International Civil Aviation Organization

WORKING PAPER

TAG/MRTD/20-WP/5
17/08/11
English only

TECHNICAL ADVISORY GROUP ON MACHINE READABLE TRAVEL DOCUMENTS (TAG/MRTD)

TWENTIETH MEETING

Montréal, 7 to 9 September 2011

Agenda Item 2: Activities of the NTWG
Agenda Item 2.5: Towards better Practice in National Identity Management

TOWARDS BETTER PRACTICE IN NATIONAL IDENTITY MANAGEMENT (Guidance for Passport Issuing Authorities and National Civil Registration)

(Presented by the NTWG)

1. INTRODUCTION

1.1 The rapid growth of identity fraud affects many areas of society and raises serious concerns globally for public security and safety. Much work has been done in the area of travel documents to increase the security of passports and the associated systems for the personalization and issuance of these documents. Also, border authorities have upgraded their document inspection systems and passenger checks to improve the security of the travel document production and inspection processes from end-to-end.

1.2 These measures have been very successful in raising the level of security of passports to deter fraud by counterfeiting, by alteration of data and from misuse by impostors. However, it has had an unwelcome side effect, shifting the focus of fraud away from the passport document itself towards the opportunities for obtaining a genuine passport in an assumed identity. If a fraudster is able to misrepresent him or herself by using a bogus identity during the passport application process and goes on to receive a passport in a false identity and then detection of that fraud after the fact becomes extremely difficult.

2. BACKGROUND

2.1 The above concerns were highlighted during the TAG/MRTD 19 Meeting, and a new work item on this subject was approved by the Group. The new work item was entrusted to the NTWG consisting on developing a Technical Report (TR) entitled "*Towards Better Practices in National Identity Management*." The TR would be the vehicle to present in a systematic way best practices and other forms of guidance on these matters, and would serve to underscore the specific nature of the foundational document problem. Thus, providing ways in which issuing authorities could enhance their abilities to assess such documents and minimize the negative impacts such documents can have on decision making.

2.2 The importance of this work item was confirmed further by ICAO Member States during the 2010 Assembly, and was included in ICAO Resolution 51/1 *"Consolidated Statement of Continuing ICAO Policies in the Air Transport Field, Appendix D – Facilitation*," in these terms:

> *"Whereas the veracity and validity of machine readable travel documents (MRTDs) depends on the documentation used to establish identity, confirm citizenship or nationality and assess entitlement of the passport applicant (i.e. "breeder" documentation)…The Assembly:*
>
> *1. Urges Contracting States to intensify their efforts to safeguard the security and integrity of the breeder documentation;*
>
> *2. Urges Contracting States to intensify their efforts to safeguard the security and integrity of their passports, to protect their passports against passport fraud, and to assist one another in these matters;*
>
> *…*
>
> *6. Requests the Council to take appropriate measures to establish guidance on breeder documentation;*
>
> *7. Requests the Council to continue the work on enhancing the effectiveness of controls on passport fraud by implementing the related SARPs of Annex 9 and developing guidance material to assist Contracting States in maintaining the integrity and security of their passports and other travel documents…"*

2.3 The Secretariat offered to lead the implementation of this work item, and a group of experts volunteered to contribute to this TR. The first draft was prepared and shared among NTWG members for feedback. Then, during the working group meeting in Berne, Switzerland the working group discussed about the scope and content of the TR. As a result, certain subject matters were eliminated and the content development was prioritized for preparing the second draft. A drafting subgroup was then formed, which met in late June 2011 at ICAO Headquarters, concentrating on defining the scope of the TR and reviewing the subjects that required further review and development.

2.4 The resulting draft was then circulated to the NTWG for comments, which is reflected in the version attached for review and support by the TAG/MRTD.

2.5 Due to the numerous subject matters to be covered and the evolving nature of the items considered therein, this TR is considered to be a living document, and its development and update will be done on an on-going basis.

3. ACTION BY THE TAG/MRTD

3.1 The NTWG invites the TAG/MRTD to:

a) acknowledge the work done on evidence of identity, documented in the attached Technical Report on *Towards better Practice in National Identity Management***,** version 1.0; and

b) approve the work done and the continuation of the development of this TR under the responsibility of the NTWG.

— — — — — — — —

APPENDIX A

MACHINE READABLE TRAVEL DOCUMENTS (MRTDs)

TOWARDS BETTER PRACTICE IN NATIONAL IDENTITY MANAGEMENT

TECHNICAL REPORT

Version: 1.0

Date: 15 August 2011

INTERNATIONAL CIVIL AVIATION ORGANIZATION

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

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

1.1 [TYPE PARA TEXT AND DELETE/INSERT ADDITIONAL PARAS AS REQUIRED]

1.2 [TYPE TEXT]

1.3 [TYPE TEXT]

2. INTRODUCTION

2.1 PURPOSE AND AUDIENCE

- The rapid growth of identity fraud affects many areas of society and raises serious concerns globally for people's security and safety. Much work has been done in the area of travel documents to increase the security of passports and the associated systems for the personalization and issuance of these documents. Also, border authorities have upgraded their document inspection systems and passenger checks to improve the security of the travel document production and inspection processes from end-to-end.

- These measures have been very successful in raising the level of security of passports to deter fraud by counterfeiting, by alteration of data and from misuse by impostors. However, it has had an unwelcome side effect, shifting the focus of fraud away from the passport document itself and towards the opportunities for obtaining a genuine passport in an assumed identity. If a fraudster is able to misrepresent him or herself by using a bogus identity during the passport application process and goes on to receive a passport in a false identity then detection of that fraud after the fact becomes extremely difficult.

- The ability of a criminal to perpetrate this and other similar types of fraud relies upon tricking the authorities into accepting a bogus identity during the application (enrolment) process. Typically this process requires, among other things, the applicant to provide "evidence of identity" in the form of official documents containing his or her identification details. These documents are often referred to as "foundational documents" a term that signifies their acceptance as proof of identity supporting the issuance of other forms of identity documents to the holder. In this way, through the use of false foundational documents it is possible for a fraudster to build up a portfolio of other security documents (passport, drivers licence, identification (ID) card, etc.) all of which are obtained in the same bogus identity and all of which may themselves be further used to strengthen a bogus chain of false identity. Contrary to popular belief, identity fraud is not a "victimless crime". Indeed it lies at the heart of some of the most heinous criminal activity in facilitating terrorism, people trafficking and many other serious types of crime where the criminal needs to disguise his or her true identity.

- A birth certificate (BC) is the single most important foundational document, because it is normally the first official record of the identity of an individual, created soon after their birth. It is therefore at the very forefront of the identity chain and is the source document used in support of evidence of identity. As such its importance cannot be over-stated.

- It is believed that most countries, although not all, require births to be registered with an appropriate government agency and most issue a document (BC) to the parent or guardian of the child confirming the registration. However, in some countries, responsibility for registration of births operates

at a regional or local level and this has led to there being many different styles of BCs in issue within country. This makes for difficulties in authenticating genuine documents outside of the area in which they were issued. Also, because until now there appears to have been no best practice guidelines for the secure design, production and personalization of BCs it is probable that some are easy targets for a fraudster.

- Typically a BC consists of a registration document issued to the parents of the child and a copy retained by the issuing authority, sometimes in the form of a digital record stored in a database. It is the document in the possession of the holder that may be used as a foundational document and could be stored in unpredictable conditions. Since a BC is valid for the entire lifetime of the holder, it is necessary for it to be produced using materials that will survive intact for a long period of time, possibly in excess of 100 years. Whilst many BCs may be carefully stored and seldom used by their holders, the possible effect of potential adverse conditions such as extremes of temperature and/or humidity adversely affecting their structure or appearance should be considered in specifying the materials to be used for manufacture and personalization.

2.2 SCOPE

- [TYPE PARA TEXT AND DELETE/INSERT ADDITIONAL PARAS AS REQUIRED]
- [TYPE TEXT]

2.3 STAKEHOLDERS

2.3..1 Roles and Responsibilities [TYPE TEXT]

2.3..2

2.4 ASSUMPTIONS

- [TYPE TEXT]
- [TYPE TEXT]

2.5 OTHER CONSIDERATIONS

- [TYPE TEXT]
- [TYPE TEXT]

2.6 HOW TO READ THIS DOCUMENT

- [TYPE TEXT]

- [TYPE TEXT]

3. THE CONCEPT OF IDENTITY MANAGEMENT

3.1 THE ISSUE

- Over the past several years, many nations have invested time, money and great expectations in enhanced travel document programs, especially in machine readable ePassports employing biometrics. The ICAO MRTD programme has pushed for security improvements to the physical document, and its use at borders. Many states have gone beyond the minimum requirements and made significant investment into the physical and technical security features in documents. The current generation of ICAO-compliant travel documents is the best and most secure the world has ever known. Travel documents are using more technical and physical security features, making the physical documents more secure, more difficult to forge, and a harder target for fraudsters. These improvements in technical quality have increased the reputation of many countries travel documents.

- There is, however, a threat that affects virtually all issuing authorities and can undermine the integrity of these highly secure travel documents: namely **weak identity management processes**. As the quality of the physical travel document improves, fraudsters find it increasingly difficult and more expensive to successfully manipulate and counterfeit documents, without detection. The targeting of the issuance process can damage reputational gains made by increasing the physical security of the document. It also undermines the state's financial investment in improvement of secure technology. Fraudsters will generally seek the path of least resistance, and in many states this path is the issuance process. If there are gaps in the process that make it easier to secure a Falsely Obtained Genuine document, then the fraudsters will seek this method, rather than forgery or counterfeit. The resulting document is genuinely issued by the Travel Document Issuing Authority (TDIA), and less likely to be detected than a fake, altered or counterfeit document, as it can be validated against source data.

- The cornerstone or 'foundation' for a TDIA's 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 in the travel document and border contexts. These in turn lead directly to the development of robust and secure processes for establishing identity, and support quality decision making on applications for travel documents and border control.

- ICAO's mandate in this area is to assist States to properly and uniquely identify individuals as part of travel document issuance, or as they move across borders. 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 organised crime to terrorism, and 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. It is also the case that in many States the TDIA is one of the most important authoritative sources of identity information, often meaning that other agencies want to access information for the purposes of verifying identity and confirming entitlement for services. As authoritative sources, there is an obligation to ensure, for the benefit of the State, that identity is established with a high degree of assurance, and the identity information is managed effectively to enable ongoing validation in a range of contexts.

- Immigration authorities are a key recipient of travel document data, which is used to validate travel documents at the border. This travel document data forms the basis of an identity within an Immigration authority's database, and this information is also managed to enable access and interrogation upon subsequent border transactions. In order to realise the investment in high security physical documents, States must establish identity to a HIGH degree of confidence, and utilise a range of tools and techniques to validate documents and identity data on an ongoing basis.

