INTERNATIONAL CIVIL AVIATION ORGANIZATION

MACHINE READABLE TRAVEL DOCUMENTS (MRTDs)

TOWARDS BETTER PRACTICE IN NATIONAL IDENTIFICATION MANAGEMENT

Guidance Material (Guide)

Version: Release 3

Status: Draft 5
Date: 30 April 2013

File:	Evidence of Identification (EOI)
Author:	New Technologies Working Group (NTWG), Subgroup on Evidence of Identity Initiative

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

ICAO has an interest in travel security and has in the past concentrated on the security of travel documents. However, ICAO's interest in this area is wider and its goal is to ensure that a consistent level of security and integrity applies to all components of the 'travel continuum' namely the: application, examination and decision processes, document printing, personalization and issuance, travel document itself and use of the travel document at border control points.

Therefore, this Guidance Material (referred to hereafter as the Guide) highlights the need for consistent efforts concerning all aspects of the travel continuum. It suggests that the examination and decision processes, and particularly the establishment of confidence in a person's identity within this process, is an area which can easily fall behind in the strength of its security when compared with that of the document itself. It proposes measures in different areas of interest throughout the issuance process where a higher level of confidence may be achieved.

The Guide does not set standards for how confidence in a person's identity should be established by relevant authorities. This will vary from state to state, dependant upon on local laws and legal framework, customs, and the nature of which 'foundational' documents are used. Throughout this Guide, the terms "breeder documents," "foundational documents" and "source documents" are used interchangeably as the documents of evidence of identification. The Guide sets out a framework of outcomes to be achieved in order to assure confidence in a person's identity prior to issuing individuals a travel document.

2. INTRODUCTION

2.1 BACKGROUND

The rapid growth of identity fraud affects many areas of society and raises serious concerns for security and safety. Much work has been done in the area of travel documents to combat document fraud and increase passport security and the associated systems for the personalization and issuance of these documents. Border authorities have upgraded their document inspection systems and passenger checks to improve security at border control points, providing increased security from both ends of the travel continuum. The increase of international data sharing and use of new technologies, including the ICAO Public Key Directory (PKD), has resulted in improved capabilities toward fraud detection.

These measures have been very successful in raising the level of passport security. However, they have resulted in the shift away from travel document fraud (alteration, counterfeit) toward attempts to obtain a genuine passport based on false identities. This effect has further highlighted the risks of fraudulently obtaining a genuine passport.

The ability of a criminal to perpetrate this and other similar types of fraud relies upon deceiving the authorities into accepting a bogus identity during the application (enrolment) process. This process requires, among other things, the applicant to provide "evidence of identification" in order to substantiate and justify the claim of entitlement. Often, to accomplish this, applications are accompanied by documentation, generally known as breeder or foundational documents.

ICAO's goal in drawing attention to the need for security and integrity in the application and enrolment for travel documents is to achieve a consistent level of security and integrity across the travel document continuum. The document itself needs to be secure, the issuing processes need to be methodical and of high integrity and the checks made on a document at borders need to be thorough and trustworthy.

2.2 RATIONALE FOR ICAO'S INVOLVEMENT IN EVIDENCE OF IDENTIFICATION

Many ICAO Member States have invested time, money and great expectations in enhanced travel document programs, specifically machine readable ePassports. The International Civil Aviation Organization (ICAO) MRTD (Machine Readable Travel Document) Programme has guided the travel community toward increased security improvements for the physical document and its use at border control points. The current generation of ICAO-compliant travel documents are very secure.

Fraudsters will generally seek the path of least resistance. This may be in some cases the issuance process. The targeting of the issuance process can damage reputational gains made by increasing the physical security of the travel document. It also undermines the state's financial investment in improvement of secure technology. If there are gaps in the process that make it easier to secure a Falsely Obtained Genuine (FOG) document, then the fraudsters will seek this method, rather than forgery. The resulting document is genuinely issued by the Travel Document Issuing Authority (TDIA), which can be validated against source data and less likely to be detected than a fake, altered or counterfeit document.

