OUTCOME DOCUMENT

Organized jointly by
The Organization for Security and Co-operation in Europe
and
the Biometrics Institute

Vienna, 11-12 April 2019

1. United Nations Security Council Resolution 2396:

In recent years, the threat posed by Foreign Terrorist Fighters (FTFs) has become a matter of intense international concern. The **increase in returning FTFs** to states of origin, previous residence, or onward travel to third states **poses a danger** that their battle-field experience will be used to plan and carry out attacks, set up new terrorist cells, or otherwise facilitate **future terrorist acts.** This is why, in December 2017, the UN Security Council adopted **resolution 2396** which marked a milestone in international efforts in detecting and countering the movement of FTFs, especially those returning or relocating from conflict zones.

2396 creates **new obligations** regarding **Biometrics and Border Security**

1. Decides that Member States shall develop and implement systems **to collect biometric data,** which could include fingerprints, photographs, facial recognition, and other relevant identifying biometric data, in order to responsibly and properly identify terrorists, including foreign terrorist fighters, in compliance with domestic law and international human rights law

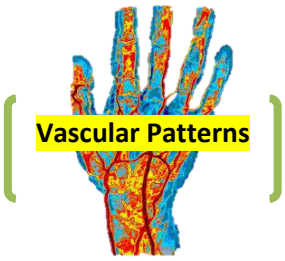
2. Encourages Member States **to share this data responsibly** among relevant Member States, as appropriate, and **with INTERPOL** and other relevant international bodies

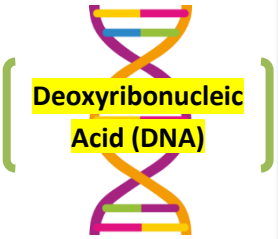
3. Calls upon other Member States, international, regional, and sub-regional entities to **provide technical assistance, resources, and capacity building** to Member States in order to implement such systems.

The primary responsibility in the fight against terrorism lays with States, however, International and Regional organizations can and should play a supportive role in supporting States to respond to these cross-border threats. This is why the **OSCE** teamed up with the **Biometrics Institute** and jointly organized the **ID@Borders and Future of Travel Conference** on 11-12 April 2019 in Vienna.

The conference aimed at **(a) raising awareness** of the benefits of using Biometrics technology at the border and the responsible use of this data in counter-terrorism and **(b) promoting best practices** for sharing Biometric data among states.

2. What are Biometrics?:





BIOMETRICS ARE BIOLOGICAL & BEHAVIOURAL CHARACTERISTICS OF AN INDIVIDUAL FROM WHICH DISTINGUISHING, REPEATABLE BIOMETRIC FEATURES CAN BE EXTRACTED FOR THE PURPOSE OF BIOMETRIC RECOGNITION.

Shared Features of Biometric Modalities

- UNIVERSAL
  - PERMANENT
    - PERFORM EFFECTIVELY
- UNIQUE
  - MEASURABLE
    - SOCIALLY ACCEPTABLE

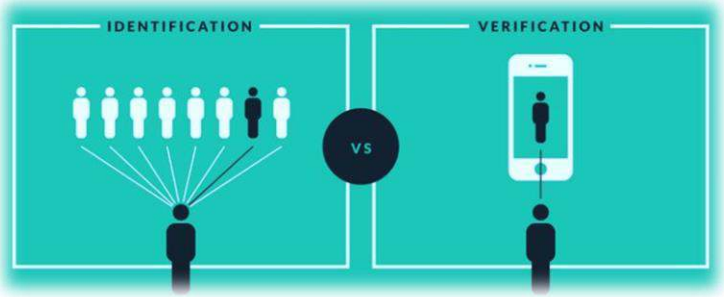
Standard Biometric Operating Model

Biometric identification systems are essentially pattern recognition systems. They use acquisition scanning devices and cameras to capture images or measurements of an individual's characteristics, and computer hardware and software to extract, encode, store, and compare these characteristics. Usually this process is fully automated, which makes decision-making very fast, in most cases, taking only a few seconds.The standard operating model of a basic biometric system contains the following stages:

