VERSION 5.4, MAY 2018

# ICAO TRIP Guide on **EVIDENCE OF IDENTITY**

ICAO Security and Facilitation

## DISCLAIMER

## EXECUTIVE SUMMARY

The International Civil Aviation Organisation (ICAO) is the only United Nations Specialized Agency that has the mandate and responsibility for establishing, maintaining and promoting Standards and Recommended Practices (SARPs) related to the issuance and verification of machine-readable travel documents and related border control processes. While in the past ICAO concentrated on the physical security of travel documents, under the new Traveller Identification Programme (TRIP) Strategy, ICAO's mandate has expanded to include traveller identification. ICAO is now focused on ensuring a holistic and coordinated approach to traveller identification - from document issuance to border inspection systems. ICAO's goal is to improve the level of security and integrity of Evidence of Identity (EOI) processes across the entire travel document and border control management continuum.

The processes that authorities follow to establish and verify a person's identity are often laxer than the security of the document or credential they are issuing. Poor quality foundational processes weaken trust and confidence in the traveller's identity and ultimately undermine States' own investment in a high security document, credential or border process.

Establishing and verifying an identity to a high degree of confidence is complex: each context is different and all authorities need to balance the risk of identity fraud against the provision of efficient services to genuine citizens and low-risk travellers. States should apply an EOI approach to designing robust and secure processes that consider the full range of data, documents and information available, covering both the foundational ('legal') and physical identity of the individual.

The ICAO Guidance on EOI provides a framework and tools that enable States to methodically consider how best to uniquely identify individuals for the purpose of traveller identification. The Guide focuses on particular core principles to be considered when establishing and validating identity, to gain confidence that:

a. the claimed identity is genuine (i.e. identity is valid and not fictitious, and that the identity is still living);
b. the presenter links to the identity (i.e. the person can be linked to the claimed identity, the identity is unique within the authority's system and the presenter is the sole claimant); and
c. the presenter uses the claimed identity (i.e. that the person is operating under this identity in the community).

The Guide does not set standards for how confidence in a person's identity shall be established. Practices will vary from State to State, depending on processes and systems in place, technologies obtainable, and the foundational documents and information available. Local laws and legal frameworks as well as cultural considerations and social context all have an impact on how a State designs its EOI approach.

The Guide is intended to provide a means for States to assess their current EOI context, and design a comprehensive risk-based approach to identity establishment and validation using available documents and information. The EOI approach is an effective way to provide high confidence in a person's identity when issuing a travel document or visa, or facilitating a passenger through the border.

# CONTENTS

# 1 INTRODUCTION

Identity fraud is an enabler for criminal activities ranging from organized crime to terrorism, and its rapid growth raises serious concerns for security and safety globally. Border authorities constantly upgrade their travel document inspection systems and passenger checks to improve security at border control points to keep pace with new threats and provide security whilst improving the facilitation of low-risk travellers. The increase of international data sharing and use of new technologies, including the INTERPOL Stolen and Lost Travel Documents (SLTD) database, and the ICAO Public Key Directory (PKD), has also resulted in improved capabilities toward fraud detection.

While such measures have successfully raised the level of aviation security, they have also caused a shift away from manipulating the physical travel document (alteration, counterfeit, forgery) towards falsely obtained genuine passports. Weaknesses in the national passport issuance process are increasingly being exploited in order to falsely obtain a genuine passport. Genuine documents that are falsely obtained can be validated against source data and Public Key Infrastructure (PKI), and are therefore less likely to be detected at Border than those based on fake, altered or counterfeit documents. Imposter fraud or lookalike fraud, where the presenter utilises another person's genuinely issued travel document, is also steadily increasing – particularly in relation to human trafficking.

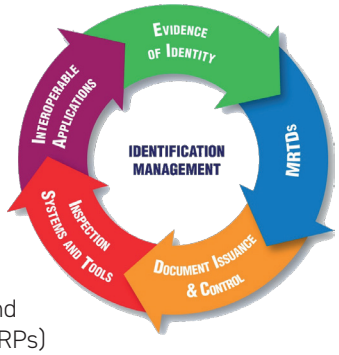
The ability of criminals to perpetrate fraud relies upon deceiving the authorities during the application or border process, either by inventing a fictitious identity or stealing a genuine existing identity that could be living or deceased. The scrutiny and verification of documents and information used to substantiate claims to an identity therefore become increasingly important. The ability to utilise broader identity-related information to corroborate claims or provide additional confidence is also emerging as a key aspect of identity management.

While the travel document itself needs to be physically secure and comply with ICAO Doc. 9303 specifications, the issuing process also needs to be of high integrity and the checks made on such a document at borders need to be thorough and effective. ICAO's goal is to improve the level of security and integrity of Evidence of Identity (EOI) processes across the entire travel document continuum. EOI is an approach States should use for the establishment, enrolment and subsequent verification of identity. The EOI approach uses a range of data, documents and information to gain a high level of confidence that individuals are who they claim they are. If quality EOI processes are not in place, trust and confidence in the traveller's identity is weakened, and States' investment in a high-security document or credential is ultimately undermined – as are its border processes.

The optimal approach for achieving a high level of EOI security and integrity can vary from State to State. The State's understanding their unique identity context, and approach to designing a high-quality EOI process, must therefore be methodical and considered – both for the issuance of identity documentation and processing travellers at the border. The approach must effectively balance security and facilitation, as most travellers pose no threat to the authorities attempting to establish or validate their identity. A well balanced approach to traveller identification can assist to improve both security and facilitation, by enabling better targeting of resources on persons of interest.

The ICAO Guidance on EOI provides a framework and tools that will enable States to uniquely identify individuals to a high degree of confidence for the purpose of traveller identification.

## 1.1 ICAO'S MANDATE ON EVIDENCE OF IDENTITY




The International Civil Aviation Organisation (ICAO) is the only United Nations Specialized Agency that has the mandate and responsibility for establishing, maintaining and promoting Standards and Recommended Practices (SARPs) related to the issuance and verification of machine-readable travel documents and related border control processes[1]. While in the past ICAO concentrated on the physical security of travel documents, under the Traveller Identification Programme (TRIP) Strategy, ICAO's mandate has expanded to include traveller identification. ICAO is now focused on ensuring a holistic and coordinated approach to traveller identification throughout the travel continuum - from document issuance to border inspection systems.

Evidence of Identity (EOI) is a fundamental element of the ICAO Traveller Identification Programme Strategy[2]. ICAO's goal with respect to EOI is to assist States to properly and uniquely identify individuals as part of the travel document issuance process or as they move across borders.

In many States the travel document issuing authority is one of the most important authoritative sources of identity information. ICAO therefore focusses on the establishment and validation of traveller identity, and within the context of aviation security and effective facilitation. If States do not undertake the necessary steps to identify such individuals effectively, the repercussions can be extremely serious. As an authoritative source, the State travel document issuing authority has an obligation to ensure that identity is established with a high degree of assurance.

ICAO's mandate includes continued work on further strengthening the security and integrity of traveller identification and border controls and developing guidance material to assist Member

1 For TRIP, the principal relevant SARP is Annex 9 to the Chicago Convention, focusing on facilitation, and ICAO Doc. 9303 specifications for machine-readable travel documents (MRTDs) is the key relevant specification.

2 TRIP was endorsed by the 38th Session of ICAO Assembly in 2013 as part of ICAO Assembly Resolution A38-16.

States to further those objectives. By creating firm linkages to essential civil registration documents and records, and giving visibility to the core role Civil Registration and Vital Statistics (CRVS) plays in traveller identity space, ICAO's EOI practice will also help support the United Nations Sustainable Development Goal of a legal identity for all by 2030.

## 1.2 PURPOSE AND APPROACH OF THE GUIDE

The purpose of the Guide is to provide States with a conceptual framework for establishing and verifying an individual's identity, as well as a range of practical tools based on the best international practices. The Guide applies to the functions of government authorities where the traveller's identity needs to be verified with high confidence, and incorrect attribution of identity may lead to serious or grave security consequences[3].

It is not feasible to prove with absolute certainty the identity of an individual wanting to obtain a travel document or cross a border. This would require an identity process so cumbersome and intrusive that the costs would greatly outweigh any benefits. The EOI approach outlined in the Guide is therefore not intended to be prescriptive. The Guide encourages authorities to take a risk-based and evidence-based approach to designing identity processes, taking into account existing processes procedures and legislation. The framework enables an agency to look at their service as a whole, balancing security with facilitation in a methodical way, evaluating identity documents and information in their own context, and providing the ability to identify gaps and issues in the process or wider identity context of the State.

Use of the Guide will give authorities greater confidence in an individual's identity prior to or during the delivery of a service to that person, whether issuing an identity credential or processing through the border.

The Guide is primarily meant for travel document issuing and border control authorities. However, it could be useful and relevant to the broader range of authorities involved in identity management[4].

## 1.3 SCOPE

The Guide outlines key EOI principles and provides examples of how they can be applied to different contexts.

The Guide is not intended to explain the complexities of identity technologies and their implementation – but rather to situate them within the EOI context, and outline how the technologies might be used to meet particular EOI objectives. Where appropriate, the Guide refers to other applicable guidance material, good practice and standards.

3 ICAO's approach to EOI draws from other international frameworks and guidance, including the New Zealand Government's Evidence of Identity Standard and Identity Assurance Framework for Government at www.dia.govt.nz. Also see the Australian Government's Gold Standard Enrolment Framework in its National Identity Security Strategy at www.ag.gov.au, and the NASPO Requirements for Security Documents. The APEC Business Mobility Group has completed their Framework for Assuring Identity in the Issuance of Biometric Machine Readable Travel Documents. For a European-focused work on the subject, see the Organization for Security and Cooperation in Europe's Compendium of Good Practices in Identity Management in the OSCE Region www.osce.org/odihr/346906.

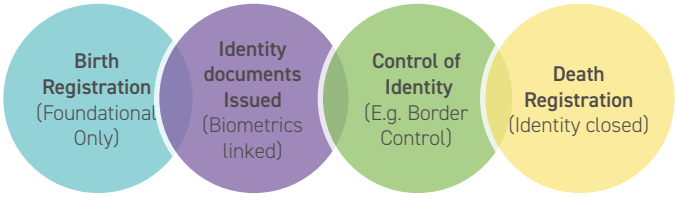
4 Where other agencies are designing a new EOI process, they should undertake a full risk assessment to determine the level of EOI required (high, medium or low) for the service being delivered. See the New Zealand Government's Evidence of Identity Standard for a comprehensive example of such a risk assessment.

