International Civil Aviation Organization

WORKING PAPER

TAG/MRTD/21-WP/4
22/11/12
Revised
05/12/12
English only

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

TWENTY-FIRST MEETING

Montréal, 10 to 12 December 2012

Agenda Item 2: Activities of the NTWG

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

(Presented by the NTWG)

1. INTRODUCTION

1.1 At the Twentieth Meeting of the Technical Advisory Group on Machine Readable Travel Documents, held from 7 to 9 September 2011 (TAG/MRTD/20), the ICAO Secretariat presented TAG/MRTD/20-WP/5 on the Technical Report (TR) entitled *Towards Better Practice in National Identification Management*. This initiative has been led by the Secretariat within the framework of the NTWG, and presents an on-going work item to expand the relevance of the MRTD Programme to today's travel document and border security needs.

1.2 The TAG/MRTD/20 acknowledged and supported the work done on evidence of identity in the Technical Report *Towards Better Practice in National Identification Management*, Version 1.0, and approved the continuation of the development of the report under the responsibility of the NTWG.

2. WORK DEVELOPMENT

2.1 A subgroup of the NTWG was formed to contribute and enhance the work achieved with the TR. A few members met in Fredericksburg on 24 to 25 May 2012, significantly progressing the development of the TR. Further exchanges were held during the NTWG meeting held in Zandvoort on 7 to 11 November 2011, and via electronic means throughout this process.

2.2 The resulting draft TR was posted as Release 2, Version 3.4 on the NTWG web site for comments. A number of comments and suggestions were received and incorporated, resulting in Release 2, Version 4.0, which is included at Appendix A. Some comments and suggestions were not included in the preparation of this version, as these may be open for discussion by Members and Oberservers at the TAG/MRTD/21 Meeting.

3. ACTION BY THE TAG/MRTD

3.1 The NTWG invites the TAG/MRTD to:

a) acknowledge the work done on Evidence of Identification, documented in the attached Technical Report on *Towards better Practice in National Identification Management***,** Release 2, Version 4.0;

b) note that the ICAO MRTD Programme is expanding its relevance to today's travel document and border security needs to ensure a common level of integrity across the issuance, production and use of travel documents, utilizing the guidance material on the issuance of travel documents to achieve the programme outcomes; and

c) approve the work done on the TR, as well as the continuing development under the responsibility of the NTWG. The current draft version will be presented for discussion and subsequent endorsement at the upcoming NTWG Meeting, scheduled to take place during the first quarter 2013. The endorsed version of the TR will then be forwarded to TAG/MRTD Members, under cover of a TAG/MRTD Memorandum.

— — — — — — — —

APPENDIX A

MACHINE READABLE TRAVEL DOCUMENTS (MRTDs)

TOWARDS BETTER PRACTICE IN NATIONAL IDENTIFICATION MANAGEMENT

TECHNICAL REPORT

Version: Release 3

Status: Draft 4
Date: 20 November 2012

INTERNATIONAL CIVIL AVIATION ORGANIZATION

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

Table of contents

1. EXECUTIVE SUMMARY

ICAO’s interest in travel security has, in the past, largely concentrated on the security of the travel document itself. However, ICAO's interest is wider with a goal to ensuring that a consistent level of security and integrity applies to all components of the 'travel continuum': the application and supporting documents, the interview (where required), and the the adjudicative decision-making processes. The provision of a highly secure blank travel document allows the approval decision to be followed by secure personalization and issuance, with interoperability at international borders. .

This Technical Report (TR) highlights the need for consistent effort across all processes. However, it suggests that in the decision processes, particularly the establishment of confidence in a person's identity,, is an area that can easily fall behind in the strength of its security when compared with that of the document itself.

Current ICAO guidance does not set standards for how confidence in a person's identity should be established, as the best way of achieving this will vary from country to country, depending on local laws, customs, and the uses to which 'foundation' documents are put. Rather it sets out a framework of outcomes which should be achieved in order to be confident in a person's identity prior to issuing a travel document.

2. INTRODUCTION

2.1 BACKGROUND

The rapid growth of identity fraud affects many areas of society and raises serious concerns for security and safety. Much work has been done in the area of travel documents to combat document fraud and increase passport security and the associated systems for the personalization and issuance of these documents. Border authorities have upgraded their document inspection systems and passenger checks to improve security at border inspection, providing increased security from both ends of the travel continuum, while the increased use of international data sharing has resulted in improved detection of identification fraud.

These measures have been successful in raising the level of passport security. However, they have resulted in the shift away from travel document fraud (alteration, counterfeit) to attempts to obtain a genuine passport based on identity fraud, which includes the creation of a fictitious identity;
the alteration of one's own identity (identity manipulation); and
the theft of a pre-existing identity..

The ability of a criminal to perpetrate this and other similar types of fraud relies upon deceiving the authorities into accepting a bogus identity during the application (enrolment) process. This could include both entirely fabricated identities (with either genuine for forged documentation), imposture to an identity, or critical modification (such as a place of birth) to the applicant's true identity, which is then supported by fraudulently-obtained documents.This process requires, among other things, for the applicant to provide "Evidence of Identification" in order to substantiate and justify the claim of entitlement. Often, applications are accompanied by false or fraudulently obtained identity records such as birth or citizenship certificates, generally known as "breeder documents, "that are used to obtain a legitimate entitlement. (Throughout this TR the terms breeder documents, foundational documents and source documents are used interchangeably to describe a document, genuine or fraudulent, that can serve as a basis to obtain identification documents or benefits).