- **Acquisition & Enrolment** – obtaining a biometric sample from an individual using a data capture device
- **Data Extraction** – converting obtained biometric sample into biometric templates
- **Data Storage** – retention of enrolled data within the system or database
- **Data Comparison** – accessing the database and retrieving one or more previously enrolled templates for comparison with the presented template
- **Data Matching** – using the algorithms to determine whether the enquiry template matches the selected database templates
- **Output** – 'Match' OR 'No-Match'

3. Biometrics Matching Systems:

All biometric systems begin with an enrolment process followed by a matching process which uses **verification** and/or **identification.** .



(1) Verification (**One-to-One or 1:1**) - This model uses an asserted identity to select just one template from the database or electronic document for comparison with the *enquiry template*.

Verification asks the question:

"Are you the same person as the one whose identity has already been authenticated and enrolled on the database?"

(2) Identification **(One-to-Many or 1:n)** - This is a search function that is not dependent on an asserted identity. The *enquiry template* checks the entire database for a potential match.

Identification asks the question:

"Are you in the database and, if so, which record do you match?"

Effective Biometric Systems integrate both verification and identification tasks to improve the assurance of identity and the reliability of comparisons to reference datasets.

e-Gates: An example of a biometric system at border

Several airports across the OSCE area have set up e-Gates. These gates scan electronic passports and compare the biometric information in the chip of the passport against a live scan of the traveler's face using facial recognition technology. In other words, e-Gates perform the Verification process. E-Gates can also be connected to watch-lists, such as INTERPOL's global databases, and compare traveler's biometric image against reference databases of known targets of concern. In this case, an e-Gate performs the Identification process. Border identity Verification will confirm the identity of the traveler against recorded and authenticated biometrics but a Biometric Watch List Search may reveal that the confirmed identity is the subject of interest.

4. Data privacy implications related to biometrics

UN Resolution 2386 makes clear that States should collect biometric data in compliance with domestic law and international human rights law. The UN Compendium of recommended practices for the responsible use and sharing of biometrics in counter-terrorism makes a number of recommendations:

Data Processing	**States should nominate a data controller to be responsible for managing all data processing activities.**
Data Sharing	**The sharing of data should be approved domestically and subject to a clear legal framework. Biometrics should only be shared with trusted recipients and for the purposes included in the law.**
Preventing Data Misuse	**States should secure all biometrics information from unauthorized access and misuse, as well as to ensure that the data is accurate and that it has been provided without malevolent intentions.**
Oversight	**Effective and impartial oversight mechanisms by an independent body to which individuals can have access should be put in place to prevent the arbitrary collection and storage of biometrics.**

5. Benefits of Biometrics in Counter-Terrorism

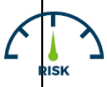
Integrated Border Management Strategies are playing a crucial role in the fight against terrorism in general and Foreign Terrorist Fighters in particular. This is why Biometric Systems and Databases are widely used in law enforcement, border management and military applications. States are also considering the benefits of **sharing biometric data on a bilateral, multi-lateral, regional and global scale within the context of international human rights.**

Biometric data when used with other intelligence data can be used pro-actively to prevent acts of terrorism. Biometric Reference or Crime Scene data can be used in: proving or disproving a person's involvement in an offence and linking a person to an activity, event, location or another person *before, during or after* an incident.