# 2 THE EVIDENCE OF IDENTITY APPROACH

## 2.1 WHAT IS IDENTITY?

A person's identity is defined by their combined biometric and biographic attributes that apply uniquely to that person. Identity establishment is the process of verifying and associating identity attributes with a particular person, which can then be enrolled into an identity management system.

Identity is commonly established in a relatively linear way, with a foundational document or record (such as a birth certificate) forming the first link in an identity chain. As with any chain, it relies on strong links throughout – and the whole chain is as strong as its weakest link.



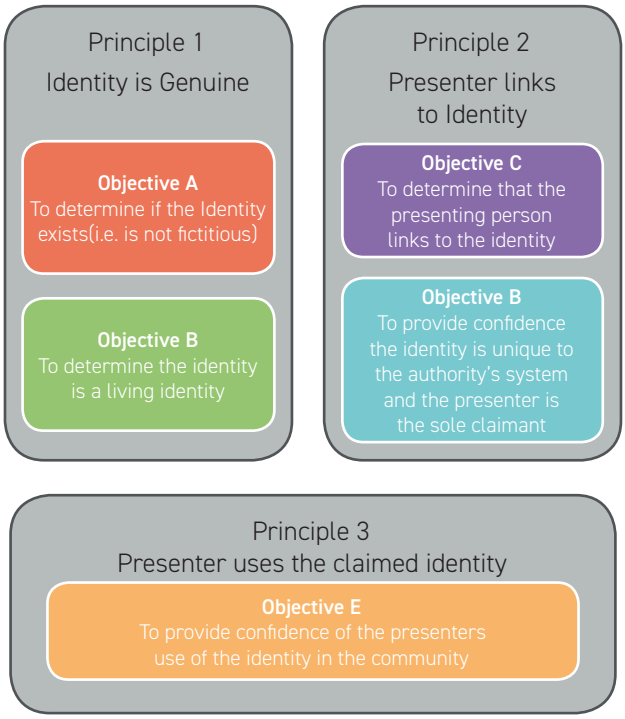

The EOI approach views a person's identity as far more dynamic and diverse than a chain, and more challenging to establish, maintain and verify than the linear model would suggest. Identity is more like an intricate interconnected system that changes over time. The traditional linear understanding of identity fails to recognize that the network of identity-related information is broad and some examples can be unique to a particular State. Identity therefore differs between cultures, as well as social and geographical contexts. Each of these contexts is unique with regard to the reliability and availability of documents and information. Establishing and verifying an identity to a high degree of confidence is therefore complex, and involves a methodical assessment of risk and value of each piece of available evidence. Adopting an EOI approach is an effective way of evaluating the identity context, and designing robust and secure processes.

## 2.2 PRINCIPLES OF EOI

The EOI processes in this Guide rely on a three-principle approach to establishing and validating identity. These principles, and their related objectives, are outlined below and in Figure 3:

1. **Claimed identity is genuine** is the confidence that the identity was genuinely born and is still living, and has not been created falsely in order to obtain something one is not entitled to (e.g., a secure document such as a passport).
2. **Presenter links to the identity** is the confidence that the person appearing at the border or applying for a secure document is entitled to claim the identity, is not an imposter, and is unique within the authority's context (e.g. the presenter is the sole claimant to the identity and appears only once in the system)
3. **Presenter uses the claimed identity** is the confidence that the person is operating under this identity within the community, and does so consistently.

Designing identity-related systems and processes along with these principles, and ensuring sufficient information is obtained to cover each objective, will provide authorities with a high level of confidence that an identity is genuine and the person owns the identity they are claiming. Each objective provides important evidence about distinct aspects of identity. On its own, each objective only satisfies part of the evidential process required to provide confidence that an individual is the true 'owner' of their claimed identity.




## 2.3 MEETING EOI OBJECTIVES

The Guide cannot be prescriptive on how to approach the key principles and their associated objectives. There is no 'one-size-fits-all' solution for EOI. How States and their authorities do so will depend on its culture, working practices and legal frameworks and will likely differ from other States. In some cases, States will not be able to gain high confidence in a particular objective, and may need to seek additional information (for example, through an interview) in order to be satisfied a claimant is legitimate.

Traveller identification authorities should seek to fulfil the EOI objectives to a high level of confidence, especially the first time they interact with an individual. If the first interaction is strong, then the States can leverage the strength of the first process for subsequent interactions such as renewal applications, border facilitation or other identity products and services provided at a later time (e.g. Citizenship). This enables States to put resources into areas of higher risk, by facilitating lower risk 'known' identities.

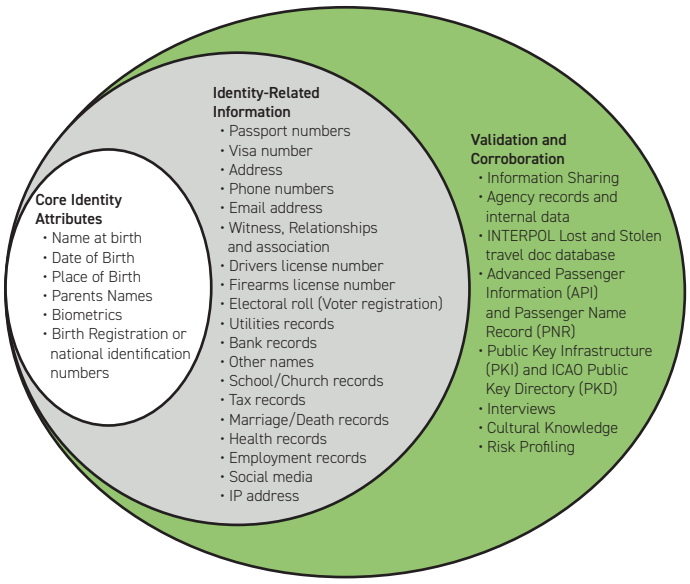
The diagram on the opposite page outlines an example of an EOI process that an authority might follow in order to achieve a high-confidence EOI.

| | |
|---|---|
| Objective A<br>Identity Exists | • 1-2 Documents, where available have been validated against sources records, or authenticated by staff trained in document recognition.<br>OR<br>• Verification of information against 1-2 source records, e.g. birth record or part of civil registration. |
| Objective B<br>Identity is Living | • Verification against the State's Death Register (part of Civil Registration).<br>OR<br>• An in-person component to the application process combined with process/es to meet Objective C. |
| Objective C<br>Person Links to Identity | • In-person verification with interview and/or against photo identification.<br>OR<br>• Assertion by a trusted referee, preferably known to the authority, and able to be verified.<br>OR<br>• Biometric recognition against the agency database, and/or other relevant databases. |
| Objective D<br>Identity is Unique to system and is Sole claimant | • Check against authority's own records for matching biometrics.<br>OR<br>• Check authority's records for matching biographical details such as similar names, addresses, contact details or other information collected. |
| Objective E<br>Identity is used in the Community | • Evidence from reliable third parties to show the identity in use for the majority of the customer's life.<br>OR<br>• Statements from trusted referees confirming use in the community.<br>OR<br>• At least 2 supporting documents/records (e.g. electoral roll, banking and utilities statements).<br>OR<br>• Where a previous passport is held, validation against agency records.<br>OR<br>• Interview of the applicant, if required to help build confidence due to lack of evidence in other areas, or suspicions raised during application process. |

## 2.4 TYPES OF EVIDENCE

An EOI approach should consider the full range of distributed information available when issuing a travel document or facilitating a traveller through the border. Evidence can be in the form documents, data and information – obtained from authoritative sources, government departments, private sector entities, individuals and the applicant themselves. Each piece of information will differ from State to State, and therefore must be evaluated within the local context to determine its value to an EOI process (see Assessing Available Evidence and the Identity Context at Appendix E).

Some examples of evidence are outlined to the right, though there are many other examples of 'identity-related' information that can be utilized depending on the State. Aspects such as phone number, Internet Protocol (IP) address, tax and social security numbers, and national ID numbers can all be used to determine the confidence in an identity, and the amount of risk posed by an applicant. Individually, they may not provide much confidence, but combined can provide a high level of confidence. This is particularly true where identity-related information demonstrates the consistent use of the identity over time, which in turn give authorities confidence in its legitimacy. Not appearing on particular lists such as INTERPOL Stolen and Lost Travel Documents database, or an authority's watch-list, is also evidence that can build identity confidence.



Each State will face different challenges and complexities in relation to evidential requirements, for example:

a. there may be multiple valid versions of foundational documents available for use (e.g. birth and/or death certificates);
b. legislation may prevent validation of documents, access to source registers or information sharing between government departments and States;
c. historic travel or foundational document records may be paper based – leading to a lengthy manual checking process;
d. databases of information may be application based rather than person centric – making it difficult to match various historical applications under the same identity; and
e. databases and registers may be incomplete or in some cases may not exist at all.

Regardless of State-specific challenges, authorities can normally still establish robust issuance processes by utilizing a range of information, documents, records and other evidence to build confidence in an identity.

## 2.5 OBJECTIVE A - IDENTITY EXISTS

A fundamental component for having high-level confidence in an identity is establishing that the identity exists. This means that the authority has confidence the identity is genuine and has not been invented. Normally an identity is established at birth and entered into a national register. The most common approach to checking that an identity genuinely exists is through civil registration records or foundational documents. This evidence forms a base for an identity, explicitly stating details such as the name, parents, and the date and place of birth. The record often includes a unique birth registration number or national identity reference. These records are often also stored in registries maintained by the State or local authorities, and may be used to verify documents, either directly or through accessing the source database.

When designing and implementing EOI processes for meeting evidential requirements it is strongly recommended that the authority's business processes capture an individual's 'name at birth' as an anchor. This allows records to be checked against both current and previous names associated with the identity, and enables the authority to link subsequent information and events back to a unique anchor.

If foundational documents are less common or less trustworthy in the State, or originate from another State than the one verifying the identity, it can be harder to gain confidence that the identity claimed genuinely exists, but confidence can still be achieved by utilising a combination of other sources. Enough evidence from schools, religious institutions, employment and other secondary government or private sector sources can assist to provide a high level of EOI confidence.