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

2.2 RATIONALE FOR ICAO'S INVOLVEMENT IN EVIDENCE OF IDENTIFICATION

Many ICAO member states have invested time, money and great expectations in enhanced travel document programs, especially in machine readable ePassports. The ICAO Machine-Readable Travel Document (MRTD) Programme has long advocated for security improvements to the physical document, and for its proper use at borders, setting standards and specifications for issuing the most secure and advance current generation of travel documents.

Fraudsters will generally seek the path of least resistance, and in many states this path is the issuance process. The targeting of the issuance process by fraudsters can damage reputation gains made by increasing the physical security of the document. It also can undermine the state's financial investment in improved secure technology. If there are gaps in the process that make it easier to secure a Falsely

Obtained Genuine (FOG) document, then the fraudsters will seek this method, rather than forgery. The resulting document is genuinely issued by the Travel Document Issuing Authority (TDIA), 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 source documents, civil registry records, databases, and other media that are used to validate an applicant's identity. Identity management is the gathering, verification, storage, use and disposal of this kind of identity information, and robust identity management is one of the keys to producing a secure travel document.

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

2.3 ICAO'S MANDATE ON EVIDENCE OF IDENTIFICATION

As part of a larger strategic scope for traveller identification, ICAO's involvement in Evidence of Identification relates to its contribution on building trust in travel documents for the international community. The goal is to assist in establishing credible and effective processes and protocols involving the tracing, linkage and verification of identity against so-called breeder documents or other sources and means of determining authenticity of identity, to ensure authenticity of the identity of an applicant seeking issuance of a travel document, confirming for that individual: a *unique* identity linked to the applicant; the identified individual's status as *still living*; and the applicant's status as an *active user* of that unique identity.

The aim of ICAO's work on this subject matter is to ensure that appropriate authorities worldwide recognize the interdependency of all aspects related to of identification and travel document management and related control functions in view of keeping the integrity and security of such systems and documents. It also aims that appropriate authorities have the ready ability to provide efficient, timely and reliable confirmation of the true identity of travellers and other persons of interest, and—where desired and relevant—to efficiently and reliably link the identity to other relevant information about the traveller or person of interest, where that can support security, facilitation and other related objectives.

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. In many States the TDIA is one of the most important authoritative sources of identity information. It is therefore the establishment of identity, and validation of identity, that ICAO is most focussed on – and largely for the purposes of security. Identity fraud is an enabler for a range of criminal activities, from organised crime to terrorism, making weak identity management processes in the travel document issuance and border sector a target to criminals. If States do not undertake the necessary steps to identify individuals effectively, the repercussions can be extremely serious. As authoritative sources, there is an obligation to ensure that identity is established with a high degree of assurance.

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

citizenship and/or nationality to assess entitlement of the passport applicant. All of which support the work developed and implemented within this TR.

2.4 PURPOSE OF THIS TECHNICAL REPORT

The purpose of this TR is to provide a full and comprehensive perspective on the kinds of factors to be considered and the nature of sources that should be consulted in order to develop a complete perspective for entitlement and document adjudication judgements and decisions. This TR seeks to bring to the reader's attention not only to documents but also to all of the other accompanying ways in which the Evidence of Identification considerations should be viewed.

This TR is intended as provide guidance material and is not to set Standards and Recommended Practices (SARPs)) as adopted by the ICAO Council in accordance with Articles 37, 54 and 90 of the Convention of the International Civil Aviation and designated, for convenience, as Annexes to the Convention (as in example, Annex 9 – Facilitation, which contains SARPs regarding the issuance of MRTDs). It is intended to be used by individuals and agencies engaged in the full spectrum of identity management, including the staff of issuing authorities, inspection and police authorities, and immigration authorities as well as those engaged in other document entitlement endeavours. This would include issuers of driver's licenses, cards of national identity, citizenship documents, voter registration et al. In addition, the TR is especially relevant to those involved in civil registry and other vital records-related management activities, in particular, those who are responsible for entitlement adjudications for birth and death records, marriages and divorces certificates, name changes and various other civil registry matters.

2.5 SCOPE

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

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

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

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

This set of criteria is expanded in Table 1 (see below). This document is not prescriptive in how to establish each of these goals. Means used to establish these, include: use of civil registration systems, social footprint checks, and verification of source documents.

3. EVIDENCE OF IDENTIFICATION (EOI)

EOI refers to the establishment of evidence through various sources of documents (i.e. driver's licence, passport or birth certificate) that, when combined, provides confidence that an individual is who he/she claims to be.