The basis for a TDIA's secure issuance process is therefore the documents, civil registry records, databases, and other media that are used to validate an applicant's identity. Identity management is the

gathering, verification, storage, use and disposal of this kind of identity information, and robust identity management is one of the keys to producing a secure travel document.

TDIAs need effective strategies and frameworks for managing and evaluating identity information for establishing identity, and supporting quality decision making processes with regard to applications for travel documents.

2.3 ICAO'S MANDATE ON EVIDENCE OF IDENTIFICATION

ICAO's mandate with respect to evidence of identification 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 TDIA is one of the most important authoritative sources of identity information. It is therefore the establishment of identity, and validation of identity, that ICAO is most focussed on – and largely for the purposes of security. Identity fraud is an enabler for a range of criminal activities, from organized crime to terrorism. Weak identity management processes in the travel document issuance and border sector will be targeted to facilitate these activities. If States do not undertake the necessary steps to identify individuals effectively, the repercussions can be extremely serious. As an authoritative source, the state agency has an obligation to ensure that identity is established with a high degree of assurance.

ICAO's mandate on developing guidance material related to better practice in national identication management refers to ICAO Assembly Resolution A37-20, Appendix D – *Facilitation*, Section II, recognized that a passport is the "basic official document that denotes a person's identity and citizenship and is intended to inform the state of transit or destination that the bearer can return to the state which issued the passport." To achieve this, the Assembly Resolution also underscored the importance of maintaining international confidence in the integrity of the passport as an essential function of the international travel system and that the veracity and validity of machine readable travel documents depends on the documentation and processes used to identify, confirm citizenship or nationality and assess entitlement of the passport applicant.

2.4 PURPOSE OF THIS GUIDE

This main purpose of the Guide is to provide guidance material and is not to set Standards and Recommended Practices (SARPs) as adopted by the ICAO Council in accordance with Articles 37, 54 and 90 of the Convention of the International Civil Aviation and designated, for convenience, as Annexes to the Convention (as in example, Annex 9 – *Facilitation*, containing SARPs on the issuance of MRTDs). The Guide is intended to be used by individuals and agencies engaged in the full spectrum of identity management; including the staff of issuing authorities, inspection, police and immigration authorities. As well as those engaged in other document entitlement endeavours including: issuers of driving licenses, national identity cards, voter registration, etc. In particular, the Guide is especially relevant to those involved in civil registry and other vital records-related management activities in order to encompass the very important and pivotal role performed by those engaged in numerous related entitlement functions such as those related to: birth and death records, citizen records, marriage and divorce records and other civil registry matters.

2.5 SCOPE

The scope of the Guide is to provide States with guidance on establishing evidence of identification in order to properly and uniquely identify individuals for the purposes of issuing trusted travel documents and contribute to overall security worldwide. It focuses on the need to achieve certain outcomes required for establishing identity and evidence that the:

a) claimed identity is valid (i.e. identity exists and that the owner of that identity is still alive);

b) presenter links to the claimed identity (i.e. person can be linked to the claimed identity and that they are the sole claimant of that identity); and

c) presenter uses the claimed identity (i.e. that the claimant is operating under this identity within the community).

The Guide is not prescriptive in how to establish each of these goals. Each state may use all or a combination of the means used to establish evidence of identity including civil registration and "social footprint" checks (evidence that the person uses their claimed identity in the community), and foundational documents.

3. EVIDENCE OF IDENTIFICATION (EOI)

Evidence of Identification (EOI) refers to the establishment of evidence that, when combined, provides confidence that an individual is who they claim to be (i.e. a driver's licence, passport and birth or citizenship certificate).

In recent years, a significant amount of work has been undertaken in the EOI field, with a number of frameworks and guidance documents produced internationally.[1] EOI frameworks provide a conceptual basis upon which agencies can design a robust process to establish, verify and manage identity information.