### 2.5.1 ESTABLISHING AN IDENTITY EXISTS USING CIVIL AND NATIONAL REGISTRIES

Civil Registration, more fully referred to as Civil Registration and Vital Statistics (CRVS) is the method by which States record the life event details of nationals and tend to include: birth, death, marriage, divorce, adoption, name change, and in some instances citizenship records. CRVS systems will normally contain the core identity attributes of an individual: name at birth, date of birth, place of birth, parents' names, and a unique registration number. Such records may be centrally or locally stored, either in paper and/or electronic form.

States may also have separate foundational national identity systems that provide for a national identity card and/or a digital identity record. This database can often be considered authoritative, provided there is assurance the core civil registration attributes have been carried through robustly and uniquely. National identity systems may have biometrics that can be used to ensure uniqueness within the database. If the national identity is issued on the strength of civil registration documents, and linked to a biometric, the travel document issuing authority will need to consider the strength of that process to ascertain whether the national identity database is reliable as an authoritative source, and consequently how much value the national identity document adds to overall EOI.

### 2.5.2 VERIFICATION AGAINST CIVIL AND NATIONAL REGISTRATION DATABASES

A birth certificate is a paper document that reflects an entry in a civil register. If the registration system is computerised and exists in the form of a database, it should be possible to obtain a digital verification. Otherwise, wherever a paper document is perceived as suspect, it can be physically verified by comparing against the register record itself.

Verification against a civil registry or a national identity system can be extremely reliable to confirm an identity exists. Some authorities do not collect physical documents to establish identity exists. Instead, direct access to the CRVS databases can confirm the details of a record given by the applicant are genuine and match the register. This approach can remove the risk of exposure to counterfeit foundational documents.

### 2.5.3 FOUNDATIONAL DOCUMENTS

Foundational documents[5] refer to evidentiary documents issued as a physical token of an event or status for a person (e.g. birth, national identity or citizenship) and are used by issuing authorities to establish identity and confirm entitlement. The documents will normally have a unique registration number.

Foundational documents are the fundamental physical evidence accepted by national authorities to establish a prime facie claim to an identity. This means that the documents being presented by the claimant are used as proof of the event. It should be noted that being in possession of a foundational document is does not necessarily provide confidence the holder and identity are linked.

5 Foundational documents are also sometimes referred to as 'breeder documents.'

#### 2.5.4 ESTABLISHING AN IDENTITY EXISTS WITH LIMITED DOCUMENTATION

Establishing that an identity exists with limited or no documentation is often the result of challenging or unusual situations, as is commonly seen where a crisis mobilises or displaces individuals (e.g. war or natural disaster). It can also occur in States where foundational life events are not routinely recorded and citizens are left without any form of legally recognised identification. The approach to EOI in these situations is considered exceptional resulting from specific circumstances, rather than as an alternative to the full EOI approach for regular travel document issuance.

EOI for exceptional circumstances is outlined in the case study on convention travel documents for refugees and stateless persons in Appendix A.

## 2.6 OBJECTIVE B – IDENTITY IS A LIVING IDENTITY

An authority can establish that an identity is living in a number of ways. Many countries record deaths as part of their CRVS. Looking up such a registry provides confirmation if a particular individual is not recorded as deceased and therefore the identity is considered 'living'. This could be a paper-based and decentralized registry, and thus confirmation should be sought from the concerned authority. With centralized and computerized records, a look-up and confirmation can be more easily obtained. There are other state records such as social services, welfare and pensions, which are required to regularly obtain evidence that the beneficiary is still living. In some States these records may be more reliable than the civil registration authority, and therefore such records can be referred to for confirmation of a living identity. Another common approach is to require the individual to appear in person to the issuing authority. This can also be useful in other ways - collecting biometrics for example. Such personal visits can be recorded as confidence that the claimed identity is a living identity, provided there is a high confidence in the link between the person presenting and the identity.

Failure to record deaths in a registry that is supposed to record deaths is not uncommon – especially when people die overseas and the death is not reported to the Consulate – or when the Consulate has no capacity to report it to the central registry in the national capital. In some States there is no social or legislative driver to routinely register deaths, and authorities may need to explore other EOI objectives as a means to gain confidence that an identity is still living.

#### 2.6.1 IDENTITY IS LIVING - SYSTEM CHECKS

The design of CRVS should support the basic search to prove an identity is living. That is, it should allow matching death data against birth data to enable easy verification of whether a claimed identity is of someone who is still alive or dead. This will not be possible in all circumstances, for example, when an individual was born or died in different jurisdictions or States.

While the existence, quality and ease of accessing such databases and civil registry systems vary from State to State, increasingly governments have been focusing on databases in addition to the documents themselves or in some cases, instead of some of the documents. Some States do link their data sources to birth and death records which serve as automatic checks and verifications of living identities. Further, if this is linked to a foundational national identity system, biometrics can provide further confidence that an identity is living, given it exists consistently in two government databases.

For border authorities at the primary line, the 'identity is genuine' component is generally established through the travel document, and confidence can be strengthened through checks such as Public Key Infrastructure, INTERPOL, and risk profiling such as PNR and API, behavioural indicators and watch-lists. For border authorities in this space, the key risks are through counterfeit documents, falsely obtained genuine documents and imposter fraud.

#### 2.6.2 ALTERNATIVE WAYS TO GAIN CONFIDENCE AN IDENTITY IS LIVING

If there is no access to centralised death register or there is no confidence in the information, then alternative approaches will be needed. Normally this assurance will be obtained through applying additional Objective E ('social footprint') checks. This can include personal interviews and matching biometrics, and will focus on evidence of an enduring and consistent use of identity.

## 2.7 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, the next objectives focus on establishing a link between the presenter and the claimed identity. Most fraudsters operate by pretending to be someone they are not. This means that the applicant does not link to the identity, either because the identity belongs to someone else, or the identity is entirely fictitious. Whilst the actual application form is a source of information that can be checked with the applicant, a well-prepared fraudster will have ensured that they are familiar with the details contained on the form and consequently may well be able to answer questions on the attributed identity accurately. Authorities may therefore need to gather and use information that corroborates the link, but is not necessarily readily available to a fraudster.

A crucial part of gaining confidence that an applicant links is to ensure that the applicant is unique within the authority's system – which means there is only one claimant to the identity, and no indication of the applicant having multiple identities within the system. Biometrics is an extremely effective way to test uniqueness in the authority's system – but it is not the only method.

#### 2.7.1 IN-PERSON PRESENTATION

Many States require in-person presentation for the issuance of travel documents and visas. For border control, there is a clear requirement for the traveller to be present. The in-person process can assist States to obtain and corroborate information,

particularly through interviews (covered in section 2.9.4). Where direct access to data and information is challenging, in-person presentation can be an important component of EOI. This process can also enable authorities to capture their own biometrics, to avoid emerging threats like photo-morphing.

### 2.7.2 TRUSTED REFEREES

Trusted referees are people who assist in establishing the identity of an individual by verifying the identity information provided by the applicant. Information provided by trusted referees can be used to link a person to an identity (Objective C) and to confirm that a person uses an identity in the community (Objective E), and has done so consistently over time. Trusted referees can be used to verify identity characteristics of an individual such as name, date of birth or photograph.

When foundational documents are less common or trustworthy, verification of an identity by a trusted referee can provide additional confidence that an identity exists and an individual links to an identity. Detailed information on trusted referees is available in Appendix F.

### 2.7.3 DOCUMENTS AND RECORDS TO PROVE UNIQUENESS

Biometric matching is becoming increasingly important in gaining assurance of uniqueness in an authority's system. However, other information can be utilised to gain confidence that an identity is unique and there is only one claimant. Collecting and validating core identity information through documents and registration records is effective – for example, names, date of birth, place of birth, parents' details, and national registration numbers. Additional identity-related data such as phone numbers and address, tax and other government numbers can be obtained and searched to ensure uniqueness. At border, passport and visa numbers and other supplementary information can be used.

## 2.8 THE ROLE OF BIOMETRICS IN OBJECTIVES C AND D

One of the main reasons for using biometrics is the increased assurance it provides when authorities need to establish and validate uniqueness. Instead of asking questions based on "what you know" or "what you do," the focus now is on "who you are" (your unique biometric), and that there is only one of you in the system. Once uniqueness is established to a high degree of confidence, authorities can more efficiently enable facilitation of known low-risk identities, and more effective identification persons of interest.

ICAO's development of ePassport standards, digital facial, fingerprint and/or iris images support automation of biometric comparisons at issuance and at border clearance points. The following comparison methods are possible:

### 2.8.1 VERIFICATION (1-TO-1 MATCHING)

Verification (1-to-1 matching) is a test to ensure a person matches to a known biometric. Two types of verification can be envisaged: with centralized storage or distributed storage.

If a centralized database exists, produced once at enrolment and updated with each application, where all biometric data and the associated identities are stored, the biometric sample of the claimed identity is retrieved from the database (i.e. by search for unique document number). This is then compared to the live sample provided, resulting in a match or a non-match[6].

If the biometric data is stored in the passport's chip that is carried by the individual, the person will provide a live biometric sample and this will be compared to the biometric data stored on the device. This is typically done by the verification system which retrieves the person's biometric data from the chip and compares them to the live sample and to the data printed on the travel document itself. If the verification process is successful, and the data is confirmed as valid through PKI validation, the traveller is confirmed to be the valid bearer of the identification document. Verification can be used for automated processing through border gates, or for document renewal.

### 2.8.2 IDENTIFICATION (1-TO-MANY MATCHING)

Identification is used to discover the identity of an individual when the identity is unknown, or when the authority is trying to ensure the biometric (who the applicant 'is') is unique and not already known to the system under another identity. Contrary to verification, the process of identification requires a central database that holds the necessary records for all people known to the system. Without a database of records the process of identification is not possible.

For an identification process, the person provides a live biometric sample (i.e. a photo or fingerprint is taken). The data is processed and the biometric sample or template is compared against all the entries in the database to find a match (or a list of possible matches). The system then returns as a response either the match (or list of possible matches) it has found, or that there is no match against the enrolled population. Since the system checks against a database of enrolled templates or full images, the maintenance of the integrity of the database is essential in protecting individuals from identity theft.