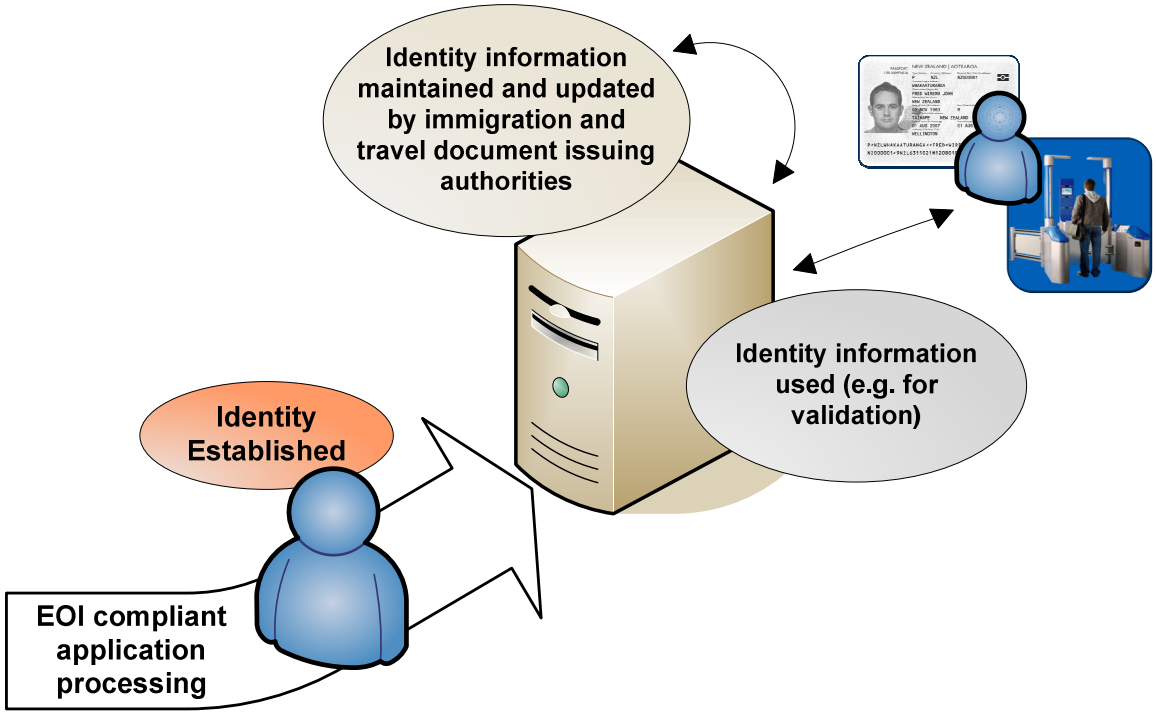


Figure 1. Identity Establishment to Identity Management

3.2 COMPONENT PARTS

Establishing Identity

Every applicant for a certificate, identity card or travel document is making a claim to a particular identity. The first step of the issuing authority is to test the claim, in other words, to establish identity.

Most countries have well-established national agencies to verify a person's identity. Typically these agencies will have a component approach to establishing identity. This approach consists of three key components that, if applied as a whole to an individual case, provide confidence that a person actually owns the identity they claim to own.

The three components for establishing identity involve:

1) Evidence that the claimed identity is valid - i.e. that the person was born and, if so, that the owner of that identity is still alive.
2) Evidence that the presenter links to the claimed identity - i.e. that the person claiming the identity is who they say they are and that they are the only claimant of the identity. This claim can be verified by asking: what does the applicant "know" about the identity that is claimed; who "is"

the applicant; and what does the applicant "have" to support the claimed identity. **(PROVIDE EXAMPLE?)**

3) Evidence that the presenter uses the claimed identity - i.e. that the claimant is operating under this identity within the community.

The above concepts will form the basis of an EOI framework, which is covered in more detail in Section 3.5.

Foundational Documents

Foundational documents, which refer to evidentiary documents issued to establish a person's identity at birth, death or at point of immigration or naturalization[1] are used by issuing authorities to establish identity and confirm citizenship and when used in combination provides part of the evidential process required to provide confidence that an individual is the true 'owner' of their claimed identity.

Foundational documents are the 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 ID fraud. A stolen, counterfeit or altered foundational document can allow the holder to fraudulently obtain genuine government documents and entitlements, including travel documents. Moreover improvements in technology has made high quality alteration and counterfeiting of foundational documents much easier and more affordable to criminals. Thus, the need to improve the security of the foundational documents and their respective issuing systems, so they can be better validated by TDIAs. Also, to avoid counterfeiting and document alteration and increase detection of fraudulently obtained genuine documents, TDIAs need to strengthen their document validation systems including meeting international standards on security and ensuring staff are well trained in travel document issuance.

Civil Registration

A critical component of establishing and authenticating a person's identity depends on the country's civil registration system, which provides records of the vital events of its citizens and residents including: birth, death, marriage, divorce, adoption. The civil registry records provide essential legal documents of identity and civil status, nationality and citizenship on which depend a wide array of individual and rights and benefits.

With increased mobility of populations, vital records have taken on additional importance. It is therefore 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 an individual's identity can be verified, authenticated and protected. For the migrant, it has become essential to have access to documents that can prove his or her civil status and nationality.

To facilitate the process of identification, a country should maintain a civil registration system whereby vital events documents conform to internationally accepted standards and where information records are maintained in secure databases.

[1] Examples of foundational documents include: birth certificates, death certificates, citizenship certificates, national identification cards, permanent residency cards, naturalisation records

Civil registration systems are discussed in more detail in Section XX.

_____

Use of Secure Registries and Databases

Governments have taken extensive and successful steps to improve the quality of identity documents including advanced security features as well as developing secure registries and databases in which these documents reside. In addition, staff training has also improved in the detection of fraudulent ID documentation. These changes have allowed issuing authorities to apply advanced techniques in a cost-effective manner while responding to the latest developments in the area of document fraud.

Increasingly, governments are focussing on the securitisation of the databases and systems that administer and record the source information. For example, some countries are beginning to automatically link databases (e.g. birth and death records) to ensure that records are automatically and routinely updated. While automatic verification and authentication of civil registration databases provide a useful approach to verifying the legitimacy of entitlement claims, there are legal and privacy considerations that may limit the amount of information sharing information between databases and jurisdictions.

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

- **Establishing Identity**

3.2..1 The claim to an identity is tested by the national authority checking:

a) What does the applicant "know" about the identity that is claimed;

b) Who "is" the applicant; and

c) What does the applicant "have" to support the claimed identity.

- **National Civil Registry**

3.2..1 In managing identity for the benefit of their communities and citizens, national civil registration and passport issuing authorities must:

a) Establish identity;

b) Confirm citizenship; and

c) Assess entitlement.

- **Secure Databases**

3.2..1 As well as the documents themselves that are the "usual suspects" used by applicants for travel documents, such as birth certificates, cards of national identity and driving licenses, often, though not universal, the information that is captured in these and other foundational documents also resides in a database of national content.

3.2..2 While the existence, quality and ease of accessing such databases and civil registry systems vary dramatically from country to country, increasingly governments have been focusing on these sources of information in addition to the documents themselves or in some cases in lieu of some documents.

3.2..3 While this is a very useful approach to verifying the legitimacy of entitlement claims, there are sometimes limitations of a legal or privacy nature that impedes the use and utility of these databases.

3.2..4 Some countries are beginning to link these data sources, for example birth and death records, to serve as automatic checks and verifications. This initiative seeks to acknowledge the importance of these secure sources of information and to offer suggestions on their use in addition to the documents themselves.

3.3 THE CONCEPT OF SOCIAL FOOTPRINT

- Testing what the client "knows" about the identity they are claiming will usually involve completion of an application form, information which can be checked at an interview.

- Corroborating checks may extend to confirmation that the claimed identity is actually being used in the community – a process sometimes described as checking the social footprint or social context.

- **The Concept of a Living Identity**

3.3..1 Some biometric features are persistent over time while others change or may change. All biometric features are deemed unique but some are less distinct than others and thus less useful for automated identification purposes. The distinctiveness of any biometric feature depends also on the effectiveness of the sampling technique used to measure it, as well as the efficiency of the matching process used to declare a 'match' between two samples.

3.3..2 Biometrics is used to strongly link a stored identity to the physical person this represents or vice versa. Since a person's biometric features derived from a person's physical characteristics, they will always be with that person where ever he/she goes and available to prove his or her identity.

3.3..3 But a person's identity is not only established by its biometrics, but also by his social footprint and his social context. These include information on where the person has his/her registered address, place of work, school and how he/she conducts payments, such as the use of credit cards.

3.3..4 Biometrics are more or less permanent, while the living identity may change over time, when people move houses or change the credit card company. This information is important to have or to investigate in situations where the established identity through a person's documents is in doubt. To know whether the person has used his identity in the past in society gives a clue whether he is the person he claims to be. 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 increases, the need for highly secure identification and personal verification technologies is becoming apparent. 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. To achieve this, the integrity of the initial enrolment process is key to the use of biometrics for confirming identity.

3.4 **USING A SOCIAL FOOTPRINT TO ESTABLISH IDENTITY**

- Citizens have the right to be able to prove who they are quickly, easily, securely and simply. A citizen's identity - who a person is - belongs to that person and to no-one else. This is a fundamental principle which everyone accepts.

- There are times however, when a citizen has to be able to prove to other people that he/she is who they claim to be. There are many possible reasons why a citizen may want or need to do this including application for a travel document or national identity card. When they do so, the other person needs to know that what the citizen says about himself/herself is true. This is also a fundamental principle which everyone accepts as it is the basis of trust between people.

- Today, in every country, we live in a world where we more and more often have to prove who we are to people we do not know. We apply for jobs, we use public services, we travel abroad, and we open bank accounts. People want and need to be able to prove who they are. They are entitled to be able to do so with confidence and in a way which works well for them. 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 parents' names.

  b) Biometric identity consists of attributes that are unique to an individual, e.g. fingerprints, voice, iris pattern, facial structure, DNA profile, hand geometry.

  c) Biographical identity, a person's social footprint, builds up over time. It covers life events and how a person interacts with structured society. For example, it includes details of education/qualifications, electoral register entries, employment history, 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 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 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. So 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.

- The concept of the social footprint check is a more robust check and a more certain means of preventing people from pretending to be someone other than their true identity. 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 that they are who they claim to be. 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, especially for a 'first time' applicant or where the previous passport has been, lost it is possible to deter potential fraudsters from attempting to make applications. As the applicant does not know what information is held by the interviewing officer or the questions that they will have to answer, there is a greater likelihood that either the fraudster will not try to obtain a document by this means or their attempted deception will be picked up at interview.

- The use of the social footprint is based on the availability of publicly available information about citizens. This might, for example, be held by credit card companies or in government databases. The basis of the idea is that the applicant for a document is questioned about facts that only he/she should know. These are all areas where public records may exist, sometimes backed up by government records. The important point is that the interviewer must know the correct answers to the questions put to the applicant. However this is not deeply private information, for example, there may be a question about:

    a) a person's bank account (which branch, how long has it been in operation) but not about the balance (which the interviewer would not know);

    b) a guarantor (if that is part of the application process); and

    c) other occupants of the address at which the applicant lives.

- **Policies and Procedures**

- It is essential that clear policy guidelines are devised to handle applications where a social footprint check is required. This will include communication with applicants to explain the reasons for the check, information about the check and the level of information that is being provided and also assurance that genuine applicants should find the process relatively straightforward and non-intrusive.

- Policy also needs to be devised in relation to handling applications where the applicant cannot wait for the document to be issued. Manipulation of the requirement for an interview to confirm identity using the social footprint data should be avoided lest it introduces a weakness that fraudsters will exploit.

- The process for integration of a social footprint check inevitably means that when an application is made for a travel document there will be a minimum of two stages involved. Stage one will involve the submission of the application form and payment of application fee. At this point the application form may be scanned in or keyed in to the travel document application system. In many travel document application systems this will then trigger a number of checks to identify 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 a social footprint check. This may be based on the profile of the applicant or the type of application. As the background checking required for this will take time, the applicant will need to be asked to return to the application office at a later date to be interviewed. This will provide time for an applicant profile to be put together from the various available sources that are being used. These will vary from country to country.

