BEYOND BORDERS

The Role of Consular Services in Legal Identity and Identity Management

IOM
UN MIGRATION

This publication adheres to the IOM Legal Identity Strategy which lays the foundation for supporting individuals, States, and governments to meet Sustainable Development Goals (SDG) Target 16.9 and Objective 4 of the Global Migration Compact. IOM is committed to the principle that humane and orderly migration benefits migrants and society. As an intergovernmental organization, IOM works with its partners in the international community to assist in meeting the operational challenges of migration, advance understanding of migration issues, encourage social and economic development through migration, and uphold the human rights, human dignity and well-being of migrants.

This publication was made with the support of the IOM Global Cooperation on Migration and Partnerships for Sustainable Solutions (COMPASS) initiative, designed to protect people on the move, combat human trafficking and smuggling, and support dignified return and sustainable reintegration.

The programme focuses on systemic changes that are critical to addressing the underlying causes of migrants' vulnerability, gender equality, and exclusion, including in humanitarian and fragile settings; supporting rights-based policies and legislation; equitable access to essential protection services; strengthening local partnerships for migrant inclusion and social cohesion; access to legal identity; reinforcing data-driven responses; and influencing social behaviours and norms. The programme is being implemented in partnership with 14 Partner States.

Publisher: International Organization for Migration
17 Route des Morillons
P.O. Box 17
1211 Geneva 19
Switzerland
Tel.: +41 22 717 9111
Fax: +41 22 798 6150
Email: hq@iom.int
Website: www.iom.int

This publication was issued without formal editing by IOM.

Required citation: International Organization for Migration (IOM)(2025). *Beyond Borders: The Role of Consular Services in Legal Identity and Identity Management*. IOM, Geneva.

Coordination: Nelson Goncalves, Aijan Boronbaeva, Julia de Bresser and Isabella Dourado.
Design: Sidi Sougou

ISBN 978-92-9278-017-3 (PDF)

PUB2025/033/R

BEYOND BORDERS

The Role of Consular Services in Legal Identity and Identity Management

CONTENTS

LIST OF FIGURES

ABBREVIATIONS

ASEAN	Association of Southeast Asian Nations
CARICOM	Caribbean Community
CRC	Convention on the Rights of the Child
CRVS	Civil Registration and Vital Statistics
eMRTD	electronic Machine-Readable Travel Document
EOI	Evidence of Identity
FALP	ICAO Facilitation Panel
GDPR	General Data Protection Regulation
ICAO	International Civil Aviation Organization
ICCPR	International Covenant on Civil and Political Rights
ICRMW	International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families
IDVT	Identification Document Validation Technology
IOM	International Organization for Migration
MRTD	Machine Readable Travel Document
MRZ	Machine-Readable Zone
PACE	Password Authenticated Connection Establishment
QR	Quick Response (QR) Code
SDG	Sustainable Development Goals
SLTD	Stolen or Lost Travel Document
TRIP	Traveller Identification Programme
UDHR	Universal Declaration of Human Rights
UNHCR	United Nations High Commissioner for Refugees
VCCR	Vienna Convention on Consular Relations
VIZ	Visual Inspection Zone

Executive Summary

This manual provides a comprehensive framework for strengthening consular services to advance the global commitment to ensuring legal identity for all, as outlined in key international frameworks such as the Sustainable Development Goals (SDG), the Global Compact for Migration, and the IOM Legal Identity Strategy. With an estimated 850 million individuals worldwide lacking proof of legal identity, this document highlights the critical role consular services play in addressing these gaps and ensuring access to essential services, human rights, and regular migration pathways.

Main highlights and insights from the Manual:

Legal Identity as a Cornerstone:

Legal identity, as defined by the United Nations Legal Identity Agenda (UNLIA), refers to the basic characteristics of an individual's identity, such as name, sex, place, and date of birth, conferred through civil registration and the issuance of a birth certificate or other official identity documents. This definition underscores the importance of legal identity for safeguarding individual human rights and strengthening public governance. The manual also aligns with international commitments, such as SDG Target 16.9, which seeks to "provide legal identity for all, including birth registration, by 2030," as outlined in the UNLIA framework." Objective 4 of the Global Compact for Migration calls for governments to "ensure that all migrants have proof of legal identity and adequate documentation."

Consular Responsibilities:

Consular services are instrumental in issuing and verifying identity and travel documents, certifying vital events (e.g. births, marriages, divorces, adoptions and deaths), and providing documentation to migrants, including those lacking proof of identity. These functions enhance migration management by enabling safe access to regular pathways, ensuring protection outcomes, and preventing fraud.

Core Components of Evidence of Identity (EOI):

- Validation Standards: The manual outlines rigorous methods for establishing identity using breeder documents, biometrics, and other verifiable data sources. In addition, validation standards ensure protection against exploitation and trafficking in persons.
- Lifecycle Identity Management: From birth registration to issuing travel documents, consulates ensure individuals' identities are recognized and protected throughout their lives.

Integration of International Standards:

Consular services are regulated by international standards set by the Vienna Convention on Consular Relations (VCCR) and International Civil Aviation Organization (ICAO) guidelines. Adopting and implementing these standards ensures the reliability and global acceptance of issued documents.

Safeguarding and Privacy Protections:

Recognizing the sensitivity of personal data, the manual emphasizes the importance of robust data protection measures, in respect of the right to privacy of individuals.

Consular services must:

- Implement privacy-by-design approaches in data handling.
- Ensure compliance with relevant data protection laws, international frameworks and ethical standards.
- Protect groups in vulnerable situations, particularly children and victims of trafficking, through trauma-informed and rights-based practices.

Strategic Capacity Development for Consular Services:

- Document verification and fraud detection techniques.
- Profiling and interview techniques.
- Handling sensitive cases with cultural and gender competence.
- Facilitating identity services for populations in vulnerable situations, including stateless individuals and unaccompanied and separated children.

This manual equips Member States to advance legal identity systems that are inclusive, secure, and aligned with global standards by fostering collaboration between consular services, international organizations, and host governments. It serves as both a practical guide and a policy resource, enabling consular authorities to fulfil their critical role in safeguarding the rights and identities of migrants worldwide.

The lack of proof of legal identity affects millions globally, with an estimated 850 million individuals unable to access the fundamental rights and services tied to official documentation. This limitation impacts their right to recognition before the law and their ability to exercise human rights, access education, health care, justice, social services, financial systems and mobility, and it often compels reliance on irregular migration pathways fraught with risks.

For migrants, consular services play a crucial role by providing safe access to civil registration processes, issuing essential identity and travel documents, and certifying key life events such as births, deaths, marriages, divorces and adoptions. These services are indispensable for migration processes, including admission, return, readmission and stay, such as legal status adjustments and extensions. By addressing documentation gaps, consular services empower migrants to access rights and services while navigating regular migration pathways more securely and predictably.

Part 1.
Introduction

Recognizing the transformative role of legal identity, the international community has established clear commitments through global frameworks. Sustainable Development Goal (SDG) Target 16.9 calls for "legal identity for all, including birth registration" as part of the 2030 Agenda's pledge to "leave no one behind." Similarly, the Global Compact for Safe, Orderly, and Regular Migration emphasizes the need for proof of legal identity in its Objective 4 and highlights the importance of consular cooperation in its Objective 14, particularly in issuing identity and travel documents.

The IOM's Institutional Strategy on Legal Identity supports these global objectives. A central component of the strategy is assisting consulates in facilitating civil registration processes, issuing identity and travel documents, and supporting nationals abroad. This approach promotes equitable access to legal identity, focusing on individuals in vulnerable situations, while helping States uphold international standards and foster inclusive identity systems.

Objectives of the Manual

This manual is designed to guide States in enhancing their consular services by equipping consular staff worldwide with a comprehensive understanding of legal identity within the context of consular assistance and protection. It serves as a resource to clarify the key principles and frameworks that underpin consular support, offering practical guidance on the general principles of assistance and protection. Additionally, it provides detailed insights into evidence of identity standards, civil registration processes, and the issuance of identity documents, while emphasizing the importance of adhering to data privacy and protection requirements.

Improved expertise in security document examination at consulates is essential for preventing the misuse of fraudulent or fake documents, detecting identity fraud, and protecting systems and affected individuals from abuse. These efforts strengthen migration governance by ensuring robust verification of individuals' identity, qualifications, and claims, including those of undocumented migrants.

The manual outlines a systematic approach to document examination, referencing key documents and actions to take when identity or document fraud is detected. It also highlights the role of consulates in document registration and issuance.

Furthermore, the manual provides an overview of international standards for travel documents and their issuance, referencing International Civil Aviation Organization (ICAO) concepts such as Evidence of Identity (EOI) and the Traveller Identification Programme (TRIP). It serves as a foundational resource for developing training materials, including instructions for trainers and slide decks to support effective training sessions.

Part 2.

General Principles for Providing Consular Services

Legal Identity

Even though international law lacks a strict definition of legal identity, the United Nations provides an operational definition: "the basic characteristics of an individual's identity, e.g. name, sex, place and date of birth conferred through registration and the issuance of a certificate by an authorized civil registration authority following the occurrence of birth. In the absence of birth registration, legal identity may be conferred by a legally recognized identification authority; this system should be linked to the civil registration system to ensure a holistic approach to legal identity from birth to death."

Operationally, legal identity is established through civil registration or the issuance of identification documents by a competent authority. It is understood as the administrative recognition of a person through official registration or identification procedures by the State under the rule of law. This process legally attests to their identity and ensures recognition of the rights that derive from it under the State's laws.

Every individual is inherently entitled to dignity and human rights without discrimination, as enshrined in Articles 1 (dignity and equality) and 2 (non-discrimination) of the 1948 Universal Declaration of Human Rights (UDHR). Everyone has the right to be acknowledged as a person and treated equally under the law without discrimination, ensuring inclusive and fair access to legal identity for all, regardless of migratory status. (UDHR, Articles 6 and 7). An individual also has the right to birth registration, to a nationality and to not be arbitrarily deprived thereof (UDHR, Article 15). Recognition everywhere as a person and equality before the law without discrimination is also established by the International Covenant on Civil and Political Rights (ICCPR, Articles 16 and 26). The right to an identity at birth – as guaranteed in Articles 7 and 8 of the Convention on the Rights of the Child (CRC) – derives from the right to be recognized as a person before the law.

Consequent to these rights and principles inherent to the human person, all States have the obligation to ensure these rights are respected, protected and fulfilled for all persons under their jurisdiction, de jure and de facto, meaning for all persons who are on the State's territory or under the State's effective control, by issuing documented proof of nationality (for their own nationals), and birth and other vital events. These documents facilitate recognition before the law by providing proof of legal identity and vital events.

The operationalization of legal identity is giving proof of it through civil registration or issuance of identification documents by a competent identification authority. Whilst "legal identity" is not defined in international law, we use it to describe the administrative recognition of a person through an official registration or identification procedure by the State under the rule of law, to legally attest to their identity and establish a relationship between individuals and the State, safeguarding rights that derive from this legal identity under the State's laws.

Legal identity belongs to the person, not to the State, but the administrative means of conferring and proving legal identity such as a passport or other documents can be the property of the State. This distinction underscores the universality of the concept of legal identity, which applies to every individual regardless of their location, citizenship, or migratory status. Access to legal identity documentation contributes to fulfilling the human right to be recognized as a person before the law (UDHR, Article 6), and is instrumental for the effective enjoyment of other human rights, including the right to a name and a nationality, the right to health, to work and to education.

Although the enjoyment of other human rights does not depend on the possession of a legal identity registered by a competent authority, lacking an official document confirming legal identity is often a barrier that prevents the enjoyment and realization of human rights for millions of people worldwide. Many migrants might face obstacles in accessing legal identity, particularly stateless individuals, stranded or vulnerable migrants, those in precarious situations, victims of human and labour rights violations or abuse, crime victims, migrants subjected to smuggling (including under aggravating circumstances), exploited migrant workers, refugees, asylum-seekers, victims of trafficking, unaccompanied and separated migrant children, persons with diverse SOGIESC, homeless persons, individuals with disabilities, Indigenous People, victims

of violence, and those displaced by conflict or adverse environmental impacts. Each of these groups faces unique challenges and vulnerabilities.

Specific examples of these impacts are addressed in the UN Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW), which highlights disadvantages and discrimination based on sex and gender that are inextricably linked to identity, and the United Nations Convention on the Rights of Persons with Disabilities (CRPD), which protects the rights of those living with disabilities to preserve their identities. For instance, gender-based barriers may prevent women, including transgender persons, in certain contexts from registering births or obtaining identity documents, limiting their access to services and opportunities.

A lack of legal identity documentation can further exacerbate these individuals' situations by exposing them to additional acts of discrimination and other human rights violations, such as restricted access to education, health care, housing and employment. It may also increase their vulnerability to exploitation, arbitrary detention, statelessness and barriers to justice and legal remedies. In some cases, a legal identity document can serve as a temporary solution in cases of conflict, emergencies and humanitarian situations, which could allow migrants unhindered access to certain rights and services during these times. For stateless persons or migrants, these documents may provide interim, time-bound relief until more durable and preventive solutions are adopted to address issues of nationality and other human rights.

Consular Assistance

Consular assistance is the support provided by States to their nationalsand in some cases to non-nationals (under bilateral or multilateral agreements) in third countries. Such assistance is delivered by consular officers or other representatives, whose roles are distinct from political or diplomatic functions.[1] All nationals of a country of origin, regardless of their migration status, have the right to access consular assistance in both emergency and non-emergency contexts. Typical services include citizen registration, issuance and extension of travel documents, urgent financial assistance, birth and death registration, return, repatriation and facilitating communication with family members during personal emergencies.[2]

The terms consular protection and consular assistance are often used interchangeably. In this context, "consular assistance" encompasses functions related to both protection and assistance. In contrast, diplomatic protection is an inter State intervention conducted by diplomatic officials on behalf of the State, distinct from consular assistance, which is focused on individual citizens and delivered by consular staff.

The rules governing consular assistance are established under national and international law, particularly the Vienna Convention on Consular Relations (VCCR). The VCCR codifies consular functions, granting States the authority or right – but not the obligation – to provide consular assistance as a matter of international law.[3] Ratified by 182 United Nations Member States, the VCCR outlines permissible consular functions, such as:

- Protecting the interests of the country of origin and its nationals in the receiving State.
- Furthering commercial, economic, scientific and cultural relations and promoting friendly relations between the sending and receiving States.
- Issuing passports, travel documents, visas and appropriate documents for those wishing to travel.
- Helping and assisting nationals of the country of origin, including in emergencies.
- Registering births, deaths and similar events; performing notarial functions; and acting as a civil registrar.
- Representing or arranging representation for nationals of the country of origin before tribunals and authorities in the receiving State to protect their rights and interests.
- Safeguarding the interests of children and other persons who may lack the legal or practical capacity to act on their own behalf.
- Administering the property of nationals of the country of origin, such as in cases of inheritance.
- Supervise or inspect vessels carrying the flag of the origin country or aircrafts registered in the origin country, assisting the crew and investigating any incidents that occurred during the voyage.

In addition to the consular functions mentioned above, Article 5(m) of the VCCR provides that consulates may perform "any other functions entrusted to a consular post by the country of origin which are not prohibited by the laws and regulations of the receiving State, or to which no objection is taken by the

1 https://legal.un.org/ilc/documentation/english/a_cn4_567.pdf.
2 www.iom.int/sites/g/files/tmzbdl486/files/documents/2023-07/consular-support-and-citizen-services.pdf.
3 www.iom.int/sites/g/files/tmzbdl2616/files/inline-files/iml_consular_assistance1.pdf.

receiving State or which are referred to in the international agreements in force between the sending State and the receiving State."[4]

Consular assistance plays a critical role in safeguarding human rights. The 1985 United Nations Declaration on the Human Rights of Individuals Who Are Not Nationals of the Country in Which They Live (adopted under United Nations General Assembly Resolution 40/144) recognizes the right of individuals to communicate with the consular or diplomatic mission of their country of origin. This right ensures access to protection, identity documentation and legal support.

Several United Nations resolutions emphasize consular assistance's role in upholding human rights, such as the right to due process, freedom from arbitrary detention, and access to legal representation, including Resolution 54/166. For instance, when migrants face detention or deportation, consular access can ensure that they are informed of their rights, can communicate with family members, and can receive legal or administrative support.

The International Convention on the Protection of the Rights of All Migrant Workers and Members of their Families (ICRMW) reinforces these principles. Articles 16(7)(a), 23, and 65(2) establish obligations for States to provide consular assistance, including in cases of detention or expulsion as well as in ensuring adequate services to meet the social, cultural and other needs of migrant workers and their families. The ICRMW underscores the duty of countries of origin to provide effective consular protection,[5] such as legal aid, expedited travel document processing, and support for migrants facing detention, expulsion or the violation of their rights.. The Committee on Migrant Workers (CMW), which oversees the ICRMW's implementation, has emphasized that embassies and consulates should play an "active role" in protecting nationals abroad, specifically migrant domestic workers. This includes training staff to handle complaints from migrant workers, expediting travel documents for those fleeing abuse, and arranging visits for detained nationals. The CMW also encourages coordination with local authorities to strengthen these protections.[6]

A 2000 United Nations Resolution on the protection of migrants reiterated the need to uphold the universally recognized human rights of all migrants, including the right to access consular assistance from the country of origin. Similarly, the Special Rapporteur on the Human Rights of Migrants urged countries of origin to provide "proper consular protection" when their citizens' rights are violated abroad, particularly in cases of detention.

The Committee on the Rights of the Child has clarified that the "best interests of the child" should be integrated into all policies and programmes that impact children, "including consular protection policies and services"[7] and that "adequate resources should be put in place in order to ensure this principle is applied in practice." The Committee further explained that in the context of best interest assessments, children should be guaranteed the right to "have effective access to [...] consular assistance, and to receive child-sensitive rights-based consular protection."[8]

Similarly, birth registration is both a normal consular function and a right of the child under both the Convention on the Rights of the Child (CRC) and the International Covenant on Civil and Political Rights (ICCPR). Birth registration is not only a right but also a foundation for realizing other rights, including the right to nationality, as it records key elements like birthplace and parentage. Consular registration of birth facilitates a child's right to legal identity and nationality, particularly for migrant children with irregular administrative status who cannot or are deterred from registering locally. Without such procedures, undocumented migrants are at increased risk of statelessness.[9]

---

4 www.iom.int/sites/g/files/tmzbdl2616/files/inline-files/iml_consular_assistance1.pdf.
5 www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.32_GC-III-EN.pdf.
6 https://digitallibrary.un.org/record/709818?ln=en&v=pdf.
7 www.ohchr.org/en/documents/general-comments-and-recommendations/joint-general-comment-no-3-cmw-and-no-22-crc-context.
8 Ibid., para. 17(e).
9 www.statelessness.eu/updates/blog/double-plight-stateless-migrants.

The right to nationality is closely tied to the right to freedom of movement, recognized under Article 12 of the ICCPR. This includes "the right to leave any country, including one's own," and not to be "arbitrarily deprived of the right to enter one's own country." The Human Rights Committee has clarified that international travel often requires appropriate documents, particularly a passport, making access to these documents an indispensable element of the right to leave a country. Consular authorities are typically responsible for issuing or renewing passports and emergency travel documents. A failure to provide such documents may deprive individuals of their right to travel or return to their country of origin, underscoring the importance of consular assistance in upholding freedom of movement.[10]

Actionable Steps to Strengthen Consular Services in Line with International Standards

— Expand access to civil registration and identity documentation

Facilitate equal and safe access for nationals residing abroad to civil registration services and the issuance of identity and travel documentation. This includes integrating consular services with central, regional, or local registries, whether these are paper-based or digital systems. Such integration should ensure linkage to a principal civil registry system in the country of origin. Consular authorities must provide tailored and comprehensive training for consular staff, equipping them to handle sensitive cases involving individuals in vulnerable situations in a rights-based manner, such as victims of trafficking, stateless persons, and undocumented migrants. Training programmes should emphasize gender, age, and cultural sensitivity, trauma-informed approaches, safety standards in managing sensitive personal information, and in-depth understanding of international legal frameworks, particularly those related to human rights and migration governance.

— Play an active role in safeguarding rights

Consular authorities must actively safeguard the rights of their nationals by informing them of their rights and providing access to services. This includes identifying, recognizing, and addressing the specific needs and vulnerabilities of nationals abroad. Consular services must act in accordance with the State's international human rights obligations, respecting, protecting and fulfilling rights such as legal identity, nationality and protection from exploitation.

Timely issuance of travel documents is critical to protecting individuals in vulnerable situations, including those with an irregular administrative status, victims of trafficking, or those at risk of statelessness. By ensuring prompt processing of passports and other travel documents, consular services uphold freedom of movement and enhance protection mechanisms. Consular authorities must also integrate the best interests of the child into their operations. Facilitating birth registration ensures a child's right to legal identity and nationality, particularly for children born to parents with irregular administrative status. Proactively engaging with communities to identify unregistered children and facilitating access to birth registration services prevents statelessness and ensures the human rights of all children. Consular offices should guarantee birth registration for children of their nationality abroad, especially when the host country is unable or unwilling to provide it.

— Assist nationals without proof of legal identity

Identify and provide targeted support to nationals residing abroad who lack proof of legal identity. A progressive, rights-based and inclusive approach should be adopted, starting with addressing vulnerabilities and providing clear signposting to services. Efforts should address the unique challenges faced by undocumented migrants, including fear of legal repercussions, language barriers,

10 www.refworld.org/legal/general/hrc/1999/en/46752; www.iom.int/sites/g/files/tmzbdl2616/files/inline-files/iml_consular_assistance1.pdf.

and limited access to resources. Simplify pathways for individuals to obtain proof of nationality and identity, ensuring efficient and timely issuance of documentation. This facilitates mobility, access to services, and compliance with host country requirements.

— Support inclusive national civil registration and identity management systems

Promote inclusive national civil registration and identity management systems to facilitate regular migration and mobility activities. Consular authorities play a key role by utilizing these systems to issue documents, including birth certificates, passports, and emergency travel documents, that enable individuals to lodge migration applications, travel elsewhere, or return to their country of origin. Collaboration with relevant national authorities to ensure these systems are accessible for all and efficient will enhance their utility and promote trust in the registration process.

— Promote interoperability

Consular authorities should work to ensure that their registration systems and processes are seamlessly connected to central government databases in their countries of origin, in line with applicable international and national data protection standards. This interoperability allows for streamlined data exchange, improving the ability to verify and authenticate identity information across different systems. For example, linking consular services with national civil registries facilitates the confirmation of birth, marriage, or citizenship records, which is crucial for securely issuing legal identity and travel documents.

— Ensure robust verification mechanisms for identity documentation

Consular authorities must prioritize implementing robust verification systems to ensure the authenticity of identity documentation, prevent fraud, protect individuals from trafficking, and safeguard the personal data of their nationals. These mechanisms are essential for upholding the integrity of the documentation issued and maintaining trust in consular services.