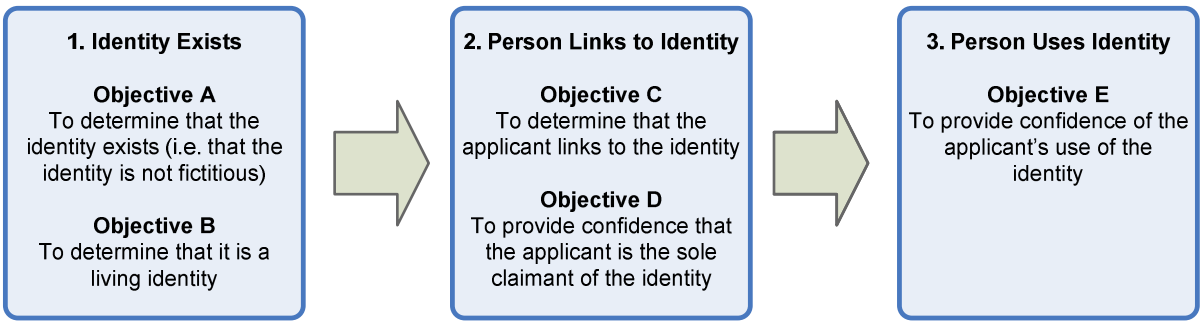
A basic premise of most EOI frameworks is that the amount of confidence an agency requires before they provide an identity-related product or service should be proportional to the risks and downstream effects that result from the incorrect or improper attribution of an identity.

As there is a HIGH degree of risk associated with issuing travel documents and processing people through borders, relevant agencies need a HIGH degree of confidence that they are properly and uniquely identifying individuals.

[1] See the New Zealand Government's *Evidence of identification Standard* and *Identity Assurance Framework for Government* at www.dia.govt.nz, the Australian Government's Gold Standard Enrolment Framework in its National Identity Security Strategy at www.ag.gov.au, and the NASPO ID-V Project http://www.naspo.info/PDFiles/ID-V_Project.pdf. The APEC Business Mobility Group has completed their *Framework for Assuring Identity in the Issuance of Biometric Machine Readable Travel Documents*, and ISO are designing a Standard for 'Entity Authentication Assurance.'

Figure 1 outlines the three key principles (1 to 3) and five underlying objectives (A to E) that are central to most EOI framework or standards, and should be central to the EOI processes a Travel Document Issuing Authority (TDIA) or Border Control Authority (BCA) undertakes as part of its issuance processes:

FIGURE 1



As previously mentioned, it is impossible to be prescriptive on how to achieve these key principles and their objectives as they are dependent on each state's customs, working practices and legal frameworks and will likely differ from one state to another. However, TDIAs should ensure that they can show that they have processes and policies in place to meet all these objectives or that other measures are in place to achieve such level of confidence.

A robust and secure travel document issuance process should seek to fulfil each of the three principles to a HIGH level of confidence, especially the first time a travel document is issued to that person. If the first interaction is strong, then the TDIA can leverage the strength of the first issuance process for subsequent interactions such as a renewal application, or the replacement of a lost or stolen passport.

The first EOI principle **Identity Exists** requires the TDIA to be confident that the identity exists and is living. This process is sometimes referred to as 'proving'. TDIAs should be confident that an actual person was born in that identity (e.g. is not fictitious), and that the identity is not deceased.

To meet the objectives under EOI principle one (1. Identity Exists) it is suggested that the TDIA:

a) ask the applicant for documents which prove that their identity exists (i.e. birth or citizenship certificate). These documents should ideally be validated against source data to combat the risk of forged foundational documents; and

b) check death records to guard against fraudulent applicants using the identity of a deceased person, if possible.

In some states foundational documents may not be required due to the availability of electronic access to birth records, which negates the risk of counterfeit and forged documents.

The second and the third principles (2. **Person Links to Identity** and 3. **Person Uses Identity)** are often collectively referred to as 'linking'. The TDIA should be confident that the person applying is

legitimately linked to the identity, and that the identity is not already in use (e.g. the applicant is the sole claimant of this identity). This aims to stop fraudsters 'hijacking' legitimate identities.