IMPORTANT

- ✓ Be aware of **threats and vulnerabilities** that are posed by altering some biometrics modalities. For more information, please see pp.42-44 of **the UN Compendium of recommended practices for the responsible use and sharing of biometrics in counter-terrorism**

- ✓ Respect **Data Privacy** in accordance to International legal standards. For more information, please see pp 30-40 of UN compendium as well as:
  - EU FRA publications: **Under watchful eyes: biometrics, EU IT systems and fundamental rights**; **Fundamental rights implications of storing biometric data in identity documents and residence cards**
  - And OSCE Human Rights Institution's publication: **Guidelines for Addressing the Threats and Challenges of "Foreign Terrorist Fighters" within a Human Rights Framework**

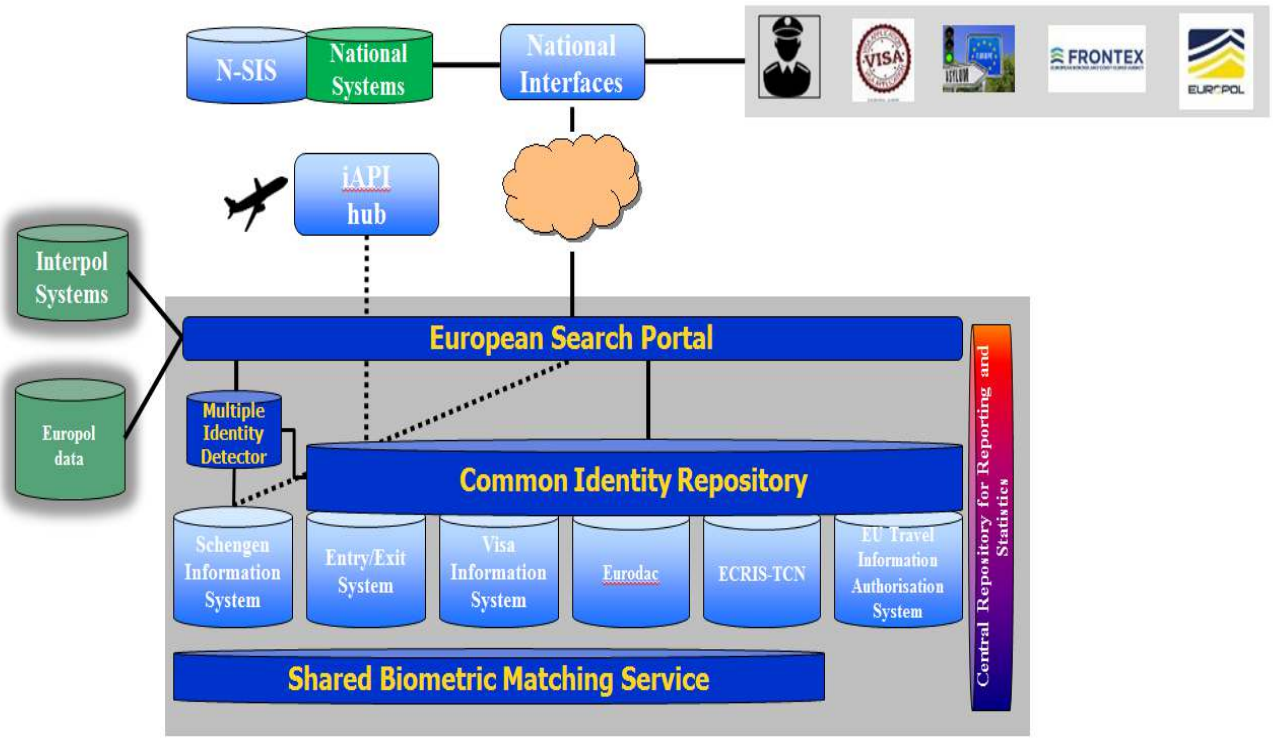


5. Updates from the EU and INTERPOL

In February 2019, the European Parliament and the Council reached a preliminary political agreement on establishing a framework for interoperability between EU information systems for security, migration and border management. The purpose of the regulations is to ensure that border guards and police officers have access to the right information.

