

Support for the Rabat Process on Migration and Development

Meeting of Experts on Civil Registry

“Improving civil status registration systems and combating document fraud”

Warsaw (Poland) – May 9 to 11 2011

Session 3: Combating document fraud

Mr Robin Chalmers

Consultant

Former Head of International Policy of UK Identity and Passport Service



Securing travel documents: from the fight against counterfeit and forgery to the fight against the fraudulent obtention of genuine documents - Background Paper

Introduction

1. Travel document fraud remains a major challenge for Governments as migratory pressures continue to influence the movement of people across international boundaries in search of better prospects or a safer environment. There are strong reasons for taking steps to prevent fraud – especially, in the context of this conference, fraud associated with the issuance of civil registration documents that form the basis for establishing a person’s identity and entitlement to a national passport. Criminality is international, often requiring travel documents in false identities. International terrorism remains a major and ever-present concern and is another user of fraudulent identity and travel documents.
2. The response of many Governments has been to increase checks at borders, impose greater restrictions on travellers from certain countries by requiring visas, and require airlines and other carrying companies to check that travellers have genuine documents before they are permitted to board ships/aircraft. A number of countries are now sharing data about suspect travellers. Document fraud – that is counterfeiting and fraudulent alteration of a document- is now becoming more difficult to use successfully to cross the border.

Protecting the integrity of the travel document

3. In addition to the steps taken to protect borders, significant developments have taken place in relation to the travel document itself. The International Civil Aviation Organisation (ICAO), a United Nations agency, has the mandate for the development of travel documents standards. ICAO has responded to the threats from fraudsters by introducing a number of security measures both for the travel document and for the application and issuance systems. The introduction of biometrics around 2005 was a major technological advance in relation to travel documents through the integration of an electronic chip in the document providing a means of verifying that it was issued by a proper authority.
4. Aside from introducing ever more secure travel document features, ICAO has also developed best practice guidance on ensuring that Travel Document Issuing Authority (TDIA) application and issuance systems were themselves protected against fraud. These measures included physical security as well as system security. There was also guidance on how to reduce the threat from internal fraud – an acknowledgement that threats to circumvent systems came not only from fraudulent applicants but also corrupt employees.
5. The use of lost or stolen passports by fraudsters has also become less attractive. Large numbers of travel documents are lost/stolen each year and their misuse has always posed a threat through alteration of the details/substitution of the photo.



Interpol maintains a central database of all travel documents reported lost/stolen (SLTD database). Until a number of years ago, this database could not be accessed in real time at the border, allowing a fraudster to use a lost/stolen passport and benefit from this weakness. However, Interpol has now developed a system that provides access to the database for border control officers making the use of such passports by fraudsters less likely to be successful.

The fraudster's response

6. Having tightened up the controls at borders, airport check in and produced highly sophisticated travel documents in secure issuance facilities and made it more difficult for fraudsters to use lost/stolen travel documents, it might be reasonably expected that the level of detected fraud would drop. However the fraudster will always find the weak spot in any system and the same is true in relation to travel documents. As there is now a much greater likelihood of being detected trying to cross a border with a counterfeit or forged travel document, fraudsters have concluded (not unreasonably) that obtaining a genuine travel document fraudulently is likely to have much greater success. The document will have all the security features that it should have, it will not feature on any lost/stolen database and it will not have been altered. It does, of course, require the fraudster to steal the identity of someone with an entitlement to an international travel document. So the threat now is increasingly around the ability of the fraudster to use someone else's identity.
7. Border control passport fraud statistics from one European country showed that in 2007, cases of identity fraud constituted 31% and document fraud 54%; in 2009, identity fraud had increased to 71% and document fraud reduced to 29%. It is evident therefore that fraudsters have homed-in on weaknesses that exist around the processes for establishing a person's identity and entitlement to a travel document and are now exploiting them.