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

A basic premise of most EOI frameworks is that the amount of confidence an agency requires before it 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:

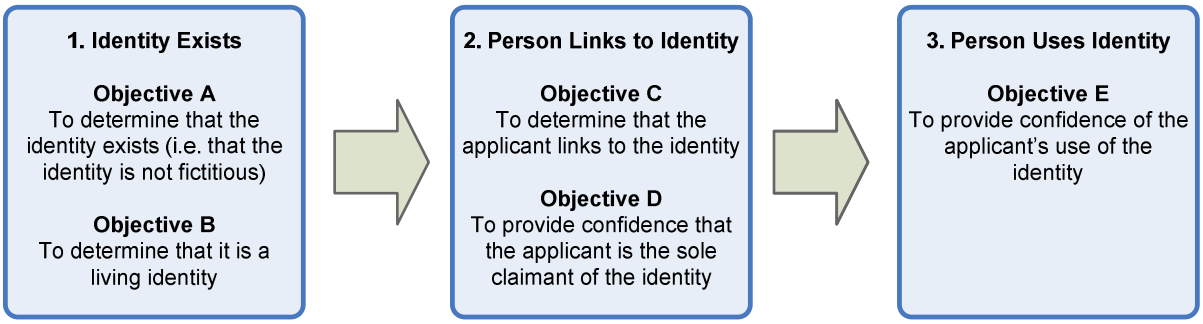


Figure 1.1

This document gives guidance on how to achieve these objectives. It is impossible to be prescriptive in how to achieve these as the appropriate means to achieve any of these objectives depends on a country's customs, legal frameworks and working practices, and will differ from one country to another. However, TDIAs should ensure that they can show that they have processes and policies in place to meet all these objectives.

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 (i.e is not fictitious), and that the identity is not deceased.

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

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

a) Ask for original documents that show that the identity exists, such as a birth or citizenship certificate. These documents should ideally be thoroughly examined and validated against source data to combat the risk of forged breeder documents.

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

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 (i.e 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 could:

a) 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)

b) Undertake checks to establish the 'social footprint' of the identity (i.e. evidence that the person has a history of using and currently uses their claimed identity in the community).

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

a) States with smaller populations may be unable to interview all applicants (there may not be sufficient infrastructure to make it viable)

b) There may be multiple valid versions of breeder documents available for use

c) Legislation may prevent validation of documents, access to source registers, or information sharing between government departments and countries

d) Historic travel or breeder document records may be paper based – leading to a highly time consuming manual checking process

e) 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 'breeder' documents and records, to understand how much confidence can be gained from the document/record's inclusion in the EOI process.

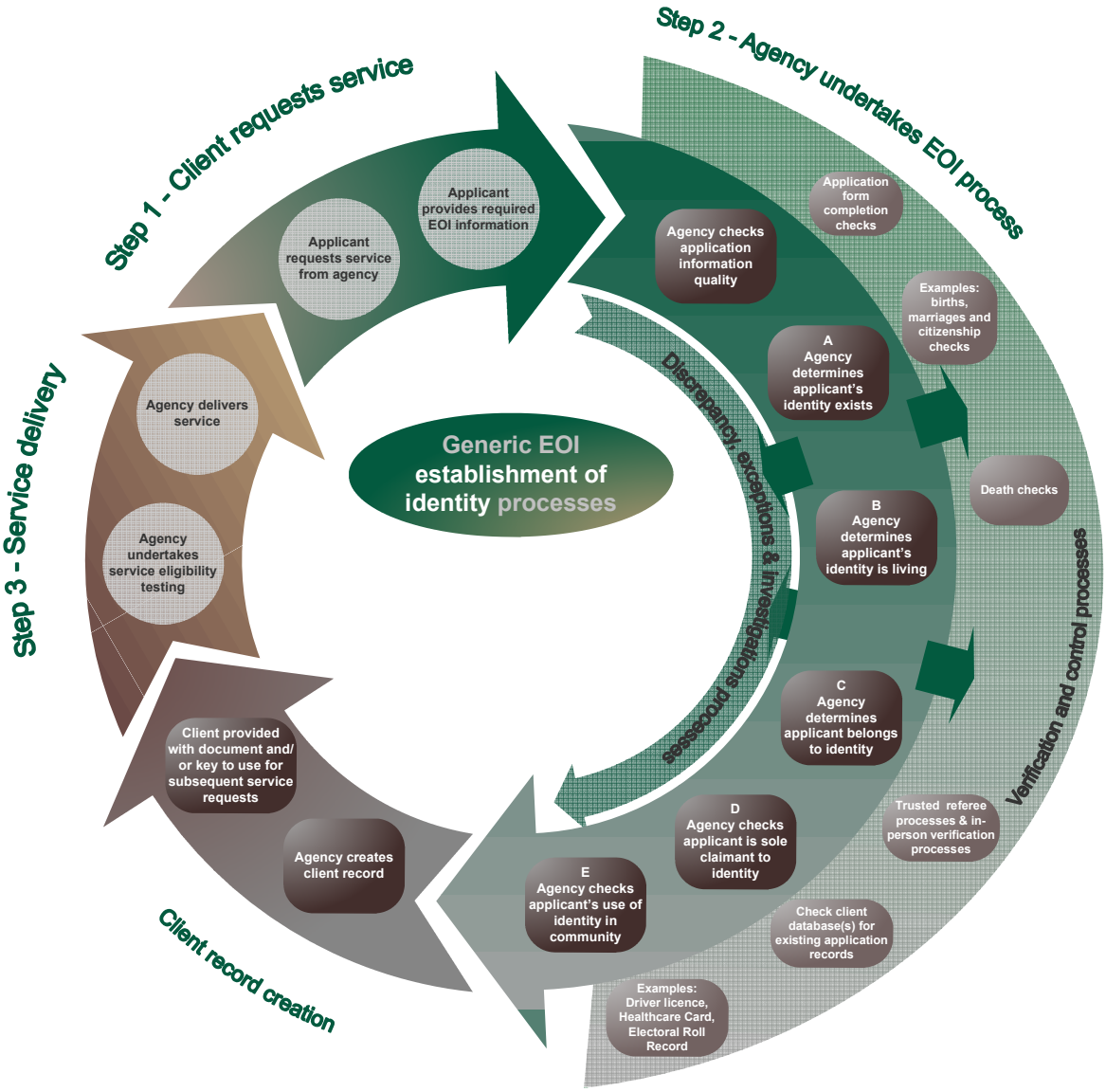
For example, if a driver's licence is being considered as a document to support a State's travel document issuance process, the TDIA needs to understand how robust the driver's licence issuance process is, and the quality of the driver's licence database for matching against records.