The new components will allow existing and future EU information systems, such as the Entry/Exit System (EES) and the European Travel Information and Authorization System (ETIAS) to talk to each other, thereby, preventing important pieces of information from going undetected. The new tools will:

- **Crosscheck existing data with one click:** A **European search portal** will allow border guards and police to carry out simultaneous checks of identity documents against all EU information systems on a single screen;
- **Better detect identity fraud:** a **common identity repository**, which will store biographical data of non-EU citizens will allow border guards and police to better identify dangerous criminals;
- **Improve access for law enforcement:** once the information searched by an officer matches information contained in one of the systems (i.e. gets a "hit"), he/she will be able to request more targeted access, in line with the specific rules for each system;
- **Protect fundamental rights:** the rules on access and purpose limitation of the EU's information systems will not change, thus ensuring that fundamental rights remain protected.

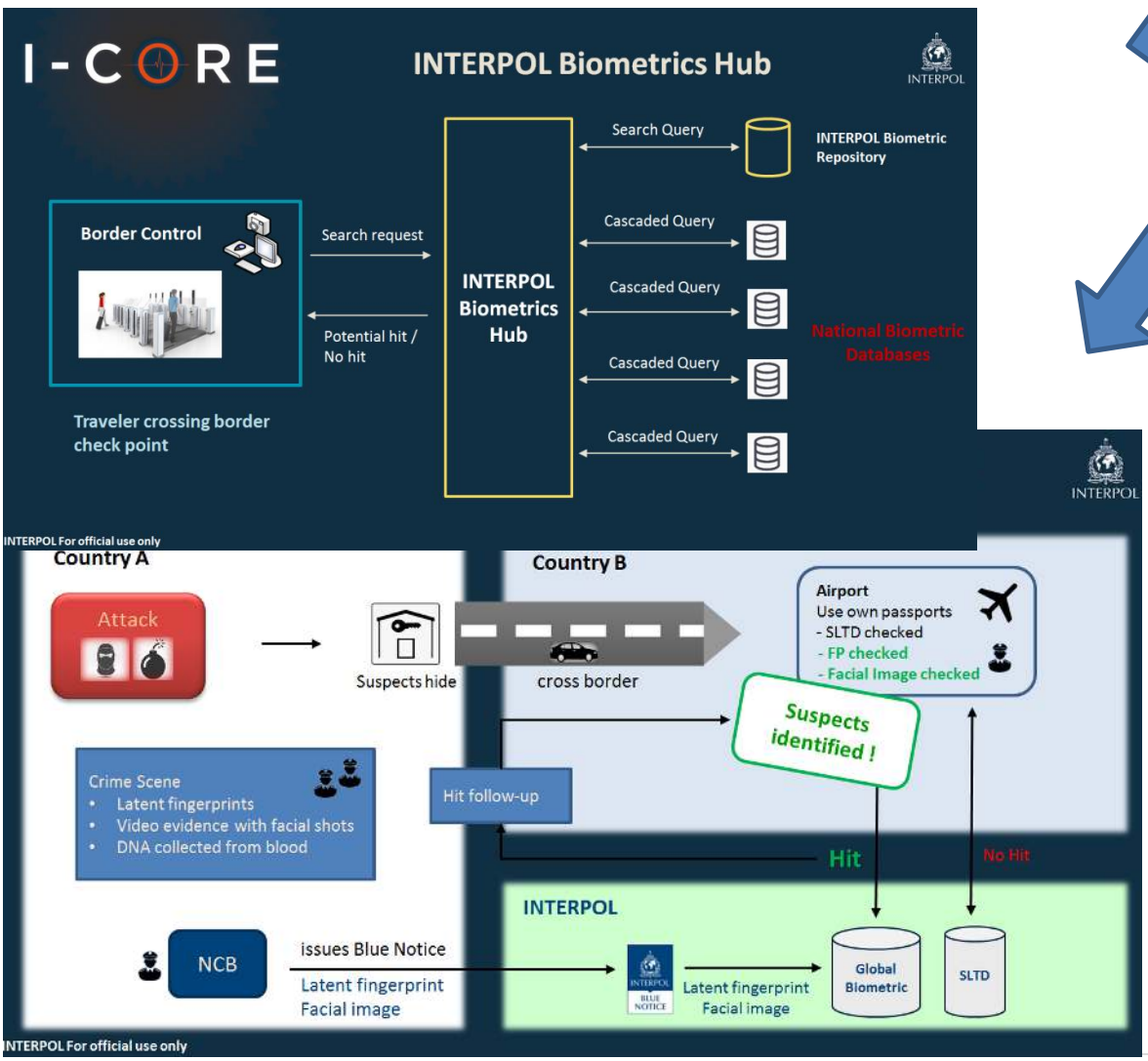


INTERPOL maintains criminal **databases of fingerprints, DNA profiles and facial images**, provided by the member countries. This allows police across the world to make connections between criminals and crime scenes. INTERPOL also trains frontline officers to assess, preserve and share evidence in line with best practices.

Authorized users in member countries can view, submit and cross-check records in the fingerprints database via a user-friendly **automatic fingerprint identification system (AFIS).**

DNA database contains DNA profiles from offenders, crime scenes, missing persons and unidentified bodies. INTERPOL does not store any nominal data linking a DNA profile to any individual. **The Facial Recognition System database** provides a dedicated platform to store and cross-check images for the purpose of identifying fugitives, missing persons and persons of interest.

INTERPOL is currently doing a study on the use of biometric data to identify persons of interest (Terrorists, Known Offenders) at border control and plans to develop a **Biometrics Hub** (secure gateway) to link member country biometric databases with INTERPOL biometric databases - a model based on shared data.



6. Examples of Good Practices from OSCE participating States:

