

ICAO 

2024 **TRIP**
ICAO
SYMPOSIUM

MONTRÉAL , CANADA | NOVEMBER 13-15



“Biometrics in Migration Management”

Nelson Goncalves

Head, Legal Identity Unit, International
Organization for Migration (IOM)

Field of use

- Birth registration and legal identity of every child
- Family tracing and family reunification
- Travel documents to ensure the right to leave and the right to return to ones' country
- Registration of migrants
 - In detention centers
 - In other centers (temporary, reception centers, etc.)
 - In need of services, including irregular migrants
 - Registration of migrants/victims of trafficking in need of protection and assistance
- Return of Internally Displaced Persons (IDPs) – registration of IDPs for access to their rights and corresponding services
- Resettlement

IOM's Data Protection Framework and Biometrics

Part 1: outlines the IOM Data Protection Principles

Part 2: includes comprehensive guidelines on each principle, considerations, and practical examples

Part 3: provides generic templates and checklists to ensure that data protection is taken into account when collecting and processing personal data



IOM's Data Protection Framework and Biometrics



Purpose specification: only process biometric data for specified, explicit, and legitimate purpose



Retention limitation: retain biometric data only for the time period that is necessary for the purposes for which such personal data is being processed



Confidentiality: data must be filled and stored in a way that is accessible only to authorised personnel and transferred only through the use of protected means of communication



Transparency: provision of information that are accessible to the data subjects who are concerned about collection of their biometric data



Proportion and necessity (data minimization): only process relevant biometric data that is adequate, relevant, and limited to what is necessary



Accuracy: keep the data up-to-date in such a way to fulfil the purposes for which it is being processed



Security: technical and operational measures to ensure integrity, confidentiality, and availability of biometric data







Privacy by design: ensuring data protection are integrated as early as possible



Accessing assistance: alternative ways for authentication

IOM's Use Cases of Biometrics

MIDAS

-  MIDAS employs multiple biometric modalities such as **fingerprinting, and live personal photo** to ensure accurate identification of individuals
-  By complementing biometric data with personal identifiers, MIDAS establishes a **comprehensive profile to improve the verification processes**
-  **MIDAS mobile capacity**, allowing border agents to access and input data in real time, vastly improving the response to irregular crossings
-  **Data management:** efficient data management processes are instilled to handle and analyze generated numbers alongside biometric information, boosting operational capacity



MIDAS: key messages

FACILITATES EFFECTIVE AND EFFICIENT BORDER MANAGEMENT

- Easily **monitor travellers** entering and exiting the national territory
- **Biometrics to curtail security risks:**
 - Collecting & screening biometric data of travellers thus eliminating use of forged/fraudulent TDs.
 - Facial recognition & facial comparison capabilities – allowing to validate that TD has not been altered + verification of traveller identity.
 - Fingerprint collection for query against a biometrically-enabled watchlist.
 - Integration with visa database - validate the authenticity of the traveller's visa.