- Stage two is the interview itself and may comprise a number of stages. The first stage is a check of the applicant to the photo and core details they gave in with 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 capture image of the applicant at this point.

- To ensure security of the process, the interviewer will not be told which applicants he/she will be interviewing until shortly before the interview. This also reduces the risk of internal collusion. The second stage will involve preparation time for the interviewing officer. Time needs to be allowed for the interviewer to plan a range of questions from the data bearing in mind individuals will have different footprints. Although it is suggested that a number of mandatory questions must be used in every interview. Interviewers should look at the core details of the application and think about what they would expect to see before consulting the profile containing information on the detailed background checks that

have been carried out. Looking at the bigger picture allows an interviewer to use his/her experience to have an idea of how much of a social footprint might be expected before the applicant is interviewed. Things like accents, credit history, etc. should confirm what the interviewer expects. For example a 17 or 18 year old may have little credit history whilst an older person may be expected to have a reasonable social footprint which might include tax information, drivers licence and tax information.

- The interview is stage three. These interviews are different from normal 'fact-finding' interviews as the interviewer already has all the facts. Successful interviewers will be skilled at putting the customers at ease and soliciting the required information to verify their identity. Genuine owners of an identity may not be able to answer all the questions put to them or may have some concerns about providing such personal and detailed information. The interviewer has to be able to ask appropriate and sufficient questions to interact with the applicant and to confirm identity as well as deal with customer issues or concerns in a relatively short period of time.

- At the beginning of the interview the applicant should be asked whether they completed and signed the application form themselves. If they have not completed it themselves, they should be asked if they are aware of what information had been provided. By asking this question at the beginning of the interview the interviewer gets a feel of how much information the applicant may know, and why possible discrepancies with the answers may occur. It also means that the interviewer may need to ask more probing questions. Part of the interview process should also include asking the applicant to provide their signature which can be compared against the signature shown on the application form.

- Whilst there may be a ‘script’ that an interviewer follows when asking questions, it is good practice to change the order in which questions are asked. This can guard against an applicant being ‘coached’ in the interview process where they may be expecting the interview questions to follow a particular order.

- The interviewer is testing whether the applicant 'owns' the identity presented on the profile. Following the interview, the interviewer has time to review the responses received as well as considering the behaviour and body language of the applicant to decide whether the person interviewed is the true owner of the identity.

- The final stage is making the decision. 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.

- The use of the social footprint does extend the application processing time and requires suitable arrangements to enable the document issuing authority to obtain enough background detail on an applicant’s identity to make the interview sufficiently testing. Nevertheless it does provide a strong defence against impersonation/identity theft.

3.5 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 increases, the need for highly secure identification and personal verification technologies is becoming apparent. 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 the ePassport, digital facial and fingerprint and/or iris images allow automation of biometric comparisons at issuance and at border clearance. The following comparison methods are possible.

- **Verification (1-to-1 matching)**

3.5..1 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**

3.5..1 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, e.g. 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**

3.5..1 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, then the traveller is confirmed to be the valid bearer of the identification document

- **Identification (1-to-many matching)**

3.5..1 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, for the process of identification a central database is necessary that holds records for all people known to the system; without a database of records, the process of identification is not possible.

3.5..2 For an identification process, the person provides a live biometric sample, e.g. 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**

3.5..1 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, or adverse information or information on individuals that requires more questioning of the individual than normal. 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 their biometric sample should in principle be discarded. In the case of a match, a human operator decides on further action.

3.5..2 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.

3.5..3 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 approach**

3.5..1 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.

3.5..2 A multi-biometric system captures more than one type of biometrics to get enrolled with the data base. This improves the accuracy in establishing the 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 data base. This is not possible with uni-biometric systems.

3.5..3 Fraudsters might focus on cheating one biometric feature, but will fail if a second biometric feature is also verified. It is nearly impossible for the criminals to obtain two samples of biometrics of the same individual. Thus, a sophisticated level of security helps the multi-biometric systems to perform better than the traditional systems.

- **Concerns**

3.5..1 There are some ethical issues centring 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 overcome 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 the data usage and data retention time, leading to trust in the system.

3.6 Evidence of Identity (EoI)

EOI refers to the types of evidence that, when combined, provide confidence that an individual is who they claim to be (i.e. a driver licence, passport or birth certificate). Generally, the more evidence an applicant can provide, the higher an agency's confidence that the identity is genuine and belongs to the presenter – particularly if the evidence can be validated at source.

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.[2] EOI frameworks provide a conceptual

[2] See the New Zealand Government's *Evidence of Identity 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 have completed their *Framework for Assuring Identity in the Issuance of Biometric Machine Readable Travel*

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.

Figure 1.1 outlines the three key principles (1-3) and five underlying objectives (A-E) that are central to most EOI frameworks 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:

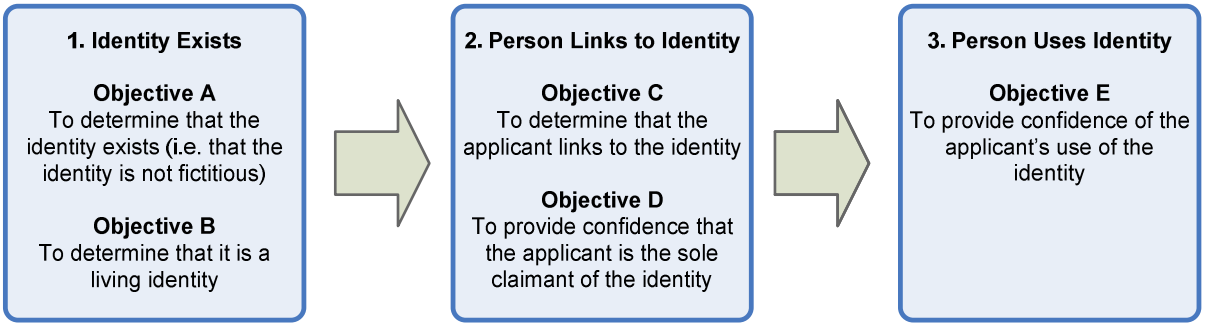


Figure 1.1

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 there is no record the identity has deceased.

To meet the objectives under EOI principle 1, the TDIA should:

- Ask for documents that show that the identity exists, such as a birth or citizenship certificate. These documents should whenever possible be validated against source data to combat the risk of forged foundational documents.
- If possible, check against the death records to guard against fraudulent applicants using the identity of a deceased person.

Documents, and ISO are designing a Standard for 'Entity Authentication Assurance.'

In some states documents may not be required as source registers can be accessed electronically to check birth records, which negates the risk of counterfeit and forged documents.

The second and the third principles **Person Links to Identity** and **Person Uses Identity** are often collectively be 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, the TDIA should:

- Verify that the link between the applicant and the claimed identity is genuine
- Check available agency databases to ensure there is no record of someone else claiming that same identity (biometric matching is advised to detect whether the applicant has a travel document under a different name)
- Undertake checks to establish the 'social footprint' of the identity (i.e. evidence that the person uses their claimed identity in the community).

Designing an EOI Process

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:

- States with smaller populations may be unable to interview all applicants (there may not be sufficient critical mass to make it viable)
- There may be multiple different valid versions of foundational documents available for use
- Legislation may prevent validation of documents, access to source registers, or information sharing between government departments and countries
- Historic travel or foundational document records may be paper based – leading to a highly manual checking process
- Databases of information may be application rather than person centric – making it difficult to match various historical applications under the same identity.

Regardless of these kinds of challenges, TDIA's can still establish robust issuance processes by utilising a range of documents and records to build confidence in an identity.

Before processes are re-developed, TDIAs need to understand the three 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, to understand how much confidence can be gained from the document/record's inclusion in the EOI process.

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

The TDIA can then assess whether access to the driver license database will help prove the 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 licence in the same name for a number of years, they may have a higher level of confidence in the identity.

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 and or documents produced by some or all of their registry offices.

If a TDIA has less confidence in their State's birth registration process or the accuracy of their birth registers, more emphasis can 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 may be increased beyond the example given in Table 1 (below). This social footprint evidence can support claims that the applicant links to the identity, especially where there is no other evidence available.

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 there are likely to be and how other back office processes can support the process. TDIAs should always look to interrogate their own databases using tools and techniques such as data mining, risk profiling and biometric matching.

Figure XX – Overview of business process for establishing an individual's identity


Step 1 - Client requests service
Applicant requests service from agency
Applicant provides required EOI information
Step 2 - Agency undertakes EOI process
Application form completion checks
Agency checks application information quality
Examples: births, marriages and citizenship checks
A
Agency determines applicant's identity exists
Death checks
B
Agency determines applicant's identity is living
C
Agency determines applicant belongs to identity
Trusted referee processes & in-person verification processes
D
Agency checks applicant is sole claimant to identity
Check client database(s) for existing application records
E
Agency checks applicant's use of identity in community
Examples: Driver licence, Healthcare Card, Electoral Roll Record
Verification and control processes
Discrepancy, exceptions & investigations processes
Generic EOI establishment of identity processes
Step 3 - Service delivery
Agency delivers service
Agency undertakes service eligibility testing
Client record creation
Client provided with document and/ or key to use for subsequent service requests
Agency creates client record

An example of the evidence required to meet the five EOI objectives to a HIGH degree of confidence is provided in the table below (Table 1).

Table 1 - Evidential Requirements for EOI Objectives

EOI Objective	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	Verification 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[3] **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, tax and social security numbers, motor vehicle registration and education) **and/or** Where a previous passport is held, validation against agency records.

[3] 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

3.7 Protocols for acceptance of documentation

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

- *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, such as watermarks and embossing. Photocopied documents are relatively easy to alter and should, therefore, not be accepted as EOI

- *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

- *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

- *Unless confirmation of long-term name usage is required, only accept evidence of 'use in the community' documents (documents/records used to meet Objective E) that are less than one year old*

- *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*.

3.8 CIVIL REGISTRY SYSTEMS

- **Contemporary Civil Registration Systems**

According to the United Nations, "civil registration is defined as the continuous, permanent, compulsory and universal recording of the occurrence and characteristics of vital events pertaining to the population as provided through decree or regulation in accordance with the legal requirements of a country. Civil registration is carried out primarily for the purpose of establishing the legal documents provided by the law. These records are also a main source of vital statistics. Complete coverage, accuracy and timeliness of civil registration are essential for quality vital statistics"[4].

[4] http://unstats.un.org/UNSD/demographic/sources/civilreg/default.htm

- Vital events that are typically recorded include live birth, death, foetal death, marriage, divorce, annulment of marriage, judicial separation of marriage, adoption, legitimization and recognition. Additionally, in some countries, immigration, emigration, and any change of residence may require notification. Among the legal documents that are derived from civil registration are birth certificates, death certificates, and marriage certificates. The purpose of a civil registration system is to create and maintain one or more data sources to provide the legal documents and notifications necessary to establish and protect the civil rights of the individuals about whom the data are being collected.

- An efficient civil registration system creates and maintains all the institutional, legal and technical prerequisites to collecting data in a technically sound, co-ordinated and standardized manner, taking into account the cultural, social and administrative circumstances of the country in which it operates. Civil registration has many uses. Birth records provide individuals with proof of identity, age, nationality and parentage. Death records can be used to purge voter registration rolls while aggregated data can be used for population estimates, health statistics and demographic forecasts. Travel and identification documents, such as passports, are usually issued on the basis of data registered in the civil-registration system. A civil register that is kept up-to-date and clean of multiple entries provides the most reliable data for issuing of travel documents thus lowering security risks resulting from attempts to obtain multiple documents based on false identities.

    a) In states with more advanced technological infrastructure, civil registration has formed the basis for the establishment of a number of citizen-oriented computerized services, also known as “e-services” and “e-government”.