### 2.8.3 SCREENING OR WATCHLIST

The third type of process is screening, which makes use of a database or watch-list. A watch-list or 'no-fly' list contains data of individuals to be apprehended or excluded. A record on the watch-list may contain only biometric data for a wanted individual or may also have identity information, depending on what is known. Everyone who passes the screening process provides a biometric sample, which is checked for matches against the watch-list. The key feature of a watch-list is that people are not, on-the-whole, identified; they will only be identified if they appear on the list. If there is no match the person passes through and his/her

6 For effective 1-1 verification using a centralized database, an authority would normally undertake a 1-many match to clean up their biometric database, de-duplicate and identify any fraudulent multiple identities, to provide high confidence of uniqueness.

biometric sample should in principle be discarded. In the case of a match, a human operator decides on further action.

Unlike the use of other forms of authentication, such as passwords or tokens, biometric recognition provides a strong link between an individual and a claimed identity.

One area where biometrics can provide substantial help is in guarding against attempts to establish fraudulent multiple identities or prevent identity fraud. By searching through the stored references, individuals who appear to have previously enrolled using a different identity can be highlighted for further investigation. Biometrics is usually the only means for this type of check.

#### 2.8.4 THE MULTI-BIOMETRIC SYSTEM APPROACH

By combining the biometric features for identification and verification, a multi-biometric system is generally considered better than a system which uses a single biometric feature. A multi-biometric system captures more than one type of biometric for enrolment in the database. This improves the accuracy in establishing identity and in cases where a person is not able to provide one of the biometric features, he/she can still enrol the second biometric feature and is hence enrolled with at least one biometric in the database.

People with criminal intentions might focus on cheating one biometric feature, but will fail if a second biometric feature is also verified. It is extremely challenging for criminals to obtain two samples of biometrics of the same individual. Thus, a sophisticated level of security helps the multi-biometric system to perform better than the traditional system.

#### 2.8.5 ALGORITHMS AND APTITUDE

With the use of biometric matching, engines and algorithms must be set at certain tolerances in order to balance security and facilitation. Like all aspects of EOI, biometrics is still working in the realms of risk and probabilities. Some biometrics lend themselves to more consistent matching than others, and a very high accuracy can be achieved across most of the key biometrics used for traveller identification. Ultimately, however, the use of biometrics should be seen as one tool in the EOI suite, as all technologies can be undermined. Biometrics is not a panacea: for example, a person could have unique fraudulent identities in multiple States' systems if the biometric information is not combined with other EOI.

The human factor in assessing biometrics is also worth noting – particularly for facial recognition. Recent studies indicate people's natural aptitude for matching faces varies greatly, and is not influenced significantly by training. Some people are naturally good at facial comparison, which impacts how States deal with exceptions that fall out of facial recognition systems (e.g. watch-lists) for manual comparison, and also who States should employ on their front line border posts.

#### 2.8.6 PRIVACY CONSIDERATIONS

There are some legal and ethical considerations centering on the collection and use of biometrics, but those issues concerning privacy rights of individuals and personal identification receive the most attention. One concern is about the ownership and the use and onward sharing of the stored biometric data. Stored biometric data must be properly protected. There should not be any unauthorized collection, use, onward sharing, or retention of biometric data, and biometrics need to be deployed in accordance with national law, where it is most effective and appropriate, and in accordance with the principles of purpose, specification, necessity and proportionality. The public must be pro-actively informed about data usage and data retention time, to gain trust in both the system and its use and oversight.

### 2.9 OBJECTIVE E – APPLICANT USES THE IDENTITY

The aim of Objective E is to provide further confidence about an individual's claimed identity. In particular, Objective E is concerned with demonstrating the consistent use of the claimed identity. Documents and records that are used to satisfy Objective E are intended to be used for the corroboration of identity information provided to meet other objectives. As a guide, these documents, records and information should be from a trustworthy source, be dated, and include the name and, where appropriate, address of the person applying for the service. Objective E documents and information can be used more extensively by authorities to counter known weaknesses in other objectives. Use of identity in the community is often referred to as 'social footprint.'

#### 2.9.1 SOCIAL FOOTPRINT

The social footprint is based on the premise that everyone has dealings with a variety of organizations in their daily life, many of whom maintain records about this engagement that are publicly available. A person's social footprint builds up over time, and the continuity and longevity of identity-related information is a valuable element of the EOI approach. It covers life events and how a person interacts with society, and can include details of education and qualifications, electoral roll, employment history, driver licenses and tax numbers, healthcare and interactions with organizations such as banks, utilities and public authorities. This can also extend to an applicant's digital footprint, whether that be social media or utilising IP address.

The exact nature of the checks made will depend on the laws and customs of the country. However, authorities should bear in mind that the use of an identity must not always be the proof of its legitimacy (e.g. occasionally people are known by acquaintances and local authorities by a nickname, aliases or another assumed name for many years). By integrating social footprint information and checks within the application process, it is possible to deter potential fraudsters from attempting to make false applications. Social footprint can also enable the authority to validate the consistency of use of information across authorities over time, which enables the adoption of a more risk based approach.

### 2.9.2 EXAMPLES OF DOCUMENTS AND INFORMATION

The list below outlines documents and records that can be used to meet Objective E.

- Driver Licence
- Car registration papers
- Social Services and Health Care Cards
- Inland Revenue or tax number
- Electoral Roll records or voting cards
- Credit cards, bank cards and bank accounts
- International Driving Permit
- Confirmation of immigration or visa status
- Student identity cards or employee identification cards
- Secondary schools and tertiary institutions, and employers
- Utility accounts and services (e.g. telecommunication, electricity and gas power providers)
- Qualifications and professional registration
- Relevant education institutions and registration boards
- Medical and dentist records
- Real estate registry
- Travel records, e.g., tickets, boarding passes, frequent flyer cards and accounts
- Court summons, speeding tickets, parking tickets

### 2.9.3 APPROPRIATE COLLECTION OF SOCIAL FOOTPRINT INFORMATION

Some of the documents listed above provide information about a person (e.g. their bank account or academic record) that is not core identity information (e.g. name, date of birth and place of birth). Authorities need to ensure that only information appropriate to establishing identity is accessed. In cases where the authority requires certain documentation to establish both identity and entitlement to the service, the individual must be made aware that the documents provided will be used for both of these purposes.

The Objective E requirements should also be flexible enough to ensure a reasonable amount of choice for the individual. For example, individuals should be able to choose to provide alternative information as EOI rather than provide sensitive personal information such as financial or health information.

Authorities should also assess whether it is more appropriate to:

- keep copies of identity-related documents;
- record the core identity-related information from those documents; or
- simply record that the document or data source was sighted, on what date, and by which staff member.

Keeping copies of identity-related documents imposes a responsibility on the authority to protect the copies and the information they contain, while simply recording that the document has been sighted carries no additional responsibility.

### 2.9.4 INTERVIEWS

Interviews can provide the opportunity to assess how much an applicant knows about the claimed identity, which can help in providing confidence that the person presenting links to the identity. Interviews can be used to deter fraudulent behaviour, identify anything abnormal or unexpected, and then make a clear visual link between the claimed identity and the supporting EOI material or records.

It is essential that clear policy guidelines are devised to handle applications where a travel document application interview is required. This may include communication with applicants to explain the reasons for the interview, information about the interview and the level of information that is being requested as well as assurance that genuine applicants should find the process relatively straightforward and non-intrusive. Interviews with children should be conducted in an age-appropriate and gender-sensitive manner.

There should also be a policy for handling interviews pertaining to emergency applications. Reducing the strength or integrity of any of the checks should be avoided as it can introduce weaknesses or vulnerabilities in the system that fraudsters will exploit.

Every applicant need not be interviewed and a policy should also be in place to determine the cases that should require personal interview. An interview involves the collection, assessment and validation of information in relation to the applicant and their application. This information will be used by a trained interview officer to inform the questioning of the applicant.

The interviewer is testing whether the applicant owns or is entitled to the identity in which they are applying. Aspects that can be tested include: questions on supporting documents and information, cultural and local knowledge, familial relationships. Certain triggers (behaviour of the applicant or incongruent information) can indicate areas requiring cross-checking.

Following the interview, the interviewer will review the applicant's responses and any other relevant factors to decide whether the person interviewed is the true owner of the identity.

The following considerations should be taken into account when undertaking a travel document application interview:

a. Before an interview, an officer should check the applicant against any biometrics (including historic photographs) and other core details of their application. Authorities can guard against collusion by having a third person involved in doing this. Measures should be taken to reduce the risk of collusion, for example by assigning interviewers only just before the interview.
b. The interviewer should use the information available to them, in combination with their training, to make the interview questions specific to the applicant. This helps to guard against an applicant being coached on the interview process.
c. Whilst the interviewing officer should make the decision on whether or not the applicant has provided enough assurance on his/her identity and that the applicant has an entitlement to the travel document, a random check of these decisions should be made by a more senior officer. Such a check is carried out not only to ensure that a correct decision has been reached on the data available but also to guard against internal fraud or malfeasance.

The use of an interview extends the application processing time. Nevertheless, the rigour provided by a face-to-face interaction between the applicant and a trained interview officer utilizing a range of information sources provides a stronger defence against impersonation, travel document-related fraud and identity theft.

An interview by a trained member of staff could be performed via a video link instead of in person if security and technical considerations are taken into account prior.

# 3 OPERATIONAL CONSIDERATIONS

## 3.1 ESTABLISHING THE IDENTITY OF CHILDREN

Establishing the identity of children can be particularly challenging where there is a reliance on the provision of documentary evidence alone. Children are less able to establish an authoritatively documented social footprint than adults. Children, particularly babies, do not usually possess photographic identification, and the value of photographic identification at very young ages is more limited as children can change appearance relatively quickly.

Authorities should therefore consider the following approaches where establishment of a child's identity is required:

- Establishing a documentary link between the child and their parent(s) or caregiver(s) (this is particularly relevant where the child is very young);
- Using a range of evidence to indicate the child's use of the identity in the community (e.g. documentation produced through the child's engagement with the health and education sectors, or social service, religious, and cultural institutions); and
- Although the use of biometrics is generally difficult for children, DNA matching can be considered to establish parenthood – though this approach is reserved for cases of significant risk or concern.