Key measures include:

- **Adopting advanced security features**: Consular offices should use internationally recognized security features in identity and travel documents, such as holograms, watermarks, and biometric data, in compliance with standards like ICAO Doc 9303 for travel documents. These features enhance document authenticity and reduce the risk of forgery.

- **International recognition of documents and apostille:** Consulates play a vital role in assisting nationals with the recognition and legalization of documents issued in the host country for use in the home country, or vice versa. In countries that are not part of the Hague Apostille Convention, consular services often handle document legalization by verifying and authenticating documents. For countries that are part of the Apostille Convention, document authentication is typically a standardized process handled by designated national authorities, rather than consulates. However, consulates may still provide guidance and resources to help nationals navigate these procedures. This support ensures that documents meet the legal requirements of both the destination and origin countries, facilitating their international recognition. Apostilles, issued by a designated competent authority (e.g. Ministry of Foreign Affairs or Justice), certify the authenticity of public documents, such as birth certificates, marriage certificates and diplomas. There are two types of apostille: paper-based and electronic, the latter known as an e-Apostille. For countries utilizing e-Apostille services, the process is further streamlined, allowing digital issuance and verification.

  While consular officers do not issue apostilles, they provide essential assistance by:

  - Advising nationals on the requirements and processes for obtaining an apostille.
  - Supporting document legalization for documents issued in countries not party to the Apostille Convention, where consular legalization may be required.

- **Implementing biometric verification**: By incorporating biometric technologies such as fingerprinting, facial recognition, or iris scanning, consular authorities can ensure that issued documents are tied to a single, verifiable identity. This prevents identity theft and facilitates seamless identification in host countries and international travel. This must be undertaken in line with applicable international and national data protection standards. More information about the application of biometric solutions can be found in IOM Biometrics Manual.

- **Data protection and cybersecurity**: Safeguarding personal data is paramount. Consular services must adopt secure data collection, storage, and transmission systems, ensuring compliance with applicable data protection standards, regulations and best practices. Encryption, access control, and regular security audits should form the backbone of these systems.

- **Training staff on fraud prevention**: Consular staff should be trained to recognize and address fraudulent activities, including document forgery and impersonation. This includes familiarizing personnel with international verification standards for security documents and providing tools to detect anomalies, as well as profiling and interview techniques.

— Engage with populations

Through consular representation, engage with individuals and communities to highlight access to legal identity processes and other types of consular support. Conduct outreach programmes to reach underserved or populations in vulnerable situations, ensuring they are informed of their rights and how to access services available to them in a way that they can understand. Share and promote good practices across consular networks and collaborative partners, fostering innovation and consistency in service delivery, and sharing of information.

— Streamline communications with host governments

Specifically, streamline communications and cooperate with the governments of host countries to ensure that documents issued through consular services are recognized and understood locally. Develop formal agreements and internal protocols to address discrepancies in legal frameworks or administrative practices, ensuring that nationals face no unnecessary barriers when using consular-issued documents.

— Maintain accurate records

Maintain comprehensive records of individuals engaging and/or effective case management with consular services in host countries. Use modern technologies, such as digital registries and communication platforms, to keep records up-to-date. Facilitate timely support by sharing relevant resources and updates through diverse communication channels, while adhering to data protection standards, including community outreach, newsletters, and other appropriate methods, tailored to the needs of different populations.

— Provide emergency assistance

Consular authorities should be equipped to assist citizens during emergencies, such as conflicts, natural disasters, or pandemics. This includes ensuring the continuity of documentation services, providing protection, and ensuring timely communication about the emergency and available options for affected individuals. Emergency preparedness should also include contingency plans, partnerships with local authorities, and mechanisms for rapidly issuing emergency travel documents or identity verification. Additionally, it is crucial to establish procedures for promptly returning identity documents to their owners in the event of service closures due to security situations. These efforts are critical to safeguarding the rights and well-being of nationals during crises.

Part 3.

Consulates Representing Another Country's Government in a Third Country to Provide Consular Services on its Behalf

Consular assistance is generally provided by a State to its nationals abroad. However, challenges arise when an individual cannot access consular assistance, either because their country does not have a consular post in the location where they are present or due to specific circumstances affecting refugees, stateless persons, and dual nationals. Additionally, even when consular posts are available, individuals may face barriers such as financial constraints, language barriers, or administrative obstacles.

The VCCR does not fully address these complications related to nationality, or lack of it, or the provision of consular protection for individuals without a clear claim to diplomatic assistance. However, other bilateral or multilateral agreements seek to address aspects thereof. For example, Member States of the European Union are required to provide consular assistance to nationals of other European Union Member States on the same conditions as to their own nationals if the individual who needs assistance is visiting a third country (a State of which that person is not a national) where their own State does not have a consular presence (Directive 2015/637).[11]

This is consistent with Article 8 of the VCCR, which authorizes a consular post, upon appropriate notification, to exercise consular functions in the receiving State on behalf of a third State. Such exercise of consular functions on behalf of a third State's nationals may also be arranged, normally pursuant to a bilateral agreement, in situations where the third State and the receiving State have severed consular (usually along with diplomatic) relations, and the protection of the interests of the third State's nationals are entrusted to a friendly power that maintains a consular presence.[12] In the Global Compact for Migration, States committed to concluding "bilateral or regional agreements on consular assistance and representation in places where States have an interest in strengthening effective consular services related to migration, but do not have a diplomatic or consular presence."[13]

Examples of Regional and Multilateral Cooperation

- **Regional Consular Centres for Nordic and Baltic Countries:**

These centres share consular and diplomatic responsibilities across Nordic and Baltic nations. For instance, the Regional Consular Centre Nordic and Baltic Countries in Stockholm provides assistance to nationals from Denmark, Finland, Iceland, Norway and Sweden, as well as the Baltic States of Estonia, Latvia and Lithuania. By pooling resources and sharing responsibilities, these centres enhance efficiency and ensure broader access to consular support in regions where individual representation may otherwise be limited.

- **Schengen visa representation arrangements:**

Schengen States have established cooperation agreements under which one Schengen State may accept and process visa applications on behalf of another. These arrangements are supported by the Visa Information System (VIS), which enables the exchange of visa data between member States, reducing redundancies and enhancing efficiency. As a result, travellers can apply for visas even in locations where the consular representation of the competent Member State (often the destination country) is not available.

- **The Association of Southeast Asian Nations (ASEAN):**

Comprising 10 member States – Brunei Darussalam, Cambodia, Indonesia, Lao People's Democratic Republic, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Viet Nam – ASEAN has established the ASEAN Plan of Action on Cooperation on Immigration and Consular Assistance Matters. This plan drives collaboration through:

11 Treaty on the Functioning of the European Union (TFEU), signed 25 March 1957, Article 23 (www.legislation.gov.uk/eut/teec/article/23).
12 https://legal.un.org/ilc/texts/instruments/english/conventions/9_2_1963.pdf.
13 https://migrationnetwork.un.org/system/files/resources_files/iml_consular_assistance1.pdf.

- Mutual assistance in crises,
- Resource sharing to support citizens in third countries, and
- Streamlined travel processes for ASEAN nationals, enhancing mobility and consular support within the region.

— **Supranational Caribbean organizations:**

The largest three organizations – the Caribbean Community (CARICOM), the Organisation of Eastern Caribbean States, and the Association of Caribbean States – include agreements on sharing consular and diplomatic responsibilities. For instance, CARICOM's Multilateral Air Services Agreement promotes mobility and facilitates streamlined consular assistance for citizens across member States. These agreements demonstrate regional cooperation to support nationals in times of need.

Examples of Bilateral Agreements for Shared Consular Services

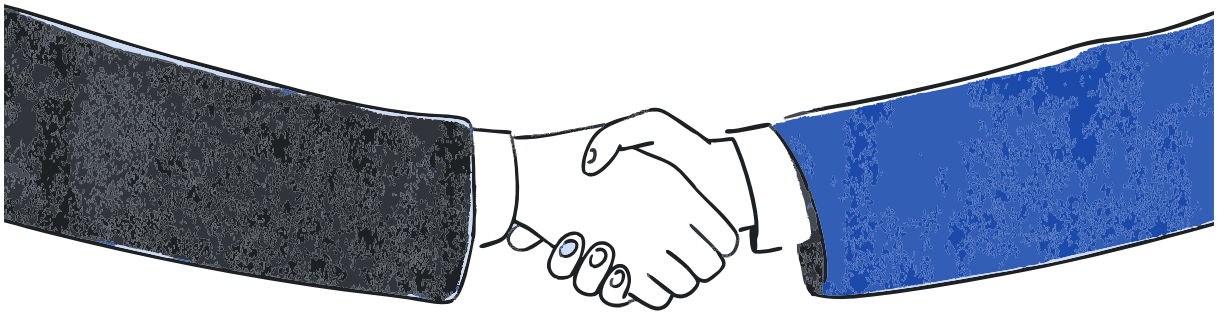
Several bilateral agreements also reflect the growing trend of sharing consular responsibilities between States to ensure nationals receive assistance in countries where their own representation is absent:

— Canada–Australia: The 2001 Memorandum of Understanding between Canada and Australia highlights a mutual agreement to provide consular assistance. It states that when citizens of one country are in areas where their own country lacks consular representation, the other country's missions will offer consular services to them.

— Argentina–Chile: The 2011 Supplementary Protocol to the Maipú Treaty of Integration and Cooperation provides for consular assistance to nationals of the other party in third countries where their own State has no consular representation.

— Brazil–Argentina: The 2003 Convention on Consular Assistance allows for mutual assistance to nationals in third countries where diplomatic or consular representation is lacking.

— Brazil–Portugal: The 1997 Agreement on Consular Cooperation facilitates protection and consular assistance to nationals of both parties in third countries where either State lacks consular representation.



Individuals with dual nationality, refugee status, or who are stateless are often unable to receive consular assistance from any specific State. Dual nationality generally does not pose an issue when a person is in a third country, as many States offer consular assistance to their dual nationals who are travelling abroad. However, when a dual national is in one of their countries of nationality, assistance may be limited by local laws. For example, the second country may not recognize the first nationality, which can restrict consular rights from the country of origin. Additionally, the type of documents an individual uses to travel can also affect the level of consular support they receive.

The treatment of refugees, asylum-seekers or stateless persons also varies. The consular assistance framework relies on nationality, whereas Stateless persons have no recognized nationality, which poses a problem in determining which State could provide consular assistance. Refugees are unable to rely on the State from which they came to provide them with consular assistance since, according to the 1951 Convention Relating to the Status of Refugees, a refugee is specifically "unable or, owing to [his] fear [of persecution,] unwilling to avail himself of the protection of that country."[14] Indeed, in some cases, the State of nationality might be unable or unwilling to protect refugees from persecution, whereas in others, that State was directly responsible for their persecution. To respond to this predicament, some States include refugees and stateless persons who have ties to them, through residence, for example, as expressly eligible for consular assistance; however, assistance may be given on a restricted basis, contingent on possession of a residence permit. In other States, assistance may be denied or considered in a more discretionary manner.

According to the 1954 Convention Relating to the Status of Stateless Persons, stateless persons residing in a State's territory are entitled to various rights and protections. For example, the Convention mandates that stateless persons receive public relief and assistance under the same treatment accorded to nationals (Article 23). Similarly, access to courts, including legal assistance, must be provided on an equal basis with nationals (Article 16(2)). Concerning administrative assistance, the Convention establishes that "[w]hen the exercise of a right by a stateless person would normally require the assistance of authorities of a foreign country to whom he cannot have recourse, the Contracting State in whose territory he is residing shall arrange that such assistance be afforded to him by their own authorities." These authorities "shall deliver or cause to be delivered under their supervision to stateless persons such documents or certifications as would normally be delivered to aliens by or through their national authorities." Host States are also required to issue identity papers and travel documents to stateless persons (Articles 27 and 28).

Related to cases where stateless persons may not be covered under the protection of the Convention, the United Nations High Commissioner for Refugees (UNHCR) has noted the importance for stateless persons to access consular assistance within the State they reside. In those cases, it is desirable that host States improve "consular assistance or make changes in policy with regard to consular assistance for such individuals".[15] Providing legal identity papers and travel documents to stateless persons or granting them immigration status to allow them to remain in a country's territory, are important steps in assisting these individuals.

14 www.unhcr.org/media/convention-and-protocol-relating-status-refugees.

15 www.unhcr.org/wp-content/uploads/sites/27/2017/04/CH-UNHCR_Handbook-on-Protection-of-Stateless-Persons.pdf.

Honorary Consul

An honorary consul is an individual appointed by a country to represent its interests in a foreign location, often in areas where the country does not maintain a formal diplomatic mission, such as an embassy or consulate. Unlike career consuls, honorary consuls are typically private citizens, often prominent members of the local community, who carry out consular duties on a part-time and voluntary basis.

Practical responsibilities

Assistance to nationals: Provide support to citizens of the appointing country, such as facilitating emergency assistance or guiding them through consular processes like passport or birth certificate applications. While they may assist with document preparation or verification, they do not issue passports or register births, as these tasks are completed by formal consulates or embassies.

Promote bilateral relations: Act as a liaison to strengthen cultural, economic and political ties between the host and appointing countries.

Facilitate access to documentation: Assist with verifying documents or forwarding applications for official documentation, within their limited mandate.

Representation: Represent the appointing country at official events or functions in the absence of career diplomats.

Community engagement: Support initiatives that promote the appointing country's culture or business interests in the host country.

Part 4.

Core Principles to Establish Evidence of Identity

The ICAO TRIP Guide on Evidence of Identity (EOI) provides States with a conceptual framework for establishing and verifying an individual's identity. It includes a range of practical tools grounded in international best practices. This guide is particularly valuable for consular staff, as it exemplifies a government authority function where identity must be verified with a high degree of confidence.

Context-specific approaches are required to balance the need for efficient services for genuine citizens with mitigating risks of identity fraud. Consular officials can leverage the EOI approach to develop secure processes that integrate all available data, documentation and information.

Although the EOI framework primarily focuses on uniquely identifying travellers, its core principles are equally applicable when considering the establishment and validation of identity in other contexts. These principles emphasize three critical aspects:

a. the claimed identity is a genuine one and still living.

b. the claimant links to the identity, as the sole claimant, which is unique to the system.

c. the presenter uses the claimed identity in the community.

The implementation of EOI practices relies on robust processes and systems, supported by technology and foundational documents. Local laws and cultural contexts shape these practices, ensuring they are adaptable to specific needs. A risk-based and protection-sensitive approach is essential for establishing and validating identity, particularly for individuals at risk of exploitation or trafficking in persons. Authorities must analyse all available data and documentary evidence while prioritizing the protection of vulnerable individuals. This approach minimizes errors, ensures the highest level of confidence in issuing identity documents and strengthens the integrity of registration processes, all while safeguarding the rights and well-being of those who may be at greater risk.

Identity fraud is a significant global concern, often linked to organized crime and security threats, including terrorism. While traditional methods of fraud, such as forging trusted documents, have been largely mitigated by advancements in data sharing and technology, criminal actors have adapted by obtaining falsely issued genuine documents, exploiting weaknesses in identity verification processes. Importantly, the challenge of identity fraud should not be conflated with the administrative status of migrants, as irregular migration itself is not a crime. Instead, addressing identity fraud requires rigorous examination and verification of the information and documents used to support identity claims, ensuring the integrity of identity systems while safeguarding the rights of all individuals.

An individual's unique identity is defined by a combination of biographic attributes (such as name, date and place of birth) and biometric features (such as fingerprints, facial recognition, or iris scans). Identity management systems rely on these attributes to create a verified profile that links all relevant information about an individual after thorough verification.

Identity is typically established through foundational or breeder documents, such as birth certificates, which form the first step in an identity verification process and provide an anchor of trust. However, the EOI approach goes further by viewing identity as dynamic – a system of interconnected attributes that evolve over time and vary across countries, cultures and social contexts. This flexibility is necessary because local differences impact the availability and reliability of supporting data, documents and information.

What Are Breeder and Foundational Documents?

Breeder and foundational documents are official records that form the basis for establishing a person's legal identity. These documents typically originate from civil registration systems and confirm key life events, such as birth, marriage, adoption, or death. For example, a birth certificate is a breeder document that establishes fundamental details like name, date, and place of birth. Marriage certificates may verify marital status or name changes, while adoption certificates confirm legal parentage and identity for adopted individuals. Death certificates are used to record the end of an individual's legal identity.

Breeder documents are referred to as "breeder" because they are used to apply for and "breed" additional identity documents, such as passports, national ID cards, or driver's licenses.

Foundational documents is a broader term that includes breeder documents as well as other records that verify identity and legal status. Examples of foundational documents include citizenship certificates, national identity cards, travel documents, and digital identity records, which link electronic data to unique identifiers, often incorporating biometric information.

The EOI approach prioritizes a methodical evaluation of all evidence to ensure the process is robust and secure. Authorities must tailor their methods to align with their legal frameworks, operational practices and cultural norms. When documentary evidence is insufficient, additional measures – such as structured interviews – can legitimize initial claims. Ultimately, a well-implemented EOI process not only supports reliable identity verification but also builds the foundation for further interactions, such as issuing identity documents or accessing identity-based services.

There is a practical set of objectives consular staff should follow to achieve reliable EOI:

1. **Objective A – An identity exists**
    - Verify the existence of the claimed identity by cross-checking documents with source records (e.g. birth, marriage, or death registers).
    - Use trained document examiners to authenticate documents when access to source records is limited.
2. **Objective B – The identity is living**
    - Confirm that the individual claiming the identity is alive through in-person applications or checks against the State's death register.
3. **Objective C – Person links to identity**
    - Ensure the claimant is uniquely linked to the identity through in-person verification. This can involve:
        - Photo identification or biometric validation using trusted databases.
        - Interviews conducted by trained staff.
        - Verification by a trusted referee who can vouch for the claimant.
4. **Objective D – Identity is unique to the system, and the individual is the sole claimant**
    - Conduct biometric checks against existing records to identify potential matches or duplicates.
    - Use biographical checks to identify similarities in names, addresses, or other data points that might indicate identity duplication.
5. **Objective E – Identity is used in the community**
    - Collect evidence that demonstrates the identity's consistent use over time. Examples include:
        - Statements from trusted referees in the claimant's community.
        - Supporting documents such as utility bills, bank statements, or school records.
        - Validation against electoral rolls or identity databases.
    - Where documents are unavailable, structured interviews can help identify discrepancies or reinforce confidence in the claimed identity.

A robust approach to EOI process involves considering all available information when issuing a document or facilitating services. Evidence may include documents, data, and other information from multiple sources, as well as statements from the applicants themselves. The type of information will differ depending on its source and must be evaluated within the local context to determine its relevance and reliability. While isolated pieces of evidence may have limited utility, collectively they can increase confidence in the legitimacy of the claimed identity. Information that demonstrates consistency over time further enhances confidence.

Authorities face various challenges in meeting evidential requirements, including:

- **Multiple valid versions of breeder documents**: For example, different formats of birth certificates.
- **Restricted access to source registers**: Limited information-sharing between government bodies.
- **Historic records management issues**: Older travel or breeder document records may be paper-based and difficult to verify.
- **Lack of person-centric categorization**: Historical data systems may not directly link records to individuals.
- **Incomplete or non-existent registers**: Some jurisdictions lack comprehensive civil registration systems.

Despite these challenges, authorities should aim to build identity confidence by utilizing a range of information, documents, and records. A methodical, multi-faceted approach is critical to ensuring secure issuance processes.

Meeting EOI Objectives

Objective A – An identity exists

Identity should be established at birth through an entry in a national register. This anchor of trust allows subsequent life events and identity records to be reliably linked back to it. For example, a birth certificate creates the first formal record of an individual's identity. However, in cases where breeder documents are unavailable or unreliable, confidence in identity can still be achieved with a combination of other sources, such as community attestations, government records, or private sector documentation which includes mobile phone registration records, bank account information, or employment contracts from private companies, for instance.

Civil Registration and Vital Statistics (CRVS) systems are central to recording life events such as births, deaths, marriages, divorces, adoptions, name changes and citizenship. These systems may also include national identity components, such as identity cards or digital identity records, and uniqueness can be supported through biometrics.

Breeder documents are evidentiary documents that serve as physical tokens of the record. They are issued with a unique registration number and are used to establish identity and confirm entitlements. These documents confirm the occurrence of a life event and supply evidence accepted by national authorities to support a claim to identity. However, holding a breeder document does not necessarily verify the rightful ownership of the document itself.

Challenging or unusual situations, such as conflict, natural disasters, or large-scale displacement can result in limited or unavailable documentation. Foundational life events may also not be routinely recorded in some areas, leaving individuals without legally recognized identification. In such cases, alternative evidence – including interviews, community-based verification, or other sources – can support the establishment of identity, aligned with Objectives C (Applicant links to the identity) and E (Applicant uses the identity).

Objective B – Identity is a living identity

Confirming that an identity is "living" involves verifying that the individual associated with the claimed identity is still alive. CRVS systems often record deaths, but their reliability can vary, especially for deaths occurring overseas or in regions with weak registry systems.

State systems such as social services often require regular confirmation that beneficiaries are alive, adding an additional layer of reliability. Requiring individuals to appear in person for identity verification can further enhance confidence by allowing biometric data collection and cross-referencing with official records.

Linking birth and death records to national identity systems, especially those incorporating biometrics, strengthens the ability to verify living identities. When centralized death registers are unavailable or incomplete, alternative methods – such as biometric matching, interviews, and evidence of consistent identity use (Objective E) – can reinforce confidence.

The design of CRVS systems should support basic searches to prove that an identity is living. However, challenges may arise when individuals are born or die in different jurisdictions or States. Increasingly, data systems are emphasized as tools to support verification, either alongside or instead of physical documentation. These systems enable automatic checks and verifications of living identities, further reducing the potential for errors.

Objectives C And D – Applicant links to the identity and is unique to the authority's system

Having established that an identity exists and is living, these objectives focus on confirming the claimant's connection to the identity and ensuring its uniqueness within the system. Most fraudsters claim to be someone they are not, by impersonating a real or fictitious identity.

Prepared fraudsters often familiarize themselves with information on application forms. Consular staff should therefore seek to verify details not readily available to the claimant that support their link to the identity.

In-person presentations for the issuance of documents are critical for obtaining and corroborating information. They allow staff to observe behaviour, collect biometrics, and verify connections, making them an essential component of an efficient EOI system. Biometric verification is particularly effective for confirming uniqueness and preventing duplication.

Trusted referees

Trusted referees are a key component of the EOI process, especially when breeder documents are unavailable or unreliable. They provide additional evidence by confirming the applicant's use of the identity in the community (Objective E), validating personal details such as name and date of birth (Objective C), and corroborating relationships and residency.