To meet the objectives under EOI principles 2 and 3, it is suggested that the TDIA:

a) Check available agency databases to ensure there is no record of a duplicate applicant claiming that same identity (biometric matching is advised to detect whether the applicant has a travel document under a different name); and

b) undertake checks to establish the social footprint identity (i.e. evidence that the person uses their claimed identity in the community by means of the electoral roll, banking and utilities statements, tax and social security numbers, healthcare registered, motor vehicle registration and education records).

Although the EOI principles outlined in the previous section are broad enough to apply in any state, each TDIA will face different challenges in relation to evidential requirements, for example:

a) states with smaller populations may be unable to interview all applicants (e.g. insufficient infrastructure and/or staff);

b) there may be multiple valid versions of foundational documents available for use (e.g. birth and/or death certificates);

c) legislation may prevent validation of documents, access to source registers or information sharing between government departments and states;

d) historic travel or foundational document records may be paper based – leading to a lengthy manual checking process; and

e) databases of information may be application based rather than person centric – making it difficult to match various historical applications under the same identity.

Regardless of these challenges, TDIAs can still establish robust issuance processes by utilizing a range of documents and records to build confidence in an identity.

Before any issuance processes are redeveloped, TDIAs need first to understand the three basic EOI principles and what information is available for incorporation into their issuance processes. TDIAs need to investigate all available documents and records that could be used to establish identity for the purposes of issuing a travel document. This includes having an in-depth understanding of the issuance and registration processes of all foundational documents and records, in order to understand how much confidence can be gained from the document/record's inclusion in the EOI process.

For example, if a driver's licence is being considered as a document to support a State travel document issuance process, the TDIA needs to understand how robust the drivers licence issuance process is and the quality of the drivers licence database for matching against records.

The TDIA can then assess whether access to the driver's license database will help prove that the claimed identity exists or that it can only be relied upon as evidence that the identity is used in the community.

Finding out additional information relating to the EOI document or record can also be useful. For example, if a TDIA knows an applicant has consistently held a driver's licence in the same name for a number of years, they may have a higher level of confidence that their identity is legitimate.

TDIAs deal with a range of documents and have varying degrees of confidence in their legitimacy, or the legitimacy of the information on them. The inherent 'value' of a document or record to an EOI process will differ from state to state. For example, 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 a TDIA has less confidence in the integrity of their state's birth registration process or the accuracy of their birth registers, more emphasis might be placed on other EOI documents. For example, for many states documents that show the applicant uses the identity in the community (e.g. social footprint) may be more reliable than birth certificates; therefore the number of documents/records required to meet Objective E – Figure 1, may be increased beyond the example given in Table 1 - Evidential Requirements for EoI Objectives (following page). The social footprint evidence can support claims that the applicant links to the identity, especially where there is no other evidence available. However, we should bear in mind that the use of an identity must not always be the proof of its legitimacy (e.g. occasionally persons are known by acquaintances and local authorities by a nick name or another assumed name for many years).

It is important to understand that issuance processes should not be totally reliant on document and register checks to gain confidence in an identity. Once the foundational document and processes are understood, states then need to consider what gaps likely exist to be and how other back-office processes can support the identification process. TDIAs should always look to interrogate their own databases using tools and techniques such as data mining, risk profiling and biometric matching.

Diagram 1 – Example of Business Process for Establishing an Individual's Identity.