## 3.2 RISK CONSIDERATIONS

An effective identity management system is vital for the issuance of secure identity documents and border control. Without it the reputation of the State could be severely impacted because other parties may not recognise or trust travel documents that are issued by that State. This could also lead to increased time to investigate crime and lengthy queues at borders as well as introduction of a visa regime that could add to both the logistic complexity as well as cost. This is to be balanced against the underlying EOI risk of accepting fake identification and therefore making it legitimate.

Identifying identity-related risks and the consequences of these risks, requires an understanding of how a person can obtain a false identity to commit identity crime. However it is worth noting that identity-related risk is only an aspect of the overall risk associated with any given service. Implementation of an appropriate EOI process helps authorities manage the identity-related risk associated with particular services, but may have no effect on other aspects of a service's risk profile.

Identity crime encompasses any illegal use of identity to gain money, goods, services, information or other benefits or to avoid obligations using a false identity.

False identities can be established in the following ways:

a. creating a fictitious identity (fake identity);
b. altering one's own identity (identity manipulation);
c. stealing or assuming a pre-existing identity (false identity); and
d. altering a pre-existing identity (false identity manipulation).

Identity theft is used to describe the theft or assumption of a pre-existing identity (or significant part thereof) with or without consent. Identity theft can occur in relation to both living and dead individuals. Identity manipulation involves the alteration of one or more elements of identity (e.g. name or, date of birth) to fraudulently obtain more access to services or benefits or to avoid establishing obligations.

However, initial establishment of identity is not the only point at which false identities can be created. False identities can also be created by methods such as internal infiltration of an authority's systems. It is critical that an authority implement the EOI Standard alongside, not instead of, other identity-related risk management processes.

For additional information on risks see Appendix G.

## 3.3 SUPPORTING DOCUMENTATION

Supporting documentation are those which contain identity information that can be used to assist with establishing or confirming an individual's identity.

Supporting documentation can assist in determining an identity exists and is not fictitious (Objective A) as identity information used within the community can be used to corroborate information found on foundational documents. Supporting documentation can therefore be particularly helpful when there is a lack of confidence in the issuance process of foundational documents.

When supporting documentation contains a photograph, it can assist in linking an individual to an existing identity (Objective C). An in-person verification of the photo document can confirm that an individual corresponds with the photo, and that the person corresponds with biographical data on the document.

Supporting documentation can also be used to achieve Objective E as it demonstrates that an individual uses an identity in the community. Knowing the identity is used within the community provides confidence that the identity claimed by an individual belongs to the individual who claims it.

Supporting documentation is particularly useful when it contains information such as:

- Given name and surname
- Sex
- Signature
- Date of birth
- Photo

If one piece of documentation does not provide sufficient identity information, multiple pieces of identification from multiple sources can be used. To prevent fraud, supporting documents should only be accepted from entities and authorities that are trusted. There should be adequate confidence in an entity's or authority's identity issuance process before supporting documentation is accepted. Issuance processes which verify information from multiple sources are less susceptible to fraud.

The authority should follow the protocols for acceptance of documentation in section 3.3.1 to gain a high level of confidence in an individual's identity and to prevent the acceptance of fraudulent documents as genuine by appropriate authorities.

### 3.3.1 PROTOCOLS FOR ACCEPTANCE OF DOCUMENTATION

Adherence to the following protocols will provide a higher level of confidence in a presenting an individual's identity, as these protocols make it more difficult for forged or altered documents to be accepted as genuine by the appropriate authorities:

a. Accept only original documents or copies certified by the issuing authority – this allows examination of all security features that are not immediately obvious and are difficult to replicate (i.e. watermarks and embossing). Photocopied documents are relatively easy to alter and should, therefore, not be accepted as EOI;
b. Verify documents against electronic or other centrally-held records where possible;
c. Preferably accept only documents that are currently valid – a currently valid document is a document that has an expiry date that has not yet passed. Documents that are not currently valid tend to be older and are less likely to contain up-to-date security features, making them easier to tamper with or forge. If expired documents are accepted, authorities should consider requiring additional documents/records to corroborate the details contained in the expired documents. Documents that are not currently valid for reasons other than expiry should not be accepted as supporting the establishment of identity;
d. Accept only full birth certificates – many government authorities worldwide no longer issue short birth certificates as they contain less identity-related information and are less reliable. Full birth certificates list gender and parental details, as well as name, date, place and country of birth. The extra information contained on the full birth certificate can prevent duplication of the authority's records, where two individuals have the same name and biographical information, and gives additional avenues of investigation in cases where an individual claimed identity seems dubious;
e. Unless confirmation of long-term name usage is required, only accept evidence of 'use in the community' documents (documents/records used to meet Figure 1-Objective E) that are less than one year old; and
f. Require documented evidence of any name change – (e.g. deed poll, marriage certificate, or statutory declaration).

If possible, you should verify the authenticity of a document with the issuing authority if there are any concerns.

## 3.4 LEGISLATIVE AND POLICY FRAMEWORK

### 3.4.1 NATIONAL FRAMEWORK

A successful EOI approach is dependent on a national strategic framework that includes:

- A policy framework which provides statements of strategy and objectives (translating the objectives of Governments into outcomes).
- A legal framework that provides the "authority" to do things and penalties for fraud and misuse
- A systems framework comprising of business processes that determine "how" things are done and an ICT framework that determines how technology supports, enables and constrains "how" things are done.
- Organizational structures and relationships that contribute to the achievement of national objectives for EOI.

In best practice jurisdictions, the expression of a Government's intentions in the policy framework is formalized into a set of binding rules in the legal framework, which determines the structure for the systems framework which are supported by organizational arrangements. The framework should cover the EOI principles as described in this guidance.

The national legislative framework should provide clear authority and the parameters of that authority for decision making and eligibility. Legislation needs to consider the privacy of the individual's personally identifiable information, the necessary safeguards and precautions to protect the individual's personally identifiable information and the requirements for sharing the data. This should include who may access the information under what circumstances. Under some circumstances (and with the appropriate controls), information could be shared between States, government agencies and occasionally with the private sector, taking into consideration the relevant data protection laws applicable, and ensuring that data collection and use is necessary and proportionate to the State's desired EOI outcomes.

One of the key considerations for States is whether there is a legislative framework that enables the sharing of data, either within the State or internationally (additional information on data sharing is in Appendix D). Confirming the integrity of identity data for individuals is a key consideration for any State, particularly in relation to the issuance of travel documents.

Legislation and policy must also be aligned with national economic and social development objectives, to ensure that the limited resources available to States are invested wisely, and potentially shared across government to maximize investment and procurement processes.

With a shared vision and common purpose, national authorities are better placed to understand their capability and capacity gaps, and assess their competing investment and development priorities. Without these insights States are more likely to invest in expensive ICT solutions that are an inappropriate response to their national EOI and Border environment.

### 3.4.2 INTERNATIONAL LAW AND TREATY OBLIGATIONS

While issuance of identity documents and processing through Border falls under the legal frameworks of individual States, there are aspects of traveller identification that operate within a framework of international law. An understanding of the interaction between the various components of international law and national circumstances is therefore critical in determining a State's obligations and priorities in relation to EOI. Major UN treaties with direct relevance to traveller identification are included in Appendix C.

In addition to their treaty obligations, States are obliged, under international law, to comply with resolutions made by the UN Security Council under Chapter VII: Action with respect to the threats to the peace, breaches of the peace, and acts of aggression of the UN Charter[7]. Some of these provisions are concerned with regulating travel, and are therefore directly relevant to EOI. UN Security Council Resolution (UNSCR) 2178 (2014)[8] adopted under Chapter VII includes extensive, detailed, specific requirements for Member States to regulate travellers including international data sharing and the responsibility of States to regulate travel not only at entry, but also at exit and transit.

UN Member States who have signed, ratified or acceded to major treaties should meet the requirements of the Chicago Convention and its annexes, and notify differences with ICAO SARPs[9].

7 Chapter VII, Charter of the United Nations, available at: http://www.un.org/en/sections/un-charter/chapter-vii/

8 Threats to international peace and security caused by terrorist acts, S/RES/2178 (2014), United Nations, 2014, available at: http://www.un.org/en/sc/documents/resolutions/

9 As per Article 38 of the Chicago Convention, States must notify ICAO if they: do not comply with a Standard in all respects; do not bring its regulations or practices into full accord with any Standard; adopt regulations or practices differing in any particular respect from the Standard.

# 4 APPENDICES

## A CASE STUDIES

The following two case studies show how you can achieve a high level of confidence in the identity of a person applying for a passport or a conventional travel document.

### A.1 MEETING OBJECTIVES FOR A PASSPORT

Passports are a primary identification document for many people around the world, enabling international travel and allowing people to assert their identity to others with ease. All authorities that issue passports need to make sure they have high confidence in their Evidence of Identity processes to prevent people obtaining passports falsely.

Consider a theoretical travel document issuance authority. After assessing its processes, it has determined that it can achieve high confidence in its individuals' identities with the evidence detailed below.

Due to a lack of electronic infrastructure supporting previous processes, they will need to rely on documentary evidence, the person applying in person, and staff knowledge of the State's culture and other local information.

The authority has a countrywide network of local information sources such as mayors and teachers they can call on to provide details about their areas and help confirm an identity exists or if the individual is using it.

