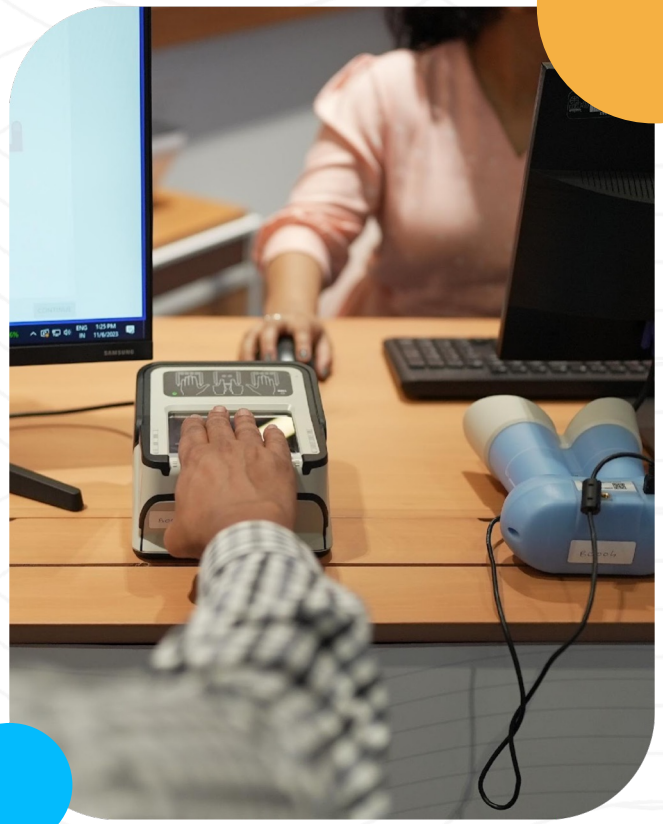
The Biometrics Journey

Ensuring Responsible and Secure Collection and Usage

Sanjith Sundaram | Head – Partner Ecosystem, MOSIP



"Biometrics is a **unique, accurate, easy-to-use and non-transferable** way to identify a person."

"Biometrics is like a **non-changeable password**; once lost, it's lost forever."

Three Key Areas

Enrolment of Good Quality Biometrics **01**

Uniqueness Assurance based on biometrics – for ID Generation **02**

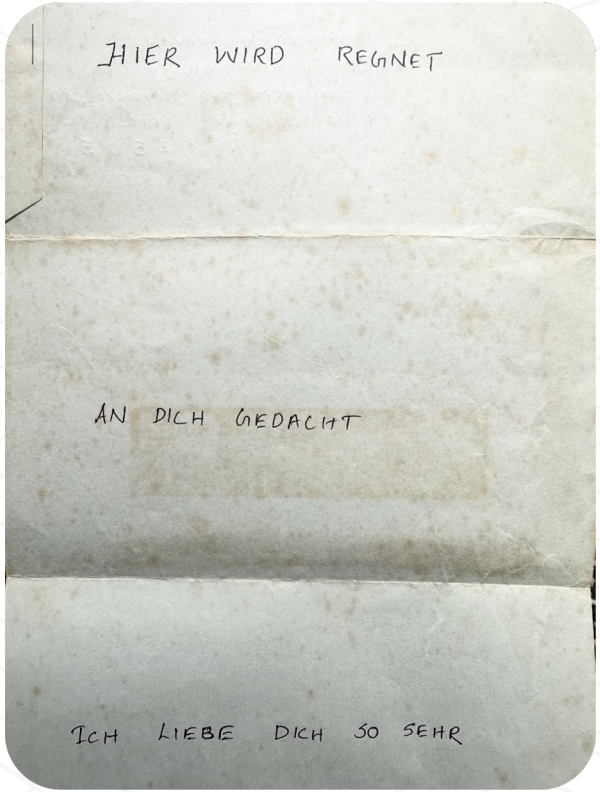
Biometric **Identity Verification** for Service Delivery **03**

