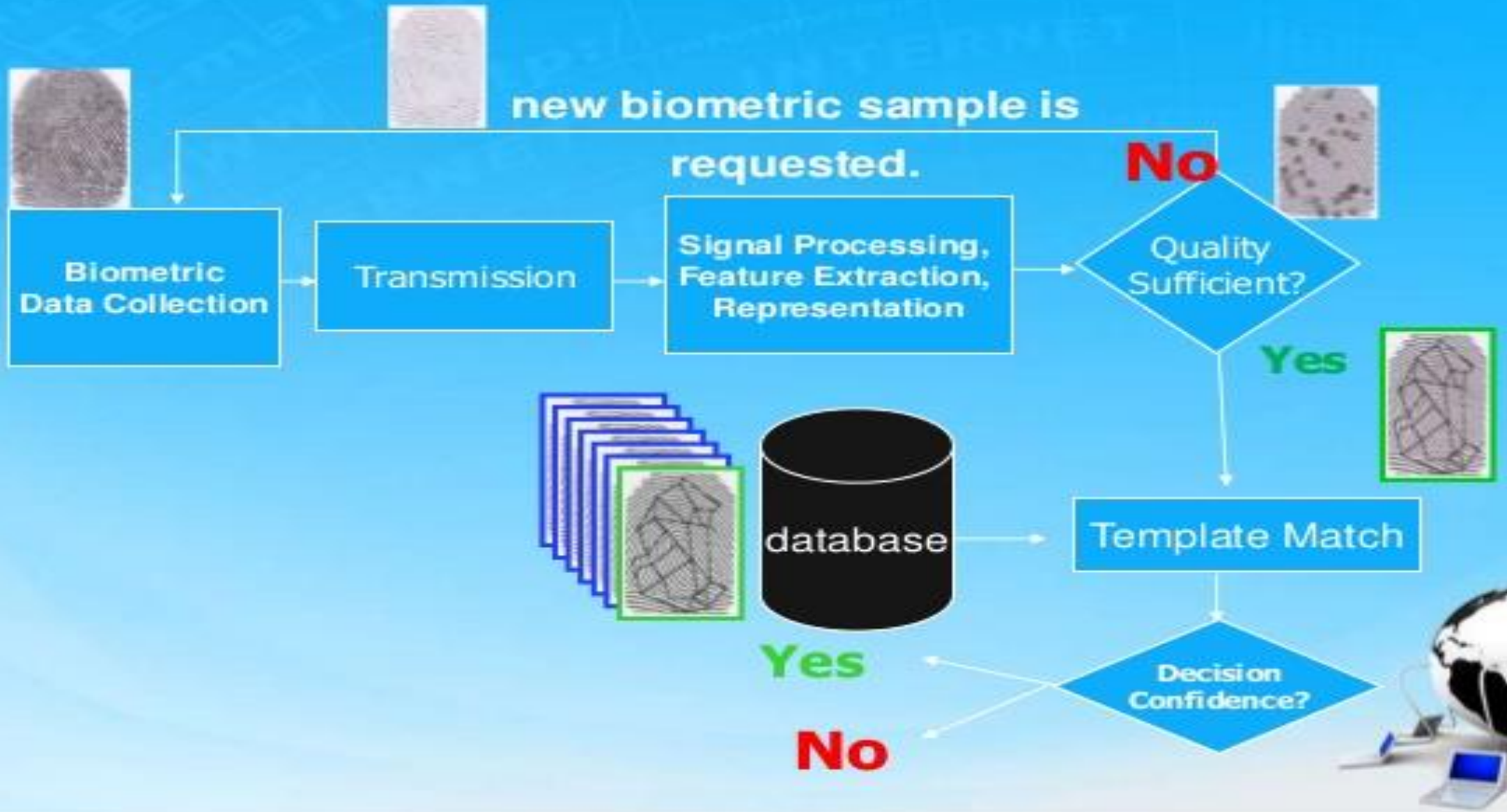
- During Authentication process, the user is required to provide a new sample of the user's biometric.

- This sample is sent to encryption.

- This current sample is decrypted & compared.(if the sample matches)

- User is considered as valid one

Biometrics Process



The common Physical characteristics are:

- Fingerprint
- Face
- Retina
- Iris
- Vein pattern
- Hand and finger geometry

The Behavioral characteristics are:

Keystroke dynamics

Voice

Gait

Signature dynamics

Signature Verification Process

- ✓ The angle at which the pen is held
- ✓ The number of times the pen is lifted
- ✓ The time it takes to write the entire signature
- ✓ The pressure exerted by the person while signing
- ✓ The variations in the speed with which different parts of the signature are written.

Aadhaar card:

One-time standardized Aadhaar enrolment establishes uniqueness of resident via 'biometric de-duplication'

- Only one Aadhaar number per eligible individual

Online Authentication is provided by UIDAI

- Demographic Data (Name, Address, DOB, Gender)
- Biometric Data (Fingerprint, Iris, Face)

Aadhaar :subject to online authentication is proof of ID

Advantages of biometrics

1. Uniqueness
2. Universality
3. Performance
4. Measurability
5. User friendly
6. Accuracy
7. Comfort