By following these procedures, the authority can have a high degree of confidence for their context. To mitigate risks in their processes, authorities will also need to ensure that:

- staff are well supported for making decisions such as matching images between old and new passports, and assessing information provided by third parties
- information being provided by third parties is accurate and audited regularly
- authorities' records are accurate to make matching of details easier.

| | |
|---|---|
| Objective A<br>Identity Exists | In the first instance, the State's Birth and Citizenship registries are checked. If a record is not found, they will request a birth certificate, or contact local information sources to confirm a birth event took place. |
| Objective B<br>Identity is Living | All customers are required to present themselves to a passport office. This gives confidence that the identity being claimed is living. |
| Objective C<br>Person Links to Identity | Customer's photographs are taken at the offices to link them to the identity. In the case of a renewal, they are matched to the previous passport. When there is no previous passport available, an interview will determine if the customer links to the identity. Questions will be based on information supplied for objective A, and by an information network about the identity being claimed. |
| Objective D<br>Identity is Unique to system and is Sole claimant | Agency records are checked to confirm the identity is not yet claimed. Details such as name, address, birth registration serial number and phone numbers are checked against previous applicants to confirm if anyone else has used them, and might therefore have a claim to the identity. |
| Objective E<br>Identity is used in the Community | The customer is required to provide two documents showing evidence of their identity being used in the community. These are also backed by the local information sources to confirm the identity is actually used. |

### A.2 CASE STUDY: MEETING EOI OBJECTIVES - PASSPORT

The issuance of convention travel document to a refugee poses particular challenges in terms of verifying identity – particularly Objective A (Identity Exists). Refugees may not be able to provide a valid passport and/or other identity documents, as they often arrive at the border or asylum states with only the barest necessities, while stateless persons often lack any kind of identity documents due to lack of registration and/or recognition in their country of habitual residence. Refugees also may not be able to obtain such documents from their country of origin, embassy and/or consulate at their time of arrival or later, as this may put them at risk of serious harm. In the event that a refugee has travelled with a national passport, or is in the possession of any document that can help confirm their identity from their country of origin, the receiving State can still face challenges in verifying the authenticity of such documents, in particular as authorities for the country of origin should not be contacted to verify their authenticity[10].

Refugee and border control authorities will therefore need to rely to a greater extent on of the evidence collected during in-person applications and interviews, as well as staff knowledge of the applicant's country of origin, local culture and other local information. For receiving asylum status, a person only has the right to a convention travel document if he or she is recognized as a refugee in that State. Therefore he or she would normally have undergone a formal refugee status determination procedure (or received prima facie status) in that State prior to requesting a convention travel document.

That means the identity should, in principle, should already have been assessed and recorded/registered.

Establishing uniqueness is the key component to processing an application for a convention travel document. Generally authorities will need to place more emphasis on Objective E techniques ('social footprint') – and utilise regular contact and validation over time to monitor consistency, manage risk and build the identity in the new context.

The starting point may be an interview, a biographic search to ensure that a similar identity is not registered elsewhere, biometric verification for uniqueness, and possibly verification through trusted referees and through possible social footprint evidence obtained from other groups and relatives. In challenging contexts, it may be useful to be able to analyse data and information that may form links between individuals in the system (where appropriate) – as mobilised and vulnerable populations will still have commonalities amongst them that will enable a degree of risk management, and in turn build confidence in some claimed identities over others.

The assessment of an applicant's credibility will be important, and given the humanitarian nature of the situation, different

| | |
|---|---|
| Objective A<br>Identity Exists | Authority may need to register new identity for a refugee or stateless person based on any documents they have or any information provided by them (if he/she is not already registered). This will form the basis for any further identity needs. If possible, check with other agencies who may have interacted with them (such as immigration authorities or authorities conducting refugee status or stateless determination procedures) to help build an identity. |
| Objective B<br>Identity is Living | A refugee or a stateless person will normally need to present themselves in person to give confidence that the claimed identity is living. |
| Objective C<br>Person Links to Identity | Authority should take, at the minimum, a photograph of the refugee or stateless person to link to the identity, and other biometrics if possible. |
| Objective D<br>Identity is Unique to system and is Sole claimant | Authority should make biographic searches on records of other refugees or stateless persons to check for likely duplicate applications, and should employ biometric matching to confirm that the refugee or stateless person doesn't already have an existing identity within the State. |
| Objective E<br>Identity is used in the Community | Refugees and stateless persons who have been in the State for some time may already have a significant social footprint that can support the assessment. Other refugees and stateless persons might not have a community footprint in the asylum state (in particular if they have arrived recently) but evidence may be gathered from among their community, family or relatives through interviews. |

10 See UNHCR, Advisory Opinion on the Rules of Confidentiality Regarding Asylum Information, 2005, para. 5 and 10, available at: http://www.refworld.org/docid/42b9190e4.html.

approaches to EOI will be applied. States are responsible for registering asylum seekers upon their arrival in the country, and to conduct refugee status determination for individuals seeking international protection. These records will very often be the key sources of evidence in terms of verifying the identity of an applicant prior to the issuance of a convention travel document. Other sources may include social footprint in the country of asylum and, when suitable, trusted referees, provided that the confidentiality of the personal data provided by the applicant is maintained during this process.

While the primary responsibility for the registration and determination of refugee status lies with the State, UNHCR will, in certain circumstances, provide support to a State that is unwilling or unable to fulfil these functions. In such situations, UNHCR may also have registration or documentary evidence that can support the verification of identity of an individual prior to issuing a convention travel document.

## B CIVIL REGISTRATION AND VITAL STATISTICS (CRVS)

### B.1 UNITED NATIONS SUSTAINABLE DEVELOPMENT GOALS AND CRVS

The United Nations defines civil registration as the Universal, continuous, permanent and compulsory recording of vital events provided through decree or regulation in accordance with the legal requirements of each country.

In 2016, the United Nations sustainable developmental goals came into force, and among these goals #16.9 States providing legal identity with birth registration to all by 2030. In many countries, large numbers of births go unrecorded and therefore the Evidence of Identity at the time of a travel document application is very weak.

It is therefore important for the Authority to have sufficient background about the existing status of legal identity and civil registration in the State. A number of UN initiatives maintain substantial data about States' CRVS context, and some of this could be useful in a preliminary risk assessment about the status of Evidence of Identity related to various countries.

Vital events that are typically recorded as part of civil registration include: live or still birth, death, name, change of name, marriage, divorce, annulment of marriage, judicial separation of marriage, adoption, legitimization and recognition. As the term indicates these are to be recorded primarily in a register. From this, various legal documents such as birth certificates, death certificates and marriage certificates can be derived. In some countries such information is found not organized as individual records but family registers. Some examples are the Familienbuch (Germany), Propiska (Russia), Hukou (China) and the Koseki (Japan). Some countries also register migration and residential addresses.

While examining a travel document of a foreign State, the nature and status of its civil registration can help assess what steps might be required to determine its reliability. Registration of vital events, of course, impacts the issuance and status of passports, and need to be well understood in order to effectively design an EOI approach to traveller identification.

Besides issuance of travel documents, civil registration impacts legal identity, nationality, social protection and inheritance as well as facilitates access to essential services like health, education, social welfare, employment, voting rights and opening bank accounts.

### B.2 CRVS AS PART OF THE IDENTITY SYSTEM MATURITY MODEL

As CRVS systems get more automated, and updated live data is available in databases, the dependence on physical foundational documents is likely to decrease. However, this might not be uniformly applicable, as even within the same country, some urban centres might provide secured and assured access to such data, while remote rural areas might still have relatively older infrastructure. Also records of older people might not be as orderly and easily authenticated as that of younger people who are born when laws and systems have been brought up to speed.

The following table represents the Identification System Maturity Model and with the current understanding can be taken as the

| Parameters | Nascent | Intermediate | Advanced |
|---|---|---|---|
| Policy | No legal backing | Pending legislation | Legal backing |
| Coverage | <50% | <80% | >80% |
| ID services | Identity | Identity and authentication | Identity, authentication and add-on services |
| Ease of integration | Paper based and system is difficult to integrate | eID gives functionality but limited integration | Services are defined and support provided to third-party users |
| Deduplication | Demographic | Biometric | Multi-biometric & demographic |
| Privacy | No law to ensure privacy | Law exists but no penal provision to prevent profiling | Penal provision and law supports prevention of profiling |
| Form factor | Paper-based | Chip-based | Form-factor agnostic |
| Linkage with CRVS | Not linked | Process of linkage in progress | Fully linked |

path for improving existing systems. This kind of framework can assist States when considering the maturity of another State's identity management infrastructure.

### B.3 CRVS REFERENCE MATERIAL

World Bank Group and Centre for Global Development (CGD), February 2017. Principles on Identification for Sustainable Development; Towards the Digital Age; http://documents.worldbank.org/curated/en/ 213581486378184357/Principles-on-identification-for-sustainable-development-toward-the-digital-age

United Nations Statistical Division (UNSD). 2014. Principles and Recommendations for a Vital Statistics System – Third Edition, https://unstats.un.org/UNSD/demographic/standmeth/principles/M19Rev3en. pdf

Harbitz, Mia and Kentala, Kristo. 2015. Dictionary for Civil Registration and Identification, Government of Canada and Inter-American Development Bank (IDB).

Harbitz, Mia and Gregson, Kendra. 2015. Toward Universal Birth Registration - A Systemic Approach to the Application of ICT, UNICEF and IDB. https://www.unicef.org/protection/files/ICS_CoPUB_Toward_Universal_Birth_Registration.pdf

Mills, Samuel (World Bank Group and Global CRVS Group) and Jagannathan, Sheila (World Bank Group and Open Learning Campus). 2017. Launch of the state-of-the-art Civil Registration and Vital Statistics (CRVS) eLearning course, http://www.getinthepicture.org/news/launch-state-art-civil-registration-and-vital-statistics-crvs-elearning-course

World Health Organization (WHO). Civil Registration and Vital Statistics (CRVS) website. http://www.who.int/healthinfo/civil_registration/en

Sanjay Dharwadker. April 20, 2017. CRVS, Deming Dual and the Forty-Five Pregnant Women, https://sanjaydharwadker.org/2017/04/20/crvs-deming-dual-and-the-forty-five-pregnant-women/

Manby, Bronwen. Open Society Foundation, 2010. Citizenship Law in Africa, A Comparative Study, http://www.unhcr.org/protection/statelessness/4cbc60ce6/citizenship-law-africa-comparative-study-bronwen-manby.html

## C REFERENCES TO RELEVANT INTERNATIONAL LAW

An important objective of the UN is "to establish conditions under which justice and respect for the obligations arising from treaties and other sources of international law can be maintained"[11].

Major UN treaties with direct relevance to EOI for TRIP include:

- 1944 Convention on International Civil Aviation, which led to the establishment of ICAO;
- 1951 United Nations Convention Relating to the Status of Refugees (and the 1967 Protocol Relating to the Status of Refugees);
- The 1954 Convention relating to the Status of Stateless Persons;
- 2000 United Nations Convention against Transnational Organized Crime (and the 2000 Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children and the 2000 Protocol against the Smuggling of Migrants by Land, Sea and Air), administered by United Nations Office on Drugs and Crime (UNODC).1948 Universal Declaration of Human Rights and the core international human rights instruments whose implementation fall under the broad responsibility of the United Nations Office of the High Commissioner for Human Rights (OHCHR).