- Conversely, where civil registration is unreliable, technically defective or misused, it can constitute an obstacle to the exercise of fundamental rights such as freedom of movement. Furthermore, sufficient safeguards may not exist to prevent fraudulent attempts aimed at creating false or multiple identities.

- Civil registration is effective and efficient if it stores data that is relevant to the person’s identity, life events and place of residence, or data that is essential to guarantee their human rights, civil rights and social benefits. In order to ensure that the data stored in the system at any point in time is relevant and accurate, registration needs to be mandatory for the entire population of the state while the records need to be updated on a continuous basis. Public trust in the registration system is very important in ensuring full and reliable information in the registration process. Such trust exists if the handling of personal information is done in confidentiality and the stored information is used only for the purposes envisaged in the law.

- The systems of civil registration in place in modern states are characterized by the manner in which authority is delegated among public administration institutions. Administrative traditions, jurisdictional rights and privacy laws play decisive roles in determining a states approach to its civil-registration system. Three different approaches can be identified:

    a) A single authority registers life events and information on place of residence (centralized system);

    b) Different authorities are responsible for recording life events and population movements (decentralized); or

- The registration of life events is entirely the responsibility of bodies of local government, while population movements are registered by the central authorities (Mixed). Civil registration systems and processes vary among countries: some countries use a centralized national registry while others use

decentralized systems or a mixed approach. A centralized system can streamline the process of confirming identity for passport issuance by reducing the reliance on the physical evidence of identity documents and eliminating the need to confirm document authenticity with separate issuing authorities. A centralized system is usually computerized and allows the information sharing between recognized authorities.

- Under a decentralized system source information is collected from different levels of government (e.g. local/municipal/state/provincial) and is often stored in separate databases by the particular issuing authority. 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, lending to inconsistencies in adjudication across the travel document issuance continuum. As well decentralized systems, which also lack an infrastructure for information sharing, often result in s multiple jurisdictions and departments to maintaining separate registers and databases. As a result, citizens are often required to provide the same information on multiple occasions, often in a certified format. These requirements are time-consuming and expensive and place an unnecessary burden on citizens, while the need to repeatedly provide the same information increases the chances of error and can compromise overall data protection.

3.8..1 Use of information technology can play an important role in increasing the efficiency of civil registration systems. Gradual introduction of modern information technologies lead to transferring of the information contained in the paper registers to computer databases, as well as consolidating various registers into a single state computer network. These steps have had two major positive impacts: (1) the efficiency of public administration has been greatly improved; and (2) communication between citizens and administrative bodies is faster and more efficient.

3.9 While the use of modern technology can support a well-designed civil registration system, practice shows that it does not guarantee the relevance or accuracy of the data in the system. That said, the efficiency of the overall system depends primarily on the legislative and administrative framework governing the registration process. In this context, information technology should be viewed as a tool for integrating existing registers and increasing efficiency in the sharing of data. In instances where the existing framework provides for the continuous registration of vital information, information technology will significantly enhance the efficiency of data-sharing within the system. But the use of information technology does not resolve problems regarding the communication and sharing of data between responsible authorities if there is no legislative and administrative framework establishing precise and adequate procedures.

4. OPERATIONAL CONSIDERATIONS

4.1 POSSIBLE NEED FOR LEGISLATION/LEGISLATIVE REFORM

- **Regulation**

4.1..1 [TYPE TEXT]

- **Policy**

4.1..1 [TYPE TEXT]

- **Procedure**

4.1..1 [TYPE TEXT]

4.2 LEGAL SYSTEMS — IDENTIY-RELATED VIOLATIONS

- **False Identity**

4.2..1 [TYPE TEXT]

- **Identity Theft**

4.2..1 [TYPE TEXT]

- **Malfeasance, nonfeasance, corruption**

4.2..1 [TYPE TEXT]

- **Synopsis of Existing Regulations and Guidance, e.g., UNSC 1373**

4.2..1 [TYPE TEXT]

4.3 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.

Generally information is shared either:

- within a State, between government agencies, and sometimes with the private sector; and/or
- internationally between governments (whether bilaterally or multilaterally).

The focus of data sharing for the State is to:

- enable issuance (validation of documents or data that relate to the establishment of identity, such as birth or citizenship)
- facilitate travel (sharing passport information with border agencies); and
- 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. (See Section 4.1 Legislative Reform)

Data Access and Matching (within the State)

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 should validate identity information at the source registry. 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 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.[5] 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 off, 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 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 sometimes not 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.

Data Sharing (International)

Accepting a travel document as a token of identity at an international border requires three questions to be answered by the border control agent:

1. Does the document belong to the person providing it?
2. Is the document authentic and was it not falsified in any way?
3. Is the document rightfully issued by the proper authority entitled to issuing it?

Only after all three questions are answered positively, the border control agent needs to 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 analyzing 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 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 in order 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

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

ePassports, is also an important example of international data sharing 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.

States will often have a neighbouring country where their citizens regularly travel (in large numbers), and data sharing will directly benefit both parties.

Interpol Stolen and Lost Travel Documents (SLTD) database

Interpol manages a database known as the Stolen and Lost Travel Documents (SLTD) database which contains detailed information on passports, identity cards, visas etc. reported lost or stolen by countries all over the world. It enables front-line border control and immigration officers to instantly check whether a travel document presented by a traveller has been reported stolen or lost.

All TDIAs should report details pertaining to lost and stolen travel documents to Interpol as soon as possible, preferably within 24 hours of receiving the data. This includes blank passport books as well as personalized documents.

The information to be submitted to Interpol SLTD includes, but is not limited to:

a) document number as displayed in the MRZ (or serial number in a blank book)
b) type of document, i.e. passport or other
c) issuing country's ICAO Code
d) whether the document was issued or blank
e) whether the document was lost or stolen
f) date and place of issuance
g) date and place of theft or loss.

Each country should endeavour to make the Interpol SLTD available to front-line border control and immigration officials for real time screening at all arriving at ports of entry. The database should be available to visa issuing authorities in order to prevent visas from being issued into lost or stolen documents and to law enforcement authorities to detect identity theft or misuse.

To help countries connect easily, Interpol has developed two integrated solutions using either fixed or mobile integrated network databases, known as FIND and MIND. Both can integrate into the existing computer-assisted verification system of a country. In addition, MIND can also be used in a country without an existing system. Access to international data and integration into existing systems are the two main benefits of using MIND or FIND.

⇒ Interpol website on MIND and FIND: www.interpol.int/Public/FindAndMind/Default.asp

Regional Movement Alert System (RMAS)

The Regional Movement Alert System (RMAS) is an APEC initiative enabling positive validation of passports. RMAS enables participating economies to verify the status of passports in real time at the source, and alert the relevant agencies if action is required. In addition to checking for lost, stolen and invalid passports, RMAS is able to determine whether a passport is recognized by its issuing authority as having been validly issued.

⇒ APEC RMAS: http://www.businessmobility.org/RMAL/RMAL.html

Advanced Passenger Information (API)

Many countries now require all airlines or cruise lines carrying passengers into their countries to adhere to the Advance Passenger Information (API) System.

API provides significant benefits by maximising the security of travel and facilitating faster processing of legitimate travellers, while reducing opportunities for travel by unauthorised or improperly documented persons. API provides for:

- Enhanced border security as it provides for more thorough checking of travellers; and
- Increased passenger facilitation because passengers have been 'pre-processed' before arriving at the border.

The implementation of API significantly enhances domestic and regional security by providing advance warning of suspect persons travelling to the country

An API system can be implemented as a batch model or an online model. An economy's choice of API model will depend on the country's business directions, budget and available resources.

A batch model is implemented by sending a list of passengers, generally after the flight departs, to the destination country. In the destination country the list is used to check passengers against the alert lists before the flight arrives.

A batch API system provides early warning of persons of concern and useful intelligence, however, because the system does not return a response to the airline, it cannot be used to prevent a passenger from boarding the aircraft.

In this context, 'online' means that the API data is forwarded electronically to the destination country using a message-based interface. An online API model may be 'interactive' or 'non-interactive'.

The Interactive API system, also known as "Advance Passenger Processing (APP)", "Board/No Board" - "Red Light/Green Light System" and "Authority to Carry", is a system whereby required data elements are collected and transmitted by airlines to border control agencies at the time of check-in.

Passenger data is checked against warning alerts, and may also be checked against visa and passport data. Border alert processing is done for each passenger as they check in, and a message is returned to the airline advising whether or not the passenger should be allowed to board.

In a non-interactive API system, data is processed after the flight closes but before passengers arrive. The data is then verified at the border when the passenger arrives. A passenger who matches a warning alert can be referred for secondary examination on arrival.

ICAO Public Key Directory (PKD)

The ICAO PKD has been established to act as a central broker to manage the exchange of certificates used for the validation of ePassports. Validation provides border control authorities with an assurance that documents are genuine and unaltered, which in turn allows the biometric information contained in ePassports to be relied on to automate aspects of the border clearance process.

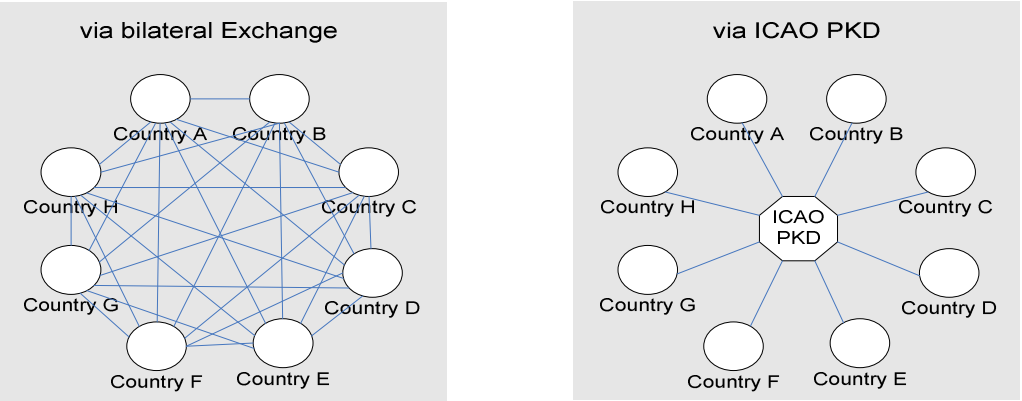
By validating ePassports, border control authorities can confirm that:

- The document held by the traveller was issued by a bonafide authority.
- The biographical and biometric information endorsed in the document at issuance has not subsequently been altered.
- Provided active authentication and / or chip authentication is supported by the ePassport, the electronic information in the document is not a copy (i.e. clone).
- If the document has been reported lost or has been cancelled, the validation check can help confirm whether the document remains in the hands of the person to whom it was issued.

ePassport validation is therefore an essential element to capitalise on the investment made by States in developing ePassports to contribute to improved border security and safer air travel globally. Because the benefits of ePassport validation are collective, cumulative and universal, the broadest possible implementation of ePassport validation is desirable.

The central role of the PKD is critical to minimise the volume of certificates being exchanged, to ensure timely uploads and to manage adherence to technical standards to ensure interoperability is achieved and maintained.