CANADA: Biometric information is a foundational tool to support the Canadian Government's modernization agenda. Accurately determining identity is at the core of all immigration decisions:
- getting identity right as early as possible by linking the person (biometrics) to key attributes (biographical);
- If identity cannot be anchored, government cannot trust that subsequent eligibility and admissibility screening can yield meaningful results.

In 2018, Canada expanded its biometrics collection:
- all foreign nationals (unless exempt) applying for temporary or permanent residence are required to provide their fingerprints and photograph

Next steps in Canada's use of biometrics:
- *Shift to a verification-based model;*
- *Establish new international information sharing arrangements;*
- *Collect biometrics from other types of applicants.*

UNITED STATES: The Homeland Advanced Recognition Technology (HART) is a state-of-the-art biometric system that expands on the Automated Biometric Identification System **(IDENT)** operated by the US Department of Homeland Security's Office of Biometric Identity Management **(OBIM).**

The HART system has introduced new services and technological advances: *Increased performance & Availability; Expanded Interoperability; Increased Privacy & IT Security; New Design with Cost Efficiencies; Enhanced Accuracy & Identity Assurance; Greater Capacity.*

In Fiscal Year 2018, OBIM:
- Processed ~113 million subjects
- Identified ~120,000 known or suspected terrorists
- Identified ~4.5 million individuals with derogatory information

As new operational challenges emerge and technology advances, HART will be able to grow and adapt to meet mission needs. To achieve this, innovative solutions are needed in partnership with industry and academia.

7. Way forward: Next Steps for the OSCE

The OSCE's Transnational Threats Department is developing a project to assist requesting OSCE participating States in collecting and sharing biometric data as mandated in UN Security Council Resolution 2396. The project will have three main phases:

1 - Awareness raising sub-regional workshops in Central Asia, South Eastern Europe, and Eastern Europe

2 - National Consultations to determine needs and objectives

3 - Technical Support in assisting States to identify, procure and use the biometric system that best fits their needs

All activities will be carried out in close cooperation and collaboration with *the Biometrics Institute, the UN Office on Counter-Terrorism and INTERPOL.*

For more information please, CONTACT us at OSCE:

Simon Deignan simon.deignan@osce.org and Magda Jugheli magda.jugheli@osce.org