The Refugee Convention and its Protocol, the Statelessness Convention, the Convention against Transnational Crime and the human rights instruments whose implementation are the broad responsibility of UNHCR, UNODC and OHCHR respectively, share as their focus the protection of the vulnerable. Their application in EOI and border management is critical to ensure that the basic human rights of vulnerable travellers, including victims of various kinds of exploitation, are protected. The OHCHR has published Recommended Principles and Guidelines on Human Rights at International Borders whose implementation ensures protection of these rights[12].

## D DATA AND INFORMATION SHARING

The exchange of data and information is becoming more common in the travel document and border communities, as authorities look to identify and validate individuals with greater degree of certainty.

Information may be shared between States, government authorities and occasionally with the private sector, taking into consideration the relevant data protection laws applicable.

The focus of data sharing for the State is to:

a. enable issuance (validation of documents or data that relate to the establishment of identity, such as birth or citizenship);
b. facilitate travel (sharing passport information with border

11 Preamble Charter of the United Nations, United Nations, San Francisco, 1945, http://www.un.org/en/charter-united-nations/index.html

12 Recommended Principles and Guidelines on Human Rights at International Borders, OHCHR, 2014, available at: http://www.ohchr.org/Documents/Issues/Migration/OHCHR_Recommended_Principles_Guidelines.pdf

authorities) and using the ICAO PKD; API, PNR and Interpol information; and

c. prevent misuse of travel documents (sharing watch-lists and lost/stolen data).

One of the key considerations for States is whether there is a legislative framework that enables the sharing of data, either within the State or internationally. Confirming the integrity of identity data for individuals is a key consideration for any State, particularly in relation to the issuance of travel documents.

### D.1 DATA ACCESS AND MATCHING WITHIN THE STATE

For documents and records used to establish that an identity exists (such as birth or citizenship records), the Authority can try to validate identity information at the source registry, to enhance the integrity of the identity validation process. This access can be online in real-time, or as part of a manual checking process.

A number of States operate Data Validation Services; these are generally web-based services that enable authorities to validate the authenticity of data on a named individual's identity documents, or the data that the individual has provided.

Public sector authorities can also undertake what is termed 'data matching', where a comparison is undertaken with another authority's databases to verify information, or identify discrepancies[13]. Authorities have particular interest in birth, death and citizenship information to gain confidence that the identity exists and is living (see objectives A and B under EOI Principle 1). If the Authority can access this information directly, documentary evidence for these establishment events may not be required. Such services increase the Authority's confidence in the documents and records they require and can facilitate a more streamlined and efficient enrolment process by removing or reducing the need for an applicant to provide documentary evidence– therefore reducing the exposure to counterfeits.

Where possible, the Authority should attempt to access and leverage other government authorities that collect identity information (which can include biometrics). As noted in sections on EOI and social footprint, information from authorities responsible for products or services such as driver licenses, healthcare or the electoral role can provide valuable information to corroborate the existence and use of an identity. Data matching against other authorities' databases can streamline this social footprint process. Although it is of huge benefit to check or validate every applicant and their documents, this is not always practical in states where the validation process is manual or labour intensive. In these circumstances, Authorities can focus efforts on high risk applications, based on a predetermined risk profile.

### D.2 DATA SHARING (INTERNATIONAL AND REGIONAL)

Accepting a travel document as a token of identity at an international border requires the border control agent to address two questions:

a. Does the document belong to the person providing it?
b. Is it an authentic document and not falsified in any way?

Only after receiving positive answers to both questions, can the border control agent assess whether this document entitles its rightful bearer to enter the country. The idea behind this process is to trace the document's validity and authenticity back to its issuing authority. The usual way of answering these questions is by visually comparing the portrait photo with its owner, and analysing physical security features of the document. Although this type of document examination is still entirely valid and useful, electronic data shared regionally or internationally can make the validation of travel documents even more effective.

Governments have recognized that cooperation is the key to answer these questions, to ensure safety and security for citizens and travellers. To that end, some international organizations have developed processes for sharing and transmitting data and information to maximize resources to identify individuals. Systems such as Interpol's Stolen and Lost Travel Documents (SLTD) database, APEC's Regional Movement Alert System (RMAS), and Advanced Passenger Information system (API) are exemplary of this trend. As globalization continues to grow, the movement towards international collaboration on security solutions will steadily increase.

The ICAO PKD Directory, which enables the exchange of digital certificates for the validation of ePassports, is also an important example of international cooperation for the purposes of travel document and border security.

Several Bilateral, regional and international partnerships have been established worldwide to improve cooperation and sharing of data between allies, and to facilitate border crossing between neighbour States. Examples include the Shengen Area, MERCOSUR, ECOWAS, and CARICOM. In addition, many States have a neighbouring country where their citizens regularly travel in large numbers, and data sharing will directly benefit both parties.

In some cases information sharing may not be recommended. This is especially relevant for asylum-seekers and refugees, in which case information sharing - particularly with the individual's country of origin - could place such individuals or their family members at risk. Personal data on a refugee or asylum-seeker should therefore never be communicated to or double-checked with the authorities from that person's country of origin, including embassies and consulates[14]. However some States share refugees' biometric with neighbouring authorities to ensure there is one unique identity (see the EU Eurodac system).

13 See the Australian Government's Data Matching: Better Practice Guidelines at www.ag.gov.au

14 See ICAO/UNHCR, Guide for Issuing Machine Readable Convention Travel Documents for Refugees and Stateless Persons, February 2017, paragraph 20, available at: http://www.refworld.org/docid/52b166a34.html.

# E ASSESSMENT OF AVAILABLE EVIDENCE

## E.1 ASSESSING THE IDENTITY CONTEXT

Before an authority redevelops any issuance processes with an EOI approach, the following points require consideration.

Firstly, the EOI approach focuses on understanding and using the information gained from various types of evidence to gain a level of confidence, rather than absolute proof. Using the principles and objectives as a guide, an authority can effectively balance risk with facilitation, at the same time as designing a process that is responsive to the complexity and diversity of modern identity within a State's own context.

Secondly, the EOI model can only be effective when grounded in methodical risk awareness, assessment, and assurance. Travel document authorities need to identify weaknesses in their current issuance processes that may be targeted and exploited in order to facilitate identity-related crime and /or other malicious activity. Authorities should always look to interrogate their own databases using tools and techniques such as data mining, risk profiling, biographic and biometric matching. An EOI approach assists an authority in addressing any weaknesses in their processes by aligning thorough threat and risk assessment with the evaluation of evidence.

The efficacy of a risk-aware EOI approach is reliant upon an authority being able to accurately determine the reliability, legitimacy, and value of each piece of evidence (whether this be in the form of documentation, information from databases, or evidence of social footprint). This requires an understanding of the registration and issuance processes which produced that evidence, in order to understand how much confidence can be gained from its inclusion (see Appendix B: Civil Registration and Vital Statistics).

For example, if an authority is considering use of a driver licence to support their travel document issuance processes, it will need to understand how robust the driver licence issuance process is. An assessment can then be made to determine its reliability, and therefore the extent to which it can be used as evidence. Depending on the availability and the quality of the driver licence database, it could be used for matching against records. Direct matching to the license database will help validate that the claimed identity exists (Objective A). Otherwise, authorities may only be able to rely upon it as evidence of use in the community (Objective E).

The inherent 'value' of a document or record to an identity process will differ from State to State. A birth certificate may be acceptable evidence that an identity exists in some States, whereas other States may have very little confidence in the registration processes or the documents produced by some or all of their registry offices. If an authority has less confidence in the integrity of their State's birth registration process or the accuracy of their birth registers, they might place more emphasis on other evidence. For example, for many States evidence that shows the use of the identity in the community (their social footprint) may be as reliable as birth certificates. In this case, the authority might increase the amount of evidence required to meet Objective E.

The result of such an approach is a travel document imbued with a high degree of integrity and identity assurance. This has a direct impact on the ability of border control authorities to identify travellers confidently as they move across borders. It follows then that the integrity of a State's travel document relies upon its robust EOI standards, as much as the security of the physical document itself.

EOI processes are also likely to be subject to ongoing amendment and modification to take account of environmental changes such as:

- policy changes
- new information about methods of misuse and abuse of identity
- changes in the processes to obtain identity-related documents
- new technologies.

Authorities should use this quick assessment tool as a basis for considering identity evidence available. It works through each objective from Section 2 of this guide. Authorities can work through items that are relevant and check the instructions at the end to assess whether there an acceptable level of confidence, or whether there is need to strengthen procedures or gain access to additional information.

## E.2 QUICK ASSESSMENT

The following page has a useful quick assessment tool. There are three tables that correspond to the three EOI principles.

Use Table 1 to determine which foundational documents are available to you. If there are other foundational documents or information that could increase confidence that is not listed, add it to the available documents section. For each document type, note if it is available and how (short form, full, electronic etc.). Also note if you can verify the document at the source - i.e. electronic connection to issuing agency.

Use table 2 to assess if the authority can perform any of the checks or measures associated with each evidence type. Write the total number in the right-hand column. If there are any additional methods or measures not listed, describe them in the space below, and add them to the total for the relevant objective.

Use table 3 to check which foundational documents or information are available from those listed. If the authority has additional documents or methods, note them in the space for other available documents below.