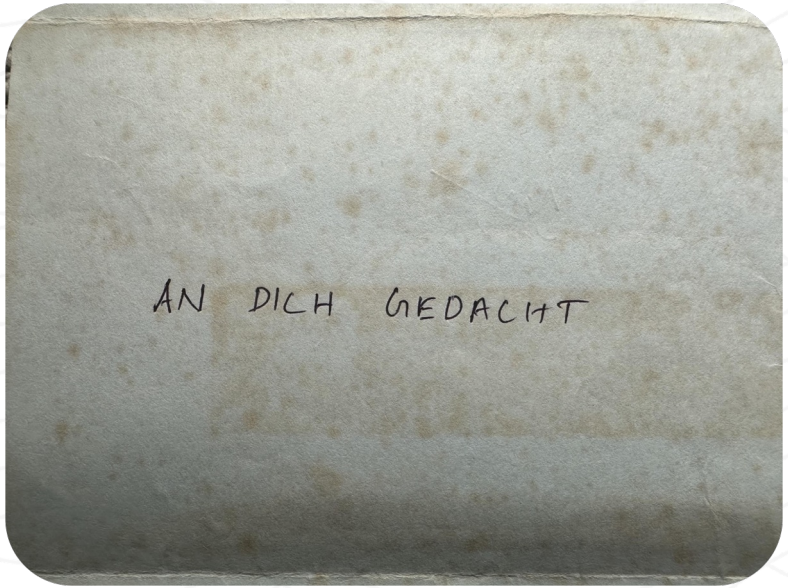
Biometric Collection

The Number Lock

Symmetric Encryption

Love
Is in the Key





The Padlock

Asymmetric Encryption

Hashing

For data integrity

FOX → Hashing Function → ACDE

FOX → Hashing Function → ACDE

FOx → Hashing Function → BDFG

Digital Signature

Authentication | Non-Repudiation | Integrity

PRIVATE KEY

Specimen Signature

PUBLIC KEY

Capture → ID System

Device

Hash + Encrypt + Digitally Sign

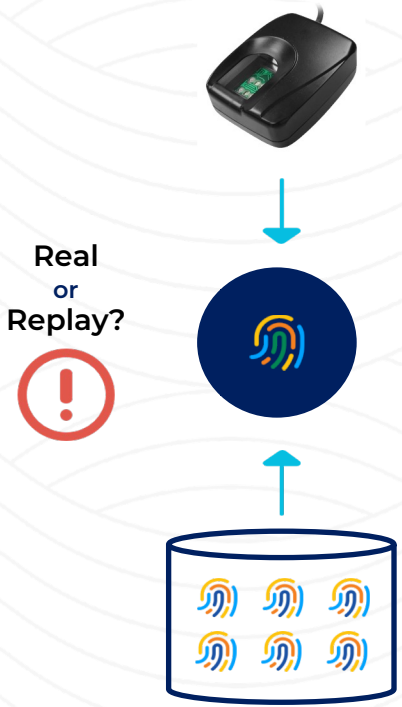
01.
Encrypt Using Random Session Key – 123

02.
Encrypt the key using ID System's Public Key

ID System

PRIVATE KEY

Is that Sufficient?



01
Is it a replay of biometrics? Scalable Attack!

02
Is it a certified biometric device used?

03
How to talk to the device in a standard way?

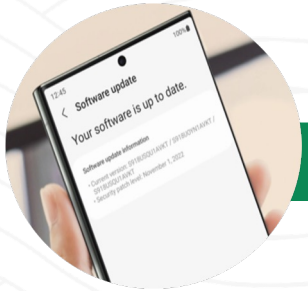
Secure Biometric Interface

SBI Service

Qualified Capture Environment ensuring no external biometrics are injected

Managed Devices

Central Server Managing the SBI and Cryptography



Just like your phone!