TABLE 1 - EVIDENTIAL REQUIREMENTS FOR EOI OBJECTIVES

EOI Objective	Example Evidence Required for High Confidence
A – Identity exists	1-2 documents which, where possible, have been validated against source records held by the issuing agency or authenticated by staff trained in document recognition. If possible, at least one document/record should contain a photograph. or Verification against 1-2 source records held by the issuing agency (e.g. birth or citizenship records).
B – Identity is a living identity (not deceased)	Verification against the State's Death Register. or Business processes for Objective C.
C – Applicant links to the identity	Assertion by a trusted referee (preferably known to the TDIA, and verifiable in their database). or In-person verification against photo document (at agency office). or Biometric recognition against the TDIA database, and/or against other government databases containing the individual's biometric[2]. and Interview (if an individual is unable to meet the specified evidentiary requirements or suspicion is raised over the individual's identity).
D – Applicant is the sole claimant of identity(is not using another identity)	Check against TDIA records for matching biographical details and/or biometrics.
E – Presenter uses identity in the community	At least 2 documents/records (e.g. electoral roll, banking and utilities statements, tax and social security numbers, healthcare registered, motor vehicle registration and education records). and/or Where a previous passport is held, validation against agency records.

3.1 A – IDENTITY EXISTS

Foundational Documents

Foundational documents refer to evidentiary documents issued to record a person's birth, death or their point of immigration or naturalization and are used by issuing authorities to establish identity and confirm

[2] For information on the use of biometrics across government, see New Zealand's *Guiding Principles for the Use of Biometric Technologies* at www.dia.govt.nz

citizenship. When used in combination they provide part of the evidential process required to provide confidence that an individual is the true 'owner' of their claimed identity.

Foundational documents are the fundamental physical evidence accepted by national authorities to establish a *prime facie* claim to an identity.

The management and protection of foundational documents by national authorities is integral in the protection against identification (ID) fraud. A stolen, counterfeit or altered foundational document may allow the holder to fraudulently obtain genuine government documents and entitlements, including travel documents.

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;*

c) *Preferably accept only documents that are currently valid* – a currently valid document is a valid 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, agencies 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 agencies 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 agency records, where two individuals have the same name and biographical information, and gives additional avenues of investigation in cases where an individual's 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 the authenticity of a particular document is questionable, verify the authenticity of that document with the issuing authority

3.2 B – IDENTITY IS A LIVING IDENTITY

Civil registration is the system by which governments record the vital events of its citizens and residents. Vital events that are typically recorded include: birth, death, marriage, divorce and adoption.

The resulting civil registry database may then be used by government officials to create legal documents that are used to establish and protect the civil rights of individuals. Among the legal documents that are derived from civil registration are: birth, death and marriage certificates, which are referred to as foundational documents (refer to 3.1 above). The civil registry system records create an important data source (i.e. compilation of statistics).

It is important that governments design and implement secure administrative and legal procedures for registering and documenting vital events and their characteristics, in such a way, as to ensure that the important life events relating to an individual can be verified, authenticated and protected.

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

Civil registrations systems and processes vary between states. While a centralized system can streamline the process of confirming identity for travel documents issuance by reducing the reliance on physical evidence of identification documents and eliminating the need to confirm document authenticity with separate issuing authorities, most states use decentralized systems. Under a decentralized system, foundational document information is collected at different levels of government (e.g. local, municipal, state and provincial) and is often stored in separate databases by the particular issuing authority. The decentralized approach is often preferred for civil registration as some states believe that centralized systems put the privacy of their citizens at risk. However, decentralized systems can present challenges to TDIAs who must validate documents from various jurisdictions and issuing authorities, each with different standards administered under different authorities, leading to inconsistencies in adjudication across the travel document issuance continuum.

As well as the documents themselves that are commonly used by applicants for travel documents (e.g. birth certificates, national identity cards and drivers licenses) often though not universal, the information that is captured for these and other foundational documents is frequently stored in electronic databases.

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.

While this is a very useful approach to verifying the legitimacy of entitlement claims, there are issues with respect to legal and privacy implications that may limit the use of these databases.

Despite limitations, some states do link their data sources to birth and death records which serve as automatic checks and verifications of living identities.

3.3 C - APPLICANT LINKS TO THE IDENTITY

D - APPLICANT IS THE SOLE CLAIMANT TO THE IDENTITY

E - APPLICANT USES IDENTITY IN THE COMMUNITY

Having established that an identity exists and that it represents a living person, the next objective is to establish a link between the applicant and that identity.