Referees must have a verified identity themselves and personal knowledge of the applicant, typically for at least 12 months. They should be trusted by the authority and have an established and verifiable identity of their own. Consular staff may designate certain professionals or public figures as referees, such as lawyers, doctors, teachers, government personnel, religious leaders, or local administrators.

The role of biometrics in objectives C and D

Biometrics play a pivotal role in establishing and validating the uniqueness of an individual's identity. They enable authorities to detect and prevent fraudulent or multiple identity claims, improving the security and integrity of identity systems. When there is a high degree of confidence in the uniqueness of an identity, authorities can efficiently process low-risk cases and more effectively identify individuals of interest. The development of ePassport standards, which incorporate digital facial images, fingerprints, and iris scans, supports the automation of biometric comparisons during document issuance.

The IOM *Introduction to Biometrics* manual serves as an operational guide for consular staff using biometric technology. In the context of the EOI objectives, understanding key principles of biometric comparison and matching is essential.

The usage of biometrics

- *Verification (1-to-1 matching)*
  Verification determines whether a live biometric sample matches a stored biometric record associated with the claimed identity. There are two primary approaches:

  1. Centralized storage: A biometric record is stored in a database maintained by an authority. For example, immigration authorities may store fingerprints or facial images collected during enrollment. When an individual provides a live biometric sample, it is compared against the corresponding stored record.
  2. Distributed storage: The biometric record is stored on a secure identity document chip, such as an ePassport. The individual presents their ePassport, and the chip's stored biometric data is compared with the live biometric sample (e.g. fingerprint or facial scan).

  Verification usually includes Public Key Infrastructure (PKI) validation, which ensures that the biometric data on the chip was issued and signed by a trusted certificate authority. This process confirms that the document is authentic, has not been tampered with, and that the biometric data genuinely belongs to the individual presenting it.

- *Identification (1-to-many matching)*
  Identification is used to confirm the identity of an individual when it is unknown or to ensure that a captured biometric is unique and not associated with another identity in the system. Unlike verification, which compares a biometric sample to a single known record, identification involves comparing a live biometric (such as a facial image or fingerprint) against all entries in a central database of biometric records.
  The process may produce one of three outcomes:

  - A match: The captured biometric corresponds to a single record in the database.
  - A list of possible matches: Multiple records may partially match the biometric, requiring further analysis.
  - No match: The biometric does not correspond to any records in the database.

  This process is essential for preventing duplicate records, detecting fraudulent identities, and ensuring the uniqueness of identities in systems such as national registries or visa management platforms.

- *Screening or watchlist checking*
  Screening involves comparing a live biometric sample against a database or "watchlist" containing biometric and/or biographic data of individuals flagged for further action. These watchlists are typically used to identify persons of interest, including individuals involved in criminal activities, terrorism, or other security-related concerns. International watchlists, such as those maintained by INTERPOL, enhance the effectiveness of screening processes by enabling global cooperation to identify individuals linked to security risks or criminal activities.

- *The multi-biometric system approach*
  Multi-biometric systems capture multiple types of biometric data, such as fingerprints, facial recognition, and iris scans. These systems enhance the accuracy and inclusivity of identity verification.
  Benefits include:

  - Improved accuracy by reducing reliance on a single biometric type,
  - Flexibility for individuals whose biometrics (e.g. fingerprints) may be difficult to capture, and
  - Greater resilience against errors or poor-quality data.

Privacy and ethical considerations in biometric data collection

The collection and use of biometric data involve critical legal and ethical considerations, with the privacy rights of individuals and personal identification paramount. The Biometrics Institute provides valuable guidance on the ethical use of biometrics. Biometric data must be protected, collected with authorization, and stored, shared and retained in alignment with its intended purpose, necessity and proportionality. Proactive engagement with the data owner is also crucial.

Privacy and data protection are foundational ethical concerns. Biometric data is inherently personal and must be collected with the utmost respect for individuals' privacy. This requires lawful collection processes and ensuring that individuals are fully informed about the reasons for data collection, its intended use, and measures to safeguard their privacy. Additionally, the collection of biometric data must be demonstrably necessary and proportionate to the objectives it aims to achieve.

The principle of non-discrimination must be strictly upheld in the collection and processing of biometric data, ensuring that its use does not result in unjustified differential treatment of certain groups. Exceptions should be strictly limited to cases prescribed by law, such as situations where processing is necessary to protect the vital interests of the data subject or another individual who is incapable of giving consent. Where biometric data is shared or transferred, Contracting States should apply purpose limitation and ensure that the data is retained only for as long as necessary for the specific, legitimate purpose for which it was collected, in line with applicable data protection standards. Robust mechanisms must be in place to prevent and address any misuse of biometric data, including risks of discrimination, profiling, or stigmatization.[16]

Security of the data is another ethical imperative. Adequate safeguards must be in place to protect biometric data against unauthorized access, breaches, and other forms of abuse. The integrity and confidentiality of personal data must be maintained throughout its lifecycle, from collection to eventual deletion. In ensuring ethical compliance, it is imperative to incorporate mechanisms for independent oversight and provide clear avenues for individuals to exercise their rights and seek redress in cases of infringement. Continuous evaluation and adaptation of data collection practices are required to respond to the evolving context and to ensure that the rights and dignity of individuals remain at the forefront of data management policies. Furthermore, the Human Rights Committee, in its General Comment No.16 (1988), emphasized that States must take effective measures to prevent information about an individual's private life from being accessed by unauthorized persons.[17] Such information must not be shared, processed, or used unlawfully. Additionally, every individual should have the right to know which public authorities, private individuals, or entities have access to or control over their personal files.

Objective E – Applicant uses the identity

The objective is to ensure confidence in a claimed identity by corroborating it with consistent use in official and social settings. Documents, records, and information used should be dated and include sufficient biographic data to establish a reliable link to the individual. The use of identity in community contexts is commonly referred to as a "social footprint."

Social footprint

A social footprint reflects an individual's interactions with various organizations over time, which often maintain publicly or officially accessible records. This identity-related information encompasses life events and societal engagements, such as education, employment, health care, financial activities and utility services. It may also include a digital footprint from social media or online platforms. The use of such information, while subject to local laws and customs, can help deter fraudulent claims and validate consistent use of identity across authorities over time.

When collecting social footprint information, it is critical to access only the data directly necessary to establish identity. Documents should be assessed for their relevance to identity verification without intruding on sensitive personal information. If documentation serves dual purposes – such as proving identity and eligibility for a service – this dual use must be clearly explained to the applicant. Flexibility in document choice ensures applicants are not compelled to share unnecessary or sensitive personal details. Recording

16 www.bazl.admin.ch/dam/bazl/en/dokumente/Fachleute/Regulationen_und_Grundlagen/icao-annex/icao_annex_9_facilitation.pdf.

17 www.refworld.org/legal/general/hrc/1988/en/27539.

information without retaining original documents reduces the administrative burden of safeguarding sensitive data.

Examples of documents and information to evidence social footprint

The checklist below suggests example documents and records that can be useful:

- Driver licences, vehicle registration documents
- Social services and health cards
- Inland revenue or tax number
- Electoral roll records or voting cards
- Credit cards, bank cards and bank accounts
- Confirmation of immigration or visa status
- Student identity cards, education records and qualifications
- Utility accounts and services
- Employee identification cards and professional enrolments
- Medical and dentist records
- Property ownership or tenancy agreements
- Court records, including fines or tickets
- Travel records (e.g. tickets, boarding passes)

Interviews

Interviews serve as a critical tool in the process of determining and verifying the identity of individuals without proof of legal identity. They provide an opportunity to assess an applicant's knowledge and connection to their claimed identity, verify the EOI collected, and deter fraudulent behaviour through targeted questioning. Abnormal or unexpected responses should be recorded as they may require further investigation. Policies and procedures must be rights-based and clearly define when and how interviews are conducted, ensuring consistency, transparency and adherence to ethical and legal standards.

Effective interviews require meticulous preparation, cultural sensitivity and adherence to ethical principles. Interviewing officers must balance building rapport with obtaining actionable information while assessing immediate needs. Pre-interview preparation includes setting the stage for a comfortable environment, such as a private, quiet, and welcoming space. Officers should avoid intimidating factors, such as visible weapons or uniforms, and should maintain a neutral or friendly demeanour. Sensitivity to cultural norms related to age and gender, eye contact, and personal space is crucial, and engaging cultural mediators is usefull to bridge linguistic and cultural gaps. These mediators not only interpret language but also provide critical cultural insights that can assist in understanding applicants' backgrounds. It is important to include considerations regarding mediators and interpreters that could represent a risk and/or affect the interviewee capacity to respond (gender, ethnicity, etc.). A calm and unhurried conversational tone is crucial, particularly when cultural sensitivities must be respected. Officers must also be trained in trauma-informed, gender-sensitive, and child-sensitive approaches to ensure ethical interactions, particularly with individuals in vulnerable situations. Whenever possible, migrants should have the option to request an interviewer of the gender they feel most comfortable with.

Explaining the purpose of the interview at the outset and emphasizing confidentiality fosters trust, consent and cooperation. The inclusion of clear and structured questioning is essential. Interviews should start with general, non-threatening questions to build trust and ease the applicant into the process. Addressing immediate health and safety needs must be prioritized before proceeding. Questions such as "Do you feel safe here?" or "Do you require medical attention?" can identify pressing concerns. These questions not only ensure humane treatment but also improve the effectiveness of the interview by addressing obstacles to engagement.

Specific and tailored questions are vital for verifying the authenticity of an applicant's identity. These questions may include inquiries about personal history, family relationships, and cultural knowledge, as well

as details about the journey and interactions with organizations during migration. Open-ended questions should be prioritized to elicit comprehensive narratives and reduce the likelihood of rehearsed answers. Behavioural cues, emotional responses, and inconsistencies in answers must be carefully noted for further investigation. Officers should remain mindful of psychological factors, which may impact the applicant's ability to respond, and should adjust their approach accordingly, seeking expert guidance if necessary. It is important to consider situations where an interview should be halted, such as when the interviewee is unable to continue due to distress, lack of capacity, or other factors that affect their ability to provide accurate or voluntary responses. Additionally, considerations should be made regarding whether interviews should take place with an accompanying person present, as this may influence the interviewee's comfort level and ability to speak freely. In some cases, it may be necessary to conduct the interview privately to ensure that the interviewee can respond without pressure or undue influence.

When children are involved, special protocols must be in place to protect their well-being. Interviews with children should only be conducted by trained child protection personnel using trauma-informed and age-appropriate techniques. The benefit of the doubt must be given to children regarding their claimed age unless substantial evidence suggests otherwise. Legal guardians must be appointed for unaccompanied or separated children to represent their best interests and assist in family tracing efforts where possible. Children must have access to essential services, such as education, health care and social support, facilitated by appropriate regular pathways. Children should not be separated from their parents or primary caregivers unless such separation is deemed necessary for the best interests of the child, as determined by a competent authority. If a child appears distressed or overwhelmed during an interview, the process should be paused and adjusted as needed.

The physical environment of the interview should be age appropriate and foster open dialogue and reduce stress. It is recommended that officers avoid displays of authority and instead adopt a calm and conversational tone. Cultural mediators can enhance communication by interpreting both linguistic and cultural nuances, particularly when discussing sensitive topics such as persecution or family dynamics. Their presence helps to ensure that interviews respect cultural practices while maintaining accuracy in information collection.

Interviews via video link may be employed where feasible to improve accessibility and efficiency, particularly in remote or resource-constrained settings. However, strict measures must be in place to uphold security and confidentiality. Third-party corroboration, such as testimonies from family, friends, or community leaders, can also strengthen identity verification processes. Responses from these sources should be cross-referenced with interview findings and documented systematically to support verification efforts.

CASE STUDY: MEETING EOI OBJECTIVES
IDENTITY DOCUMENTATION

Issuing identity documents to individuals who are undocumented involves challenges in verifying identity, particularly for Objective A (Identity exists). Individuals seeking assistance may lack valid identity documents due to loss, lack of registration, or non-recognition in their country of origin. In such cases, consular representatives rely primarily on evidence collected during face-to-face applications and interviews, alongside verifiable information about the applicant's country of origin and local context.

Establishing uniqueness is key to processing an application for identity documentation through consular services. The process often begins with a biographic or biometric search to ensure that the claimed identity is not registered elsewhere. This is followed by interviews, verification through trusted referees, and analysis of the applicant's social footprint over time to monitor consistency, manage risks, and support the applicant in building an identity claim.

When central databases or government records are unavailable, other sources of evidence can play a critical role. These may include records from education institutions, employment history, health care services, financial transactions, or utility accounts. Evidence from interactions with local authorities, such as municipal services or police reports, may also provide important verification. Each source should be carefully assessed for reliability and relevance to the individual's identity claim.

Social media interactions, where reviewed with informed consent, may also provide supporting evidence, provided the confidentiality of the applicant's personal data is safeguarded. Data analysis can also reveal patterns or connections between individuals, such as shared community ties or family relationships, which may help verify claims and manage risks associated with fraudulent applications.

To ensure the identity is linked to a living individual, in-person presentation is essential. Where legally permissible, biometric data, including a clear photograph in compliance with ICAO Doc 9303 standards, should be collected. Searches and checks on available databases should identify duplicate claims or inconsistencies. Any matches or discrepancies must be investigated to address potential risks.

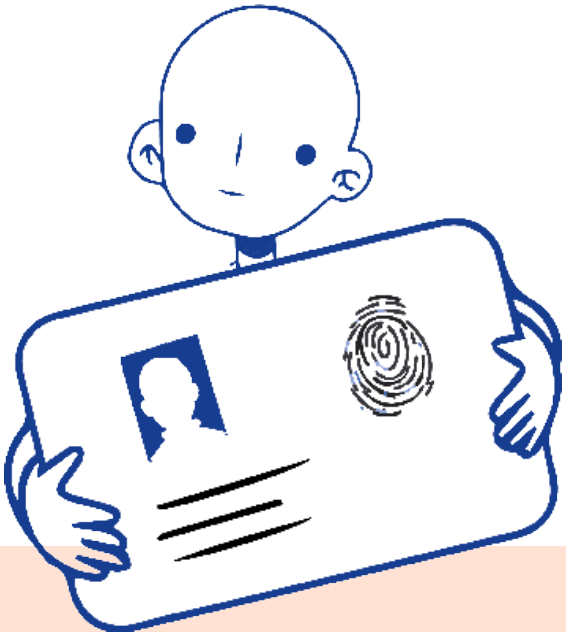
Establishing the Identity of Children

Establishing a child's identity can present unique challenges, particularly when relying on documentary evidence alone. Children may have limited access to identification documents or social records due to their age, dependency on caregivers, and systemic gaps in registration or record-keeping. Additionally, photographic identification and biometric data can be less reliable as children grow and their physical appearance changes.

To address these challenges, consular staff should adopt a rights-based, comprehensive and protection-oriented approach when establishing a child's identity and act in respect of the best interest principle:

- Documentary links: Establish connections between a child and their parent(s), legal guardian, or caregiver through available civil registration records, such as birth certificates or family books.
- Engagement with trusted institutions: In fixed locations, children may be known to education and health authorities, social services, or recognized religious and cultural organizations. Verification of records from these institutions can support identity establishment.
- Legal guardianship and childcare arrangements: For unaccompanied children, assigning a legal guardian and ensuring age-appropriate childcare arrangements are essential safeguards.
- Biometric and DNA considerations: Collecting biometric data from children may be unreliable due to developmental changes. DNA matching, while available, should be a measure of last resort and only considered in cases where there is a significant risk of trafficking, abduction, or disputes regarding the child's identity. Its use must adhere to established ethical and legal safeguards to protect the child's rights.

To protect the rights of children and act as responsible authorities in this regard, it is important to have in place comprehensive safeguards that establish higher standards and added protective measures. Such safeguards should include provisions for the automatic deletion of children's data after a predetermined timeframe to prevent unnecessary retention and ensure that children or their guardians have access to review their data, request corrections, and delete records when no longer needed. Access to and sharing of children's data should be subject to stringent controls, ensuring that their information is handled with the utmost care and respect for their privacy and security.



Child Safeguarding Principles

Child safeguarding is about ensuring that children are protected from any direct or indirect harm resulting from actions of officers or staff, or as a consequence of any organizational policy or practice. Safeguarding actualizes the humanitarian principle of "do no harm" and principles relating to Sexual Exploitation and Abuse (SEA). The following principles ensure the protection of children's rights in line with internationally recognized frameworks, particularly the United Nations Convention on the Rights of the Child (CRC) and broader humanitarian protection standards:

Non-discrimination

All children, regardless of nationality, migration status, gender, race, disability, or any other status, are entitled to equal protection and support. Safeguarding measures must respond to the specific needs of vulnerable children, including those who are unaccompanied, separated, displaced, or at risk of exploitation or abuse.

Best interests of the child

The best interests of the child must be a primary consideration in all actions affecting them. This includes ensuring their safety, dignity, and well-being, while facilitating their participation in decisions in age- and context-appropriate ways.

Duty of care

Staff and all individuals interacting with children have a professional and ethical responsibility to uphold the highest standards of conduct. This includes actively preventing, identifying, and reporting any form of harm, abuse, exploitation, or neglect, as well as ensuring timely and appropriate responses to safeguarding concerns.

Trauma-informed and age-appropriate practices

Staff should adopt trauma-informed practices to minimize distress and ensure that interviews or other interactions with children are conducted in an age-appropriate manner. This may include using child-friendly spaces and culturally sensitive approaches.

Informed participation

Children have the right to be informed about safeguarding measures, their rights, and available reporting mechanisms. Information must be communicated in a clear, age-appropriate, and culturally sensitive manner to ensure understanding and participation.

Accountability and feedback

Organizations must establish clear, accessible and child-friendly complaints and reporting mechanisms. Allowing for individuals to safely access clear, accessible, and effective complaints and report mechanisms support authorities to improve services, while providing a space for individuals to express concerns safely, and have a voice in the decisions that affect their life. Staff are accountable for implementing safeguarding policies, and violations or concerns must be addressed promptly through appropriate channels. Feedback mechanisms should empower children to express concerns safely.

Confidentiality

Personal information and safeguarding records must be managed securely to protect the child's privacy. Access to information should be strictly limited to individuals directly responsible for addressing safeguarding concerns, with measures in place to prevent unauthorized sharing or misuse.

CASE STUDY: CHILDREN IN EMERGENCY SITUATIONS
UKRAINE

In February 2022, the conflict in Ukraine intensified following military actions by the Russian Federation, leading to significant humanitarian consequences, including the widespread separation of children from their families. Many children, including those unaccompanied, separated, in institutional care, or forcibly transferred, faced heightened risks and vulnerabilities. Some children were brought to border areas and left by family members who returned to retrieve other relatives, while others were entrusted to neighbours or acquaintances for evacuation. These circumstances placed children at greater risk of trafficking, particularly when they were not identified by national child protection systems in countries of transit or destination, or when the capacity of caregivers to support them diminished over time.

To prioritize the best interests of the child, it was essential to establish robust systems for sharing information about children on the move, both within Ukraine and across borders. Family reunification efforts posed additional challenges. Temporary arrangements, such as placing children with relatives during emergencies, sometimes exposed them to unsafe environments that contravened their best interests. This was further complicated by the principle of free movement within the European Union, which enabled children to cross borders without sufficient monitoring, increasing risks of neglect, abuse, or exploitation.

Additional risk considerations

The misuse of false identities poses significant risks to children. Fraudulent or manipulated identity documents can obscure a child's true identity, hindering their identification by authorities and complicating family tracing and reunification efforts. Traffickers and exploiters may exploit falsified documents to facilitate cross-border movement of children, while well-meaning caregivers or family members may unintentionally place children at risk by failing to ensure proper safeguards.

In 2018, Mexico's Foreign Ministry introduced the Consular Assistance Protocol for Mexican Victims of Human Trafficking Abroad. This protocol was developed by Mexico with the assistance of IOM and the United States Embassy in Mexico.[18] It is designed to facilitate the capacity of Mexico's consular network to identify victims and possible victims of trafficking abroad. It also outlines criteria, guidelines and specific actions for assistance and protection. Mexico developed two other consular protection protocols with the help of United Nations agencies: one on unaccompanied migrant children and adolescents (in partnership with UNICEF) and another on victims of gender-based violence (in partnership with UN Women).

False identities can be established through various means, including creating fictitious identities, altering biographic information, assuming stolen identities, or compromising identity management systems. Identity

18 https://migrationnetwork.un.org/minisite/gcm-tools/gcm/pdf/English/23-GCM-Objectives/14-CONSULAR-PROTECTION.pdf.

theft is a particular risk for children, as their identities can be misused undetected for extended periods, often resulting in long-term consequences. These risks underscore the importance of implementing EOI Standards alongside comprehensive identity risk management measures.

Supporting documentation

Supporting documents contain identity information that helps establish or confirm an individual's identity. They serve to verify that an identity exists (Objective A) and to substantiate information found in foundational documents. Supporting documentation is particularly helpful when the authenticity of foundational documents is in question.

Documentation with a photograph is useful for linking an individual to an identity (Objective C), while verification of such documents against the individual can confirm the connection between biographic data and the photograph. Supporting documents also strengthen confidence in identity claims (Objective E) by demonstrating identity use within the community. Reliable supporting documents may include biographic data such as name, sex, date of birth and signature. Multiple pieces of reliable evidence provide greater confidence than a single document, particularly if there are doubts about its origin or authenticity.

Best practices for document verification

- Request original documents to examine their security features, or certified copies from the issuing authority. Uncertified copies are prone to tampering.
- Verify documents against electronic records or centralized registers where feasible.
- Accept only valid documents within their expiry dates. Expired documents may require corroboration through additional records.
- Community-based documents should ideally be issued within the past year.
- Full birth certificates are preferred, as they include critical information such as name, sex, parents' names, and place and date of birth. Short-form certificates have become less commonly issued by governments.
- Evidence of name changes should be provided through official documentation.
- Any doubts about document authenticity should be referred to the issuing authority for verification.

CONSULAR SUPPORT IN ADDRESSING MIGRANT DEATHS AND DISAPPEARANCES

Consular support plays a crucial role in preventing migrant disappearances, searching and identifying those that have died and gone missing and supporting families. Consulates are an essential component of transnational coordination and information exchange mechanisms on missing migrants. Their work directly contributes to preventing disappearances and alleviating the suffering of families who do not know the fate and whereabouts of their loved ones. Consular authorities can help migrants communicate with their families to inform them that they are alive by facilitating access to means of communication or by reaching out to families on behalf of migrants, including in contexts where migrants are in detention.

Search and identification of migrants that have died or gone missing

The search and identification of migrants who have died or gone missing is a transnational effort that relies heavily on consulates.

When a missing migrant case is reported (usually in the migrant's country of origin by a family member), governments turn to their consular offices in countries where the migrant might be to support search efforts. Consular officials liaise with relevant government authorities, civil society organizations, international organizations, and other stakeholders to obtain information on the fate and whereabouts of their co-national. If information is obtained, consular officials then share it with relevant governmental focal points in the country of origin.