Fraudulently obtained genuine documents and supporting documents

8. There are two main methods of obtaining a fraudulently obtained genuine (FOG) travel document. Either through the services of a corrupt employee in the TDIA or through the use of supporting documents relating to another person's identity that has a presumed entitlement to a travel document. In relation to the first, it is becoming increasingly difficult to circumvent travel document issuance systems. As mentioned earlier, ICAO has provided guidance and best practice which, if followed, affords a good level of protection against employee corruption. Whilst it is accepted that no systems are 100% foolproof, they can be protected to a very high degree. There is also much less evidence that employee corruption accounts for any significant portion of FOG documents almost certainly due to the computerisation of travel document issuance systems and move to more centralised production.



9. The use of supporting (or foundational) documents in another person's identity is currently the major threat in the area of FOG documents. Foundational documents such as birth, death and marriage certificates play a key role in how applicants and TDIA establish identity and entitlement to a travel document. These documents form the basis for a person to establish a prima facie claim to an identity. Unlike travel documents, there are no internationally agreed standards for foundational documents. This is understandable since foundational documents are generally for internal use whilst a travel document must be in a format that ensures international acceptability and global interoperability. However, given the focus of the fraudster is now on these foundational documents, Civil Registration (CR) authorities need to be more aware of the misuse of their documents and take steps to make them and their registration/issuance systems more secure.

Misuse of CR documents for identity documents

10. It is common practice for foundational documents (birth, death marriage certificates) to be required in order to obtain identity documents. Foundational documents provide a person's prima facie claim to an identity. Poor processes in the CR system can facilitate the issue of identity documents in false identities. As outlined above, with the increasing incidence of use of foundational documents to carry out identity fraud, it is important that the systems and processes in place for the recording of life events (birth, death, marriage etc) are framed in such a way as to provide sufficient protection. Where legislation exists setting out the processes for CR it may not have been designed to counter the type of identity fraud that is now current.
11. There are two key areas that CR authorities need to consider in relation to countering the increased risk of identity fraud. Firstly, the level of existing fraud needs to be examined to understand if there is a need for new or additional legislation. How easy is it to assume another person's identity? Does the legislation provide sufficient protection against identity fraud? Are there appropriate sanctions/penalties in place for those who are caught? And are these consistently and always applied?
12. The second area relates to those who are charged with administering the system. It is essential that those who deal with recording/certifying births, deaths etc are well trained and competent. They must be aware of the appropriate legislation and must also be aware of the potential for their records to be misused. The importance of keeping accurate CR records needs to be highlighted. Maintaining an appropriate level of privacy around CR information is also an important aspect. Given the level of risk of identity fraud, there needs to be a strong framework in place which ensures that a citizen's personal details are protected from misuse. Data protection legislation should be used to ensure confidentiality is assured and that appropriate penalties are in place. Citizens have a right to expect that their personal information is not disclosed or used by unauthorised persons or for unauthorised reasons. Taking steps



to make the processes around CR more secure will undoubtedly help deliver that expectation

13. By taking steps to protect the CR system, government can reduce the level of distress and inconvenience caused to citizens whose identity may be stolen; financial loss can be reduced through non-entitled persons accessing services; government can prevent the issue of an identity document based on a certificate obtained fraudulently from the CR authority.

Identity Fraud and CR documents

14. Given the increasing use of CR documents by fraudsters, a number of questions surround such documents when they are presented as part of an application for a travel document:
 - Is this a genuine birth certificate? Can it be compared with a known genuine example provided by the CR authority? Are there too many formats to allow effective checking of the document? Does it have verifiable security features?
 - If it appears genuine, could it be a stolen blank? Does the CR authority routinely advise TDIA (and others) of the loss of certificates?
 - If it is genuine and there is a system in place to inform TDIA of lost/stolen blank certificates, how secure is the issuing process in the CR authority? What level of checks takes place by the CR as to the identity of those to whom it issues certificates?
 - Is there a chance that the applicant is using the identity of a deceased person? Is there a system in place to match births and deaths – even on a limited scale?