The TDIA can then assess whether access to the driver's 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's licence in the same name for a number of years, they may have a higher level of confidence in that their identity is legitimate.

TDIAs deal with a range of documents, and have varying degrees of confidence in their legitimacy, or the legitimacy of the information on them. The inherent 'value' of a document or record to an EOI process will differ from state to state. For example, a birth certificate may be acceptable evidence that an identity exists in some states, whereas other states may have very little confidence in the registration processes or the documents produced by some or all of their registry offices.

If a TDIA has less confidence in the integrity of its state's birth registration process or the accuracy of its birth registers, more emphasis might be placed on other or secondary EOI documents. For example, for many states, documents that show the applicant uses the identity in the community (i.e., '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 breeder 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 more public process. TDIAs should always look to interrogate their own databases using tools and techniques such as data mining, risk profiling and biometric matching. These are discussed later in this Technical Report.



Figure

Diagram 1 – Example of business process for establishing an individual's identity

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

EOI Objective	Example evidence Required for High Confidence
A – Identity exists	1-2 documents which, where possible, have been validated against source records held by the issuing agency or authenticated by staff trained in document analysis techniques. If possible, at least one document/record should contain a photograph. or Verification against 1-2 source records held by the issuing agency (i.e birth or citizenship records).
B – Identity is a living identity (not deceased)	Verification against the State's Death Register or Business processes for Objective C
C – Applicant links to the identity	Assertion by a trusted referee (preferably known to the TDIA, and verifiable in their database) or In-person verification against photo document (at agency office) or Biometric recognition against the TDIA database, and/or against other government databases containing the individual's biometric2 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; Trusted referee helps provide evidence	At least 2 documents/records (i.e 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.

Table 1 - Evidential Requirements for EOI Objectives

3.1 A – IDENTITY EXISTS

Foundational Documents

As explained before, throughout this TR the terms breeder documents, foundational documents and source documents are used synonymously as the documents of Evidence of Identification.

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

Foundational documents refer to evidentiary documents issued to record a person's birth, death or their point of immigration or naturalization and are used by issuing authorities to establish identity and confirm citizenship. When used in combination they provide part of the evidential process required to provide confidence that an individual is the true 'owner' of his/her claimed identity.

Foundational documents are the fundamental physical evidence accepted by state authorities to establish a *prime facie* (or *first view* or *first appearance*) 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 may allow the holder to fraudulently obtain genuine government documents and entitlements, including travel documents.

Protocols for acceptance of documentation

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

a) *Accept only original documents or copies certified by the issuing authority* – This allows examination of all security features that are not immediately obvious and are difficult to replicate, such as watermarks and embossing. Photocopied documents are particularly easy to alter and should, therefore, not be accepted as EOI.

b) Verify documents against electronic or other centrally-held or state-held records.

c) *Preferably accept only documents that are currently valid* – A currently valid document is a document that has a future expiry date. Documents that are not currently valid tend to be older and are less likely to contain up-to-date security features, making tampering or forgery easier. 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. However, you should keep in mind that older documents may assist in showing a continuity of identity, an element that newer documents may lack.

d) *Accept only full birth certificates* – Many government agencies worldwide no longer issue short birth certificates as they contain less identity-related information and are less reliable. Full birth certificates list gender and parental details, as well as name, date, place and country of birth. This more comprehensive extra information can prevent duplication where two individuals have the same name and biographical information. Differing parental information helps establish individuality. The exact match of all information, including parental, may alert the adjudicator to seek additional avenues of investigation if the claimed identity seems dubious.

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

f) *Require documented evidence of any name change* – (i.e deed poll, marriage certificate, or statutory declaration).

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

3.2 B – IDENTITY IS A LIVING IDENTITY

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

The resulting civil registry database is then used by government officials to create legal documents that are used to establish and protect the civil rights of individuals. Among the legal documents that are derived from civil registration are birth certificates, death certificates and marriage certificates, so called "foundational documents" (see above). The civil registry also creates a data source for the compilation of statistics.

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

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

Civil registration systems and processes vary among countries. While a centralized system can streamline the process of confirming identity for passport issuance by reducing the reliance on physical Evidence of Identification documents and eliminating the need to confirm document authenticity with separate issuing authorities, most countries use decentralized systems. Under a decentralized system foundational information is collected from different levels of government (i.e local/municipal/state/provincial) and is often stored in separate databases by the particular issuing authority. The decentralized approach is often preferred for civil registration as some countries believe that centralized systems put the privacy of their citizens at risk. However, decentralized systems can present challenges to TDIAs that must validate documents from various jurisdictions and issuing authorities, each with different standards administered under different authorities, leading to inconsistencies in adjudication across the travel document issuance continuum. A fuller overview of civil registration is in Annex 5.

As well as the documents themselves that are commonly used by applicants for travel documents, such as birth certificates, national identity cards and driving licenses, often, though not universally, the information that is captured for these and other breeder documents is stored in a database.