Distribution of Certificates and CRLs



This example shows 8 states requiring 56 bilateral exchanges (left) or 2 exchanges with the PKD (right) to be up to date with certificates and CRLs. In case of 188 ICAO States 35,156 bilateral exchanges would be necessary while there are still 2 exchanges necessary with the PKD.

Without sharing critical information with other nations via the ICAO PKD (or with huge efforts via bilateral agreements), an electronic MRTD has little or no benefit as compared to a non-electronic one.

An ePassport issuer who participates in the ICAO PKD will:

- utilize eMRTD features
- save costs and efforts

- achieve the highest security

- **Internal to an Agency**

4.3..1 [TYPE TEXT]

- **Internal to a National Government**

4.3..1 [TYPE TEXT]

- **Bilateral**

4.3..1 [TYPE TEXT]

- **Multilateral**

4.3..1 [TYPE TEXT]

4.4 RISK ANALYSIS AND MANAGEMENT

- **Profiling**

4.4..1 [TYPE TEXT]

- **Privacy**

4.4..1 [TYPE TEXT]

- **Accessibility**

4.4..1 [TYPE TEXT]

- **Security and Facilitation**

4.4..1 [TYPE TEXT]

4.5 HUMAN RESOURCES

- **Selection and Vetting**

4.5..1 [TYPE TEXT]

- **Performance Measures**

4.5..1 [TYPE TEXT]

- **Rewards and Sanctions**

4.5..1 [TYPE TEXT]

- **Training and Refreshment**

4.5..1 [TYPE TEXT]

4.6 OTHER IDENTITY INTERSECTIONS

4.6.1 A modern and secure document system safeguards identity by linking every issued document to a comprehensive civil registry and identification system. Such a step promotes national and international credibility of a travel document, thereby strengthening border security and helping to prevent terrorist movement. Moreover, it builds the basis for a functioning state infrastructure by developing address systems, death records, tax registers, election lists, etc., thereby strengthening the rule of law and addressing long-term conditions which terrorists exploit.

a) The link between poverty and birth registration; and

b) Chronicling of life events – its relevance for good governance.

Points from "Paper Citizen" worth expanding:

- A record of a life event has significance both as a legal document and as a source of data that are much needed by state policymakers
- Birth registration system
- Birth and identity cataloguing systems
- Blurred membership is informal membership
- A person who lacks proof of identity is, in the eyes of officials, a non-person
- Infrastructure of citizenship – is weak
- Minimal identity infrastructure
- Birth certificate is the first proof of citizenship in many countries and it can led to other documents such as a ration card, voter ID or passport
- Documentary legality has very little meaning in poorer states

Evidence from the field suggests that children go unregistered in developing countries due to:

a) lack of access to the offices responsible for recording births

b) expensive fees and costs associated with the registration process

c) corruption among state officials, who demand bribes for registration

d) lack of understanding among the poor on the need to register a birth

- Citizenship means having access to welfare services and voting rights

- Population registration became a priority in all of these newly states as welfare and other public services were implemented for the benefit of the poor

UN Convention on the Rights of the Child (CRC)

- The child shall be registered immediately after birth and shall have the right from birth to a name, the right to acquire a nationality. Despite this, over 50 million births year globally not registered.

To legalize is to become visible to the state, the sovereign and hence become a star of the state-instituted infrastructure of citizenship. By becoming legal, the individual becomes part of the circle of members who form the political community – the nation that forms the state – and eligible for social=, political and economic rights. In short recognition of the individual is crucial for national sovereignty and for citizenship, yet many states in the developing world can barely confirm the citizenship of individual members.

- Specifically highlight the need to register after Natural catastrophes, wars and civil unrest that produce IDPs and refugees.

- **Voting**

4.6..1 Many states use data from the population register and/or civil register to compile voter lists, to contact voters, and to plan the location of polling facilities.

4.6..2 If the population-registration system is functioning effectively, an election can be planned and executed within a short time period providing that the administrative conditions (i.e. long period required for creation of voter lists) do not impede the process.

- **Immigration**

4.6..1 [TYPE TEXT]

- **Driving**

4.6..1 Over time, the driver's licence has come to be used by many retailers as a reliable document to verify identity. Many organizations and individuals in fact treat the driver's licence as a universal identity card and use it to record information when individuals make purchases, conduct financial transactions or for other purposes.

4.6..2 This is in addition to its main purpose, the physical and administrative proof that a person is certified to operate a motor vehicle. A driver's licence is issued by a government authority and

therefore needs to be considered dependable. It contains a great deal of personal data: photograph, address, birth date, signature, physical description (i.e. height or need for corrective lenses).

- **Health Care**

4.6..1 Government can save time and money on implementing comprehensive health systems that track entire processes. This reduces unnecessary health care costs, increases administrative efficiency, decrease paperwork, enlarges the access to affordable care and increases the level of health care in general. Records and personal medical information must be secured by access control. The cost of an inefficient and non-secured health care system is dangerous, expensive and deadly. An example could be used in United States of America, where 5,8 per cent of American adults or 1.5 million people were victims of Medical Identity theft in 2009. The cost per victim is over $29 000.[6]

4.6..2 Many developing countries struggle to provide universal health care. However, most effort is due to the lack of sufficient resources, or inappropriate use of existing funds. Health inequality, therefore, is quite common and is exacerbated by poverty. In some developing countries health facilities have improved significantly, creating a health divide where those who can afford it can receive good quality care. Health gaps typically mirror equality gaps. For the enormous numbers of people without access to health, there is a terrible irony: poverty exacerbates poor health while poor health makes it harder to get out of poverty. This is compounded in rural settings, where access to health care, as well as other Government services, is not widely accessible.

- **Other**

4.6..1

4.7 VISAS AND PASSPORTS

- **Purposes and Differentiations**

4.7..1 [TYPE TEXT]

- **Entitlement Judgments**

4.7..1 [TYPE TEXT]

- **Information Sharing**

4.7..1 [TYPE TEXT]

4.8 TECHNOLOGICAL TOOLS

- **Rules Based Adjudication and Filtering Software**

4.8..1 [TYPE TEXT]

- **Data Sharing Protocols**

4.8..1 [TYPE TEXT]

[6] http://www.secureidcoalition.org/index.php/news/blog/35-blog/80--identity-authentication-is-the-best-medicine-for-the-healthcare-system

- **Other**

4.8..1 [TYPE TEXT]

4.9 CAPITALIZING ON EXISTING RESOURCES

- **Training**

4.9..1 [TYPE TEXT]

4.9..2 **US DHS Packages**

4.9..3 [TYPE TEXT]

4.9..4 **Fraudulent Document Detection (Fundamentals and Advanced)**

4.9..4.1 [TYPE TEXT]

4.9..5 **Targeting and Risk Management**

4.9..5.1 [TYPE TEXT]

4.9..6 **Legislative Infrastructure Development**

4.9..6.1 [TYPE TEXT]

- **Groundwork of Other Organizations**

4.9..1 **UNCTED**

4.9..1.1 [TYPE TEXT]

4.9..2 **IOM**

4.9..2.1 [TYPE TEXT]

4.9..3 **OSCE**

4.9..3.1 Through its programme on Travel Document Security (TDS), the OSCE Action against Terrorism Unit (ATU) has been instrumental in undertaking programmes and other initiatives that have served to improve the quality and integrity of travel documents in a number of countries. Along with focal concerns for the document itself, the OSCE from the systems sides has specifically defined a corollary mandate on handling and issuance with intent to insure that strong emphasis is placed on securing the identity chain (birth, name change, death, etc.). This has been done through encouraging the development of robust issuance systems which address foundational documents as well as a number of the other systemic factors discussed in this Technical Report (TR).

4.9..3.2 In addition to strengthening handling and issuance systems, the TDS Programme seeks to ensure that MRTDs and eMRTDs in the OSCE region meet ICAO standards and specifications. Moreover

the programme aims to provide border control personnel and check points with the skills and technology to detect fraudulent travel documents or those flagged in INTERPOL databases, is yet another work area of the OSCE.

4.9..3.3 Recognizing that eMRTDs can only be as secure as documents "feeding" into it, future OSCE activities will increasingly need to focus on establishing better practices for national identity management. This will be done through strengthening evidence of identity - foundational documents, civil registry systems and other media used to verify and/or validate a travel document applicant's identity. The international standardization of foundational documents such as identity cards and birth certificates would significantly enhance the issuance process. Similarly identity management systems will have to be bolstered to streamline the decision making process of travel document issuers as issuance systems are modernized to keep pace with document technology.

4.9..3.4 Electronic MRTDs and Public Key Infrastructure (PKI) should be part of a solid national identity management system. Securing the identity chain through the development of robust issuance systems interlinked with civil registry information is a prerequisite that criminals or terrorists do not obtain a genuine travel or identity document under a false identity. In addition, any state investing in the PKI should also consider its versatile applicability beyond travel document security and border control purposes. It could form part of an even more advanced and harmonized border, travel, and identity management environment that makes use of the latest technologies in line with broader state security and mobility objectives in areas such as aviation and trade.

4.9..3.5 Furthermore, electronic validation of eMRTDs strengthens identity infrastructure thereby providing the backbone to a functioning and viable state by securing civil, population, and tax registers, as well health care benefits and election lists. These steps strengthen the rule of law, foster good governance and address long-term conditions which terrorists, extremists and criminals exploit. The vehicle for this is an electronically enabled Card of National Identity, which would perform primary domestic functionalities such as social, commercial and banking services. Moreover, it could be used a travel document in the regional setting when issued in accordance with ICAO Doc 9303, Part 3, Volume 2. For these purposes, the ID card will need to have an electronic data storage medium and, like an eMRP, make use of PKI, which will allow the Country Signing Certification Authority (CSCA) to validate the document and, as a corollary, the authenticity of its bearer.

4.9..3.6 The concept of worldwide enabled signature validation with the ICAO Public Key Directory (PKD) is already a widely accepted precondition for fast and convenient international travel without any security compromise on the basis of the chips contained in eMRTDs. Identity verification at border control through the electronic validation of digital signatures that secure the biographic and biometric data stored on the chips of eMRTDs has already proven to significantly enhance border security measures. This has contributed to strengthening identity management at the border and contributed to counter terrorism measures and to the prevention of illegal cross-border activities involving organized or trafficking in all its forms.

4.9..3.7 In 2010 the OSCE participating States adopted an OSCE Ministerial Council Decision on Travel Document Security to promote the ICAO Public Key Directory (PKD). The Decision calls upon the participating States to consider becoming participants in the ICAO PKD, subject to administrative and financial resources, and thereby to contribute to enabling border control and other relevant national authorities to validate digital signatures of electronic eMRTDs.

4.9..3.8 With this decision, the OSCE participating States took note of the wide scale implementation of eMRTDs by the OSCE participating States and recognized the need to enable relevant national authorities to effectively validate the authenticity of electronic security features and biometric

data stored in eMRTDs. The decision considers this a precondition for the verification of the identity of the bearer of an eMRTD on the basis of the electronic security features and biometric data.

4.9..4 **Other Multilaterals**

4.9..4.1 [TYPE TEXT]

4.9..5 **Other Regionals**

4.9..5.1 [TYPE TEXT]

- **Initiatives Completed or Underway**

4.9..1 EU: [TYPE TEXT]

4.9..2 UN: [TYPE TEXT]

4.9..3 **United States Birth Document Standards**

4.9..3.1 [TYPE TEXT]

4.9..4 **Other**

4.9..4.1 [TYPE TEXT]

4.10 DEVELOPMENT AND INFRASTRUCTURE BUILDING

- **Agreements in Place**

4.10..1 [TYPE TEXT]

- **Agreements Underway**

4.10..1 [TYPE TEXT]

- **More Effective Collaboration with Regional Authorities**

4.10..1 [TYPE TEXT]

5. STANDARDS

5.1 This section of the TR contains guidance on the security of Birth Certificates (BCs), including the security design, printing and personalization of a BC.

