

Stolen Blank Documents

Current situation and future developments

by Isabel Baltazar & Fons Knopjes

According to recent American statistics, there are currently some 25 million stolen security documents in circulation around the world. What's more, some 80% of all documents seized were declared stolen before or after they were issued. According to the same source, nearly 70% of all document fraud involves the use of someone else's ID document. Isabel Baltazar and Fons Knopjes explain the pitfalls and solutions.

Although the national statistics of many countries are generally in line with recent American findings, only about 3% of all document fraud involves documents that have been stolen prior to issuance (ie, blank documents). Although this figure is based on national statistics, the number of blank documents that have been stolen has historically been very low, even on a global basis.

While blank documents are, on the whole, forged using the same techniques as personalised documents, they tend to be more accurate and, from a technical perspective, more complex and ingenious. The quality of the resultant forgery is often much better, making it harder to detect. Blank documents are not used by the same people who use ordinary forgeries. Instead, they are of particular interest to those involved in organised crime and smuggling networks, who often require and receive highly structured 'bank-office support'.

In view of the above, the only way to catch someone using a stolen blank ID document is to use profiling techniques. Police authorities - and border authorities in particular - are on the constant lookout for timely and accurate information about the validity of identity and travel documents.

Future solutions

There is no single solution to crime involving false identities. Instead, the multiplicity and complexity of variables that give rise to crime call for a combination of well-targeted and effective measures. In the end, the best approach is both preventive and proactive.

The following solutions prevent the theft of blank documents while simultaneously allowing invalid/ stolen documents to be identified.

1. The creation of a global database containing details of lost and stolen documents.
2. A coherent approach to the Identity Chain. Crime can be reduced considerably if (i) the security of breeder documents is improved and (ii) the personalisation process (issuing procedures) is centralised.
3. Harmonisation of the security standards applied to the storage of (blank) security documents.

Each of the above alternatives is explained below.

1. Global database (data interchange)

In the short term, only Interpol seems able to comply with this requirement. Although authorities all over the world maintain national and regional databases for stolen documents, none of these are as broad-based as the Interpol database. At this stage, nearly all countries in the world are affiliated to Interpol, while 166 of the 182 member states contribute data to Interpol's STD (Stolen Travel Documents Database). This bodes well for the future. After all, the security of every individual is optimised if information is globally accessible.

Growth in Interpol's STD is ongoing, with many countries providing information on a voluntary basis. A global interchange along the lines of the STD offers several benefits.

- it improves border integrity;
- it allows instances of identity theft to be detected;
- it increases the likelihood of criminals being detected and identified;
- it helps with the recovery of national passports;
- it limits the value and illegal use of lost, stolen or invalid documents.

According to Interpol, which has made a series of recommendations, "issuing authorities shall improve information sharing (...) by promptly reporting to INTERPOL about all invalid, lost or stolen blank travel documents". The organisation also stresses that "blank travel documents, once reported stolen, should never, therefore, be issued, even if they are still blank when recovered." Moreover, "all travel documents shall bear a unique number, affixed at the production site, and repeated, during the personalisation process, on the bio data page."



Isabel Baltazar heads the ID and Fraud Unit of the Portuguese Servico de Estrangeiros e Fronteiras, specialising in fraud and forgery. Isabel is a member of ICAO's DCFWG (Document Content and Format Working Group) and EPWG (Education and Promotional WG).



Fons Knopjes is a forensic document expert and director of the IDManagement Centre in the Netherlands. He has advised on the development of more than 20 ID documents and is currently working on an electronic ID card. Fons is also a member of ICAO's EPWG.

The above recommendations create an opportunity to share information on a global scale. They also open the door to a unified system that derives details of lost, stolen and invalid passports from a diversity of national databases. In order for member states to contribute to and benefit from this system, further progress is needed in terms of its interoperability and technical specifications.

2. Coherent identity chain and centralisation

COHERENCE

To improve quality, and raise overall security and efficiency, a coherent policy on security documentation is needed. Ideally, the requirements of the various agencies and other participants in the identity chain should be homogenised - this covers Registration, Production, Deliverance and Control with birth and death records playing a crucial role.