When human remains are discovered in a migration context, the consulate (either confirmed or suspected to be of the deceased migrant's nationality) is usually contacted to support the management of remains and the identification process. Consular services support the identification process by coordinating with relevant authorities, including forensic institutions, law enforcement, and international organizations. This process requires cross-border cooperation to ensure the exchange of ante-mortem and post-mortem data, allowing for accurate identification and case resolution.

Consular responsibilities include:

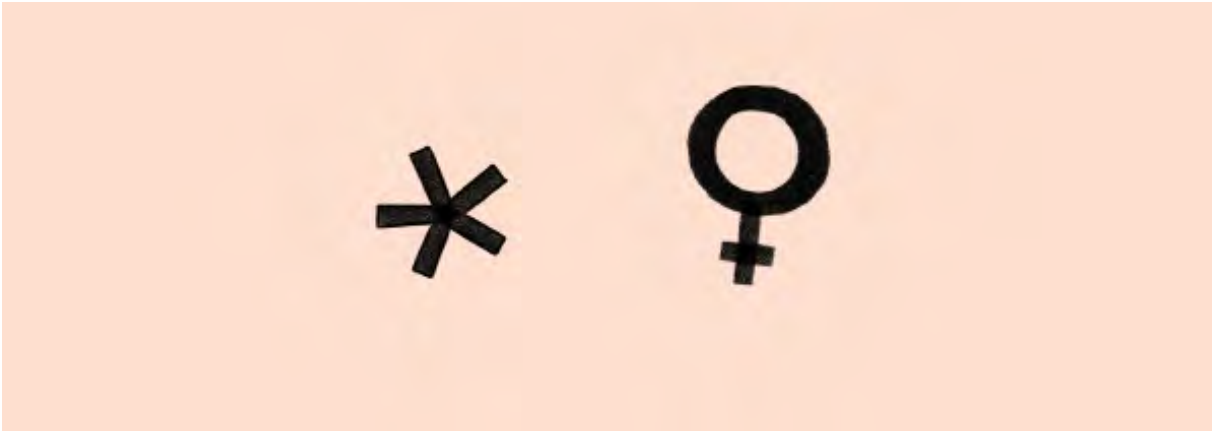
- Coordinating with local authorities: Consular offices liaise with forensic institutions, police and morgues to support in the identification of deceased migrants.
- Supporting collection and sharing of ante-mortem data: Consulates can serve as conduits to ensure that ante-mortem data is collected, including DNA from family members, fingerprints stored in databases of the country of origin, or dental records, all of which help identify remains.
- Facilitating transnational coordination channels and cross-border data exchange: Consular officials can ensure the effective exchange of information between the countries involved to facilitate identification. It is helpful for consular officials to have one governmental focal point in their capitals who, in turn, is responsible for liaising across government entities in the country of origin and with families.
- Issuing documentation: Consulates may assist with issuing death certificates and other legal documentation, ensuring these are shared with government entities and family members in the country of origin. This legal documentation is usually required for the repatriation of remains or burial in the country of death.

SUPPORT TO FAMILIES OF THE DEAD AND MISSING

Consular authorities can serve as a bridge between families and relevant national or international mechanisms for tracing missing persons. Ultimately, the work done by consular officials to prevent disappearances and search for and identify the dead and missing will help alleviate the suffering of families.

Key support functions include:

- Receiving and processing missing persons reports: In countries of transit or destination, other migrants, including co-travellers, might not feel comfortable approaching local authorities to report a missing person and may instead prefer to go to the consulate of the missing migrant. Consulates can collect detailed information from families, including physical descriptions of the migrant, photographs, migration history and details on where biometric information and DNA samples might be available.
- Providing information and referrals: Consular staff can guide those searching for missing migrants on available legal avenues, including access to humanitarian organizations that specialize in locating missing migrants.
- Issuing certificates of absence: In some jurisdictions, consulates may facilitate or provide guidance on obtaining Certificates of Absence, which serve as official recognition that a person remains missing. These documents can help families manage legal and administrative matters, such as accessing social benefits, guardianship arrangements, or handling financial obligations in the absence of a confirmed death.
- Navigating legal and financial barriers: Some governments through their consulates provide financial support or work with humanitarian organizations to help cover repatriation costs.
- Ensuring dignified burial: In cases where repatriation is not possible, consulates can liaise with local authorities to arrange a dignified burial, respecting religious and cultural considerations.
- Legal support: Consular officials can play an important role in supporting families who seek justice, accountability and redress for their loved one's death or disappearance.



Part 5.

Data Protection and Privacy in Consular Services

National legal identity systems play a critical role in verifying identities, but they also pose significant privacy risks that can impact a broad range of human rights, including the right to privacy as articulated in Article 17 of the International Covenant on Civil and Political Rights (ICCPR). These risks are amplified with the digitization of these systems, particularly concerning the security of personal data such as names, dates of birth, photographs, fingerprints and other biometrics. Mishandling this data may infringe on privacy rights, lead to discriminatory practices, or endanger individuals through data leaks.

Consular services play a vital role in supporting the development and implementation of legal identity systems that respect privacy and align with international, regional and national data protection laws and standards. Frameworks such as the General Data Protection Regulation (GDPR) in the European Union, the African Union Convention on Cyber Security and Personal Data Protection, and relevant national legislation should guide their approach. Personal data must be collected lawfully and used only for specified, legitimate purposes that are transparent to the data subject. Any further use requires explicit, prior, and informed consent or must align with compatible purposes. Only data strictly necessary for the specified purpose should be collected, and it must be accurate and kept up to date. Excessive data collection heightens privacy risks and increases the likelihood of misuse.

EXAMPLE: EUROPEAN UNION'S GENERAL DATA PROTECTION REGULATION

The General Data Protection Regulation (GDPR) is a landmark legislation that sets the standard for data protection and privacy in the European Union and beyond. Enacted in 2018, the GDPR establishes stringent requirements for organizations that collect, process, or store personal data of individuals within the European Union.

Key provisions of the GDPR

- Lawfulness, fairness and transparency: Data must be processed lawfully, fairly, and in a transparent manner. This requires organizations to provide clear information about data processing activities and to obtain consent where necessary.
- Purpose limitation: Data should only be collected for specified, explicit, and legitimate purposes, and not further processed in a manner incompatible with those purposes.
- Data minimization: Only data that is necessary for the intended purpose should be collected and processed.
- Accuracy: Personal data must be accurate and up to date. Inaccuracies must be corrected or deleted promptly.
- Storage limitation: Data should not be retained longer than necessary. Organizations must establish data retention policies that outline the duration for which data will be stored.
- Integrity and confidentiality: Data should be processed in a manner that ensures security, including protection against unauthorized or unlawful processing and accidental loss or damage.
- Processing of sensitive data: The GDPR prohibits processing certain special categories of personal data, such as racial or ethnic origin, political views, religious beliefs, trade union membership, genetic or biometric data, health data, and sexual orientation, unless explicit consent is given or public interest grounds justify processing.

Data subject rights under the GDPR

The GDPR strengthens data subject rights, providing individuals with greater control over their personal data:

- Right to access: Individuals can access their personal data and obtain information about its processing.
- Right to rectification: Individuals can have inaccurate data corrected.
- Right to erasure: Individuals can request the deletion of their data under certain conditions, such as when the data is no longer necessary for its original purpose.
- Right to restriction of processing: Individuals can request the limitation of data processing, especially in cases where accuracy is contested, or processing is unlawful.
- Right to data portability: Individuals can obtain and reuse their personal data for their own purposes across different services.
- Right to object: Individuals can object to data processing based on legitimate interests or direct marketing.
- Rights related to automated decision-making and profiling: Individuals have the right not to be subject to decisions based solely on automated processing that significantly affects them.

Consular services should ensure that data subjects are fully informed about how their data will be collected, processed, stored and shared. Consent must be voluntary, explicit and revocable. Informed consent should be facilitated through clear communication with populations in vulnerable situations, with accessibility measures for those facing language or literacy barriers. Transparent policies and protocols on data use and retention must be publicly accessible, and any changes communicated promptly to ensure trust and accountability. Robust cybersecurity measures, including encryption, multi-factor authentication and access controls, should safeguard data against breaches, tampering, or unauthorized access. Confidentiality must be guaranteed at every stage of data processing. Mechanisms for monitoring and ensuring compliance with ethical and legal standards are essential. Internal and external oversight bodies should review data practices, and violations must be subject to sanctions. Personal data should only be retained for as long as necessary to fulfill the purpose for which it was collected. Once the purpose is achieved, data should be anonymized and securely deleted to mitigate risks. When sharing data across borders or with third parties, consular services must ensure adequate safeguards are in place to protect confidentiality and ensure compliance with applicable data protection laws in all jurisdictions. Individuals should have the right to access their data, request corrections or deletions, have access to complaint mechanisms and remedies, and be informed of any breaches affecting their personal information.

Ethics must underpin all data collection and processing activities, especially when consular services work with migrants or individuals in vulnerable positions. All actions should prioritize the humanity and dignity of individuals, regardless of their migration status. Data collection and identity verification processes should empower individuals and avoid coercive practices. Stronger safeguards should be applied when handling sensitive data, such as biometrics or data related to children and individuals in vulnerable situations.

The use of advanced technologies in migration management presents unique challenges. Data breaches, loss, or unauthorized disclosure can have severe consequences, particularly for migrants who may face discrimination, harm, or threats to their safety. Ethical, rights-based approaches must be adopted to address these risks, ensuring that personal data is handled with care and aligned with human rights norms. The handling of sensitive data can have significant implications for protection outcomes, particularly for vulnerable individuals such as those in detention or survivors of trafficking in persons. Mishandling or unauthorized sharing of personal data may expose individuals to further risks, including potential harm or exploitation. In these situations, improper data management can jeopardize the safety and well-being of individuals, making it essential for authorities to implement strict safeguards to protect their personal information.

Data protection is an evolving field, requiring continuous adaptation to emerging technologies and threats. By integrating data protection by design and by default, consular services and national systems can ensure that identity data is collected, processed, and shared responsibly. Adhering to these principles helps to safeguard privacy, build trust, and uphold the human rights of all individuals, ensuring that systems remain effective and equitable.

Building on these foundational considerations, the following principles should apply to both electronic and paper records of personal data. While they may be supplemented by additional protective measures, they are essential to underpin efforts to safeguard privacy and ensure compliance with data protection standards:

- Personal data must be collected lawfully, fairly, and with the knowledge and explicit consent of the data subject.
- The purpose for which personal data is collected and processed must be specified, legitimate, and clearly communicated to the data subject at the time of collection. Data should only be used for the specified purpose unless the data subject consents to further use or if such use aligns with the original purpose.
- Personal data collected should be adequate, relevant, and not excessive in relation to the specified purpose. Data controllers must take all reasonable steps to ensure that personal data is accurate and up to date.
- Consent must be obtained at the time of collection or as soon as reasonably practical thereafter. Special attention should be given to the legal capacity and condition of individuals in vulnerable situations.
- Personal data should only be transferred to third parties with the explicit consent of the data subject, for a specified purpose, and under adequate safeguards to protect the confidentiality and rights of the data subject.
- The confidentiality of personal data must be respected, applied, and guaranteed at all stages of data collection and processing.
- Data subjects should be given opportunities to verify their personal data and must have access insofar as it does not undermine the specified purpose. There should be a general policy of transparency regarding developments, practices, and policies related to personal data.
- Personal data must be securely stored and protected against unauthorized modification, tampering, unlawful destruction, accidental loss, improper disclosure, or undue transfer.
- Personal data should only be retained as long as necessary to fulfill the specified purpose. Once the purpose is achieved, data should be anonymized and securely destroyed to mitigate risks.

Part 6.

Processes – Issuing Identity and Travel Documents

The creation and issuance of legal identity documents by consular services play a pivotal role in assisting individuals who face barriers to formal identity recognition, particularly in countries where civil registration systems are inaccessible or restrictive. Consulates increasingly address the lack of legal identity among migrants, stateless individuals, and children born in host countries, offering documents distinct from traditional travel documents (emergency travel documents, identity cards, etc.). These consular-issued legal identity documents serve as vital tools for accessing services, confirming identity, and facilitating migration or return. Issuing travel docs can be a key protection measure for stateless persons and those at risk of detention or exploitation. Moreover, it is important to emphasize the need for safeguards against the misuse of documents, particularly in cases involving trafficking in persons and smuggling of migrants. Traffickers and smugglers often exploit vulnerabilities in identity verification and document issuance processes to create or use false identities. This enables them to facilitate border crossings, manipulate vulnerable individuals, and perpetrate exploitation.

Use-case: ID issuance for migrant workers in Türkiye

Consulates of countries such as Pakistan and Bangladesh in Türkiye have developed systems to issue consular identification cards to their nationals working in the country. These cards, equipped with security features, are recognized by Turkish authorities for accessing services such as remittances, legal aid, or health care. Cooperation between Turkish authorities and these consulates ensures the dual utility of these documents: legal recognition and practical support for migrants.

Use-case: matricula consular for undocumented migrants in the United States of America

The Mexican consulate's "Matrícula Consular" programme in the United States is a leading example of consular-issued legal identity documents. These identification cards are issued to Mexican nationals living abroad, including undocumented migrants. They include basic biographical information and a photograph and are recognized by many U.S. institutions for opening bank accounts, accessing health care and engaging in legal processes. This programme has demonstrated the importance of collaboration between consulates and host country institutions to enhance the utility and recognition of such documents.

The integrity of passports, travel documents, and other proof of identity is a key component of national and international anti-crime and anti-terrorism strategies. These documents can be powerful tools in the hands of criminals or terrorists, so controlling the security of a country's identity documents and its issuance processes directly impacts national and international security as well as the global reputation of the issuing authority.

Recently, the development of new technologies and new security techniques has led to a shift of identity document fraud. In the past, people who committed fraud concentrated on the end of the document production chain by falsifying or forging physical documents. Now, they are more likely to concentrate their efforts at the beginning of the chain - document issuance systems, as well as any kind of document register

as the first step in the chain. Consequently, the security of handling and issuance processes has become more critical.

The ICAO Guide for Assessing Security of Handling and Issuance of Travel Documents provides practical guidance tools to help ICAO Member States to either self-assess or assist in evaluating the security of another country's travel document handling and issuance systems. The guide is divided into three parts containing best practice recommendations to prevent and mitigate security threats, provide a comprehensive evaluation tool checklist to assess vulnerabilities, and summarize the important elements from each section for each step of issuing a travel document, as an example of an identity document.

Application Process for Obtaining Travel Documents

To obtain an identity document, applicants must follow a defined, sustainable, and consistent application process including the completion of forms, submission of necessary documentary evidence, providing photographs, and, in some cases, secondary biometrics. Information and documentation collected during this process enable issuing authorities to verify the applicant's identity, eligibility, and entitlement to a document.

The information the applicant submits must be protected during the whole issuance process and after issuance. Privacy and protection of data are essential elements to ensure the security of the document issuance process

Key considerations:

- Application forms and supporting guidance must be clear, accessible, and understandable to ensure accurate and complete applications. Ensure that processes accommodate individuals of all ages, with disabilities, language barriers, or limited digital literacy.
- A uniform, consistent, and auditable process should be in place to enhance transparency and mitigate corruption or misuse. Migrants should be informed about the processes in place and how they can provide feedback or file complaints.
- Policies and procedures must be clear and well-documented to support officers making entitlement decisions.
- The application process must be tailored to the type of application (e.g. first-time or renewal), local circumstances, and the need to capture relevant identity information effectively and securely.
- Digitized photographs must meet ICAO Doc 9303 specifications, and identity validation should be robust.
- Personal data, including biometrics, must be securely stored, with access limited to authorized personnel. Security protocols should align with best practices for data protection.
- Data collection, including biometrics, should be necessary, proportionate, and retained only for as long as required. Retention periods must be clearly defined and limited to what is strictly required for the intended purpose.

Entitlement Process

The entitlement process ensures the integrity of travel documents by verifying three critical elements for issuance:

1. Evidence of the applicant's identity – confirming that the claimed identity is real and belongs to the applicant.
2. Proof of citizenship – verifying that the applicant holds the nationality of the issuing country.
3. Travel restrictions – ensuring the applicant is not subject to any restrictions that may affect eligibility, such as a criminal record, a history of lost or stolen travel documents, or unpaid obligations (e.g. failure to pay child support).

Key considerations:

- The identity-checking process must be robust for both first-time applications and renewals to minimize risks.
- First-time applications should follow a different process from renewals, reflecting the additional checks required for establishing a new identity versus validating an existing one.
- Documentary evidence provided by applicants must be appropriate, reliable, and sufficient to support their claims. The human rights of all migrants must be respected at every stage, regardless of their sex, sexual orientation, gender, age, race, ethnicity, indigenous status, and disability, must be respected at all stages. In addition, all the requirements regarding documentary evidence should be clearly communicated and accessible to everyone.
- Steps must be in place to verify that the information provided by applicants is accurate and authentic.
- In-person interviews may be conducted to establish identity. Where legally permissible, this may include the use of supplementary information, such as digital footprint data.
- Existing records, such as passport databases, should be consulted to validate applicant information and ensure consistency.
- Personnel involved in the entitlement process must be trained in detecting forged documents and understanding the use of supporting or breeder documents presented during the application process.
- If biometrics are collected, they should be cross-checked against other authorized biometric databases, subject to legal permissions, to enhance identity verification and prevent duplication or fraud.
- Mechanisms for appeals and reconsideration must be in place for applicants whose entitlement is denied.

Protection and Secure Management of Stock Used in the Application Process

To maintain the integrity and security of travel and identity documents, all materials used during the application process – including raw materials, blank books, and other document elements – must be securely stored, transported, and accounted for at all times. Any loss or theft of these materials can lead to the creation of counterfeit documents, which would negatively impact the reputation of the documents and jeopardize security.

Key considerations:

- Stock control policies and procedures are well documented.
- Storage of blank documents at the production site and elsewhere is secure and transport between these sites is secure with a limited access vault as a minimum.
- Stock manifests are used when stock is moved between sites.
- A unique, unalterable book number appears on each page of multiple page books (for tracking, mitigating book alteration or use of pages in a new document).
- All raw materials and books are always accounted for, including at manufacturing facilities, at the issuing site and between sites.
- Book usage is accounted for on at least a daily basis and more frequently if different staff have custody of books for personalization purposes. The number of staff who have access to blank books should be limited.
- There should be a separation of duties for those responsible for book custody and control and those staff responsible for book personalization.
- Waste material and any spoiled books or their elements are destroyed on a regular basis.
- Books that have been lost by the holder and recovered by the issuing authority are recorded and destroyed under supervision.

Personalization and Delivery

Once a blank booklet has been personalized and delivered, the holder can use it. Any errors during the personalization process could have a negative impact on the holder during its use. The delivery process should ensure that only the rightful holder obtains the document, to mitigate the risk of use by an impostor. It is crucial to include procedures for the expedited issuance of documents for individuals in emergency situations, such as displaced persons or victims of natural disasters. These procedures ensure that affected individuals can quickly obtain the necessary documentation to access protection, assistance, and their rights, minimizing delays during critical times and preventing further vulnerability.

Key considerations:

- Personalization premises are secure against intrusion and have access control.
- Access to the machines used in the process, blank books and production batches are controlled and secure (logging, approval by at least two people independently, random batch assignment).
- Quality checks of the personalized document or books are conducted (consistency between VIZ, MRZ and chip data on the document, readability of MRZ and chip with appropriate readers, expiry dates, integrity of signature).
- Proper processes and identification checks are in place for in-person pick-ups, either by the applicant or a trusted third party.
- A system is in place for handling unclaimed documents (monitoring, destruction after a reasonable period),
- Any transportation services used such as mailing or courier handling are reliable, and receipt of documents is confirmed; and
- A system is in place for handling non-delivery reports (investigations, voiding of validity through lost and stolen databases).

Document Security

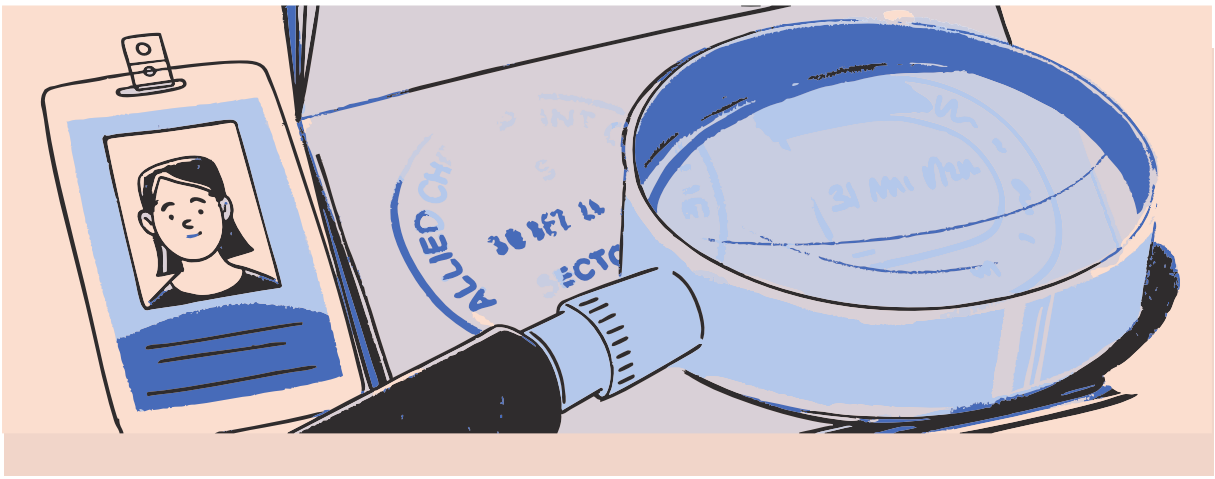
Security features are necessary to prevent alterations and counterfeiting of all identity documents. Travel documents must include robust security features to prevent alterations, counterfeiting, and other forms of fraud. Ensuring compliance with ICAO Doc 9303 standards for Machine-Readable Travel Documents (MRTDs) and electronic Machine-Readable Travel Documents (eMRTDs) is essential. These global standards enhance security and ensure international interoperability between countries.

Note: The IOM Passport Examination Procedures Manual (PEPM) offers detailed guidance on identifying fraudulent documents. It explains security features, indicators of tampering, and techniques for detecting alterations. This manual is a valuable resource for consular staff examining travel documents. The third version of the PEPM Manual is available upon request from IOM.

Key considerations:

- All travel documents must meet the requirements outlined in ICAO Doc 9303, the international standard for machine-readable travel documents, including passports, visas, and other forms of identification.
- To prevent forgery, counterfeiting, and tampering, travel documents should incorporate essential security features such as advanced printing techniques (e.g. microtext, guilloche patterns, intaglio printing), watermarks, ultraviolet (UV) features visible under specific light, holograms, optically variable devices (OVDs), and polycarbonate data pages for durability and tamper resistance.
- A risk-based approach should guide the design and issuance of travel documents. Periodic assessments of threats and vulnerabilities ensure that security features and processes remain effective. Regular reviews of document features and issuance processes are necessary to address evolving risks.