Identity can be said to be a combination of three elements:

a) Attributed identity: consists of the components of a person's identity that are given at birth, their full name, date and place of birth, and names of parents.

b) Biometric identity: consists of attributes that are unique to an individual (e.g. fingerprints, voice, iris pattern and hand geometry).

c) Biographical identity: a person's social footprint which builds up over time. It covers life events and how a person interacts with society and includes details of education and qualifications, electoral roll, employment history, healthcare and interactions with organizations such as banks, utilities and public authorities.

Most fraudsters operate by pretending to be someone they are not. They are using an attributed identity that is either fictitious or not their own. 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.

Where a biometric check is being carried out as part of the application process, this will only highlight a record of the applicant where they have come to notice previously and had their biometrics recorded (i.e. the biometric identity) is only useful to establish identity if the applicant has had their biometrics recorded as part of a similar application in the past, although if the current application is successful there is merit in recording biometrics to 'lock' the applicant into the claimed identity. Therefore there needs to be a third method of establishing identity which protects against the misuse of an attributed identity or where there is no previous biometric record.

Social Footprint Concept

The concept of the social footprint check, or examining the applicant's biographic identity is a robust check and a mean of preventing people from pretending to be someone other than their true identity. The exact nature of the checks made will depend on the laws and customs of the country. Allied to other checks that are carried out in the normal process of an application for a travel document, it is a way of using the applicant's claimed biographical identity to check against their claimed identity. Social footprint evidence is evidence that an individual uses their claimed identity in the community; for example, this may include evidence such as driver licences and tax numbers. 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.

By integrating a social footprint check within the application process for a travel document, it is possible to deter potential fraudsters from attempting to make false applications. As the applicant does not know what information is held by the person reviewing their application or the questions that they will have to answer if interviewed there is a greater likelihood that either the fraudster will not try to obtain a document by this means.

Policies and Procedures (Travel Document Application Interviews)

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.

Policy also needs to be devised in relation to handling emergency applications. Reducing the strength or integrity of any of the checks made should be avoided in the event that it introduces a weaknesses or vulnerabilities in the system that fraudsters will exploit.

In many travel document application systems the receipt and processing of an application will trigger a number of checks including whether the applicant is previously known, whether there is any adverse information about them, and other relevant information. It may also be at this point that a decision is taken on whether to carry out an interview. This may be based on information held by the issuing authority about the applicant or the type of application being made.

The travel document application 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 seeking a travel document. 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 the photo (including historic photographs) and other core details of their application. It is suggested that this is done by someone other than the interviewer as a guard against collusion. It may also be appropriate to take a live image capture of the applicant at this point.

b) Measures should be taken to reduce the risk of collusion, for example interviewers should not be told which applicants they will be interviewing until shortly before the interview.

c) The interviewer should use the information available to them, in combination with their training, to make the interview questions specific to the applicant (interviewee). This helps to guard against an applicant (interviewee) from being coached on the interview process.

d) 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, passport related fraud and identity theft.

4. USE OF IDENTITY DATA

4.1 DATA AND INFORMATION SHARING

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

Information may be shared between states, government agencies and occasionally with the private sector.

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 agencies) and using the ICAO PKD; 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.

For documents and records used to establish that an identity exists (such as birth or citizenship records), the TDIA can try to validate identity information at the source registry in order 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 agencies to validate the authenticity of data on a named individual's identity documents, or the data that is provided by the individual.

Public sector agencies can also undertake what is termed 'data matching', where a comparison is undertaken with another agency's databases to verify information, or identify discrepancies.[3] TDIAs have particular interest in births, deaths and citizenship information to gain confidence that the identity exists and is living (see objectives A and B under EOI Principle 1). If the TDIA can access this information directly, documentary evidence for these establishment events may not be required.

Such services increase the TDIA'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 TDIA's exposure to counterfeits.