5.2 BCs are typically produced as paper documents incorporating security features intended to protect them against counterfeiting and against falsification of the personalised data. This TR also contains recommendations for Issuing Authorities and suppliers on the threats to the security of BCs and describes some of the counter-measures that can be deployed to minimize those risks. Also included are measures to protect against theft of blank BCs and the misuse of a genuine document by an imposter.

5.3 It is recognized that a BC is only one important element of a larger system for capturing and recording the identity details of a newborn child, and effective security requires that the entire registration system is itself robust and secure.

5.4 FUNDAMENTAL PRINCIPLES

- Due to the importance of BCs for confirming evidence of identity and their value as foundational documents, blank (impersonalized) BCs are a prized target for theft during their production, transit and storage. It is therefore important that blank BCs are manufactured and stored in a secure environment with appropriate security procedures in place to prevent theft and to account for all the good and waste documents produced at every stage of production. The audit trail should contain sufficient detail to enable a missing BC to be traced to the last stage of the process at which the document was present and the person responsible for it at that time.

- Likewise, there should be a mechanism to centrally record lost and/or stolen BCs after issuance. When a replacement BC is issued to a person whose original document has been lost, damaged or stolen, care shall be taken to verify the identity of the applicant. The replacement BC should contain a unique document number, different to the number on the originally issued document. It should also be clearly indicated on the replacement BC that it is a replacement and whether it is a first, second or third replacement of the original document. A record should be kept of all BCs issued associating the document number(s) to the identity of the holder. A linkage to the death registry is also strongly recommended to 'close' a record, thus deterring impostors from assuming the identity of a deceased person.

- The practice in some countries of issuing a copy of a BC to someone other than the rightful holder, or his or her parent or legal guardian should be discouraged. However, where it is necessary to continue this practice, the document issued should clearly state that it is a copy and is not valid as proof of evidence of identity. In such cases it is recommended that issuing authorities consider alternative ways of providing the data in a format that is distinctly different to a standard BC document.

- All BCs should contain, as a minimum, a set of security features that will help to protect against possible attempts to counterfeit them and/or tamper with the personal data recorded on them. Some security features that could be included are described later in this section of the TR. These features, if appropriately integrated into a BC, will provide a basic level of protection for the document, but issuing authorities may choose to supplement them with additional features in order to further increase the security of the document. This TRs intent is not to restrict authorities from including additional security above the recommended minimum, in their BCs. On the contrary, raising the level above the minimum is strongly supported, but it is important to establish a baseline, a level below which security should not be permitted to fall, to serve as a guideline for issuers and suppliers of BC's.

- **Physical Document Commonalities**

5.4..1 The production of BCs should be entrusted only to state printing works or other suitably qualified security suppliers and should take place in a secure, controlled environment with appropriate security measures in place to protect the premises against unauthorized access.

5.4..2 Typically, blank BCs are manufactured in one location and despatched to local government offices for completion with the personal details of the newborn child and parents. Secure transport and distribution of the blank BCs from the manufacturer to the local offices is therefore essential, also secure storage and accountability for their use in local government offices. It is important to understand that a stolen, blank BC is a serious threat to the security of the system as it presents the criminal with a genuine document with little risk that the document will be detected as a fake.

5.4..3 Where possible, personalization of BCs in a single central location is the most secure option as it eliminates the need for distribution and storage of blank BCs at multiple sites. Centralised personalization has the added advantage of enabling control over the method of personalization and its compatibility with the blank BC documents. For example, the type of ink or other materials used to infill the personal data on the BC can be uniformly and consistently applied to all documents, while ensuring quality standards are upheld. Uniformity of the personalization technique makes it easier for inspectors to validate the authenticity of the document.

5.4..4 Where centralized personalization is not possible then issuing authorities are strongly recommended to implement robust procedures to ensure security at the local offices. This should include secure storage of all blank BCs and audit and reconciliation procedures to account for all the BCs used, including all waste certificates.

5.4..5 Quality checks and controls at all stages of the production process and from one batch to the next are essential to maintain consistency in the finished birth certificate. This should include quality assurance (QA) checks on all materials used in the manufacture of the documents. The importance of consistency in the finished birth certificate is paramount because government authorities rely on being able to recognize fake documents from variations in their appearance or characteristics. If there are variations in the quality, appearance or characteristics of the State's genuine birth certificate, detection of counterfeit or forged documents is made more difficult.

- **Main Threats to the Security of Birth Certificates**

5.4..1 The following threats to the security of BCs, listed in no particular order of importance, are ways that have been identified in which the document, its issuance and use may be fraudulently attacked:

a) Counterfeiting;

b) Deletion, alteration and substitution of personalised data;

c) Theft of genuine blank documents or genuine component materials;

d) Criminal collusion between workers in issuance offices;

e) Threats to and within an existing system and infrastructure; and

f) Misuse of a genuine BC by an imposter.

5.4..2 To provide protection against these and other threats, a BC requires a range of security features and techniques combined in an appropriate way within the document. Although some security features can offer protection to more than one type of threat, no single feature can offer protection against all types of threat. Likewise no security feature is 100 per cent effective in eliminating any one category of threat. The best protection is obtained from deploying a balanced set of security features and techniques, providing multiple layers of security in the document that combine to deter or defeat fraudulent attack.

5.4..3 It is worthy of mention that of the six types of threat identified above, only the first two (counterfeiting and tampering) can be combated solely through the design and production of a BC document. The other four types of threat require additional security measures to afford protection. In the case of theft or criminal collusion, good physical security in the production environment and effective security procedures are required to ensure that all BCs and components are safeguarded from theft. Also,

there should be full accountability of all BCs produced, personalised and issued including all waste documents. When properly implemented these measures should reduce the risks of fraud and provide an audit trail and traceability in the event that blank BCs or components go missing.

5.4..4 The final category of threat, misuse of a genuine BC by an imposter is potentially the most difficult to detect, because in this case the document itself is genuine but it doesn't belong to the person presenting it. Approaches to combating misuse are:

a) An effective enrolment or registration process to record and store details of all BCs issued by an authority and the ability for that authority to easily access the recorded information.

b) Background checks to further investigate the "social footprint" or "identity footprint" of a person whose details have previously been registered, in order to confirm his or her identity. This may involve comparing information drawn from a number of different sources to ensure that all records correspond. Discrepancies between different records should be further investigated to understand any doubt over the claimed identity.

5.4.6.5 In future, it is possible the development of biometrics technologies may provide a viable mechanism for providing unique personal identification of children at birth. More information on this subject is contained in this TR.

- **Security Features Not Controversial**

5.4..1 [TYPE TEXT]

- Protection against counterfeiting

5.4..1 Techniques that may be employed to protect against counterfeiting include;

a) The use of secure graphics in the design of the document. The images and graphics used to create the document should be designed in such a way that they are difficult to reproduce by copying or scanning. Also, it should not be possible to re-originate the entire image using widely available software design packages. It is strongly recommended that state printing works or other suitably qualified security suppliers should not depend solely on the use of publicly available software for originating the security designs of BCs, but should supplement this with specialist security design software, available only to accredited organizations.

b) The use of secure materials (substrates, inks, holograms etc.) in the document. Using special materials that are not widely available makes it more difficult and more costly for the counterfeiter to reproduce a BC. The materials used in the manufacture of BCs should be sourced only from accredited security suppliers who should manufacture the materials under secure conditions. The specifications of all materials must be compatible with the processes employed in the manufacture and personalization of a BC and it is strongly recommended that discussions are held with all parties in the supply chain before finalising the materials' specifications. Additionally, it should be remembered that BCs may have a very long validity period and hence durability and permanence are important factors to be considered in the choice of component materials. Some security features, for example many types of ultraviolet inks, may not be sufficiently stable to endure for the possible lifetime of a BC and therefore should be avoided unless proper due diligence is performed.

c) The use of special equipment and processes in production of the document. State Printing Works and other suitably qualified security suppliers utilize a range of equipment and processes that are not available outside of the security industry to produce documents that cannot be reproduced by conventional methods of printing. Including, for example, rainbow printing, intaglio and multi-colour close register printing using special inks. The deployment of these effects in a BC should help make the document more resistant to counterfeiting and assist the authentication of genuine documents.

d) The application of specialist knowledge to the security design and production processes. Drawing upon the core expertise of specialist security suppliers and their knowledge of how to design and produce secure documents will help to optimise resistance to counterfeiting. It is important to understand it is not simply the choice of which security features to include that will determine the level of protection achieved, but also the way the features are used and combined within a BC. A good security document is one in which the various features included within it complement and support one another. When this works well it can force the counterfeiter into a compromise in which enhancing one feature adversely affects another so that the combined effect of the features is greater than their individual contribution. In such circumstances, the counterfeiter is forced to trade off one part of the design against another in order to achieve a good rendition of one feature at the expense of a poor result of another, or settle for a sub-optimal reproduction of all the features. In either case the risk of detection is increased and the deterrent to the crime is strengthened.

- **Protection against tampering**

5.4..1 The security techniques required to protect a BC against tampering are different from and in addition to those required to prevent counterfeiting of the document.

5.4..2 Typically this type of fraud involves the unauthorized alteration or manipulation of the personal data entered on a BC after the document has been issued by the authority. This might be to remove, amend or substitute some or all of the original data on the document with false data.

5.4..3 A variety of techniques are used for the removal of personal data from documents, typically these include mechanical erasure (scraping or rubbing) of the data and solvent or chemical attacks. In either case the approach to protecting the document is to ensure that removing the image causes a high degree of collateral damage to the surrounding area of the document. The principle here is that, whilst it may not be possible to prevent tampering, it should always be possible to detect that tampering has occurred. Most security features used to combat this type of fraud are therefore designed to reveal the attack and to increase the visualisation of tampering.

- **Protection against mechanical erasure**

5.4..1 This is normally achieved by ensuring that the document contains an effective printed security background design in the area where personal data is to be entered. In scraping away the personal data, the forger also removes some of the printed design along with the data, adding to the difficulty of repair and concealment of the fraud when substituting new data.

5.4..2 An important consideration when selecting the method of personalization for a BC is to ensure that the inks or other materials used to print the image penetrate the surface of the substrate, so maximising the damage to the surface if the image is removed. Optimization of tamper evidence requires

careful matching of the inks, or other imaging materials used in personalization, with the properties of the substrate.

5.4..3 Where the substrate is paper or another porous material, absorbency is an important factor determining the amount of penetration of ink into the surface of the material. The degree of absorbency can be controlled during papermaking, normally by a process known as sizing, and must be maintained within limits appropriate for the paper's end use. In the case of a BC personalised using a liquid ink, too little absorbency will cause the ink to sit on the surface of the paper making it easier to remove, whilst too much absorbency will cause the ink to spread and will adversely affect the quality and legibility of the image. Inks used for personalization must combine securely with the substrate and must also be highly resistant to fading over the long lifetime of the document.