Biometric Deduplication

ABIS Engine

New Enrolment

1:N Match

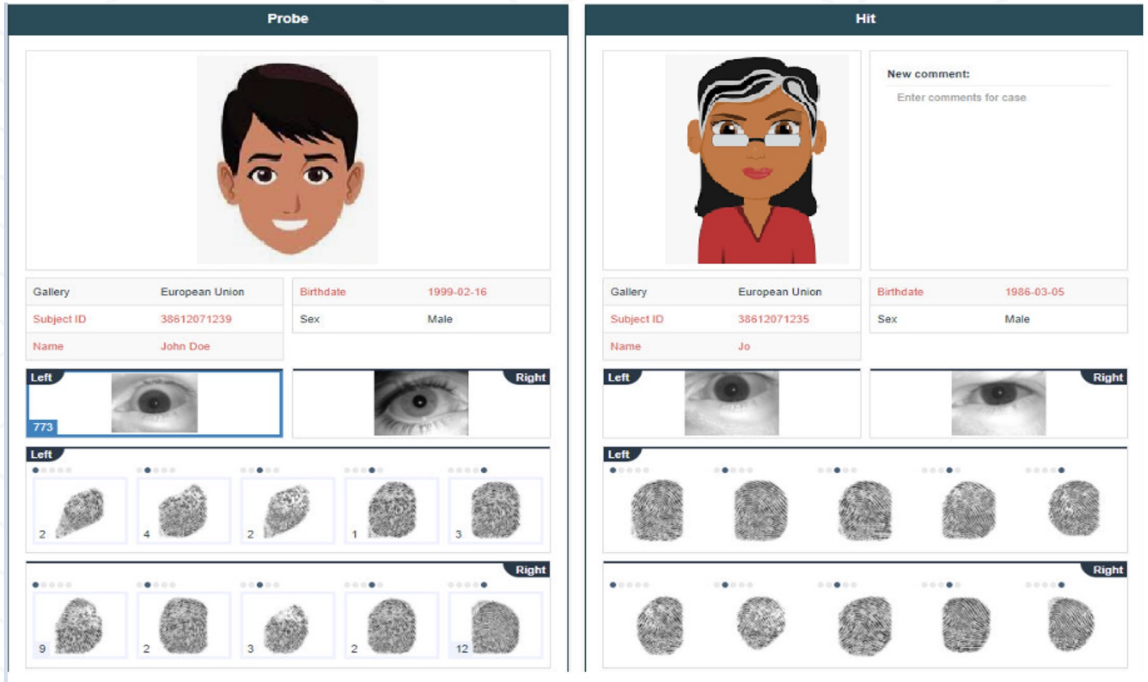
Possible Results

01
Not matching with any previous IDs
Safe to generate new ID

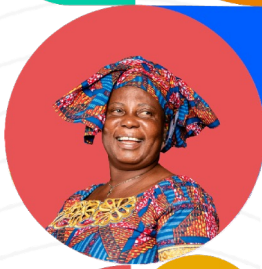
02
Matching with previous IDs
Check carefully before issuing ID

Abstracted: Avoiding Identification!

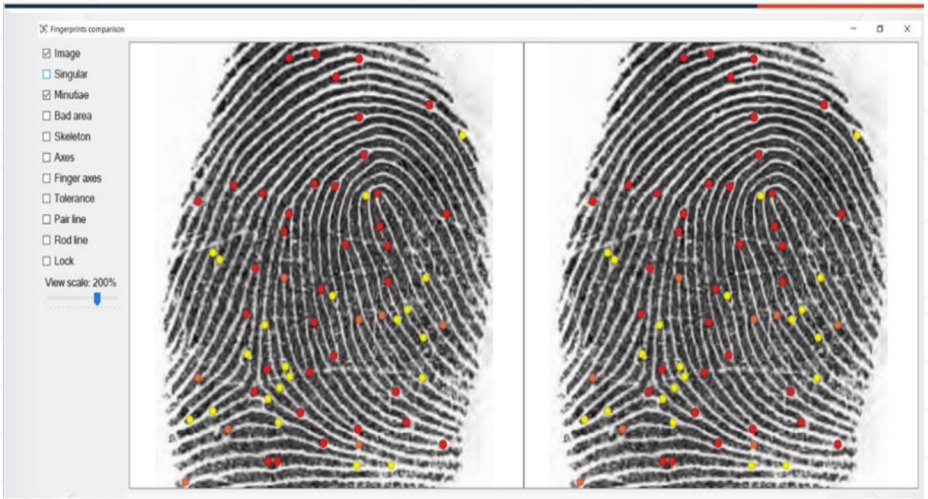
Manual
Adjudication



New Registration **Potential Match**



Manual
Adjudication



New Registration **Potential Match**

Possible Results

01 It is a duplicate;
Do not issue an ID

02 It is not a duplicate;
Issue an ID

What's your Tolerance?