Often, the source documents that are used by applicant to obtain travel documents, are stored electronically in government database or are accessible through on-line civil registry systems. While the existence, quality and ease of accessing such databases and civil registry systems can greatly vary 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.

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 impede the use of these databases.

Some countries link these data sources, for example birth and death records, to serve as automatic checks and verifications.

3.3 C, D, E – APPLICANT LINKS TO THE IDENTITY, APPLICANT IS THE SOLE CLAIMANT TO THE IDENTITY, APPLICANT USES IDENTITY IN THE COMMUNITY

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

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

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

b) Biometric identity consists of attributes that are unique to an individual, i.e face, fingerprints, voice, iris pattern, hand geometry.

c) Biographical identity, a person's social footprint, builds up over time. It covers life events and how a person interacts with 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 either fictitious or not their own. Whilst the actual application form is a source of information that can be checked with the applicant, a well prepared fraudster will have ensured that they are familiar with the details contained on the form and consequently may well be able to answer questions on the attributed identity accurately.

Where a biometric check is being carried out as part of the application process, this will only highlight a record of the applicant if he/she has come to notice previously and had his/her biometrics recorded – i.e. the 'biometric identity' is only useful to establish identity if the applicant has had his/her biometrics recorded as part of a similar application in the past, although if the current application is successful there is merit in recording biometrics to 'lock' the applicant into the claimed identity. Thus, 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, or examining the applicant's biographic identity is a more robust check and a more certain means of preventing people from pretending to be other than their true identity. The exact nature of the checks made will depend on the laws and customs of the country. Allied to other checks that are carried out in the normal process of an application it is a way of using the applicant's claimed biographical identity to check against his/her claimed identity. Social footprint evidence is evidence that supports an individual's claimed identity in the community; for example, this may include evidence such as driver's licences and tax numbers in places where these have not been already used as breeder documents. The social footprint is based on the premise that everyone has dealings with a variety of organizations in his/her daily life, many of which maintain records about engagement(s) that are publicly available.

By integrating a social footprint check within the application process for a travel document, it is possible to deter potential fraudsters from attempting to make false applications. As applicants does not know what

information is held by the person reviewing the application, or the questions that will have to answer if interviewed, there is a greater likelihood that the fraudster will not try to obtain a document by this means.

The use of the social footprint is based on the availability of publicly held information about citizens. This might, for example, be held by credit card companies or in government databases. The basis of the idea is that a social footprint demonstrates consistency with the information given on the application form. If the applicant's social footprint is examined through an interview, 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 the account has existed) but not about the balance (which the interviewer would not know);

b) a guarantor or counter-signatory (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 emergency applications. Reducing the strength of any of the checks made 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 may be several stages. First, there will be 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 him/her 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.

Second, the social footprint check may then involve the collection and validation of a range of information from public and private sector sources. If applicant interviews are not routine, based on the social footprint check, a decision is made as whether to interview the applicant. If an interview is indicated, the information collected will be used to generate the questions asked at the interview.

Before an interview a check of the applicant to the photo and core details in the application will be made. 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, interviewers will not be told which applicants they 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 interviewers to use their experience to have an idea of how much of a social footprint might be expected before the applicant is interviewed. Accents, credit and banking 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, driver's licences and tax information.

Third, the interview itself is 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 interviews 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 for 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 applicants 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 will review the responses received as well as consider 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. While the interviewing officer should make the decision on whether or not the applicant has provided enough assurance of 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 malfeasance.

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. Nevertheless it does provide a strong defense against impersonation/identity theft.

4. USE OF IDENTITY DATA

4.1 DATA AND INFORMATION SHARING (FOR ESTABLISHING IDENTITY)

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

Information may be shared either a State, between government agencies, and sometimes with the private sector;

The focus of data-sharing for the State is to:

a) enable issuance (validation of documents or data that relate to the establishment of identity, such as birth or citizenship);

b) facilitate travel (sharing passport information with border agencies); and

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

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

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

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

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

Such services increase the TDIA's confidence in the documents and records, required, and can facilitate a more streamlined and efficient enrolment process by removing or reducing the need for an applicant to provide documentary evidence – therefore reducing the TDIA's exposure to counterfeits.

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

Although it is of huge benefit to check or validate all applicants 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.

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

4.2 RISK CONSIDERATIONS

Identity-related risk

Identifying identity-related risks, and the consequences of these risks, require 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:

a) creating a fictitious identity

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

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

d) stealing or assuming a pre-existing identity, which is subsequently manipulated

e) identity sale.

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

Identity sale typically done by the incarcerated, homeless, or drug addicts, who otherwise have little use for their formal identity.