5.4..4 Naturally the same requirement for longevity applies to the substrate and all other materials contained in the document. It is important to ensure that the specifications of all materials to be used recognize these requirements and that the materials will combine harmoniously in a BC. Although the print produced by most laser printers is lightfast and is unlikely to fade to a point where it can no longer be seen during the life of a BC, typically laser printing does not penetrate the surface of the substrate and is therefore at greater risk of becoming detached from the surface of the substrate. This may occur with ageing due to normal wear and tear, or, it may be the result of fraudulent alteration. For this reason laser printing is not recommended for the personalization of a BC unless additional precautions are taken to secure the image to the substrate, for example by the addition of a protective overlay or laminate.

5.4..5 A second protection against mechanical erasure is the printing of small background fields ("data boxes") where data is expected to be infilled. The background in each box is micro printing of the type of data to be provided. NAMENAMENAME repeated for a name field, DATEDATEDATE for a date field, etc. The light but distinct letters provide a powerful but inexpensive "tell-tale" to physical tampering. The data boxes do not require borders.

- **Protecting against erasure by chemicals or solvents**

5.4..1 Protection is typically achieved by using reactive inks to print the security background design and by including chemical sensitizers in the substrate. Reactive inks are special types of printing ink which "bleed" or otherwise react visibly when the printed image comes in contact with a wide range of commercially available solvents. They are normally used to print the security background design in a document, often in rainbow (iris) printing.

5.4..2 Chemical sensitizers are materials added to the paper during the papermaking process that, in the finished paper product, react when they come in contact with a wide range of solvents that might be used to erase data on a BC, to leave an irreversible stain on the paper. Whether in the inks or the paper, the effect of chemical sensitizers is to cause collateral damage to the areas around the attack, either through the removal of part of the security background printing or by staining of the substrate. These two techniques (paper sensitization and reactive inks) are frequently used in combination in a document to afford maximum protection to chemical erasure.

5.4..3 It must be stated that some chemical sensitizers may not be sufficiently stable to survive the life of a BC and some may have a reaction to extreme conditions of temperature and humidity. Issuers are therefore recommended to discuss with their suppliers the specific selection of these materials and to ensure that appropriate testing is undertaken to confirm their fitness for purpose.

5.4..4 The key message to be drawn from the above paragraphs on protection against counterfeiting and tampering with a BC is that the best results are obtained by adopting an end-to-end approach in which a BC is designed and printed with cognisance of the method of personalization, be it

by pen and ink or by an automated system. It is important that in specifying requirements to suppliers and sub-contractors that compatibility of the overall solution is clearly defined and understood by all parties in the supply chain also where the responsibility lies at each process interface.

- **Authentication of a birth certificate**

5.4..1 Authentication is the process whereby a document is checked and its provenance determined. Documents may be authenticated using a variety of methods: by visual examination; by the use of equipment designed to detect machine verifiable features; and by machine-readable data stored in the document. In the case of BCs it is assumed that the primary method of authentication, at least in the short to mid-term will be by visual checks. For these checks to be effective, the examiner must possess a level of familiarity with the document and ideally some understanding of what to expect of the various security features it contains. The following paragraphs offer some suggestions to facilitate authentication.

5.4..2 Provide information to examiners on what to check for in a BC. This can be done in a variety of ways including printed instructions, training programmes and on-the-job training. These types of education programme are important ways of communicating "what to look for in the document" to the examiners who play a key role in the whole process. No matter how good the security design of a BC may be, it can only be effective if the people responsible for inspecting it understand how to check its authenticity. Where appropriate, on-line delivery of information and services is recommended to distributed inspection points in support of document authentication. Reduce the number of variants of a BC issued by an authority. The more variants in circulation the more difficult it is to acquire familiarity with them and the greater the risk that fraudulent documents will pass inspection. Rationalizing the number of variants in circulation at any given time will help to reduce the potential for confusion. Also, where possible, a "reference library" of all the variant BC types issued by an authority, ideally accessible to Examiners on-line, would be highly desirable.

5.4..3 If possible, where variants are necessary, adopt a common design theme at a national level for the security background printing and a common layout and format for the personal data fields. This will help examiners to recognize a BC as belonging to a specific set of similar documents and will assist in locating personal data on a document.

5.4..4 Adopt a set of secure recognition features that are common to all variants for example; watermark, hologram, intaglio etc. Using a common set of security features on all variant types of BC issued by an Authority reduces the training requirement for Examiners and aids recognition.

5.4..5 Adopt a single size of document for all variants If possible standardize on a single size of document for all the BC variants issued by an authority. Again this will help to aid recognition and simplify the production of BCs. Larger size documents (A4 or Letter) are also recommended, to deter the holder from carrying them in a wallet or purse.

5.4..6 Standardize materials' specifications across the full range of BC variants: This will help to preserve the "look and feel" of all the documents and should ensure they all react to ageing in a similar way.

5.4..7 Adopt a common personalization technology: Using the same method of personalization for all BCs issued by an authority will help to aid recognition and will enable the security of the personalization process to be optimised and matched to the properties of the substrate.

5.4..8 Maintain a record of all issued, cancelled (damaged), lost or stolen BCs and the means to cross-reference the record of their issuance. This provides the means to check that the data on a BC under examination corresponds exactly with the certificate at the time it was issued. However, it is important to

understand that this check, whilst it may confirm that the BC contains a valid data record, it does not guarantee that the person presenting it is its rightful owner. This is another aspect of identity confirmation and a major subject in its own right: Readers wishing for further information on this topic are referred to ICAO Doc 9303, Part 1, Vol. 1; Appendix 3 to Section III, entitled "The Prevention of Fraud Associated with the Issuance process".

- **Substrate materials**

5.4..1 The selection of the substrate, security features and the personalization technique must reflect the intended lifecycle of the document. Particular attention should be given to the environmental conditions in which documents will be stored or used, and the longevity of individual components and security features over extended periods of time.

5.4..2 All components of the document should be fully tested to ensure their suitability for the life of the document. Areas requiring particular attention are:

a) The archival (ageing) properties of the substrate material used.

b) Light and chemical fastness of inks and other materials used in manufacture, including any fluorescent materials.

c) Resistance of any metallic components (inks, holograms etc.) to degradation over time.

d) Resistance to deterioration over time of any polymeric materials used in manufacturing the documents, including any holographic features.

e) The ageing properties and performance over time of any taggant materials used in the manufacture of the documents.

5.4..3 It is recommended that birth certificates issued at different jurisdictions within the state adhere to a minimum set of security features and general appearance, to facilitate inspection by the other stakeholders involved with identity management (e.g. border officials, passport issuing authorities, etc.) Similarly, it is recommended that guidance material regarding the security features is available to authorized recipients involved with document inspection.

- **Paper forming the substrate of a birth certificate**

5.4..1 [TYPE TEXT]

- Basic features

a) UV-dull paper, or a substrate with a controlled response to UV, such that when illuminated by UV light it exhibits a fluorescence distinguishable in colour from the blue used in commonly available fluorescent materials;

b) Watermark comprising two or more grey levels;

c) Appropriate chemical sensitization in the paper to be compatible with the life of the document the personalization technology and protective laminate if used;

d) Paper with appropriate durability, permanence and image receptivity and substance of at least 120 gsm; and

e) Appropriate chemical properties (i.e. pH neutral) reflecting the intended lifecycle of the document.

- **Additional features**

a) Watermark in register with security printed design;

b) A cylinder mould watermark;

c) Visible and/or invisible fibres;

d) A security thread (embedded or windowed) containing additional security features such as micro print;

e) A taggant designed for detection by special equipment

f) Preferably a large size (e.g. A4, US Letter, etc), which deters the document from being carried in a wallet.

- **Synthetic Substrates**

a) UV-dull substrate, or a substrate with a controlled response to UV light such that when illuminated by UV light it exhibits a fluorescence distinguishable in colour from the blue used in commonly available fluorescent materials; and

b) appropriate chemical sensitisation in the substrate to be compatible with the personalization technology.

- **Additional features**

a) Transparent window features;

b) Colour shifting substrates;

c) A taggant designed for detection by special equipment;

d) Features visible through transmitted light (similar to a watermark);

e) Security printing; and

f) Background and text printing.

5.4.19 **Basic features (see glossary of terms)**

a) Single-colour intaglio printing, including a latent image, outside the data field areas of the document;

b) Two-colour guilloche security background design pattern (*);

c) Rainbow printing;

d) Micro-printed text; (e.g. used as a background in the data fields to deter “cut and paste”);

e) Duplex security pattern; and

f) Unique document number printed on every blank BC.

5.4.20 **Additional features**

a) Multi-coloured intaglio printing comprising a “black-line white-line” design;

b) Latent intaglio image;

c) Anti-scan pattern;

d) Relief (3D) design feature;

e) Front-to-back (see-through) register feature;

f) Deliberate error (e.g. spelling);

g) Tactile feature; and

h) Unique font(s).

(*) Where the guilloche pattern has been computer generated, the image reproduced on the document must be such that no evidence of a pixel structure shall be detectable. Guilloches may be displayed as positive images, where the image lines appear printed with white spaces between them or as negative images, where the image lines appear in white, with the spaces between them printed.

5.4.21 **Inks**

5.4.22 **Basic features**

a) Reactive inks which are compatible with the document life, substrate and personalization technique; and

b) Optically variable or reflective feature (to deter reproduction through copier/scanner technology).

5.4.23 **Additional features**

a) Metallic ink;

b) Penetrating numbering ink (compatible with the life of the document);

c) Metameric ink;

d) Infrared drop-out ink;

e) Infrared wavelength shifting ink (anti-Stokes);

f) Phosphors

g) Tagged ink; and

h) Fluorescent inks (compatible with the life of the document).

- **Numbering**

5.4..1 It is strongly recommended that a unique document number be printed on every BC and a record kept associating the number to the identity of the Holder and used to facilitate the creation and use of a document database. (See also para. 3.1 Background and text printing)

5.4..2 **Basic features**

a) Blank birth certificates shall contain a unique document number;

5.4..3 **Additional features**

a) Special style (font) of figures or typeface;

b) Penetrating numbering ink (compatible with the life of the document);

c) Machine readable font or barcode to facilitate tracking of documents;

d) Protection against copying of blank documents; and

e) Need for anti-copy protection.

- The current state of development of generally available digital reproduction techniques and the resulting potential for fraud means that high-grade security features in the form of optically variable features or other equivalent devices may be required as safeguards against copying and scanning. Emphasis should be placed on complex optically variable feature technologies, or equivalent devices, complementing other security techniques. Particular emphasis should be given to easily identifiable, visual or tactile features which are examined at level one inspection.

- Appropriate integration of optically variable feature components or other equivalent devices into a birth certificate will also help to protect against other forms of counterfeiting. If such features are attached to the BC by the use of adhesives, the bond strength and permanence of those adhesives must be suitable for the lifecycle of the document and must also be resistant to tampering.

- Anti-copy protection methods

- The document should incorporate basic printed features such as micro text, anti-copy patterns and colour selections which deter simulation by conventional means.

- One or more optically variable features should be used on the birth certificate as a “basic feature”. The feature should not impair the legibility of the entered data;

- When the birth certificate is made entirely of a synthetic substrate; devices such as a windowed or transparent feature, a laser-perforated feature, and/or others that are considered to offer equivalent protection may be used in place of an optically variable feature;

- When the BC is to have no overlay or laminate protection with a DOVID, then an optically variable feature (preferably based on a diffractive structure) should be included in the document. Where the birth certificate is to be protected with a laminate or overlay, the material and its adhesive must be suitable for the lifecycle of the document and must be tamper resistant.

- **Personalization**

5.4..1 **Birth certificate personalization**

5.4..2 This is the process by which the biographical data of the holder of the birth certificate is applied to the document. It adds the personalised details of the holder to the document and, after issuance of the document, this data is at risk of fraudulent alteration.