Why Fine Tune the ABIS?

FNIR

(False Negative Identification Rate)

High FNIR = More duplicates in the system

FPIR

(False Positive Identification Rate)

High FPIR = More load on Manual Adjudication

How many duplicates can you allow in the system?

How trustworthy is your system?

Balance is the key!

Biometric Match

Inclusion – Identity Verification

Possible Results

01 I am not confident;
Not a match!

02 I am confident;
It's a match!

Threshold = The level of confidence needed to declare a match!

How do you set the match success criteria (or threshold) ?

How inclusive are you?

FRR
(False Reject Rate)

A genuine person is not able to authenticate

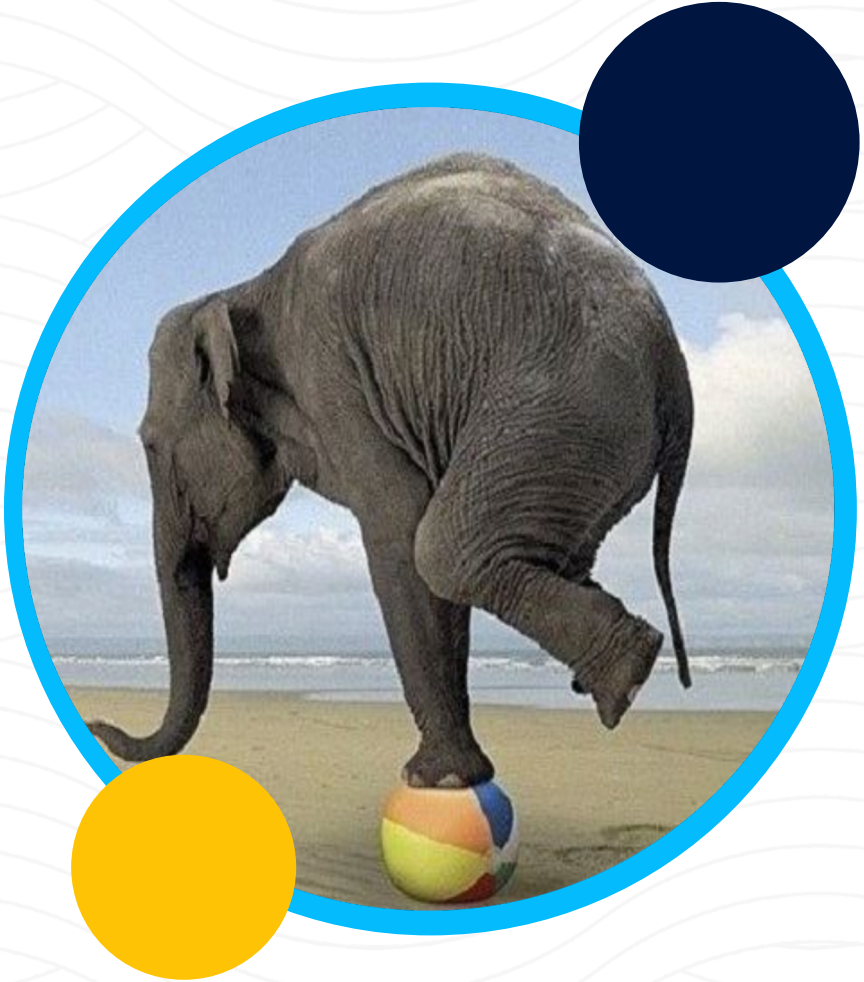
FAR
(False Accept Rate)

An Imposter is able to authenticate

<2% FRR @ 0.01 FAR

Match thresholds = Genuine people failing

Match thresholds = Imposters being successful



Again, Balance is key!

Thank you!