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

a) *Financial loss or liability* - The incorrect attribution of identity can cause significant problems for any affected party. For example, a benefit payment to any person who uses a stolen or fictitious identity, and who is not entitled to receive that benefit creates a direct financial loss to the Government. At worst, this could cause severe or catastrophic unrecoverable financial loss to any party, or severe or catastrophic agency liability.

b) *Inconvenience, Distress or Damage to Existing Reputation* – The result of incorrect attribution of identity can inconvenience, distress, or damage the standing or reputation of any party in a number of ways. For example, a stolen identity will have a significant impact on an individual's ability to participate effectively in the community and to receive the services to which he/she is entitled. Widespread misuse and abuse of identity could also potentially impact negatively on the international reputation of the State, leading to a reduction of investment in businesses and migration, and increased difficulty in obtaining visas.

c) *Harm to Public Programs or Public Interest* – Incorrect attribution of identity has the potential to disrupt the effectiveness of agency programmes. This may result in a negative public or political perception that some people are not receiving the services from these agencies for which they are entitled or that people who are *not* entitled *are* receiving services. At worst, this could have a severe or catastrophic adverse effect on agency operations or assets and 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.

d) *Unauthorized Release of Sensitive Information* – This can result in loss of confidence in an agency and directly result in or contribute to negative outcomes for the affected individual (i.e personal safety, financial loss, job loss). Personal information needs to be protected and appropriately and closely managed. At worst, a release of confidencial, sensitive information or information with a National Security classification to unauthorised parties, results high impact loss of confidence in tehe agency and collateral damage up its chain of command.

e) *Domino Effects of an Improper Identity Document Used to Acquire Services of a Third party or Another Document* – Incorrect attribution of identity can impact on agencies other than the agency delivering the service. For example, a passport that is issued to a fictitious identity could be used as the basis for fraudulent activities that directly impact on other government or non-government organizations. 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.

f) *Personal and Public Safety* - Incorrect attribution of an identity for an individual can compromise personal safety. For example, an individual incorrectly provided with a passport using a fictitious or stolen identity could commit acts of terrorism, where there is a risk of serious injury or death. These types of risks have severe and lasting consequences for any State.

These categories of risk can have immeasurably negative impact on innumerable parties. Examples include the individuals whose identities have been stolen and those personally and publicly related to these victims; government agencies; the general public; organizations (both public and private); businesses; property; and the simultaneously same categories of risk for other countries.

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:

a) Establishing the scope of the assessment;

b) Determining the threats, and assessing the likelihood and impact of their occurrence;

c) Assessing the adequacy of existing safeguards and vulnerabilities; and

d) Implementing any supplementary safeguards to reduce the risk to an acceptable level.

Threats the underlying reasons for fraud attempts and even the definition of fraud may differ significantly from country to country, and/or region to region. Thus, it is also important to add that threats also come from internal sources. The TDIA needs to ensure that processes and systems for supporting staff and managing risks for misconduct and corruption are well defined and transparent.. This results in the protection of staff and a positive international reputation for the issuing state's internal fraud prevention efforts..

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 could 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 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).

5. ANNEX 1: GLOSSARY

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.

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.

Evidence of Identification

False identity

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 i.e 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.

Identity crime

Identity theft

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 (i.e 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 in filled 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.

6. ANNEX 2: INTERNATIONAL ORGANIZATIONS

THE ORGANIZATION FOR SECURITY AND CO-OPERATION IN EUROPE (OSCE)

The OSCE Secretariat's Travel Document Security (TDS) programme, implemented by the OSCE Action against Terrorism Unit (ATU) has been instrumental in undertaking capacity-building and supporting initiatives that have served to improve the quality and integrity of travel documents in a number of countries. Along with focal concerns for the travel 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 breeder documents as well as a number of the other systemic factors discussed in this Technical Report (TR).

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.

Recognizing that eMRTDs can only be as secure as those 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 Identification - breeder documents, civil registry systems and other media used to verify and/or validate a travel document applicant's identity. The international standardization of breeder 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.

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 to ensure 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.

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 cannot 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 as 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.

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; to counter-terrorism measures; and to the prevention of illegal cross-border activities involving organized or trafficking in all its forms.

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.

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.

The OSCE Office for Democratic Institutions and Human Rights (ODIHR) has substantial programmes in supporting voter registration and population registration systems.

Voter Registration. Voter registration and the transparency, accuracy and inclusiveness of voter lists are taken into account in every election activity that the ODIHR Elections Department undertakes.

ODIHR is experienced with the use of biometrics in both processes, population registration and elections (voter list management and at polling stations, as well as biometrics and use with electronic voting systems). Currently no OSCE participating State uses biometrics in any aspect of its electoral process: OSCE participating States have not committed themselves to specific standards with regard to the possible use of biometric voting systems; ODIHR has thus had no opportunity to identify best practices in this respect and has not developed any recommendations. More generally, the introduction of biometrics has received a mixed response, with concerns raised regarding cost, trust, and data protection.

Population Registration. ODIHR's work in this area results also from observed shortcomings in voter registers deriving from or linked to population registration systems. ODIHR is often invited to provide expertise in modernizing population registration systems to bring them in line with OSCE commitments on freedom of movement.

In many OSCE participating States, residents are required to register their place of residence with the relevant authorities. All states employ mechanisms for registration of vital life events, such as birth, death and marriage. The authorities use this information for ensuring the exercise of fundamental rights, such as the right to vote and the eligibility, planning and delivery of state services, such as access to education, health care, and other social services. Registration of vital life events and the place of residence are the key information that is stored by population registration systems.

In response to the requests from OSCE participating States for expertise and policy advice in reforming population registration systems, in autumn of 2009, ODIHR published *Guidelines on Population Registration* . *The Guidelines* were developed in consultation with population registration experts from all

regions in the OSCE area. While the *Guidelines* primarily represent an ODIHR internal tool used when assisting population registration system reforms, it also provides a tool for political decision-makers, practitioners and relevant authorities when assessing the appropriateness and efficiency of national systems of population registration and, as appropriate, provide guidance on their reform.