By sharing knowledge and coordinating investments at different levels, synergies can be created in a number of areas. These measures additionally facilitate the creation of a broad-based and integrated approach that will benefit individual parties and governments (figure 1).

Governments are responsible for issuing documents that contain identity data (such as passports, identity cards, birth certificates and driving licenses). The difference between these documents lies in their intended purpose and their position within the document hierarchy. To improve security, authorities cannot afford to focus on the final document only (in other words, the top of the hierarchy). Instead, they need to consider the overall chain that supports the issuance (or delivery) process.

Different schemes and procedures apply to the issuance of these documents. As a consequence, we conclude that there is no systematic organisation that brings the entire process together. Even though governments hold final responsibility, the authority to issue security and identity documents is assigned to several agencies whose requirements and standards have emerged and improved over time. Mostly on a stand-alone basis, however (this is highlighted in figure 2).

CENTRALISATION

An identity architecture that is based on a centralised and harmonised system ensures that all parties are treated equally. It also results in (i) consistency over time, (ii) best performance in terms of standards, (iii) guaranteed levels of security, and, above all, (iv) a clear overview of all processes based on standard procedures (significantly reducing the risk of blank documents being stolen). It should be borne in mind that a centralised, conspicuous and coherent system

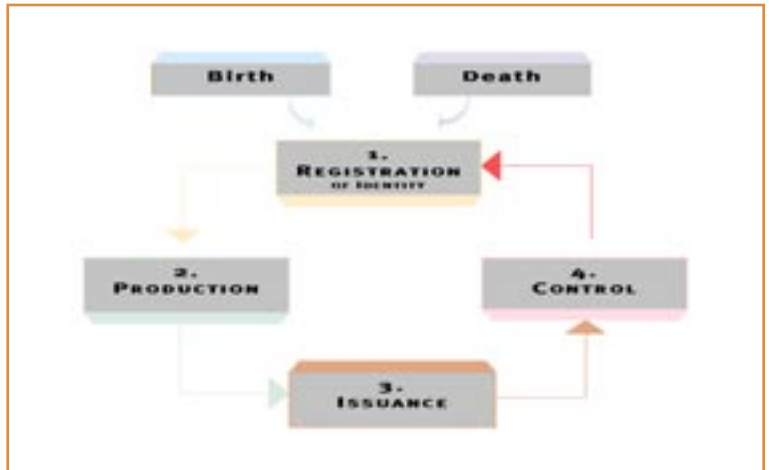


Figure 1
The ID chain approach

will enhance the reputation of national governments, boost public confidence and instil trust among (inter)national partners. A coherent document policy should be rooted in a thorough assessment and a comprehensive analysis, which must also facilitate migration to a centralised system (figure 3).

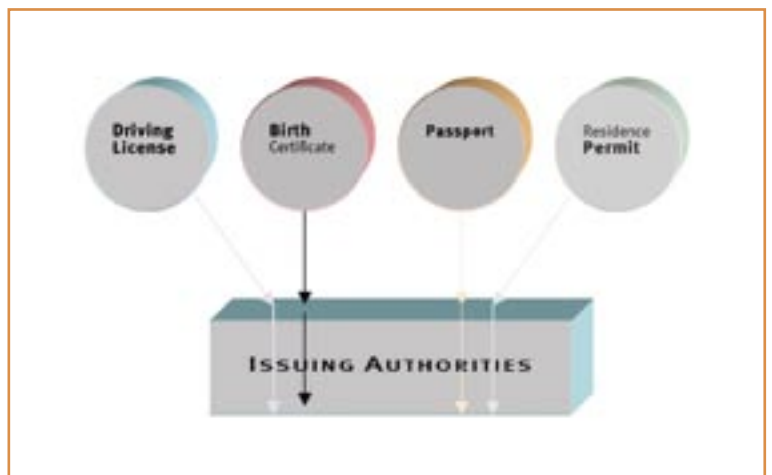
ISSUING AUTHORITIES

The establishment of a coherent document policy is time-consuming, not least because it requires several procedures to be re-evaluated or even discontinued. To arrive at a new standard, it is imperative that the migration of document architectures and schemes is gradual. This also applies to any fine-tuning of the policy, which should be spread over a longer period.