CR authorities may take the view that these are issues that need to be addressed by the TDIA but they are equally of relevance to the authorities who are responsible for the effective administration of the CR system.

Ensuring the security of foundational documents

15. There are a large number of recommendations that can be made to reduce the risk of identity fraud through the misuse of foundational documents. They can provide a greater level of assurance to those using the foundational document as the basis for the issue of a travel document or for the provision of a service. In many cases they do not require legislation. They are simply good practice. The key recommendations include the following:
 - a) Due to the importance of certificates, they should be held securely and regularly audited to ensure none are missing. This applies equally to the location where blank certificates are printed. The auditing function should be carried out on a daily basis. There should



be ad hoc and unannounced checks of the records against the stocks held

- b) All certificates should have unique identification numbers – these should be included on the blank documents as early as possible in the production process to enable audits to identify missing certificates. A process should be established to notify other users of CR certificates of the loss or theft of blank certificates
- c) All certificates should have minimum levels of security features included to help protect them against counterfeiting/tampering with the personal data on them. These might include the use of watermarked paper, printing techniques and both overt and covert security features

Risk

16. In addition to the above recommended practices, CR authorities need to consider the level of risk which currently exists in their individual systems and processes. CR systems in Africa are fairly disparate being based often on former colonial systems. In general systems may not be designed to prevent fraud but, understandably, to ensure the registration of a country's citizens. It is also important that a citizen's ability to access CR services is not hampered by over-complicated requirements to prevent fraud. So a sensible balance needs to be struck between facilitating access to citizens and maintaining a secure system that makes it difficult for the fraudster to circumvent. Nevertheless there may be examples from other countries in the region where action has been successfully taken to improve the security of the CR system. Exchanging examples of good practice would be a step forward.
17. No matter how sophisticated a system may be designed, the human dimension will always pose a risk. As indicated earlier, travel document systems are mainly computerised nowadays enabling unusual activity to be identified and investigated. Nevertheless, instances of internal fraud within TDIA still occur, primarily due to employees finding ways to circumvent the checks that are inbuilt into the system. Even the common practice of ensuring that more than one employee must be involved in the authorisation process for the issue of a passport, can be circumvented through a misplaced level of trust between employees. Just as this can happen within a TDIA, there is no reason to believe that CR systems will not be subjected to similar types of threat.
18. The physical environment in which CR services are provided can also help reduce the risk from fraud. For example, ensuring that all areas in which back office CR functions take place are inaccessible to the public; ensuring as much as possible that the public cannot select which member of staff they deal with; ensuring that archived records are held securely with controlled access only permitted.



19. Risk of fraud can also be reduced by ensuring that TDIA and CR authorities work more closely together. The identification of fraudulent CR documents by TDIA can help the CR authority identify where there are weaknesses in their systems, enabling them to remedy the situation. CR authorities should also work closely with other agencies that commonly require CR certificates to prove entitlement to a service.

Conclusion

20. It is acknowledged that many of the approaches recommended in this paper may be considered as too much of an imposition for CR authorities – due to cost, lack of human resources or other reasons. Whilst there are international organisations that may provide assistance in relation to capacity building for CR systems – for example the International Organisation for Migration, UN agencies – much could be gained from regional exchanges of best practice. This approach could identify the steps that other countries in the region have found to be successful; that by itself might help in developing a business case for any necessary funds or ensure that available funds were directed towards the most cost effective investment
21. Enabling easier and more accurate checking of identity is not just for the benefit of travel document issuers but provides wider benefits to the citizen and government. For example, citizens can access government services with less difficulty, can prove citizenship to vote, and government has a more comprehensive and accurate record of its citizens necessary for a functioning state infrastructure. It also contributes to risk reduction – a weak civil registration system can lead to inconvenience, distress or damage to a country's reputation; it can lead to financial loss, liability; it can harm the public interest. It is evident therefore that improvements in civil registration systems and practices can deliver multiple benefits.