The *Guidelines on Population Registration* define "population registration" as a system based on a consistent legal framework which sets out terms and conditions for continuous registration of eligible persons within a specific area of a public authority with the purpose of establishing identity, civil status (including vital life events) and place of residence, and provides proof thereof on the basis of documented evidence.

7. ANNEX 3: TECHNICAL DOCUMENT FEATURES

This annex is intended as a general discussion on security features which might be used in documents. Whether use of advanced security features in foundation documents is appropriate will depend on the individual country and its legal frameworks culture, the status of such documents and how they are used. This annex should not be read as implying that such security features are a necessary step towards achieving security of issuance for travel documents.

While this section is entitled "Technical Document Features," it focuses only on Birth Certificates (BC) providing guidance on the security of BC, including the security design, printing, and personalization. Over time there likely will be additional documents and respective standards and specifications.

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.

BCs are typically produced as paper documents incorporating security features intended to protect them against counterfeiting and against falsification of the personal 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.

7.1 FUNDAMENTAL PRINCIPLES

Due to the importance of BCs for confirming Evidence of Identification and their value as breeder documents, blank (non-personalised) 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 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.

For states where the original BC is valid proof of identity/an identity document in its own right, 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, differenciating it from 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, etc. 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 imposters from assuming the identities of a deceased persons.

For states where the original BC is valid proof of identity/an identity document in its own right, the practice in some countries of issuing a copy of a BC to someone *other than* the rightful holder, or, unless a minor, to his or her parent or legal guardian, should be discouraged. However, where certificates are public documents and are *not* a valid proof of identity, any copy issued should clearly state that it is a copy and is *not* valid as proof of Evidence of Identification (or citizenship). 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.

Where there is reliance on the physical document rather than electronic records, BC should contain security features that will help protect against attempts to counterfeit and/or tamper with the personal data recorded on them.

All BCs should contain, at a minimum, a set of security features that will help 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 document security. 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 suppliers of pre-personalized BC's and issuers of personalized BCs.

Physical Document Considerations

The production of pre-personalized (also known as "blank") BCs should be entrusted only to a government printing works or other suitably qualified security suppliers and should take place in a secure, controlled environment with appropriate measures in place to protect the premises and documents against unauthorized access.

Typically, blank BCs are manufactured in one location and despatched to a 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 government offices is therefore essential, as is secure storage and accountability for their use in 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 and little risk that the document will be detected as a fake.

Where possible, personalization of BCs in a single central location, coupled with increased internal controls, because 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 print/complete 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.

Where centralized personalization is not possible, issuing authorities are strongly advised to implement robust procedures and regularly monitor their implementation, to ensure security at the local/decentralized 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, also to protect staff by requiring more than one signature to document the status of used, unused, and waste certificates.

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

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 and fantasy (or unreal) BC;

b) Deletion, alteration and substitution of personal 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.

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 deploying a balanced set of security features and techniques, providing multiple layers of security in the document that combine to deter or defeat fraud attack.

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 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 risk of fraud and provide an audit trail and traceability in the event that blank BCs or components "go missing."

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 this misuse are:

a) An effective enrolment or registration process to record and store details of all BCs issued by an authority and the ability of 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 among different records should be further investigated to understand any doubt over the claimed identity.

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

Protection Against Counterfeiting

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 such software 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 materials' specifications. Additionally, it should be remembered that BCs may have a very long use 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, which are not available outside of the security industry to produce documents that cannot be reproduced by conventional methods of printing. For example, these include: 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

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

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.

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, while it may not be possible to prevent tampering, it should always be possible to detect tampering. 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

This is normally achieved by ensuring that the document contains an effective printed security background design in the area where personal data is 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.

An important consideration when selecting the method of personalization for a BC is to ensure that the inks or other materials used to print penetrate the surface of the substrate, maximising the damage to the surface if the personal information is removed. Optimization of tamper evidence requires careful matching of the inks, or other materials used in personalization, with the properties of the substrate.

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 it 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.

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 requirement, 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 aging 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 printing to the substrate, for example by the addition of a protective overlay or laminate.

A second protection against mechanical erasure is the printing of small background fields ("data boxes"), where personal information is expected to be printed. 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

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 personal information comes in contact with a wide range of commercially available solvents. Reactive inks are normally used to print the security background design in a document, often in rainbow (iris) printing.

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.

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.

The key message to be drawn from the above 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

Authentication is the process whereby a document is checked and its derivation 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.

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.

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.

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.

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.

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.

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.

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

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.

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 (aging) 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 incorporated that tag/reveal it as the manufacturer of the documents.

It is recommended that birth certificates issued in 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 (i.e 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 substrate of a birth certificate (Refer back to drafters to redraft language, heading and numbering through 5.5.31)

The following offers guidance for paper-based BCs.

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 absorbency, roughness and substance of at least 120 gsm; and

e) Appropriate chemical properties (i.e. pH neutral) that reflect 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 (or nonreactive substance) designed for detection by special equipment; and

f) Preferably a large size (i.e. 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.

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; (i.e 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.

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 (i.e 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.

Inks

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).

Additional Features

a) Ink with optically variable properties;

b) Metallic ink;

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

d) Metameric ink;

e) Infrared drop-out ink;

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

g) Phosphors

h) Tagged (or nonreactive) ink; and

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

Numbering

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 paragraph 3.1 Background and text printing)

Basic Features

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

Additional Features

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

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

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

e) Protection against copying of blank documents; and

f) 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

Birth Certificate Personalization

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

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 personalized data is compatible with the lifespan of the document and is suitably resistant to fraudulent alteration.