Table 1:

| | | Foundational Document | Available as? | Source Verified? |
|---|---|---|---|---|
| Principle 1: Existence of Identity | A: Identity Exists | 1: Birth Registration | | |
| | | 2: Citizenship Registration | | |
| | | 3: Marriage Registration | | |
| | | 4: Name Change Records | | |
| | | 5: Divorce Records | | |
| | | 6: Adoption Records | | |
| | B: Living Identity | 7: Death records | | |
| | | 8: Equivalent checks | | |
| | Additional Evidence | | | |

Table 2:

| | | Foundational Document | Checks and Measures | | | | Number of checks available |
|---|---|---|---|---|---|---|---|
| Principle 3: Presenter uses Identity | C - Applicant links to the identity | 1: Assertion by a referee | Known by Authority | Matches your database? | Referee trusted by your authority | Matches a trusted group of people | |
| | | 2: In-person verification | Self-Supplied Photo ID? | Trusted photo-ID authorities | Are they in the authority's records? | Staff trained in document comparison | |
| | | 3: Biometric recognition | Applicant photo database | Other biometrics databases | External authority databases | Historic biometric information | |
| | | 4: Interview | Staff trained to conduct interview | Information on applicant sufficient | Enough capacity and infrastructure | Policy on acceptance of evidence | |
| | D – Sole claimant to unique identity | 5: Check authority records | All applications recorded | Staff trained in identifying records | Systems for data matching | Historic records available | |
| | | 6: Biometric recognition | Photographs of all applicants | Availability of historic biometrics | Biometric comparisons | Other biometrics stored | |
| | Additional Evidence | | | | | | |

Ta ble 3:

| | | Foundational Document | Available as? | Source Verified? |
|---|---|---|---|---|
| Principle 3: Presenter uses Identity | E – Presenter uses identity in the community | 1: Internal Authority Records | | |
| | | 2: Referee Declaration | | |
| | | 3: Bank Statements | | |
| | | 4: Utility Statements | | |
| | | 5: Motor Vehicle Registration | | |
| | | 6: Education Records | | |
| | | 7: Electoral Roll | | |
| | | 8: Work Records | | |
| | | 9: Social Media Checks | | |
| | | 10: Tax Records | | |
| | | 11: Benefit Records | | |
| | Additional Evidence | | | |

### E.3 CONFIDENCE LEVEL

Use the following table to assess the level of confidence you can gain from the previous tables. Check the ratings column for each objective and write the level in the final column.

| | Ratings: | Confidence level |
|---|---|---|
| A: Identity Exists | **High Confidence:** All items 1 through 4 are available in short-form, full or electronic form, with source verification, and where required, 5 and 6 are available.<br>**Medium Confidence:** All items 1 through 4 are available in some form without source verification<br>**Low Confidence:** Any of items 1 through 4 are available in some form. | |
| B : Living Identity | **High Confidence:** Item 7 or 8 is available in some form, and can be verified with the source registry.<br>**Medium Confidence:** Item 7 or 8 is available in full or electronic form, with no source verification.<br>**Low Confidence:** Item 7 or 8 is available as a short-form document only, with no source verification | |
| C: Applicant links to the identity | **High Confidence:** At least 3 checks or measures are available for item 1 or item 2, or both items 3 and 4<br>**Low/Medium Confidence:** If you are able to perform item 1 or Item 2 or both items 3 and 4 you will have high confidence. If none are available, you cannot have any confidence in meeting this objective. | |
| D – Sole claimant to unique identity | **High Confidence:** At least 3 checks available for either of Item 5 AND 6.<br>**Medium Confidence:** At least 3 checks available for either of Item 5 OR 6.<br>**Low Confidence:** There is no low confidence for this objective - meeting either method provides medium confidence. | |
| E – Presenter uses identity in the community | **High Confidence:** Item 1 or 2 is available in full or electronic form and at least 2 of items 3 through 11 are available in some form.<br>**Medium Confidence:** At least 2 of items 3 through 11 are available.<br>**Low Confidence:** At least 1 of items 3 through 11 is available | |

## F TRUSTED REFEREES

### F.1 WHO CAN BE A REFEREE?

To ensure that a trusted referee can effectively verify an identity, a trusted referee must have the following two attributes:

a. Have personal knowledge of the individual: trusted referees must have a personal knowledge of the applicant in order to verify personal elements relating to the identity of an individual. As such, a trusted referee should know the applicant for a minimum of 12 months.
b. Be trusted by the authority: the authority may trust the ability of an individual to act as a trusted referee if the authority has already established the identity of the trusted referee. Therefore, the issuing authority may require that trusted referees hold a valid document ensuring that the authority has already verified the personal information of the referee. This requirement may prevent a trusted referee from fraudulently verifying an identity. It can also help the authority make links between persons of interest.

The authority may designate certain professionals or public figures to act as referees, who would have had continual personal interactions with an individual over an extended period of time, have records of the individual, and would be able to accurately verify an identity of an individual. It is recommended that professions or public figures be selected that maintain records that can be verified of the individual's membership within a recognized organization or community. Professions or positions designated by authorities could include lawyers, government personnel, doctors, religious personnel, teachers etc.

The authority may allow other individuals to act as trusted referees who have personal knowledge of an individual and who are in a position to confirm an identity such as community elders or district administrators. To gain trust in an individual's ability to act as a trusted referee, the authority should require an individual to provide adequate evidence to confirm their identity and ability to act as a trusted referee.

To ensure confidence in the verification of the identity of an individual and to prevent fraudulent verification of identities by trusted referees, authorities should require that trusted referees:

- be unrelated to the applicant
- are not the applicant's partner or spouse
- do not live at the same address as the applicant
- be older than 18

- provide an address and phone number, and be available for contact by the document issuing authority
- have known the applicant for a specific amount of time (e.g. 12 months or more) and
- are not being paid to verify an identity.

### F.2 WHEN CAN A REFEREE BE CONTACTED

An authority should establish risk based criteria to determine when to contact a trusted referee. As a part of their process to establish an identity, an authority may want to contact a trusted referee to determine if an identity exists (Objective A), to determine that an applicant links to the identity (Objective C) or to determine the identity an applicant uses in the community (Objective E).

An authority may contact a referee when additional identity verifications are needed to accurately identify an individual such as in the following cases:

- The issuance processes for foundational documents are not trustworthy;
- An applicant does not have foundational documents;
- An applicant has limited supporting documentation displaying the identity used in the community;
- Integrity concerns exist with an application for a travel document (i.e. urgent service, missing information in application).

### F.3 WHAT INFORMATION IS ASKED OF THE TRUSTED REFEREE

Contacting trusted referees is integral in processing an application. In addition to verifying information provided by the applicant, a trusted referee may provide pertinent information that may not have been initially divulged by the applicant (i.e. additional information regarding eligibility for a travel document such as citizenship status, or criminal activity.)

To verify an applicant's identity, referees should be asked broad questions which allow the issuing authority to gather information for processing an application. The following questions may be asked:

- Place of Birth information;
- General information about the applicant;
- Where the applicant lives;
- Relationship of the trusted referee to the applicant;
- Names used by the applicant in the community.

## G RISK ASSESSMENTS

### G.1 MAJOR RISK AREAS

Types of risk consequences that can arise from the incorrect attribution of identity include:

a. Financial loss or liability: the result of incorrect attribution of identity can cause significant problems for any affected party. For example, a benefit payment to any person who uses a stolen or fictitious identity and who is not entitled to receive that benefit creates a direct financial loss to the Government. At worst, this could cause severe or catastrophic unrecoverable financial loss to any party, or severe or catastrophic authority liability.
b. Inconvenience, Distress or Damage to Existing Reputation: the result of incorrect attribution of identity can inconvenience, distress, or damage the standing or reputation of any party in number of ways. For example, a stolen identity will have a significant impact on an individual's ability to participate effectively in the community and to receive the services they are entitled to. Widespread misuse and abuse of identity could also potentially impact negatively on the international reputation of the State, leading to a reduction of investment in businesses and migration, and increased difficulty in obtaining visas.
c. Harm to Public Programs or Public Interest: incorrect attribution of identity has the potential to disrupt the effectiveness of authority programmes. This may result in a negative public or political perception that some people are not receiving the services from these authorities that they are entitled to or that people who are not entitled are receiving authority services. At worst, this could cause a severe or catastrophic adverse effect on authority operations or assets, or public interests, including severe function degradation or loss to the extent and duration that the authority is unable to perform one or more of its primary functions, and major damage to authority assets or public interests.
d. Unauthorized Release of Sensitive Information: can result in loss of confidence in an authority and directly result in or contribute to negative outcomes for the affected individual (e.g. personal safety, financial loss, job loss). Personal information needs to be protected, appropriately and closely managed. At worst, a release of in-confidence, sensitive information or information with a national security classification to unauthorized parties can result in loss of confidentiality with a high impact.
e. Domino Effect of an Improper Identity Document Used to Acquire Services of Third Party or Another Document: incorrect attribution of identity can impact on authorities other than the authority delivering the service. For example, a passport that is issued to a fictitious identity could be used as the basis for fraudulent activities that directly impact on other government or non-government organizations. Further negative consequences could result if, for example, the holder of that passport uses it to gain illegal access to another country to commit an unlawful act.
f. Personal and Public Safety: incorrect attribution of an identity for an individual can compromise personal safety. For example, an individual incorrectly provided with a passport using a fictitious or stolen identity could commit acts of terrorism, where there is a risk of serious injury or death. These types of risks have severe and lasting consequences for any State.

These types of risks can have significant impacts on numerous parties, including government authorities, the individuals whose identities have been stolen, other organizations (both government and non-government) and the public. These impacts may be extremely negative for those affected.

### G.2 THREATS AND RISK ASSESSMENTS

It is recommended that the Authority take appropriate action to risk manage the security threats and vulnerabilities to its identity establishment and validation processes.

Regular threat and risk assessments are important as they help determine current threats to the system and identify which processes, systems and areas are most at risk. Assessments lead to recommendations for prevention and mitigation measures that will reduce risks to acceptable levels.

Threat and Risk Assessments Involve:

a. establishing the scope of the assessment;
b. determining the threat and assessing the likelihood and impact of threat occurrence;
c. assessing the risk based on the adequacy of existing safeguards and vulnerabilities; and
d. implementing any supplementary safeguards to reduce the risk to an acceptable level.

Threats and the underlying reasons for attempts at fraud may differ significantly from State to State and even region to region. It is also important to note that threats also come from internal sources and the Authority needs to ensure that processes and systems for supporting staff and managing risks for misconduct and corruption are covered. The people who work with the systems and procedures for establishing and validating identity are those who know best where the threats and weaknesses are in the system. It is wise to ask staff what they think the vulnerabilities are and what should be done to minimize them.

Reporting of concerns should be encouraged and there should be appropriate recognition for those who identify problems. It is good practice to maintain statistics on threats or risks that materialize, to focus resources on making changes in the process to prevent future incidents or attacks of a particular type. The Authority must continuously monitor for any change in the threat environment and make any adjustment necessary to maintain an acceptable level of risk and a balance between operational needs and security.