Where possible, TDIAs should attempt to access and leverage other government agencies that collect identity information (which can include biometrics). As noted in sections on EOI and social footprint, information from agencies responsible for products or services such as driver's licenses, healthcare or the electoral role can provide valuable information to corroborate the existence and use of an identity. Data matching against other agencies' 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, TDIAs can focus efforts on high risk applications, based on a predetermined risk profile.

4.2 RISK CONSIDERATIONS

Identity-related Risk

Identifying identity-related risks and the consequences of these risks, requires an understanding of how a person can obtain a false identity to subsequently commit identity crime.

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

False identities can be established in the following ways:

a) creating a fictitious identity;

b) altering one's own identity (identity manipulation);

c) stealing or assuming a pre-existing identity (identity theft); and

d) stealing or assuming a pre-existing identity, which has been subsequently manipulated.

[3] See the Australian Government's *Data Matching: Better Practice Guidelines* at www.ag.gov.au

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) in order to fraudulently obtain more access to services or benefits or to avoid establishing obligations.

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 agency 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 a 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 agency programmes. This may result in a negative public or political perception that some people are not receiving the services from these agencies that they are entitled to or that people who are *not* entitled *are* receiving agency services. At worst, this could cause a severe or catastrophic adverse effect on agency operations or assets, or public interests, including severe function degradation or loss to the extent and duration that the agency is unable to perform one or more of its primary functions, and major damage to agency assets or public interests.

d) *Unauthorized Release of Sensitive Information:-* can result in loss of confidence in an agency 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 agencies other than the agency 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 agencies, 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.

Threat and Risk Assessments

It is recommended that the TDIA and BCA 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 TDIA 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 are the threats and weaknesses in the system. It is wise to periodically 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 in order to focus resources on making changes in the process to prevent future incidents or attacks of a particular type.

The organization 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. For more information refer to the International Standards Organization, ISO 31000 at http://www.iso.org/iso/catalogue_detail.htm?scnumber=43170.

APPENDIX 1

THE UTILITY OF BIOMETRICS

Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. As the level of security breaches and transaction fraud decreases, the need for highly secure identification and personal verification technologies increases. One of the main reasons for using biometrics is the increased security it provides. Instead of asking questions based on "what you know" or "what you do," the focus now is on "who you are." This makes security more personal. Checking who the client “is” will usually involve the collection and comparison with prior records of unique biometric information; for passports, photographs and signatures were the traditional biometrics.

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

Verification (1-to-1 Matching)

Verification (1-to-1 matching) is a test to ensure whether a person is really who he or she claims to be. Two types of verification can be envisaged: with centralized storage or distributed storage.

Verification with Centralized Storage

If a centralized database exists, produced once at enrolment and updated with each additional user, 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 by the traveller, resulting in a match or a non-match.

Verification with Distributed Storage

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 memory 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, the traveller is confirmed to be the valid bearer of the identification document.

Identification (1-to-Many Matching)

Identification is used to discover the identity of an individual when the identity is unknown (the user makes no claim of 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.

Screening

The third type of process is screening, which makes use of a database or watch-list. A watch-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 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 are more or less the only means for this type of check.

The Multi-Biometric System Approach

By combining the biometric features for identification and verification, a multi-biometric system is considered to be the better and more accurate performer than a system, which uses only single biometric feature for the same.

A multi-biometric system captures more than one type of biometrics to get enrolled in the data base. 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. This is also possible with uni-biometric systems.

People with bad intentions might focus on cheating one biometric feature, but will fail if a second biometric feature is also verified. It is nearly impossible 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.

Concerns

There are some ethical issues centering on 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 of the stored biometric data. To address public discussions on ethical issues, stored biometric data

must be properly protected. There should not be any unauthorized collection, use, and retention of biometric data, and biometrics need to be deployed where most effective and appropriate. The public must be proactively informed about data usage and data retention time in order to gain trust in both the system and its use and oversight.

— END —