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

To ensure that data printed in this way is properly secured against attempts at forgery or fraudulent alteration it is very strongly recommended that the biographical data be integrated 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.

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

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

Choice of Document Personalization Technology

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 state issues birth certificates centrally or decentrally. The personalization technology should be uniformly deployed at all issuing sites to ensure consistency in the finished document.

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 or breakable 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 (i.e. tactile features) on the BC.

Protecting the Personalization Against Fraudulent Alteration

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

Basic Features

a) Personal data integrated into the basic material;

b) The security printed background (i.e 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 personal data or an alternative combination of a personalization technology and substrate material that provide an equivalent resistance to fraudulent alteration.

Additional Features

a) Personalization using a special type face;

b) Penetrating inks;

c) Overlay or laminate containing advanced optically variable devices.

Protection Against Theft and Abuse of Genuine Blank Birth Certificates

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

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 (i.e 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 (i.e, 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 among government departments and internationally as appropriate;

g) Appropriate controls to be in place to protect the production procedures from internal fraud (i.e., multiple signatories on counts of controlled materials; and unscheduled audits within and without direct supervisory chain) ;

h) Thorough security vetting of staff.

Additional Security

CCTV coverage / recording of all production areas, where permitted

8. ANNEX 4: - THE UTILITY OF BIOMETRICS

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

With ICAO’s development of the ePassport, digital facial, 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)

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

Verification with Centralized Storage

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

Verification with Distributed Storage

If the biometric data is stored in the passport’s chip that is carried by the individual, the person will provide a live biometric sample and this will be compared to the biometric data stored on the memory device. This is typically done by the verification system which retrieves the person’s biometric data from the chip and compares them to the live sample and to the data printed on the travel document itself. If the verification process is successful, the traveller is confirmed to be the valid bearer of the identification document

Identification (1-to-Many Matching)

Identification is used to discover the identity of an individual when the identity is unknown (the user makes no claim of identity). Contrary to verification, for the process of identification requires a central database that holds the necessary that holds records for all people known to the system; without a database of records, the process of identification is not possible.

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

Screening

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

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

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

The Multi-Biometric Approach

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

A multi-biometric system captures more than one type of biometrics to get enrolled in the data base. This improves the accuracy in establishing identity and in cases where a person is not able to provide one of the biometric features, he/she can still enroll the second biometric feature and is hence enrolled with at least one biometric in the database. This is also possible with uni-biometric systems.

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

Concerns

There are some ethical issues centering on biometrics, but those issues concerning privacy rights of individuals and personal identification receive the most attention. One concern is about the ownership and the use of the stored biometric data. To address public discussions on ethical issues, stored biometric data must be properly protected. There should not be any unauthorized collection, use, and retention of biometric data, and biometrics need to be deployed where most effective and appropriate. The public must be proactively informed about data usage and data retention time,in order to gain trust in both the system and its use and oversight.

9. ANNEX 5: CIVIL REGISTRY

(OAS Civil Registry – To provide text on Establishing Identity, Recording Identity, Civil Registry and best practices related)

(*Comment: Text below needs review after OAS sends its portion.)*

Contemporary Civil Registration Systems

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, coordinated and standardized manner, taking into account the cultural, social and administrative circumstances of the country in which it operates.

When operating effectively, a system of civil registration can provide reliable information that can be used for various purposes. Following are the most common uses:

a) 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.

b) In many OSCE participating States, voter registers are linked to or produced from the civil register, and hence, the quality of the latter directly affects the exercise of universal and equal suffrage. In those participating States where population registration is a part of administrative tradition, the voter lists tend to be more accurate if they are based on the data from the civil register, assuming that the register is updated in a timely manner.

c) An up-to-date civil register can be a vital element of public sector planning. In many OSCE participating States data on the local population is used in development of public housing, public schools, roads and other public transportation infrastructure. The ability to access historical data in order to identify trends and developments in different areas is also vital.

d) 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.

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 tradition played a decisive role when states were determining approaches to the modernization of their civil-registration systems. In essence, three different approaches can be identified:

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

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

c) The registration of life events is entirely the responsibility of bodies of local government, while population movements are registered by the central authorities.

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, registration needs to be mandatory for the entire population of the state while the records need to be updated on the continuous, permanent 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 with confidentiality and the stored information is used *only* for the purposes envisaged in the law and *only* by those authorized to do so.

Modern civil registration systems are designed to provide for multiple use of information registered in the system as opposed to practice of multiple registrations of the same information by different public authorities. In accordance with the principle of single registration and multiple uses, the information is registered and stored only once. The system, which in most of the instances is computerized, provides that this information can be accessed and obtained by any authority who is legally entitled to access the information. Multiple registration of information, on the other hand, is common for the systems that lack a framework for information-sharing. When this is the case, individual institutions often begin to maintain their own registers or databases for their own purposes. As a result, citizens are required to provide the same information on multiple occasions, often in a certified format. These time-consuming and expensive requirements place an unnecessary burden on citizens, while the need to repeatedly provide the same information increases the chances of error. Finally, multiple registration of information severely reduces the level of control that can be exercised in terms of data protection.

Use of information technology plays an important but not decisive, role in increasing 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 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.

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.

- END -