- All travel documents issued by a country, including temporary or single-trip documents, must have identical security features. Consistency reduces the likelihood of misuse and ensures all issued documents adhere to the same security standards.
- As outlined in the Annex 9 to the Chicago Convention, each individual must hold their own unique passport or travel document. This principle eliminates family or group passports, ensuring enhanced identity verification and accountability at all stages of document use.
- ICAO suggests that applicants for identity and travel documents should be physically present at the application office to improve the integrity of the issuance process. This allows for direct verification of the applicant's identity through biometrics, and document checks, thereby reducing the risk of identity fraud, including morphing attacks.



Part 7.

Processes – Civil Registration and Civil Records Updates

Civil registration is a critical function of State governance, responsible for recording vital events such as births, deaths, marriages, divorces, annulments, judicial separations, adoptions, legitimations, and the recognition of children born out of wedlock. These processes serve as the foundation for legal identity and ensure individuals' recognition before the law.

Civil registration encompasses the entire administrative, legal, and institutional framework supporting these actions. This includes the personnel, registration network, procedures, record-keeping systems, issuance of certificates, preparation of outputs, data transfer, service provision to other agencies, and all related activities. These functions are typically conducted by a State-run public institution and consulates that upholds both general and individual interests. Civil registrars at consulates gather, screen, document, file, safekeep, correct, update, and certify vital events, thereby providing permanent, official records that establish identity and family circumstances.

Traditionally, civil registration forms have been a key source of vital statistics. These forms often consist of two parts: one capturing legal information and another for statistical data. Governments rely on these data for planning and delivering services, as well as ensuring access to rights. Consequently, civil registration and vital statistics are integral components of a unified CRVS system. The collection and analysis of vital statistics derived from civil registration systems support policymaking and resource allocation, helping States to monitor health, demographic trends and service needs effectively.

In many contexts, the purpose of civil registration has evolved beyond generating vital statistics to serve as a foundational mechanism for conferring legal identity. Advances in information and communication technologies have created opportunities for digital data sharing across government agencies, increasing the demand for accurate and up-to-date identity data. Where implemented, this integration can support timely service delivery and equitable access to rights, enabling governments to respond more effectively to the needs of their populations. However, many Member States are still working to strengthen their civil registration systems to fully achieve these objectives.

Historically, systems processing personal identity data – such as national identification systems, voter registers, tax registers, and social welfare databases – have often operated independently. In some contexts, digitization and data interoperability have enabled these systems to function as elements of a cohesive national legal identity system. Even within such systems, each component remains distinct, governed by its regulatory framework for data collection and processing. For Member States pursuing greater integration, data sharing across components must be carefully regulated, with robust safeguards in place to ensure privacy, compliance with relevant laws, and the maintenance of public trust.

At the national level, the CRVS system is a key pillar of the legal identity ecosystem, providing the most current identity data for use by other systems. Its integration with other components enhances its role as a key indicator of the overall strength of the legal identity framework. CRVS systems not only serve to document vital events but also establish the civil status of individuals, thereby determining their capacity to act within the legal system of a country. Consular offices play a crucial role in extending these functions to citizens abroad, ensuring their vital events are registered and recognized in line with national regulations.

Core Principles of Civil Registration

Civil registration operates on four key principles: continuity, permanence, compulsion, and universality. These principles ensure the reliability, inclusivity and functionality of civil registration systems and support their role as the foundation of legal identity systems.

Continuity and permanence

Civil registration records are permanent and must be maintained indefinitely. This permanence is achieved through stable institutions mandated by civil registration laws, which guarantee the sustainability and reliability of the system over time. Continuity ensures that civil registration records are not only created but

also preserved and updated as needed, providing a reliable source of evidence for identity and civil status across generations.

For example, a birth record created today must remain accessible for decades to support an individual's access to services such as education, employment, health care, and inheritance. The ability to maintain such continuity and permanence depends on strong institutional capacity, appropriate funding, and adherence to legal and administrative frameworks that prioritize long-term record preservation.

Compulsion

The principle of compulsion ensures that the registration of all vital events, such as births, deaths, and marriages, is mandated by law. Compulsory registration guarantees that vital events are systematically recorded, creating a comprehensive and accurate source of information for the State to monitor demographic trends and plan service delivery.

This mandatory aspect underpins the reliability of civil registration systems. Without compulsion, individuals might opt out of registration processes due to lack of awareness, access barriers, or sociocultural factors, which could lead to gaps in data and services. Ensuring compliance often requires targeted outreach and awareness campaigns to educate communities on the importance of registering vital events.

Universality

Civil registration systems must cover all individuals, regardless of their race, religion, gender, nationality, or other characteristics. This principle aligns with international frameworks, particularly international human rights, which emphasize equity and non-discrimination. Universal coverage ensures that all individuals are included in the civil registration system, fostering access to rights and services for the entire population.

Universal coverage is essential for ensuring inclusivity in public service delivery and protecting individuals' rights. For instance, the absence of a birth certificate can deny a child access to education, health care, and social protections. By including marginalized and vulnerable groups – such as stateless persons, refugees, and individuals living in remote areas – civil registration systems strengthen equity and promote the principle of non-discrimination.

Confidentiality, Accuracy and Timeliness

Confidentiality is essential for trust in the registration process. This requires strict adherence to rules and regulations, professional ethics, competent civil registrars, and effective archiving practices. Safeguarding the personal information collected through civil registration systems builds public confidence and ensures compliance with data protection principles.

Timeliness and accuracy are equally critical. Accurate records of age, sex, parentage, and nationality have profound implications for individuals' rights and obligations. Delays in registration can result in errors or failure to register vital events, undermining the system's reliability and impact. Timely registration ensures that individuals can access services, benefits, and protections associated with their legal status without unnecessary barriers.

Elements of the Vital Events Registration Process

The registration of vital events, such as births or deaths, typically follows a similar business process model:

- Notification of the event
- Declaration of the event by a relevant informant
- Formal registration and issuance of the registration certificate

Other vital events, such as adoption, marriage, and divorce, may involve different business process models. For example, the registration of divorce often includes judicial authorities or other agencies, reflecting the legal complexity of these events, including the change of names (e.g. change of the first name, change of surname upon marriage).

The United Nations Statistics Department (UNSD) provides a detailed overview of recommended practices on the registration of all vital events in its Handbook on Civil Registration and Vital Statistics Systems. Comprehensive CRVS improvement strategies can also be found in documents developed by key international organizations such as in the following documents and their publishers:

- United Nations Department for Economic and Social Affairs (UN DESA) - Guidelines on the Legislative Framework for Civil Registration, Vital Statistics and Identity Management
- United Nations Development Programme (UNDP) - Through their Legal Identity Agenda
- The United Nations Children's Fund (UNICEF) - The Right Start in Life: Global levels and trends in birth registration, 2024 update
- World Health Organization (WHO) - Civil Registration and Vital Statistics
- Vital Strategies - Vital Stories: Making Every Person Count, which incorporates 2 toolkits to improve CRVS Strategies
- Inter-American Development Bank (IDB) - Toward Universal Birth Registration: A Systemic Approach to the Application of ICT
- World Bank (WB) - Incentives for Improving Birth Registration Coverage: A Review of the Literature

These documents collectively offer a roadmap for developing robust CRVS systems, ensuring the rights of individuals to be registered and to have their vital events recognized, which in turn promotes their access to services, such as health care, education, and social protection.

Notification of vital event

The notification process begins when an individual or institution legally mandated to inform the registrar reports the occurrence of a vital event, such as a birth or death. This notification triggers the creation of an official legal record for the event.

In many cases, health institutions such as hospitals and clinics, or professional birth attendants, act as notifiers. In some cultural contexts, local government officials, such as village chiefs, may also fulfil this

role. Clearly defining and legally designating the notifier's role is essential to ensure consistent and timely registration, contributing to the accuracy and reliability of civil registration systems.

Declaration of birth by the informant and evidence required

Civil registrars can legally register vital events only upon receiving a verbal or written declaration from a designated informant. The informant is the individual legally responsible for reporting the event to the local registrar, along with information about the persons involved and the characteristics of the event.

According to UNSD recommendations, appropriate informants for a live birth include:

1. The head of the institution (or designee) where the birth occurred, if in a health facility.
2. The mother of the child.
3. The father of the child.
4. The attendant at the delivery.
5. The nearest relative of the mother.
6. Any other adult person with knowledge of the facts may record the birth details independently using mobile phones or other means for date, time, location and witness testimonies.

Most countries designate one or both parents as the legal informants for live births, though some prioritize health staff in accordance with UNSD guidelines.

Informants must present proof of identity through documentation or witnesses. In most cases, the vital event is reported where it occurred. In some jurisdictions, however, registration may take place at the informant's usual place of residence. The informant's declaration must be accurate and is often supplemented by documentary evidence, such as a medical certificate of birth from a hospital or midwife.

Where documentary evidence is unavailable, countries should implement special procedures to accommodate these cases within a defined time frame. Alternative proofs of identity may include affidavits or community attestations. If registration is delayed beyond the legally prescribed period (ranging from a few days to a year), a different procedure – often requiring a court decision – may apply. In instances where large segments of the population lack access to registration, special legislation and mass enrolment initiatives can address these gaps.

Registration of Birth

Every child has a right to birth registration, to a name, and to acquire a nationality. These rights apply equally to all children, including those born to migrant parents, regardless of their migration status. While birth registration alone does not prevent statelessness, it provides essential proof of birthplace and parentage which are key factors in determining nationality under national laws.

Once an informant declares a birth, the registrar records the event in the birth register. The entry is reviewed and signed by both the registrar and the informant. For security purposes, it is recommended to create and store a duplicate record in a separate location under the custody of the registration authority.

A birth registration record should include the following minimum information:

- The child's name at birth.
- The child's sex.
- The child's date and place of birth.
- The names and addresses of the parents.
- The citizenship of the parents.

This information is critical for the legal and administrative purposes of birth registration.

Issuance of Birth Certificates

When a birth registration record has been created, the registrar may issue a birth certificate. A birth certificate serves as a certified extract from the birth register and is an essential document that legally proves the registration of a birth. It is a critical component of civil registration systems, supporting individuals' access to services, fulfilling legal obligations and asserting rights.

The UNSD Handbook on Civil Registration and Vital Statistics Systems emphasizes that a birth certificate must contain accurate and legally valid information to fulfill its purpose. While the specific design and security features of birth certificates vary across countries, international best practices recommend incorporating security elements to prevent forgery and ensure authenticity.

Unlike travel and identity documents, which are governed by ICAO Doc 9303 standards, there are no international standards for the design or security features of birth certificates. However, countries are encouraged to adopt secure design principles to ensure that these documents are tamper-resistant and widely recognized for legal and administrative purposes.

Security features of birth certificates

To safeguard the integrity of vital records, birth certificates should include features that deter forgery and ensure authenticity. Security features such as secure substrates (e.g. watermarked paper), specialized printing techniques, and unique identifiers (e.g. serial numbers) are widely recommended by experts and international organizations. These features align with global best practices in document security and are particularly important in preventing identity fraud.

While organizations like INTERPOL provide general guidance on secure document issuance, their specific recommendations often pertain to travel and identity documents, such as passports. However, the principles of secure document design can be applied to civil registration documents, including birth certificates, to enhance their reliability and credibility.

It is also essential for civil registries to store vital records securely and ensure they are readily available for verification purposes. Robust physical and digital storage systems should protect against unauthorized access, tampering, or loss.

Key elements of birth certificates

To ensure their validity, security, and recognition domestically and internationally, birth certificates should include the following elements

1. Child's information: full name, date of birth, place of birth;
2. Parent(s) or guardian's information: full names, nationality, place of residence;

3. Official registration information: registration number, date of registration, registrar details, seal or stamp to validate the document;
4. Security features: watermarks, holograms, barcodes or QR codes.

Use Case: Issuance of Birth Certificates in the United Kingdom

In the United Kingdom, birth certificates serve as a proof of identity and are vital for accessing services and fulfilling legal requirements, such as obtaining a passport or enrolling in school.

The registration of all births in England, Wales and Northern Ireland should be carried out within 42 days of the child's birth. This can be completed at a local registry office in the district where the birth occurred or at another registry office elsewhere in the country. During the registration process, the registrar collects key details about the child, including their name, date and place of birth, as well as information about the parents, such as their full names, occupations and places of birth. This information forms the official birth record, which is used to issue a birth certificate.

There are two types of birth certificate: the short version, which contains only the child's details and the full version, which also contains the parents' details. Both kinds are chargeable, and if the birth is registered in the area where it took place, available immediately, whereas if the birth is registered in another area, it's available later. All birth certificates are printed on high-grade paper that includes security features such as watermarks, typically a crown with the letters "G.R.O." (General Register Office), which become visible when held up to light.

The United Kingdom's registration system is designed to ensure universal coverage and includes mechanisms to support individuals who may face challenges in registering births. Assistance is available for individuals with language or literacy barriers, and provisions exist for late registration to accommodate those unable to meet the initial deadline. Specific measures are in place to assist migrant families and those experiencing unstable housing conditions, ensuring that no child is excluded from the system.

Source: www.gov.uk/government/publications/birth-registration/birth-registration#about-birth-registration.

Keeping of Registration Records

Civil registration systems vary widely across States, with models tailored to administrative procedures, legal frameworks, and technological capacities. These systems consider several factors, including the division of responsibilities between central and local administration, the level of data decentralization, methods of data communication and storage formats.

Book register

A book register is a traditional system used to document vital events such as births, deaths and marriages. It comprises preprinted, blank forms bound together into a physical book, where registrars manually enter official records. These entries are typically made in chronological order based on the date of the event or are updated with new information as necessary. While many countries are transitioning to digital registration

systems, book registers remain in use, particularly in regions where digital infrastructure is not yet fully implemented.

In this system, each type of vital event – such as a birth, death, or marriage – is recorded in a separate book. This categorization ensures information is well-organized and accessible. A well-maintained book register should meet the following criteria:

- Entries must be written neatly, preferably in ink, to prevent alterations.
- Records should include all relevant details, such as the names of the individuals involved, the dates of the events, and specific registration numbers or references.
- Registers must be securely stored to prevent tampering, unauthorized access, or physical damage.

Although book registers are considered traditional, they are valued for their reliability and tangibility, particularly in jurisdictions where paper-based records remain the primary tool for maintaining a civil registry. Historically, these systems have used a two-book approach, with one book retained locally and the other sent annually to the central register. However, compliance with this practice has not always been consistent.

In addition to bound registers, some countries have used alternative formats, such as loose-leaf or card-based registers. Despite increasing efforts toward digitization, these manual systems continue to play a crucial role in ensuring the accurate and legal documentation of vital events in certain contexts.

Digitization of Registration Records

Digitization is the process of changing from analogue to digital form, also known as digital enablement.[19] The digitization of registration records involves transitioning from traditional paper-based systems to computerized registers, where records are stored in digital formats. A key principle in designing digital databases is that each record is entered only once, even if accessed or used across multiple programmes or services.

In some countries, digitization is implemented at the local registry level. Registration records are stored as electronic databases, often mirroring the structure of traditional paper-based registration books and cards. For each type of vital life event (e.g. birth, death, marriage), there is typically a corresponding digital "book" that forms part of a unified local database. Some States are further upgrading local databases to integrate them into single networks, enabling secure data sharing in compliance with national data protection frameworks. This networked system allows for querying registration information across multiple local databases to verify civil registration records. However, such systems may have limitations when conducting nationwide queries or preventing duplicate registrations.

Other countries have taken digitization further by developing centralized databases that aggregate all vital life events registered at the local level. In well-connected environments with reliable internet or national infrastructure, local offices may input data directly into a central database via computer terminals. Access to the database is often permission-based, ensuring compliance with privacy and data security requirements.

While there is no single universal standard for digitizing registration records, best practices have emerged to guide implementation:

- File format standards: Use non-proprietary, open file formats such as TIFF or PDF/A for long-term preservation. These formats are designed to maintain the quality and integrity of digital records over time, ensuring compatibility with future systems and technologies.
- Metadata standards: Adopting internationally recognized metadata standards, such as those from the International Organization for Standardization (ISO), facilitates consistent record structuring, retrieval and management. Metadata

19 www.gartner.com/en/information-technology/glossary/digitization.

ensures that critical contextual details about the records, such as creation date, source and version history, are retained.

- Data security: Implement robust data security protocols, including encryption, secure access controls, and regular vulnerability assessments, to protect sensitive information. Compliance with national and international data protection laws, such as the GDPR where applicable, is essential to safeguard privacy.
- Quality assurance: Establish quality control mechanisms throughout the digitization process to verify that digital records accurately reflect the original documents. This includes regular checks for scanning resolution, legibility, and completeness of data.
- Long-term preservation: Develop comprehensive strategies for preserving digital records over time, including routine system updates, data migration to new platforms, and the use of reliable backup solutions stored in geographically diverse locations to prevent loss due to technical failures or disasters.
- Interoperability: Design systems that enable seamless data sharing and integration across platforms and government departments, while adhering to established data-sharing agreements and privacy frameworks. Interoperable systems enhance functionality and reduce duplication of efforts.

Digitalization of civil registration processes

Digitalization is transforming CRVS systems by enabling modern, efficient, and secure processes. For consular services, these advancements provide opportunities to better serve nationals abroad and enhance coordination with in-country civil registration authorities.

Digitization refers to converting traditional paper-based records into digital formats, creating electronic databases that mirror existing registration books or cards. This process improves record-keeping, retrieval and integration with other systems. For example, digital databases can enable real-time data sharing across local and central registration offices.

Digitalization goes beyond digitization by leveraging digital technologies to reform business models, streamline operations, and improve public service delivery. In civil registration, digitalization facilitates interoperability between systems, enables remote registration and supports data-sharing under appropriate legal and security frameworks. The United Nations Department of Economic and Social Affairs (UN DESA) *Principles and Recommendations for a Vital Statistics System* emphasize that new technologies significantly enhance CRVS systems by improving efficiency, data quality, and service delivery.

Consular offices play a critical role in ensuring nationals living abroad have access to civil registration services. Digital solutions enhance the efficiency and accuracy of consular operations by:

- Allowing real-time registration of vital events through secure online platforms that connect to national civil registration systems.
- Reducing processing times for issuing documents such as birth, death, and marriage certificates.
- Providing robust mechanisms for verifying identity and preventing fraud, using secure access controls and encryption.
- For instance, integration between consular platforms and centralized civil registration systems ensures seamless updates and immediate access to accurate data. This eliminates the need for physical transfers of records and reduces errors caused by manual data entry.

Integration between consular platforms and centralized civil registration systems ensures seamless updates and immediate access to accurate data. Such integration aligns with best practices highlighted in the *Africa Programme on Accelerated Improvement of Civil Registration and Vital Statistics* (APAI-CRVS) Digitization Guidebook, which provides step-by-step guidance for planning, designing and implementing digitalized civil registration and vital statistics systems. Although originally developed for Africa, the guidebook's principles offer universal insights for maximizing investment returns, extending registration coverage and securely storing data at scale.

To maximize the benefits of digitalization, consular offices should implement systems that integrate seamlessly with national CRVS frameworks and other government databases. This integration must be achieved while safeguarding data privacy to ensure trust and compliance with relevant laws. Robust data security protocols, including encryption and access controls, should be established to protect sensitive personal information from unauthorized access and breaches.

Digital tools should be designed with a user-centred approach, prioritizing accessibility, inclusivity, and ease of use. This ensures that individuals in vulnerable positions can effectively interact with the systems and benefit from the services offered. Consular staff must receive comprehensive training on the use of these digital systems, as well as on best practices for data protection and management, to ensure consistent and effective implementation.

Additionally, public awareness campaigns are essential to educate communities on the advantages of digitalized registration systems. By fostering understanding and trust, these efforts promote widespread adoption and engagement with the digitalized processes, ultimately strengthening the overall effectiveness and reach of civil registration services.

Finally, digitalizing national identity databases requires ensuring backward and forward compatibility. Backward compatibility keeps legacy systems and old documents operational during the transition, reducing disruptions. Forward compatibility allows the digital infrastructure to adapt to future technologies and standards. These measures create resilient systems, support interoperability, prevent redundancy and provide a seamless user experience.

Country examples of the digitalization of registries

In Namibia the Government has implemented a fully integrated civil registration and identity management system through the National Population Registration System (NPRS). This system centralizes the processing of vital events and integrates various identity-related data sources, improving both the accuracy and accessibility of records. Births and deaths are registered through e-birth and e-death notification platforms at health facilities, which are directly linked to the NPRS. This digitization not only makes the registration process faster but also enables better data sharing between government departments.

Similarly, Pakistan has made strides in digitizing birth registration with its Digital Birth Registration project. This initiative uses mobile technology to register births in remote areas, eliminating the need for travel and reducing administrative costs. The system securely transmits birth data in real-time to the National Database and Registration Authority (NADRA), ensuring that birth certificates are issued locally at the Union Councils. This approach improves birth registration rates, especially in under-registered regions and integrates with health systems for follow-up notifications, such as immunization updates.

Population register

A population register is a centralized, State-administered database that maintains comprehensive and continuously updated records of all residents within a country. It serves as a foundational tool for modern public administration, enabling governments to efficiently manage identity information and deliver public services. Unlike systems that store fragmented data across multiple agencies, a population register consolidates information into a single, authoritative source.

Typically, a population register contains key personal details such as name, date of birth, sex, residential address, family composition, and legal status. Different government authorities, such as civil registration offices, immigration agencies, and tax administrations, contribute data based on their legal mandates. This integrated approach ensures consistency, reduces duplication, and facilitates real-time updates.

By centralizing identity data, a population register enhances governance and public administration in several ways. It enables public services to operate more effectively, ensures accurate planning and resource allocation, and improves access to essential services like health care, education and social welfare. Furthermore, it supports electoral processes, taxation, and national security efforts by providing accurate, up-to-date population data.

The implementation of a population register requires a well-structured and secure database system that allows interoperability across public institutions. Ensuring adherence to international standards and best practices – such as robust data protection measures and privacy safeguards – is critical to building trust and ensuring the effective operation of the system.

To achieve this, international standards and best practices can guide the design and operation of population registers. One of the most widely recognized frameworks is the International Organization for Standardization (ISO) 2108 on metadata for population data, which establishes best practices for organizing and managing data entries. Another key international standard is ISO/IEC 27001, which outlines information

security management systems, ensuring that the personal data in the population register is protected from unauthorized access and breaches.

Best practices in public administration often involve creating interoperable databases that facilitate seamless data exchange between government entities

Estonia is renowned for its advanced digital identity infrastructure, which forms the backbone of its e-Residency system.[20] This system ensures that all citizens are registered and can access services securely and efficiently. Through real-time data sharing between public and private sectors, Estonian citizens enjoy streamlined access to services, with their data automatically updated across various government departments. This level of interoperability eliminates redundancy and enhances efficiency, making Estonia a global leader in digital governance.