5.4..3 Traditionally, data has been applied to BCs manually by pen and ink, and, where this is the practice, care must be taken to ensure the permanence of the personalised data is compatible with the lifespan of the document and is suitably resistant to fraudulent alteration.

5.4..4 Many States may wish to enter the personalised data into a database and print it onto a BC using one of the computer-printer technologies.

5.4..5 To ensure that data printed in this way is properly secured against attempts at forgery or fraudulent alteration it is very strongly recommended to integrate the biographical data into the basic material of the birth certificate. A variety of technologies are available for personalising the document in this way, including the following, which are listed in no particular order of importance and without precluding the development of new technologies:

a) Laser toner printing;

b) Thermal transfer printing;

c) Laser engraving;

d) Impact printing;

e) Inkjet printing.

5.4..6 All dyes pigments polymers and other materials used by any personalization process must be stable to last the intended lifecycle of the document

5.4..7 Laser toner printing should not be used to personalise birth certificates that are not protected by a secure laminate or overlay.

5.4..8 Choice of document personalization technology

5.4..9 The choice of a particular personalization technology is a matter for individual States and will depend upon a number of factors, such as the volume of birth certificates to be produced, and whether the country issues birth certificates centrally or from decentralised sites. The personalization

technology should be uniformly deployed at all issuing sites to ensure consistency in the finished document.

5.4..10 Whichever method is chosen, it is essential that precautions be taken to protect the personalised details against tampering. This is important because the unprotected biographical data remains vulnerable to alteration. The application of a heat-sealed laminate with frangible properties, or an overlay or equivalent technology that provides evidence of tampering can provide additional protection. Where a protective laminate or overlay is introduced, care should be taken to ensure it does not interfere with other security features (e.g. tactile features) on the BC.

5.4..11 **Protecting the personalization against fraudulent alteration**

5.4..12 The following security features, correctly deployed in the document, will help protect the personalised data from manipulation.

5.4..13 **Basic features**

a) Personalised data integrated into the basic material;

b) The security printed background (e.g. guilloche) merged with but not obscuring the personalised data;

c) Use of reactive inks and chemical sensitizers in the paper;

d) Use of a heat-sealed, secure laminate or overlay to protect the personalization data or an alternative combination of a personalization technology and substrate material that provide an equivalent resistance to fraudulent alteration of the data.

5.4..14 **Additional features**

a) Personalization using a special type face;

b) Penetrating inks;

c) Overlay or laminate containing advanced optically variable devices.

5.4..15 Protection against theft and abuse of genuine blank birth certificates

5.4..16 Blank birth certificates should be stored in locked and appropriately supervised premises. The following measures should be adopted:

5.4..17 **Basic measures**

a) Good physical security of the premises with controlled access to delivery / shipment and production areas, and document storage facilities;

b) Full audit trail, with counting and reconciliation of all materials (used, unused, defective or spoiled) and certified records of same;

c) All document blanks and other security-sensitive components (e.g. laminates) serially numbered with full audit trail for every document from manufacture to dispatch, as applicable;

d) Where applicable, tracking and control numbers of other principal components (e.g. security paper, laminates and security inks);

e) Secure transport vehicles for movement of blank documents and other principal document components (if applicable);

f) Details of lost or stolen birth certificate blanks to be rapidly circulated between government departments;

g) Appropriate controls to be in place to protect the production procedures from internal fraud;

h) Thorough security vetting of staff.

5.4..18 **Additional security**

a) CCTV coverage / recording of all production areas, where permitted

5.4..19 **Civil Registry Procedures**

5.4..20 [TYPE TEXT]

- **Civil Registration Eligibilities and Entitlement Parameters**

5.4..1 [TYPE TEXT]

- **Vital Records Database Specifications**

5.4..1 [TYPE TEXT]

5.5 ADVANCED

- [TYPE TEXT]

6. BEST PRACTICES

6.1 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 including 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:

- creating a fictitious identity
- altering one's own identity (identity manipulation)
- stealing or assuming a pre-existing identity (identity theft)
- stealing or assuming a pre-existing identity, which is subsequently manipulated.

NOTE –
(1) 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.

(2) Identity manipulation involves the alteration of one or more elements of identity (e.g. name, date of birth) to dishonestly obtain dual or more access to services or benefits or to avoid establishing obligations.

What are some types of identity-related risk?

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

- *Financial loss or liability* as a 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.
- *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.
- *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 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.
- *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 and appropriately and closely managed. At worst, a release of in-confidence, sensitive information or information with a National Security classification to unauthorised parties, resulting in loss of confidentiality with a high impact.
- *Domino Effects 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 organisations. Alternatively, severe downstream consequences may occur if the holder of that passport uses it to engage in a destructive act made possible by using that passport to gain access to another country.
- *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.

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 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:

- Establishing the scope of the assessment;
- Determining the threats, and assessing the likelihood and impact of threat occurrence;
- Assessing the risk based on the adequacy of existing safeguards and vulnerabilities; and
- 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 country to country, 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 know best what the vulnerabilities are, are the people who work with the systems and procedures for establishing and validating identity. It is wise to ask the staff periodically 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 ISO 31000 (http://www.iso.org/iso/catalogue_detail.htm?scnumber=43170).

- **Financial Loss or Liability**

6.1..1 [TYPE TEXT]

- **Inconvenience, Distress or Damage to Existing Reputation**

6.1..1 [TYPE TEXT]

- **Harm to Public Programs or Public Interest**

6.1..1 [TYPE TEXT]

- **Unauthorized Release of Sensitive Information**

6.1..1 [TYPE TEXT]

- Domino Effects of an Improper Identity Document Used to Acquire Serives of Third party or Another Document

6.1..1 [TYPE TEXT]

- Personal and Public Safety

6.2 GENERALLY ACCEPTED FRAUD INDICATIORS

- [TYPE TEXT]

6.3 CURRENT FRAUD REFERENCE MATERIALS

- [TYPE TEXT]

6.4 USE OF BIOMETRICS

- [TYPE TEXT]

6.5 PUBLIC INFORMAITON AND AWARENESS PROGRAMS

- [TYPE TEXT]

6.6 BORDER AND INSPECTION PROGRAMS

- [TYPE TEXT]

6.7 OTHERS

- [TYPE TEXT]

6.8 A FEW EXAMPLES

- Accept only original documents or copies certified by the issuing authority of the particular document. This allows examination of all security features that are not immediately obvious and are difficult to replicate, such as watermarks and embossing. Photocopied documents are relatively easy to alter and should, therefore, not be accepted as evidence of identity.

- Accept only documents that are currently valid. A valid document is one that has an expiry date that has not yet passed. Documents that are not valid tend to be relatively old and are less likely to contain security features, making them easier to forge or tamper with. Where documents that are not valid are accepted, consideration needs to be given to requiring additional documents/records to corroborate the details contained in the older document.

- 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, in addition to name, date, place and country of birth, also list gender and parental details. 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.

- Unless confirmation of long-term name usage is required, only accept evidence of 'use in the community' documents that are less than one year old.

- Require documented evidence of any name change - (e.g. property deed, marriage certificate, or a statutory declaration).

- Where the authenticity of a particular document is questionable, verify the authenticity of that document with the issuing authority.

7. REFERENCE MATERIALS

1. xxx
2. xxx
3. xxx

8. GLOSSARY

8.1 The glossary of terms in this document is included to assist the reader with understanding the general meanings of such terms within the context of this document. This glossary is not intended to be authoritative or definitive.

Anti scan pattern: An image usually constructed of fine lines at varying angular displacement and embedded in the security background design. When viewed normally, the image cannot be distinguished from the remainder of the background security print but when the original is scanned or photocopied the embedded image becomes visible.

Black line white line design: A design made up of fine lines often in the form of a guilloche pattern and sometimes used as a border to a security document. The pattern migrates from a positive to a negative image as it progresses across the page.

Chemical sensitizers: Security reagents to guard against attempts at tampering by chemical erasure, such that irreversible colours develop when bleach and solvents come into contact with the document.

Civil Registration System: The civil registration system refers to governmental machinery set up in the country, state, province or any other territorial subdivision of the country for the purpose of legal recording of vital events related to the civil status of the population on a continuous basis, as provided by the laws and regulations of the country, state, province, etc.

Counterfeit: An unauthorised copy or reproduction of a genuine security document made by whatever means.

Document blanks: A document blank is a birth certificate that does not contain the personalised details of the document holder. Typically, document blanks are the base stock from which personalised birth certificates are created.

Duplex design: A design made up of an interlocking pattern of small irregular shapes, printed in two or more colours and requiring very close register printing in order to preserve the integrity of the image.

Embedded image: An image or information encoded or concealed within a primary visual image.

Fibres: Small, thread like particles embedded in a substrate during manufacture.

Fluorescent ink: Ink containing material that glows when exposed to light at a specific wavelength (usually UV) and that, unlike phosphorescent material ceases to glow immediately after the illuminating light source has been extinguished.

Forgery: Fraudulent alteration of any part of the genuine document e.g. changes to the personalised data.

Front to back (see through) register: A design printed on both sides of a birth certificate which when viewed by transmitted light forms an interlocking image.

Guilloche design: A pattern of continuous fine lines, usually computer generated, and forming a unique image that can only be accurately re originated by access to the equipment, software and parameters used in creating the original design.

Heat sealed laminate: A transparent protective material designed to be bonded to a birth certificate by the application of heat and pressure after personalization of the document.

Impostor: A person who assumes a false name and identity to represent himself or herself as another person for the purpose of using that person's birth certificate.

Infra red drop out ink: An ink which forms a visible image when illuminated with light in the visible part of the spectrum and which cannot be seen in the infra red region.

Laser perforation: A process whereby images (usually personalised images) are created by perforating the substrate with a laser. The images may consist of both text and tonal images and appear as positive images when viewed in reflected light and as negative images when viewed in transmitted light.

Latent image: A hidden image formed within a relief image which is composed of line structures which vary in direction and profile resulting in the hidden image appearing at predetermined viewing angles, most commonly achieved by intaglio printing.

Metallic ink: Ink exhibiting a metallic like appearance.

Metameric inks: A pair of inks formulated to appear to be the same colour when viewed under specified conditions, normally daylight illumination, but which are a colour mismatch at other wavelengths.

Micro printed text: Very small text printed in positive and/or negative form, usually as part of the background security design.

Optically variable feature (OVF): An image or feature whose appearance in colour and/or design changes dependent upon the angle of viewing or illumination. Examples are: features including diffraction structures with high resolution (Diffractive Optically Variable Image Device/DOVID), holograms, colour shifting inks (e.g. ink with optically variable properties) and other diffractive or reflective materials.

Overlay: An ultra thin film or protective coating that may be applied to the surface of a document in place of a laminate.

Penetrating numbering ink: Ink containing a component, normally coloured, which penetrates deep into a substrate.

Personalization: The process by which the document holder's personalised data are applied to a birth certificate

Personalised data (biodata): The personalised details of the holder of the document infilled as text on the Birth Certificate.

.

Phosphorescent ink: Ink containing pigment, which glows when exposed to light of a specific wavelength, the reactive glow remaining detectable and decaying after the light source is removed.

Photochromic ink: An ink, which undergoes a reversible colour change when exposed to UV light.

Physical security: The range of security measures applied within the production environment to prevent theft and unauthorised access to the process.

Planchettes: Small visible (fluorescent) or invisible fluorescent platelets incorporated into a document substrate material at the time of its manufacture.

— END —