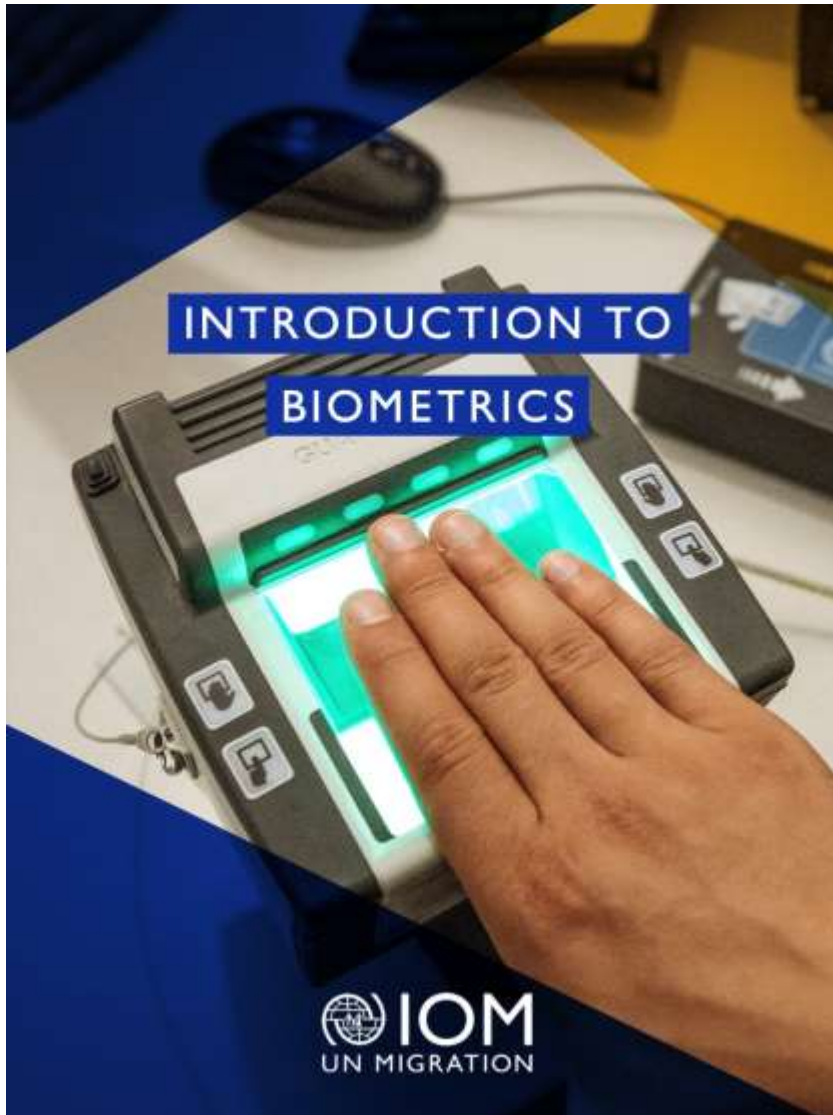


SUPPORTS EVIDENCE-BASED POLICY MAKING

- Comprehension of **migration trends and patterns** through a systematic analysis of the collected data.
- Sound **statistical basis** on migration data.

FOSTERS CROSS-BORDER E-GOVERNANCE

- MIDAS is **interoperable** with diverse solutions allowing to enhance border management controls.



- Provides **introductory operational guidance** on the recording, matching, and evaluating biometric data with a focus on technology (fingerprints, facial recognition, and iris)
- The manual highlights not only existing concerns **about vulnerabilities, threats, and potential discriminatory application of biometrics** but **also promotes the examination of new risks** and enhances the importance of data protection and human rights frameworks.
- IOM has designed the **Biometrics Master Class** – a 3-day capacity-building activity to elevate the expertise and operational capabilities of government authorities in biometric identity management

Figure 1. Initial process of collecting biometric data



Source: Visualization by the authors with elements from Shutterstock.

Identification

Identification is the process of determining who the subject is. The biometric information presented is cross-referenced to an existing database of registered individuals, identifying who the presenter is. It is also called 1:N matching, in that one person is compared against the rest of the database.

Figure 2. Process of biometric identification



Source: Visualization by the authors with elements from Shutterstock.

Authentication

Authentication is the process of establishing the claimed identity, termed as 1:1 matching. The presented biometric is cross-referenced against the pre-registered information of the claimed identity. As mentioned previously, this is also referred to as Verification.

Content of the Manual:

Part 1. Introduction to Biometrics

Part 2. Society, History, and Responsible Use

Part 3. Governance and Safeguarding

Part 4. Management of Biometrics

Part 5. Technical Implementation

Part 6. IOM Programming with Biometric Components

Part 7. Technology Looking Ahead



PEPM MOBILE APP

Border control at your fingertips
Funded by the Government of The Netherland

APP SPECIFICITIES AND CAPABILITIES

ICAO 800 • TRIP 2024

- Near Field Communication (NFC)
- Android operating system only
- On-device computation / Offline
- Scans (OCR) the Machine-Readable Zone
- Basic Access Control (BAC) / Supplementary Access Control (SAC) - Password Authenticated Connection Establishment (PACE)
- Display biometric and biographical data
- Active Authentication
- Facial matching

DOWNLOADED AND USED IN

- Angola
- Cuba
- Democratic Republic of Congo
- Egypt
- Iraq
- Lebanon
- Mozambique
- Nigeria
- OSCE
- Sudan
- United Republic of Tanzania

FUTURE DEVELOPMENTS

- iOS Operating system
- ID cards verification
- Chip malfunction vs Chip fraud software
- Connectivity / Sync with BMIS (**Upon MS request**)

Thank You

ngoncalves@iom.int