In Norway, the National Population Register, managed by the Norwegian Tax Administration,[21] demonstrates how integrated data systems can simplify public service delivery. Citizens can access services such as health care, taxation and voting without repeatedly entering their personal information. The system operates under strong legal frameworks that prioritize data privacy and ensure accuracy.

Chile offers another example with its Unified National Register, which consolidates civil registry data with information from tax, health, and electoral databases. This system improves service delivery by ensuring consistency across public records. At the same time, Chile's commitment to strict compliance with national privacy laws guarantees the protection of personal information. This balance between integration and privacy reflects a thoughtful approach to managing public data.

Enablers for Civil Registration System Strengthening

A rights-based approach to strengthening civil registration systems includes recognizing the critical role consular services play in ensuring the registration of vital events for nationals living abroad. Consular offices act as key access points, especially for individuals in vulnerable situations, enabling them to obtain legal identity documents and exercise their rights.

Consular offices should address cultural norms and sensitivities that may affect registration uptake, such as differing views on traditional versus civil marriages or the perceived necessity of registering births and deaths. Tailored public awareness campaigns by consular authorities can promote the importance of civil registration while ensuring the process is inclusive, accessible, and free from discrimination.

Legal provisions should empower consular offices to register vital events and issue documents with the same authority as in-country civil registration offices. Clear policies should ensure cost-free or affordable services, particularly for the first issuance of vital certificates, while adhering to principles of non-discrimination, inclusivity and privacy protection. Digital solutions can improve efficiency, allowing consular offices to connect seamlessly with national civil registration systems while maintaining robust data security safeguards.

20 www.e-resident.gov.ee/.
21 www.skatteetaten.no/en/person/.

A well-coordinated system is essential for consular offices to contribute effectively to civil registration. This includes centralized oversight by the civil registration authority, capacity-building for consular staff, and clear workflows to handle registrations promptly and accurately. Consular offices must also collaborate with relevant ministries and stakeholders to ensure consistency and accountability in registration processes.

To enhance the role of consular offices, interoperability between civil registration systems and consular platforms is essential. Digitized processes allow consular staff to register vital events in real time, linking directly to the central civil registry while upholding strict data protection standards. This ensures records are accurate and integrated, supporting individuals' access to legal identity regardless of location.

Part 8.

Consular Protection and Assistance in Challenging Circumstances or Special Situations such as an Emergency or Crisis

Migrants are confronted with a myriad of challenges and vulnerabilities, such as a foreign language and culture, barriers to accessing individual documentation, unfamiliarity with the legal system, fear of deportation, discrimination and exploitation – in some cases on account of their irregular or undocumented status. These obstacles have serious consequences, and it is critical for the international community to cooperate in facilitating access to consular assistance for migrants who find themselves in challenging circumstances, including proof of legal identity, nationality and the provision of documents. For example, migrants in vulnerable situations wanting to return to their country of origin, may need replacement or issuance of identity, nationality and travel documents. Also, in cases of emergencies, such as natural or human-made disasters, consular assistance can ensure protection and safe evacuation including help in obtaining necessary documents.

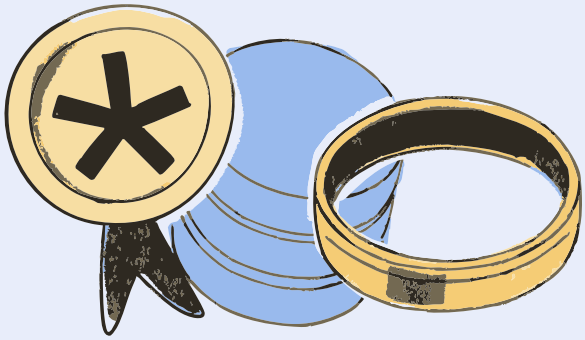
Preventing Statelessness

Statelessness can be both the cause for and a consequence of migration. Conflicts in nationality laws, discrimination in the application of laws to migrants, lack of access to identity documents and barriers to birth registration are frequent catalysts of statelessness that become harder to resolve in migratory contexts, and increasingly so with every generation of undocumented migrants and their descendants.

Although access to rights and services should not be conditioned on possession of documentary evidence of nationality, such documentation remains a practical prerequisite for accessing economic, social and cultural rights. Stateless and at-risk migrants face increased vulnerabilities and are often subject to oppression.

Consular measures to prevent statelessness should focus on:

- Locating migrants' birth certificates.
- Ensuring the issuance of late birth certificates to migrants whose births were not registered in their birthplace, whether in the country of nationality or a third country. (*Note:* Issuing late birth certificates at consular level may require legal or policy reforms in the frameworks governing civil status documentation in the country of origin.)
- Issuing other documents of identification, such as nationality certificates, national ID cards, or passports.
- Coordinating with local authorities to locate families of unaccompanied children.
- Facilitating the registration of births at the consulate for children born in the country of destination, particularly when migrant parents are unable to register the birth in the host State's civil registry due to documentation or legal barriers.
- Advocate for policies that allow dual or multiple citizenships to prevent statelessness caused by renouncing nationality for naturalization in another country.



Birth registration by Consulates in Libya

In Libya, the issuance of birth certificates to the children of migrants and foreign nationals poses unique challenges due to Libyan legal restrictions. Under Libyan law, only Libyan authorities can issue official birth certificates, which are generally limited to Libyan citizens. This leaves migrant children, including those born in Libya to foreign nationals or undocumented parents, at risk of remaining without official identity documentation. To address this gap, embassies of various countries operating in Libya have stepped in to issue birth certificates or similar documents to their nationals born in the country.

Embassies typically rely on documentation provided by parents, such as proof of nationality or identity documents, to confirm the child's eligibility for registration. Where such documentation is incomplete or unavailable, embassies often conduct interviews and request affidavits or other forms of evidence to verify the parents' identity and nationality. In some cases, consular officials collaborate with local hospitals or care facilities to obtain birth records or medical documents as supporting evidence for registration.

Despite these efforts, the lack of a unified legal framework or formal agreement between Libyan authorities and foreign embassies complicates the process. To mitigate this, some embassies adopt creative solutions, such as issuing consular birth certificates or emergency documentation that can later be formalized in the home country. These measures not only provide a degree of legal recognition but also safeguard the child's access to services and rights linked to citizenship. This practice underscores the critical role of consular services in bridging gaps left by local legal constraints, ensuring that children are not left stateless or without identity.

Assistance in the Event of Emergency or Crisis Abroad[22]

Consular assistance becomes a lifeline for migrants stranded or in distress during emergencies or crises, including armed conflicts, natural disasters, political upheaval, or health emergencies. Services provided during such events include locating missing family members, issuing travel documents on an emergency basis to facilitate safe departure, and offering protection for victims of trafficking or other crimes to ensure access to justice. During the COVID-19 pandemic, for example, restrictive border management measures heightened vulnerabilities, particularly for migrants with regular temporary status who faced risks of falling into irregularity due to cancelled flights and border closures. Countries that adopted flexible procedures, such as extending visas or establishing bilateral agreements, helped mitigate these impacts, demonstrating the critical importance of consular flexibility and preparedness.

The pandemic also underscored the need for consular services to remain operational and adaptable during crises. Remote consular services emerged as a vital tool to ensure continuity, even when physical access to consular offices was limited. However, the digital divide posed challenges, particularly for migrants in remote or resource-poor areas who lacked access to internet or digital tools. Creative solutions, such as expanding communication methods to include hotlines, SMS platforms, and community networks, proved effective in disseminating accurate information and providing necessary assistance to migrant and refugee communities.

22 https://migrationnetwork.un.org/system/files/resources_files/iml_consular_assistance1.pdf.

Emergencies often disrupt migrants' access to identification, verification and documentation, creating significant barriers to receiving consular support. Many migrants lose their documents due to destruction, loss, or lack of prior issuance, which can leave them undocumented and vulnerable. These challenges are exacerbated in crisis settings by the destruction of local civil registration records, restricted access to secure databases, and widespread misinformation. Communication barriers, including language differences and disrupted infrastructure, further hinder migrants' ability to contact consular offices or access timely support. During crises, consular offices often experience a surge in demand, which can overwhelm their staffing and logistical capacities. To address these challenges effectively, consular operations must rely on pre-established agreements with host governments, enabling streamlined processes for tasks such as visa issuance, safe passage, and evacuation. Contingency plans should include training consular staff in crisis management and ensuring their safety in high-risk or conflict-affected areas.

Effective consular services during emergencies must prioritize accessibility, ensuring that all nationals, regardless of their location or circumstance, can receive support. Rapid responses are crucial for addressing urgent needs such as evacuations or the issuance of emergency travel documents. Collaboration with local authorities, international organizations, and other diplomatic missions is essential to optimize assistance and prevent duplication of efforts. Clear and timely communication with affected citizens and their families helps build trust and ensures that individuals can make informed decisions. Inclusive services must consider the needs of vulnerable populations, including children, the elderly, individuals with disabilities, and those without prior identification. Furthermore, it is essential to emphasize the need for trauma-informed and culturally sensitive practices, especially when working with victims of trafficking in persons and gender-based violence. These individuals often face significant emotional and psychological trauma, and it is crucial that services and support are tailored to their specific needs.

Innovative approaches can address many challenges associated with identification, documentation, and outreach during crises. For example, biometric systems, such as portable facial recognition and fingerprint technologies, enable consulates to verify identities on-site, even in remote or conflict-affected areas. These systems are particularly valuable when traditional identity documents are unavailable or destroyed. Secure and interoperable channels for accessing national civil registration databases facilitate real-time verification, reducing delays and enhancing the accuracy of assistance. When conventional identification methods are not feasible, alternative solutions such as sworn affidavits, community attestations, or temporary identification documents can help bridge the gap. For instance, during the conflict in Libya, the Philippines effectively used mobile registration kits to identify and repatriate its nationals, demonstrating the utility of such tools in crisis contexts.

Emergency travel documents are a cornerstone of consular assistance during crises. To ensure their effectiveness, these documents must incorporate security features such as QR codes, which allow authorities to quickly authenticate traveller information and maintain the integrity of the documents. Pre-prepared digital templates or pre-printed forms can expedite the issuance process, ensuring that support is delivered promptly. Communication strategies tailored to the affected population are equally critical. Dedicated crisis hotlines, mobile applications and SMS platforms provide timely updates and ensure that individuals can access accurate information about available services and next steps.

Maintaining civil registration and vital statistics systems during emergencies is equally critical. Civil registration establishes an individual's legal identity, which is essential for accessing health care, humanitarian assistance and other social services. During crises, such as the COVID-19 pandemic, these systems must be recognized as essential services and maintained to the greatest extent possible. Governments should adapt registration processes to accommodate the unique challenges of crises, such as enabling remote or staggered operations, expanding eligibility for notifying registrars, and waiving certain documentation requirements.

The resilience of CRVS systems in emergencies and their preparedness to manage such circumstances depend on the nature and scale of the crisis, as well as the strength and capacity of the existing system, including its human resources. This varies depending on whether the system operates offline, is paper-based or online, the size and composition of the affected population, and the regulatory requirements for registration processes. Although some physical offices may need to close or limit their hours, operations

should continue as far as possible through in-person or virtual means. Priority should be given to the registration of births and deaths, while other registrations may be temporarily deferred with recovery plans clearly established to address backlogs.

Adaptations should be tailored to fit the unique circumstances in countries of destination whilst maintaining privacy and confidentiality as primary principles, with the following considerations:

- Prepare a comprehensive guidance note to support the continuity of services, developed in collaboration and consultation with governmental authorities and other key stakeholders. This document should outline strategies for maintaining registration processes during crises and include enhanced public outreach efforts that are clear, concise, and specifically targeted at vulnerable populations to ensure they are informed of available services.
- Adjust registration procedures to expand the range of individuals eligible to notify registrars, particularly in situations where health facilities are inaccessible. For example, enabling community health workers or local leaders to notify registrars can help ensure continuity in registering vital events like births and deaths.
- Anticipate and plan how changes made to registration processes during the crisis will be verified and formalized after the emergency subsides. Agreements should be reached on acceptable methods for verifying records created under adjusted procedures to maintain the integrity of the registration system.
- Introduce specific waivers or simplified procedures for individuals who may lack required documentation, ensuring no one is excluded from registration services due to barriers created by the crisis. This approach promotes equitable access to services and safeguards the rights of those most affected.
- Ensure trust in the civil registration system by balancing accessibility with robust verification standards. Evidence used for registration should be sufficient to prevent duplication or inaccuracies, which could undermine the system's reliability.
- Establish processes for verifying information remotely, such as confirming health notifications with family members or health-care providers, to validate registrations when in-person confirmation is not feasible.
- Prepare for fluctuations in the number of registrations based on the nature and scale of the crisis. Allocate resources accordingly to manage potential surges or disruptions effectively, avoiding backlogs that could hinder recovery efforts.
- Enhance the use of remote and secure online platforms (e-governance) to facilitate registration processes. This includes enabling digital submission of documents and remote access to registration services, ensuring continuity even when physical offices are inaccessible.
- Foster close collaboration with police, health officials, and host governments to address operational challenges, resolve service continuity issues, and enhance the effectiveness of registration systems during crises.
- Ensure all adapted processes comply with relevant data protection and privacy laws. Special attention must be given to the risks faced by vulnerable groups, ensuring their personal information is protected and used responsibly.

IOM Support to Consular Services in Libya

In Libya, IOM is actively assisting consulates in addressing challenges related to the identification and registration of migrants, many of whom are undocumented. One significant area of support is enhancing the technological and procedural capacity of the embassies of the Sudan, Nigeria and Somalia. IOM supports the provision of biometric equipment, passport scanners and webcams, which are critical for improving the accuracy and reliability of identity verification processes, particularly in a context where many identity documents are of poor quality or non-existent. For instance, IOM's Migration Information and Data Analysis System (MIDAS) has been installed in the Burkina Faso embassy in Tripoli, offering a platform to register Burkinabe nationals residing in Libya.

Another crucial element of IOM's support involves developing guidelines for consular staff. These include recommendations for conducting interviews, applying standardized trade tests, and addressing the poor quality of photographs and identity documents submitted by applicants. Such measures ensure a more consistent approach to determining identity, particularly in crisis situations where proof of identity can be challenging.

In cases where the demand for consular services exceeds capacity, States may contract private entities to provide assistance with services such as passport, identity, or permit applications. To ensure the protection of nationals abroad, States should adopt laws and policies that prioritize consular assistance, including birth registration and document issuance. Bilateral agreements allowing other States to provide consular support where a country's own presence is limited can also strengthen service delivery. Consular officials should receive regular training on responding to the needs of migrants, particularly those in vulnerable situations, to uphold a rights-based and inclusive approach to assistance.

Case Study: Ensuring Continuity of Civil Registration Services During the COVID-19 Pandemic: Lessons from Africa

The COVID-19 pandemic significantly disrupted the registration of vital events across Africa, with many births in private homes initially going unregistered due to health concerns, while registrations at health facilities experienced delays. To address these challenges, various measures were implemented to ensure continuity of civil registration services despite the crisis.

Key measures included prioritizing the issuance of paper certificates for emergencies only, thereby reducing in-person interactions and focusing resources on critical cases. Staff were reorganized to work in shifts or remotely, minimizing contact risks while maintaining essential operations. Communication with the public was enhanced through increased use of email and social media platforms, which kept citizens informed about service availability and procedural changes. Closer collaboration with suppliers ensured the uninterrupted availability of registration materials and equipment.

In Kenya, the Nyumba Kumi Initiative (NKI), a community policing model aimed at fostering social cohesion and security, was leveraged to support reporting and registration of vital events through neighborhood networks. Community Health Workers also played a pivotal role in extending the reach of reliable recording and subsequent registration. Their efforts ensured timely submissions to government administrations, central registration authorities, and local offices, even in the most challenging circumstances.

Rwanda's Irembo platform demonstrated the effective use of online systems for certificate delivery. This web-based portal enabled citizens and health facilities to upload required documents, allowing Civil Registration Officers to issue certificates through the same system. The widespread use of smartphones, often facilitated by agents, ensured that even individuals without digital access could benefit from the platform's services.

Part 9.

Consular Challenges in Identification and Verification of Identity, Document Examination and Fraud Detection

Consular offices are tasked with a critical responsibility: ensuring the accurate verification of identities and the authenticity of documents submitted for various legal, travel, and immigration-related purposes. However, the landscape of consular operations is rife with complexities including disparities in civil registration systems, the increasing sophistication of fraudulent practices, and the need to navigate diverse cultural and legal frameworks. Document forgery, identity theft, and discrepancies in international standards for identity verification are among the most common hurdles faced by consular officers.

Identification challenges form the foundation of consular work involving establishing the true identity of an individual. Challenges in this area often arise due to incomplete or inconsistent civil registration systems in many countries. For example, individuals from rural areas or conflict zones may lack birth certificates, national IDs, or other official records, making it difficult to ascertain their identity. In such cases, consular officers must rely on alternative methods such as personal affidavits, community references, or secondary documents like school records. However, these substitutes are prone to inaccuracies and can be exploited by fraudsters. The lack of standardized international identification systems further compounds the issue, necessitating innovative approaches and tools to bridge the gaps in documentation.

In order to overcome challenges related to identification of individuals, the following recommendations should be considered.

1. Conduct comprehensive needs assessments to analyse common issues, such as lack of valid documentation or discrepancies in applicant details.
2. Leverage advanced technology including biometric systems to validate identity and reduce reliance on traditional documents, develop or access central databases to cross-reference personal information, ensuring consistency and authenticity, or enable mobile application for applicants to pre-submit identification data.
3. Employ secondary identification methods, including community verification through testimonies from recognized community leaders who can vouch for the applicant's identity, accept and validate historical records (school records, employment letters, etc.), and conduct in-depth interviews to cross-verify personal details and detect inconsistencies.
4. Establish clear procedures: develop SOPs for handling various identification scenarios, from document verification to interviews, introduce protocols for flagging high-risk cases, such as applicants with unverifiable backgrounds or discrepancies in provided information, and create mechanisms for consular staff to report challenges and suggest improvements.
5. Collaborate with protection actors, such as NGOs, UNHCR and IOM, to support consular responses during complex emergencies. This cooperation will contribute to addressing the multifaceted needs of affected individuals, ensuring a more coordinated and effective response. These partnerships can provide critical expertise, resources, and support to consular services, particularly in situations where large-scale humanitarian assistance is required.

Verification challenges

Verification involves ensuring that the identity claimed by an individual matches the documentation they provide. This process can be particularly complex when dealing with documents issued in different countries, each with its own standards, languages, and formats. The lack of a centralized global database for verifying credentials often forces consular offices to depend on local institutions for confirmation, a process that can be time-consuming and unreliable.

Moreover, technological disparities between countries exacerbate the problem. While some nations have advanced biometric databases and digitized records, others still rely on manual processes, creating inconsistencies in the verification process. Consular officers must also contend with cultural nuances that may affect how identity is perceived and documented, further complicating verification efforts.

In order to overcome challenges related to verification of identities, the following steps should be undertaken.

1. Foster cross-border collaboration through establishing agreements with other countries for sharing biometric and civil registry data, leverage resources from international agencies such as INTERPOL to verify identities and uncover fraud patterns and facilitate consular networks to identify best practices and exchange information.
2. Establish clear verification protocols, including checklists with lists of criteria for validating different document types, outline the forms of documentation acceptable for verification, including those that might require supplementary evidence.
3. Invest in advanced verification technologies, including document scanners with capabilities to detect watermarks, holograms, and other security features, biometric verification systems to match the individual's biometric data against the existing records, and access centralized or international databases to cross-check information and detect inconsistencies in real time.
4. Introduce crisis response mechanisms through setting up rapid-response protocols for urgent verification needs.
5. Address data discrepancies through in-depth interviews, requesting supplementary documents, and verifying historical records.
6. Developing fraud-resistant processes through providing staff with specialized training, implementing multi-layer verification (biometric comparison, manual inspection, and database cross-checking), and utilizing fraud detection software (AI powered tools).
7. Tailoring verification protocols to the local context by recognizing alternative documents (tribal certificates, community issued IDs, etc.), and engaging local experts to verify the accuracy.

Document fraud

Document fraud is a pervasive challenge for consular services worldwide. This includes the forgery, alteration, or misuse of documents such as passports, visas, educational certificates, and financial records. The sophistication of counterfeit operations has increased significantly, with fraudsters leveraging advanced printing technologies and digital manipulation tools to create convincing fake documents, which may facilitate the smuggling of persons.

Consular officers must be adept at detecting these forgeries, which often requires specialized training and access to high-quality forensic tools. Collaboration with issuing authorities and the use of security features such as holograms, watermarks, and microtext are critical in combating document fraud. However, fraudsters continually adapt, necessitating ongoing vigilance and technological innovation to stay ahead.

To overcome document fraud related challenges, the following actions are advised.

1. Build awareness of document fraud techniques and train consular staff in fraud detection (hands-on workshops, scenario-based learning identifying alterations, forgeries and counterfeit features).
2. Invest in advanced document authentication tools including forensic document examination equipment (UV light scanners, infrared viewers and magnifiers), digital verification tools to analyse security features of the documents.
3. Strengthen coordination with issuing authorities to ensure access to reliable information to confirm the authenticity of documents and exchange data on known fraud cases.
4. Develop policies for document handling by enabling risk-based screening for facilitating high-risk case checks and defining clear steps for escalating suspicious cases to senior officials or investigation units.

Further look into document examination and fraud detection practices will be covered in the next chapter.

Part 10.

Document Examination and Fraud Detection

IOM has developed the Passport Examination Procedure Manual, which in its 3rd version, provides a comprehensive and standardized approach on examination of travel documents. It places a particular emphasis on the importance of combatting identity fraud. By providing a comprehensive guidance on the identification of fraudulent documents, including security features and other indicators of tampering or alteration, it serves as a valuable resource. The following chapter highlights the key aspects of document examination and fraud detection, which were derived from the PEPM (Passport and Emergency Travel Document) guidance. It summarizes the essential strategies and techniques outlined for effectively identifying fraudulent documents, ensuring security, and maintaining the integrity of travel documentation processes.

Document Examination – Equipment

Magnifying glasses are helpful to identify mechanical erasures, printing and personalization techniques, microtext and the general quality of the printing.

Ultraviolet (UV) light sources can identify fluorescent security features, chemical erasure and the base fluorescence (optical brightness) of the substrate.

Compact devices are used to identify mechanical erasures, printing and personalization techniques, micro text, general print quality, OVDs, UV luminescence, biometric chips, inks with fluorescent inks or unusual qualities and retro-reflective features. **Identification Document Validation Technology (IDVT)** is widely available via apps and software interfaces to identify mechanical erasures, printing and personalization techniques, microtext and general print quality. In more advanced document examination environments such as the back office of a border control, larger scale and more sophisticated IDVT technology machinery is used as a second line of examination.