In view of the above, we would repeat our belief that adopting a different solution to the above problem(s) is risky - it could compromise system integrity and result in a loss of reputation.

Viewed within the context of machine readable functionality (and control), it seems reasonable to conclude that a decentralised issuance system is more

Figure 2
Issuance system on stand-alone basis. There is no systematic organisation that brings the entire process together.



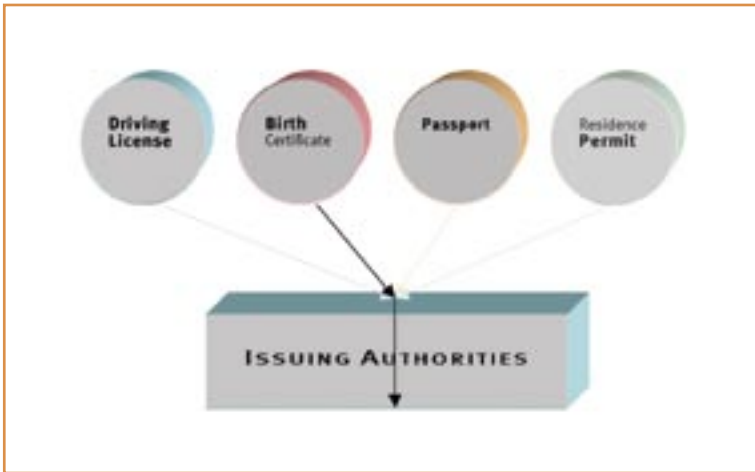


Figure 3
A centralised and harmonised Issuance system ensures that all parties are treated equally.

susceptible to non-conformity and inconsistencies. Over time, it also drains more resources and gives rise to a significantly larger number of challenges. This particularly applies in terms of biometry and future generations of e-passports.

The above considerations and arguments are also reflected in the following:

EU/ False Documents

- Adoption of security standards for the issuance of supporting / breeder documents
FAUXDOC 30 11155/00

EU/ False Documents and Visa WP

- Council Resolution 310 of 17OCT2000, concerning the minimum security standards for travel documents of the European Union/EU Member States.
- Council Resolution 2252 of 29DECO4 on reinforced security standards and biometric identifiers on passports.
- Both emphasise the need for centralised personalisation/ issuance procedures.

ICAO/ International Civil Aviation Organization

- Security Standards for Machine Readable Travel Documents/ MRTDs
Technical report to Doc. 9303

INTERPOL

- [...] Issuing authorities (...) shall improve security in the issuing procedures for travel documents in conformity with the approved specifications of the ICAO and be machine readable [...]
AGN/ 61/RES/7 ”
- [...] Centralized issuing procedures [...]

3. Storage of stolen blank documents

Although centralised issuing procedures improve security considerably, there is still room for additional theft prevention measures. The adoption of security

standards for the storage of blank documents and the implementation of a procedural code are widely accepted solutions. However, the nomination of authorised personnel, the rules applied to briefings and debriefings and the specification of materials should also be considered on a best practice basis.

The EU, ICAO and Interpol have each expressed concern about these issues, and Interpol has called for blank security components, such as security paper and substrates, to be traced (this applies to all key elements needed to assemble security documents).

The following working papers provide additional information in this regard:

EU/ False Documents working party

- Adoption of security standards for storage of blank documents
FAUXDOC 8 7858/01

INTERPOL

- “Strict security control shall be maintained over security materials, including blank paper stocks, seals, stamps, visas”
AGN/42/RES/9

To conclude

Paying due attention to the issues we have raised will undoubtedly improve efficiency, quality, security and safety. It will lift confidence among all parties involved in the identity chain and boost public awareness as well as trust. As processes tend to be dynamic and synergetic, the latest technological developments will continue to throw up new obstacles and new solutions, however. The most obvious example being biometry, which will add a new dimension to document security by establishing a unique link between the document and its holder.

Last but not least, a system that facilitates the interoperability of global identifiers and the fine-tuning of enrolment processes and identity checks will minimise the value and usefulness of stolen documents (or e-documents for that matter).