All IDVT devices consist of a way to scan the document – some use using different light sources – including readers, smartphones, webcams and scanners to capture an image of the document, and some use **Near Field Communication (NFC)** to also read chipped documents. These devices can quickly and easily assist to establish the authenticity of documents presented for identity verification purposes including passports, biometric residence permits and identity cards, which can be enhanced with offline facial matching systems, such as the PEPM 3 App. They link to software and template libraries to check security features and compare the image of the document against a template stored in the library. Algorithms are used to draw together and score them to indicate authenticity.

Different types of illumination using various types of light sources are most useful to examine secure documents and the safeguards protecting them. Transmitted light is using a regular (white) light source to shine through substrates and is useful to check for watermarks and security threads. Oblique light uses a white light source to transmit the light across a substrate to examine embossing seals and other relief features on the document. Intaglio print – as a raised feature – can be examined this way and alterations to print or damage to paper are highlighted using this method.

UV light sources show up the base fluorescence or "whiteness" of a substrate and highlight hidden features such as security fibres and OVDs. They are widely available as hand held torch like devices, or bulbs built into scanners. Infra-Red (IR) light sources are most often built into scanning equipment as one of the checks against template libraries. They check for any unauthorized changes and security safeguards built into the substrate or inks used in construction and personalization, measuring reflection or absorption against expected results.

Identifying Document Fraud

In all diagrams or photographs, a green border indicates genuine, and a red border indicates an element of fraud.

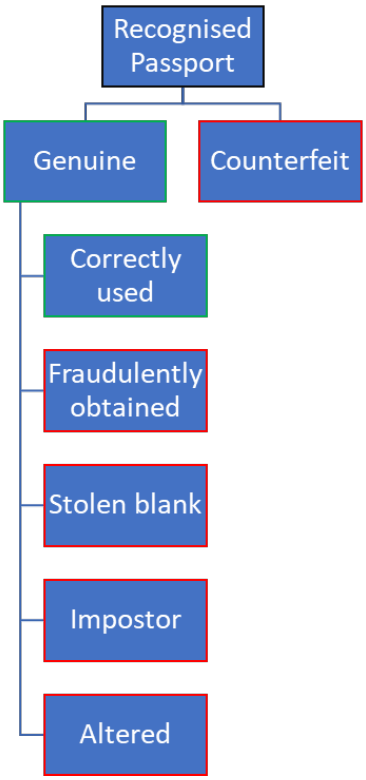
There are three basic steps to spotting fraud in an identity or travel document as a consular officer:

1. Conclude that the presenter is not an impostor (Chapter 15 of PEPM 3 can provide guidelines on this topic).
2. Check that the document presented is from a recognized State.
3. Check the document firstly with any document readers available to validate through chip security mechanisms and databases, then
4. Check the document as an examiner.

Documents looking like identity documents can be issued by bodies never recognized as States – called Fantasy Documents. They can also be issued by countries which no longer exist or have a new name – Camouflage Documents. Neither of these satisfy the requirement of establishing nationality and identity, so with countries or issuing authorities that are unfamiliar always check with on-site records, databases or online resources.

Consular staff have free and full access to the **EDISON TD** and **EU PRADO** databases. These tools offer extensive information on international identity and travel documents, aiding in the verification of questionable documents, including fantasy and camouflage passports. Regular database use enhances accurate document assessment and combats fraud. Checking documents as an examiner does not need expensive equipment; it needs examiners to learn the right skills and apply them in an effective way, in the time available. We will look at how fraudulent documents are created, and how do examine them to identify irregularities which point to evidence of fraud.

Figure 1. Passport fraud may involve the use of genuine or counterfeit documents



Source: Passport Examination Procedure Manual - third edition.

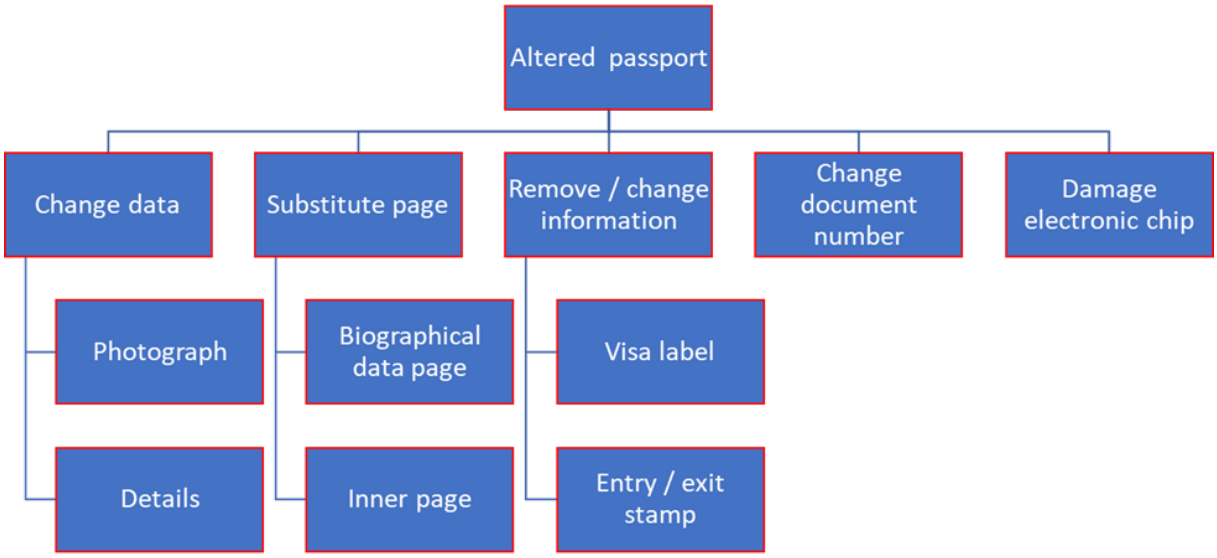
How Fraudulent Documents are Created

Passport fraud occurs in several ways. In some the original document itself is genuine, for instance if used by impostors or obtained corruptly. In these cases, fraudulent activity needs to be spotted by other means (such as facial comparison for impostors), as the document is genuine.

On occasions counterfeit passports will be presented. These are identified through not being of the expected quality of production and not containing the expected security features or the poor quality of these features. More commonly though, genuine passports will be altered, by replacing elements or changing, removing or hiding original information. The quality of altered passports ranges from extremely poor to highly professional.

There are various methods used by forgers to create counterfeit and altered documents, possibly in combination:

Figure 2. Common methods used to alter secure travel documents



Source: Passport Examination Procedure Manual - third edition.

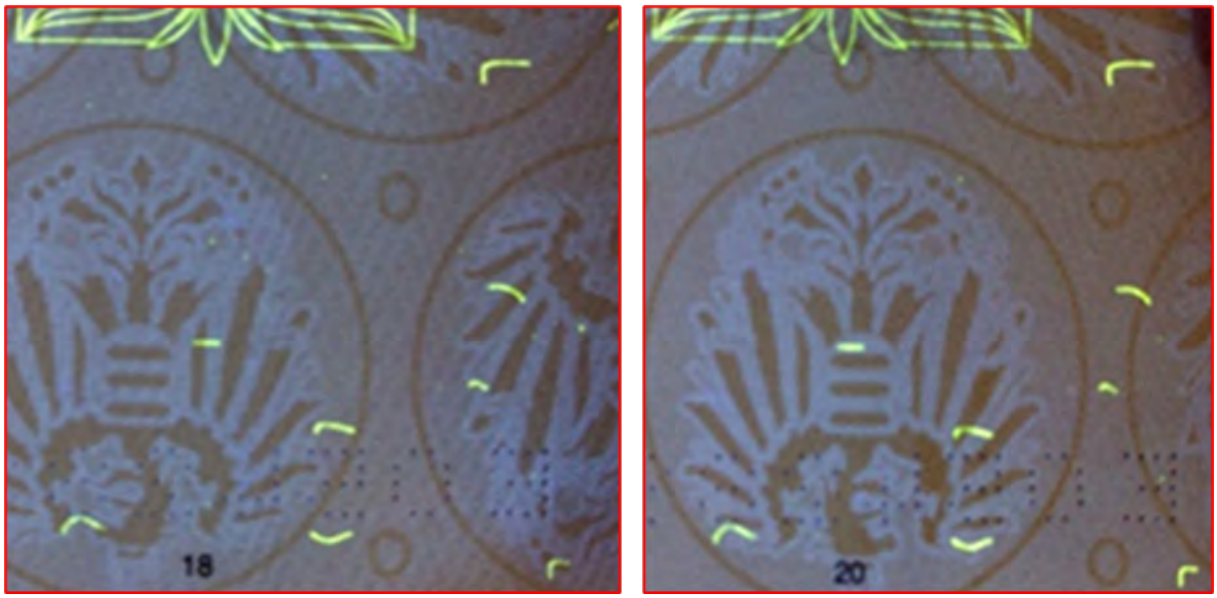
Counterfeit pages can replace any page in a passport. They are entirely fake and may have simulated (or lookalike) security features. It is common for paper security features to be printed onto counterfeit pages. In many cases, replacing a genuine page with a counterfeit page will require the passport to be disassembled (pulled apart) and reassembled (stitched or stuck back together).

To determine whether a page is counterfeit, the paper, printing, and any other safety features should be examined carefully. A counterfeit page within a passport will have differences to the genuine pages within the same passport, so it is useful to compare a suspect page with the others. Counterfeit paper is often commercially available paper, not security paper that has restricted availability. Examination under UV light will often show the counterfeit paper to be UV bright, which is not correct.

Counterfeit Pages – Security Fibres

Simulated security fibres (and planchettes) are often printed or drawn onto counterfeit paper, often in UV reactive ink. A magnified examination under visible light or UV light will show that the simulated fibres are printed on the surface of the paper. Where multiple counterfeit pages have been created, simulated fibres may appear in the same place from page to page, which is not correct. These security safeguards are created during the document manufacture process and are necessarily randomly distributed.

Figure 3. Simulated security fibres

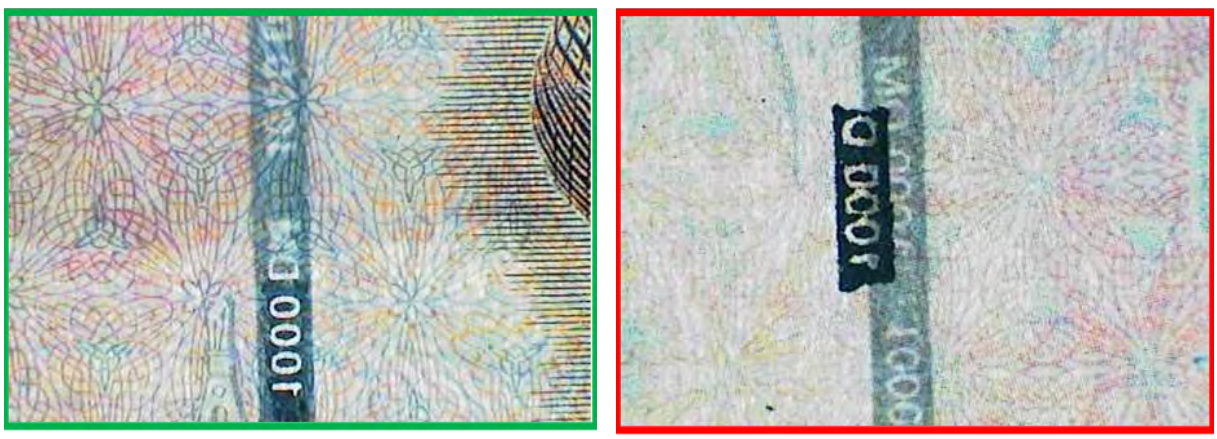


Source: Passport Examination Procedure Manual - third edition.

Counterfeit Pages – Security Threads

Simulated security threads can be printed onto counterfeit paper. The printing can be on one side of the paper, both sides of the paper, or two thin pieces of paper can be stuck together. Genuine security threads are most visible when examined with transmitted light. A simulated security thread can be more visible under normal light, and not have the correct appearance when examined with transmitted light. As security threads regularly contain microprinting and UV reactive features, these will also need to be simulated in forged examples.

Figure 4. Genuine and simulated security treads



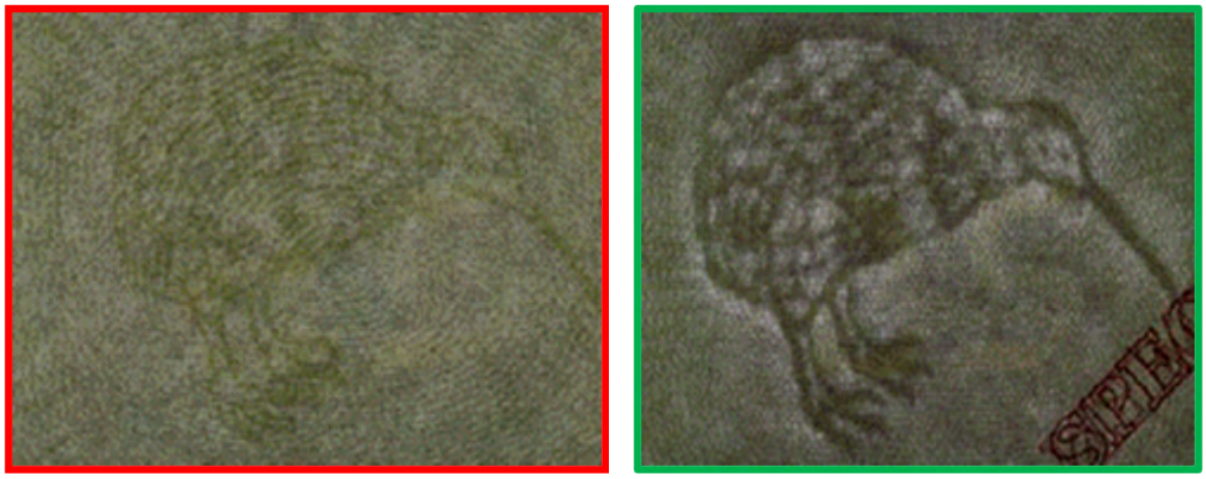
Source: Passport Examination Procedure Manual - third edition.

Counterfeit Pages – Watermarks

Genuine watermarks are very difficult to simulate, as they are introduced while the paper is being formed and cannot be inserted later. Forgers sometimes print the simulated watermark using a clear varnish on the substrate, so it is visible with transmitted light but not visible under normal light. Another method is to emboss the paper in some way, creating an uneven feature to the surface, but this is unlikely to be visible with transmitted light.

A simulated watermark can have crisp well defined edges, whereas a genuine watermark will have indistinct edges because of how it is created. UV light will not show a genuine watermark clearly, but a counterfeit watermark is often visible in UV light.

Figure 5. Simulated and genuine watermarks

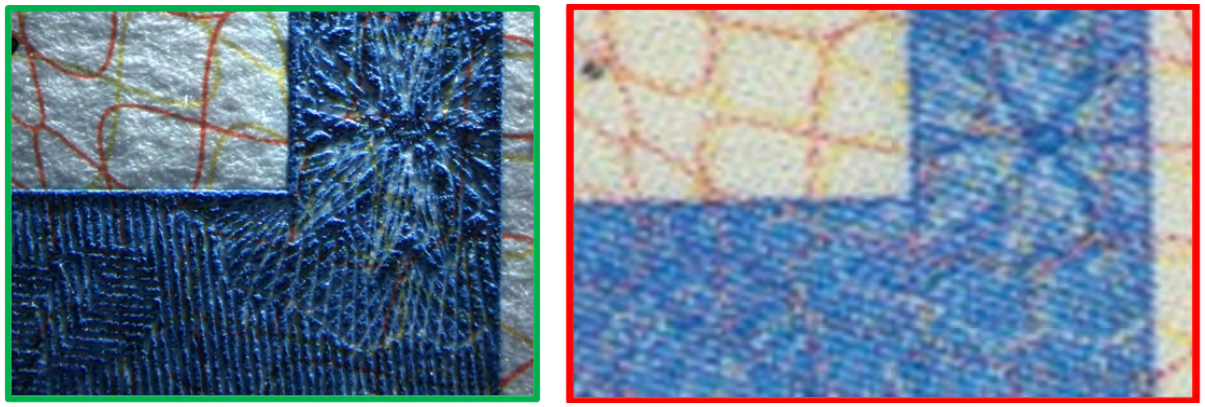


Source: Passport Examination Procedure Manual - third edition.

Counterfeit Pages – Printing

Any document can be scanned and stored as an electronic file, including passport pages. The scanned image can then be printed on any printer. When this occurs, security features will mostly be printed in a series of cyan, magenta, yellow and black dots, expected quality of the genuine printing will be lower, and any security feature (such as microprinting, OVI, OVD or latent image) will not look, feel or operate correctly.

Figure 6. Example 1 of counterfeit and genuine pages

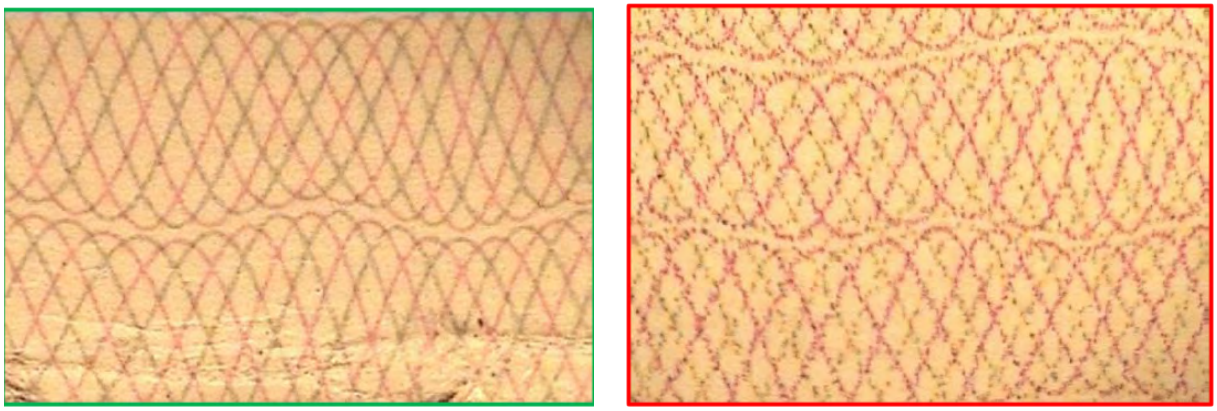


Source: Passport Examination Procedure Manual - third edition.

Where counterfeiters have access to expensive commercial equipment, they can produce better quality counterfeits. Counterfeiters often have access to commercial offset lithography printing presses to print secure document pages.

Whilst some features of a genuine passport page can be created, we can expect a lower quality of print. Closer examination will show the counterfeit to have subtle differences in ink colour and background pattern. Where text is included, layout, spelling and microprinting may show errors. Using simple magnification equipment enhances detection of these issues.

Figure 7. Example 2 of counterfeit and genuine pages



Source: Passport Examination Procedure Manual - third edition.

Where the counterfeiter attempts to simulate the raised feel of intaglio print, they may apply clear resin to the wet ink and heated to form a raised look and feel. This is called thermography, and the effect of the resin can be seen under magnification.

Intaglio ink never hardens, therefore if we will rub it against a blank white paper, it will leave marks.

Figure 8. False intaglio print: genuine intaglio (left) compared with intaglio imitated by thermography (right)

Source: Passport Examination Procedure Manual - third edition.

Counterfeit Pages – Perforations

Counterfeiters try to create holes in the page to look like genuine perforated holes. Where laser perforations are used, the counterfeiter is unlikely to have the right equipment. It is difficult to create the smooth paper surface expected, together with the gradually reducing hole size or laser burn marks. Attempts to simulate needle perforations generally result in a poorer quality result, and misalignment is an important detection point.

Page Splitting

It is possible for a passport page to be "split" into two or more thin sheets. Two separate pages may be split, with the front of one being attached to the rear of the other to make a new page. One side of the split may be counterfeit and the other may be from a genuine passport, or both sides may be from genuine passports.

When pages are split, it affects security features. Watermarks will lack definition, the paper can be wrinkled, security threads may be damaged, corners and edges misaligned.

Page Recycling

A recycled genuine page can be used to replace any other page, so whilst security features may look right, they will be in the wrong place. For instance, an internal page is often used to create a replacement biographical data page. When pages are recycled, changes will usually be required, such as number alterations, or if from a different document, perforations need to be filled or changed.

If a biographical data page is replaced using a visa page from the same passport, that visa page will either be missing from the passport or be replaced by a counterfeit page.

Data Alterations and Erasures

Physical and chemical alterations and erasures can be made to data that has been assigned to an identity or travel document but most of it is retained in its original state. Physical alterations are a manual process, where the substrate is physically altered such as by cutting or scratching the surface. Chemical alterations use a substance to remove information, such as stamps from a visa page or printed ink.

An alteration occurs by either removing or adding something, and alterations are mostly found to the biographical data (photograph, the name or the date of birth) and other printed information such as document number or validity. Alterations or erasures can also be found on the visa pages, often to disguise travel movements.

Page Removal

Pages can simply be removed from a passport, to remove information that is not wanted, or to use the removed page elsewhere for fraudulent purposes. Page numbering should reveal cases where this has been done.

Paper visa labels can also be removed, to use elsewhere or to disguise travel, with evidence of this being found in the adhesive left on the visa page, discolouration of the page, indentations in the paper or the presence of traces of entries such as wet stamps on adjacent pages.

Disassembly and Reassembly

There are times when a passport needs to be pulled apart to allow an alteration to occur. After alteration it needs to be stitched back together. It is difficult to dismantle a passport without affecting the materials that have been used when it was first assembled. Pages can be damaged, or stitching may need to be cut.

Once the alteration has occurred, it is necessary to reassemble the booklet to have the same appearance as when it was genuine. In addition to any changes to the pages in the passport, some form of adhesive may be required, replacement stitching may be needed, and the booklet may have to be trimmed.

All these actions will leave evidence; pages may have hand cut corners or be slightly misaligned, edges may not be straight or line up, stitching may be loose.

Stolen Blank Documents

A stolen blank is a genuine unissued document obtained illegally. These documents may be stolen in bulk during transit, or from the issuing authority. Access to a stolen blank document means that a forger has a quality product to forge and is only required to add and secure the biographical data onto it.

Where blank passports are stolen, the document numbers of these documents are provided to national databases and INTERPOL for inclusion on the Stolen and Lost Travel Document (SLTD) database.

Inclusion of the personal details (and a laminate) is still required, and it may be that these details are not added to expected standard, or that a counterfeit laminate is used. It may be necessary for the document number to also be altered, to try and disguise its detection in national and INTERPOL SLTD.

Fantasy and Camouflage (aka alternative documents)

Fantasy and camouflage "passports" are a form of document that is made using materials with little or no security value. These documents may present as a "passport" based on their size and content, but they are not real documents and have no value as an identity document, or for any form of legitimate travel.

Figure 9. Fantasy and camouflage passport

Source: Passport Examination Procedure Manual - third edition.

Fantasy documents - These documents are created by individuals, groups or organizations, and include simulated features and characteristics of genuine secure travel documents. The groups or organizations have no authority to issue a document that can be used for legitimate travel purposes. Examples of fantasy documents include the "World Service Authority passport" and the "Hutt River Principality passport", the "Principality of Sealand ID card" and several "drivers" licenses.

Camouflage passports - These documents are created using country names that no longer exist. They may have a similar appearance to the genuine secure travel documents in use when the country was recognized or may simply use the country name. As the country no longer exists, there is no recognized authority to issue a legitimate document. As with fantasy passports, these documents will contain very few security features. Examples of camouflage passports include British Honduras (now Belize) and Rhodesia (now Zimbabwe).

For additional info, please check: https://home-affairs.ec.europa.eu/list-known-fantasy-and-camouflage-passports_en.

The Process of Examination

Use of identification document validation technology

Identification document validation technology (IDVT), where it is available through mobile phone Apps or document scanners, is a modern and very effective way of initiating a document examination.

Swiping a document on a scanner gives the document reader and the available databases an opportunity to check the document and alert in case of issues such as stolen or lost documents and the security mechanism of any contactless chip. A methodical approach is required:

- It is important to be patient and wait for the reader to finish all the processes.
- Pay attention to the photos of the document taken by the reader in UV and IR light.
- Compare the photo displayed from opening the chip to the one on biodata page – they should be identical.
- If any of the processes responds with a warning indicator, follow up appropriately.

The Process of Examination – Physical: Checklist

LOOK

- Is the passport booklet well bound, or misaligned?
- Any pages loose or coming away?
- Is the crest lined up properly on the cover?
- Do the pages open freely, or are some sticking together?
- Does the MRZ have the correct appearance?
- Is the colour of the printing consistent throughout the document?
- If there is more than one face image in the document, are they identical?
- Is the person in the photograph the same person in front?
- Using magnification and a UV light, is the biographical data page dull under UV, or is it bright?
- Does any other page give a different reaction to others?
- Is the printing on the biographical data page solid or made up of dots?
- Are the corners of the biographical data page rounded, or hand cut?

FEEL

- Does the cover feel smooth and is it in appropriate condition for its age and use?
- Is the front-end page stuck evenly to cover?
- Is the cover lifting away from the end pages?
- Is there a page or pages that "stick out" from any edge?
- Is there unexpected glue or any other substance on cover or pages?
- Do any pages have a different feel to others in the passport?
- Are any pages different to the pages in similar passports handled before?
- If the biographical data page is polymer, is any print raised?
- Running a finger across the biographical data page, are there any irregular bumps or lines around the photograph, the personal data or security features?

TILT

- Is there an Optical Variable Device (OVD) or Diffractive Optical Variable Device (DOVID)? Does it have a strong colour change?
- Is there movement in the OVD? Does it change colour?
- Is there an optical variable ink (OVI)? Does it change of colour?
- Is there a latent image? Does the hidden image become visible when angled to the light?
- Is the biographical data page perforated with an image or pattern? Can it be seen with transmitted light?

The Examination Process

Although most documents presented to Consular Officers are genuine, it is very important to spot a potentially fraudulent document. Failure on a document reader should be attended to carefully. National passports and identity cards are high quality documents and production standards are generally high.

All passports will have a biographical data page, a cover and end pages. All identity cards will contain biographical data in a reduced format. Even if they include very different materials in their make-up, the approach to recognizing when it is not genuine involves looking carefully at different areas of the document.

The examination of documents is a difficult role and there are lots of challenges:

- Limited time to detect issues.
- The variable nature of security features in documents.
- Whether equipment is available to assist in the examination process.
- Different methods used by forgers.
- Documents in various conditions, from brand new to old and mutilated.

In any type of booklet, such as a passport, begin with the cover, then work through the document methodically, addressing each area, using the examples of fraud detection points to highlight any possible issues.

Evidence of Fraud – Cover

The cover is protecting the passport content. It is a high-quality material adhered to the booklet using strong adhesives. When a document has been altered, the cover may have been removed and reattached. When something looks or feels wrong it should be examined closely, as the inside pages may have been altered.

Poor quality, smudged gold blocking, glue coming away or in excess, and wrinkling are all indicators that something could be wrong.

Evidence of Fraud – Biographical Data Page (paper)

A paper biographical data page is an area of the passport most likely to be altered or replaced. Alterations can occur to personal data, document numbers or authority details, or the whole page may be substituted. There may be physical or chemical evidence present to show that changes have occurred.

Irregular corners – not die-cut as expected, substandard printing quality, stitching coming away from the booklet or missing stich holes and laminate lifting are all indicators that something could be wrong.

Evidence of Fraud – Biographical Data Page (polymer, etc.)

The quality of these pages creates more of a challenge for the forger. Alterations can occur to personal data, document numbers or authority details, or the whole page may be substituted. There may be physical or chemical evidence present to show that changes have occurred.

Scratches around/on data elements, or a raised area of data, poor quality microprinting on the card, any area of damage or a high base fluorescence under UV light are all indicators that something could be wrong.

Evidence of Fraud – Machine Readable Zone

The format of the MRZ is the same for all passports and Identity Cards. When an alteration occurs to the personal details on a passport, it is necessary for the MRZ details to also be altered, which can result in errors or physical or chemical evidence of alterations. Dates of birth not matching or inconsistent lengths of data lines are negative indicators.

ICAO Doc 9303 gives clear specifications for the MRZ for comparison purposes.[23]

Evidence of Fraud – End Pages

These pages are the inside front and back pages, which are firmly affixed to the front and back cover. If a passport is pulled apart, the end pages may be destroyed and need to be replaced, or there will be some damage to the page, the security features, and the way that they are attached to the cover. Latent images (see Chapter 14) are often present on end pages, so look out for patches of darker print which could indicate these.

Evidence of Fraud – Stitching

Stitching helps retain the overall quality and construction of a passport. When it is removed and reintroduced to a document, there may be evidence of this removal or tampering. Stitching, which is not tight, missing holes or otherwise of poor quality are indicators that something could be wrong.

Evidence of Fraud – Inner Visa Pages

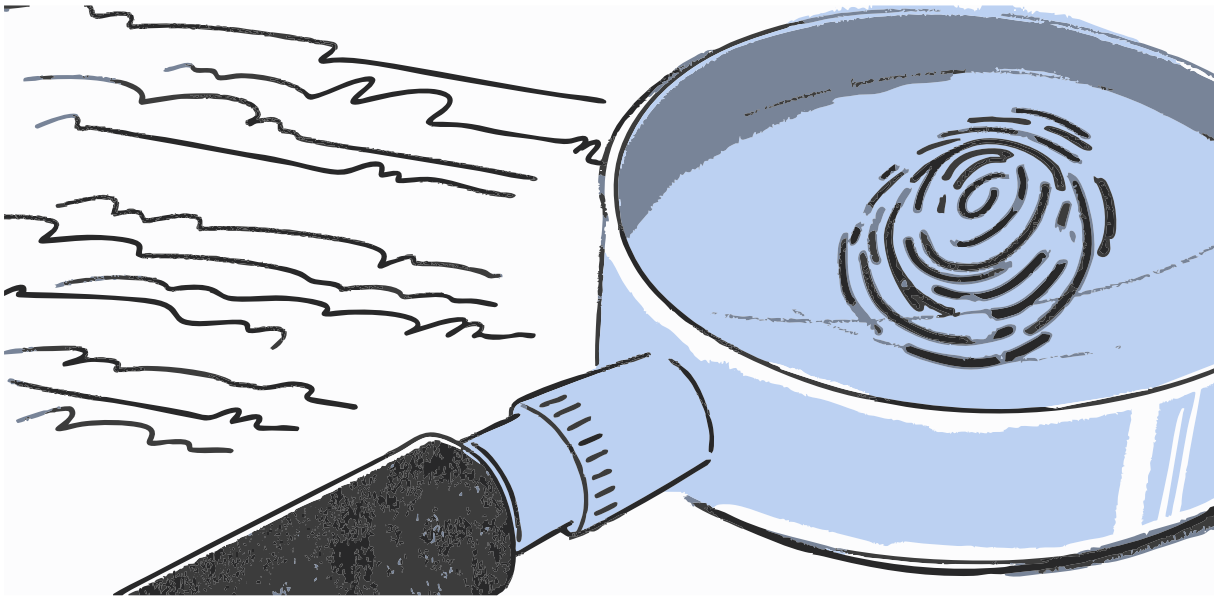
The inner visa pages form most of the passport. Visa labels and arrival/ departure stamps will be present. If a biographical/photo page is removed, the visa page at the other end of the booklet, could be as well.

Visible "watermarks" (not as they should be visible – with transmitted light), poor quality printing, irregular perforations on one or more pages, irregular or missing page numbering are all indicators that something could be wrong.

23 ICAO Doc 9303 - Machine Readable Travel Documents. Part 3: Specifications Common to all MRTDs. Eighth Edition, 2021 (www.icao.int/publications/Documents/9303_p3_cons_en.pdf).

Evidence of Fraud – Visa Stickers and Stamps

Where a visa label is still used, it will be placed on an inner visa page of the passport. The visa label, together with the arrival and departure stamps, provides important information about the history of where and when the passport has been used. Visa labels display many of the security features seen in passports. As the information on visa labels or stamps must match the passport detail, they may be subject to alterations in line with document changes, so close attention to data such as names and validity should be carefully checked.



Part 11.

What to do if Fraud is Detected

Forgery examination usually occurs at authority control points – mostly at border controls but also at consular representations and other points where examination and acceptance of identity documents is routine. In these environments there are different stages or "lines" of examination.

Personnel carrying out initial examination and assessments are considered as first-line officers, and initial stage examinations by Consular Staff, responsible for conducting frontline tasks, can be equated with this role.

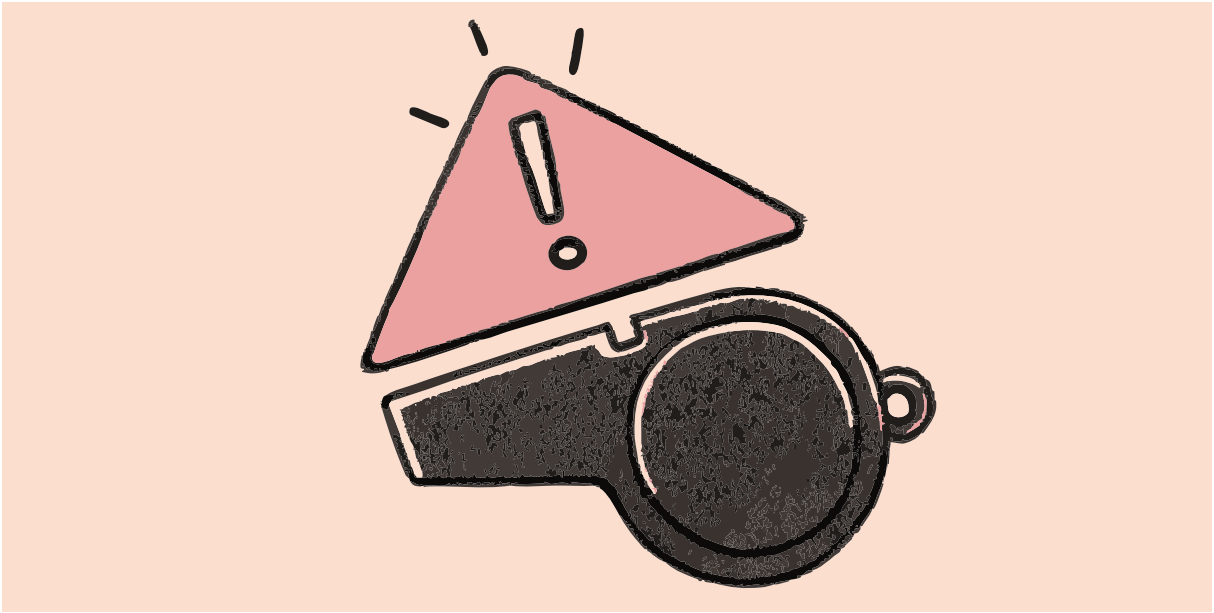
First line officers have the most difficult role and are required to:

- Check that the identity document is valid, and appropriate for travel if that is a requirement for the service;
- Scan the document on a reader/scanner if one is available;
- Compare face to passport, and passport to chip image, if displayed;
- Carry out the examination process.

If the examination takes place at a border control, first-line officers have very limited time to do all this, and whilst the examination is quite basic, they need to recognize and refer anything suspicious. Consular staff performing front line tasks should aim to avoid feeling pressurized by time or the other working constraints that arise in border controls.

If there is capacity to do so, it may be possible to refer to a second team member for an opinion in cases of doubt. In a border control scenario, this process is more formalized with a secondary-line officer. These officers have a higher knowledge and deeper understanding of document fraud and usually make the decision of whether a document is genuine or not. Secondary-line officers have access to and need to be able to correctly operate the advanced equipment available to them and access any reference materials necessary (such as online databases) to assist with an examination.

Consular officers need to be guided by local instruction on what action is appropriate if a forgery is suspected or determined, which will vary according to requirements of the State or local regulations and protocol. It is good practice to organize for appropriate intelligence material to be developed and distributed as this may be helpful to other staff and embassies.



Part 12.

Overview of International Standards Concerning Travel Document Issuance

The first international standard for machine-readable passports was developed by ICAO in 1980 and became known as ICAO Document 9303. Since then, that document has been updated, expanded, and reformatted to meet international needs in the modern international travel environment. The standards provide guidance on such things as the size, format and security requirements for secure travel documents, as well as biometric solutions for international interoperability, which contributes to reliable and efficient civil aviation operations across borders.

In this chapter, the different topics relating to international standards are: ICAO standards, Machine Readable Travel Document (MRTD) Standards and Recommended Security Features and Biometric Identification.

Aspects of the standards that have relevance to The Manual use information primarily sourced from three key parts of ICAO 9303:[24,25,26]

ICAO standards for Machine – Readable Travel Documents (MRTDs)

The MRTD, and its method of issuance, shall be designed to incorporate safeguards to protect the document against fraudulent attack during its validity period. In 2005 ICAO approved that all countries must begin issuing machine readable passports, meeting the standards, by 2010. In addition, all non-machine-readable travel documents must have expired by 25 November 2015. With this standard in place and accepted, only machine-readable travel documents should now be available for international travel, with the possible exceptions of emergency passports and other forms of temporary document capable of being used for travel.

Figure 10. ICAO standards for eMRTDs lead to interoperable documents

Source: Courtesy of Document Examination Solutions, Australia.

To assist with interoperability across States, documents are categorized according to their purposes and sizes are dictated as follows:

- TD-1, measuring 54 x 85.6 mm, for official travel documents (ID cards);
- TD-2, measuring 74 x 105 mm, for larger ID cards and smaller machine-readable visa labels (MRV-B);
- TD-3, measuring 88 x 125 mm, for passport biographical data pages.

Historically, ICAO categorizations with similar measurements were called ID-1, ID-2 and ID-3. A fuller explanation of these measurements with tolerances and margins for photographs and biographical data is given in ICAO Document 9303 parts 4 (TD-3), 5 (TD-1) and 6 (TD-2).

A machine-readable passport will be a booklet which has at least eight pages and includes a cover and a biographical data page. It will be manufactured to meet requirements relating to its ability to withstand certain conditions (such as light, temperature, humidity, etc.) for the time that it is valid.

24 Doc 9303 Machine Readable Travel Documents Eighth Edition, 2021 Part 2: Specifications for the Security of the Design, Manufacture and Issuance of MRTDs: (www.icao.int/publications/Documents/9303_p2_cons_en.pdf).

25 Doc 9303 Machine Readable Travel Documents Eighth Edition, 2021 Part 3: Specifications Common to all MRTD's: (www.icao.int/publications/Documents/9303_p3_cons_ en.pdf).

26 Doc 9303 Machine Readable Travel Documents Eighth Edition, 2021 Part 9: Deployment of Biometric Identification and Electronic Storage of Data in MRTDs: (www.icao.int/publications/documents/9303_p9_cons_en.pdf).

The biographical data page layout will be in a standard format, with both a visual inspection zone (VIZ) and a machine-readable zone (MRZ), easily recognized by people and machines internationally. This means the position of information such as dates, photographs, etc., is generally in the same place on the passports of different countries, with some flexibility allowed to meet individual country needs.

The following information relates specifically to standards associated with the placement of personal information on the biographical data page.

Figure 11. Visual inspection zone on a passport

Source: Courtesy of Document Examination Solutions, Australia.

The visual inspection zone is above the machine-readable zone on a passport. This formatting will be the same on all ICAO compliant passports. (Courtesy of Document Examination Solutions, Australia).

Visual Inspection Zone (VIZ) Data

The Latin alphabet, i.e. A, B, C … Z, is used. The Arabic numerals, i.e. 1, 2, 3 …., are used.

Typeface, type size and fonts used in the VIZ can be chosen by the issuing State and Organization, but it is recommended that the font be approximately 10pt (no more than 15pt) and the text be in upper case characters.

To ensure consistency, the Gregorian calendar is used for dates. Within VIZ, dates are written as follows:

- Days are written as two numbers, i.e. 06 or 23
- Months are written with up to four letters, i.e. JUN, AUG, JUIN, AOUT

Complete dates can be written in numerical form i.e. DD MM YY or DD MM YYYY (spaces are between day, month and year). X's are used to substitute, i.e. XX XX XX where dates are unknown.

Facial Image (Photograph)

Figure 12. Facial Image

Source: Courtesy of Document Examination Solutions, Australia.

A photograph that is less than six months old at the time the passport is issued, looks like the holder, and is not altered, should be used. The pose in the photograph should be a close-up of the head and shoulders with the face looking at the camera. Eyes should be visible, the expression should be neutral, the mouth should be closed, and there should be nothing that is hiding the eyes or the face.

Glasses should only be included in the photograph if they are worn permanently. An acceptable standard of digital reproduction is necessary, with correct lighting, exposure and colour balance according to ISO/IEC 19794-5.

Signature

Figure 13. Digitally reproduced signature into the passport data page

Source: Courtesy of Document Examination Solutions, Australia.

The signature can be either written or digitally reproduced into the passport. Although uncommon, it can also be written onto a substrate and stuck into the passport if specifications are followed.

When digitally reproducing the signature, it cannot be less than 50 per cent of the original size and scaled appropriately so that not stretched or compressed in any direction.

Fingerprint

Where fingerprints are included in a passport, they can be original or digital with no scaling.

Figure 14. Fingerprint

Source: Internet.

Machine Readable Zone (MRZ)

Figure 15. Machine readable zone

Source: Courtesy of Document Examination Solutions, Australia.

The Machine-Readable Zone (MRZ) contains data essential for passport processing in a format that machines can read. It is mandatory in all types of MRTDs. For machines to be able to read the zone, standards that are accepted internationally need to be followed, found in ICAO Doc 9303 (2021) and relate to ink type, font, format, transliterations, placement and check digits.

ICAO standards (MRTD security features)

ICAO 9303 outlines security features which should be incorporated into machine readable travel documents internationally. The aim of this list of basic security features is to ensure a consistent baseline level of travel document security. Rather than controlling the features, and ensuring all countries have the same, countries can choose different systems, substrates and combinations of security features to suit their individual needs, while still establishing the baseline requirements and some countries choose to include more advanced security features.

The recommendation is that all the basic features listed in the 4 different phases within Doc 9303 be incorporated, along with some of the additional features available.

These 4 different phases of production are: Substrate Materials, Security Design and Printing, Protection against Copying Counterfeiting or Fraudulent Alteration, and Personalization Techniques. A description of these phases is provided within ICAO Doc 9303 (2021) and extensive elaboration on them, together with practical guidance is provided in the IOM Publication: Passport Examination Procedure Manual (Second Edition).

Biometric Identification

Biometric identification is a generic term used to describe automated means of recognizing a living person through measurement of distinguishing physiological and behavioural traits. Biometric identification capability is well established in international border management and legal identity fields.

The IOM "Introduction to Biometrics" manual is an operational guide to the subject, useful for consular staff using and operating with biometric technology. It outlines the approach to capturing, comparing, and assessing biometric data from individuals such as fingerprints, facial features, and iris scans. It also addresses some concerns regarding vulnerabilities, threats, and the possible discriminatory use of biometrics.

Where a document is a biometrically enabled and globally interoperable MRTD, containing a contactless integrated circuit with sufficient storage capacity and data secured with the specified digital signature (commonly referred to as a chip), it is referred to as an electronic Machine-Readable Travel Document (eMRTD) and displays the following standard format symbol.

In Doc 9303, ICAO considers three types of biometric identification systems for encryption in relation to secure travel documents. Facial recognition is a mandatory requirement, and both fingerprint and iris

recognition are optional requirements. Key considerations for ICAO In developing an approach to the application of biometric technologies are Global Interoperability, Uniformity, Technical Reliability, Practicality and Durability.

Standards associated with the development of biometric capabilities have been in a transitional stage since 2020. The ISO/IEC 39794 document details the international standard for encoding biometrics, defining that from 01/01/2030 passport issuers must use those standards.

Figure 16. ICAO eMRTD symbol

Source: Courtesy of Document Examination Solutions, Australia.

ISO/IEC 39794 also specifies application specific profiles including constraints, photographic properties and digital image attributes, and provides a generic face image data format for face recognition applications. The document also addresses mechanisms to maintain backward and forward compatibility.

Proposed changes to Standards from Amendment 30

The ICAO Facilitation Panel (FALP) has recently proposed additional standards be incorporated into Annex 9. FALP/13-WP/4 13/12/23 (Amendment 30)[27] refers to these standards in full detail but briefly, the recommended changes and associated timescales are:

- States issuing eMRTDs shall implement Password Authenticated Connection Establishment (PACE) as of 1 January 2025. This will give greater protection of personal data using enhanced encryption between the system and document chips. Legacy eMRTDs without PACE shall cease to be issued as of 1 January 2028 and be completely out of circulation by 1 January 2038.

- States issuing eMRTDs shall update their facial image encoding to the specifications contained in Doc 9303 by 1 January 2030 at the latest. States implementing checks on eMRTDs at inspection systems shall implement the specifications contained in Doc 9303 for decoding the facial image data in the document chips by 1 January 2026.

27 FALP/13-WP/4 13/12/23 Whereby the ICAO Facilitation Panel (FALP) in Feb/Mar 2024, made a proposal for certain standards related to Doc 9303 to be incorporated into Annex 9 – Amendment 30. (www.icao.int/Meetings/FALP/Documents/FALP13-2024/FALP13-WP4.EN.pdf).


IOM
UN MIGRATION